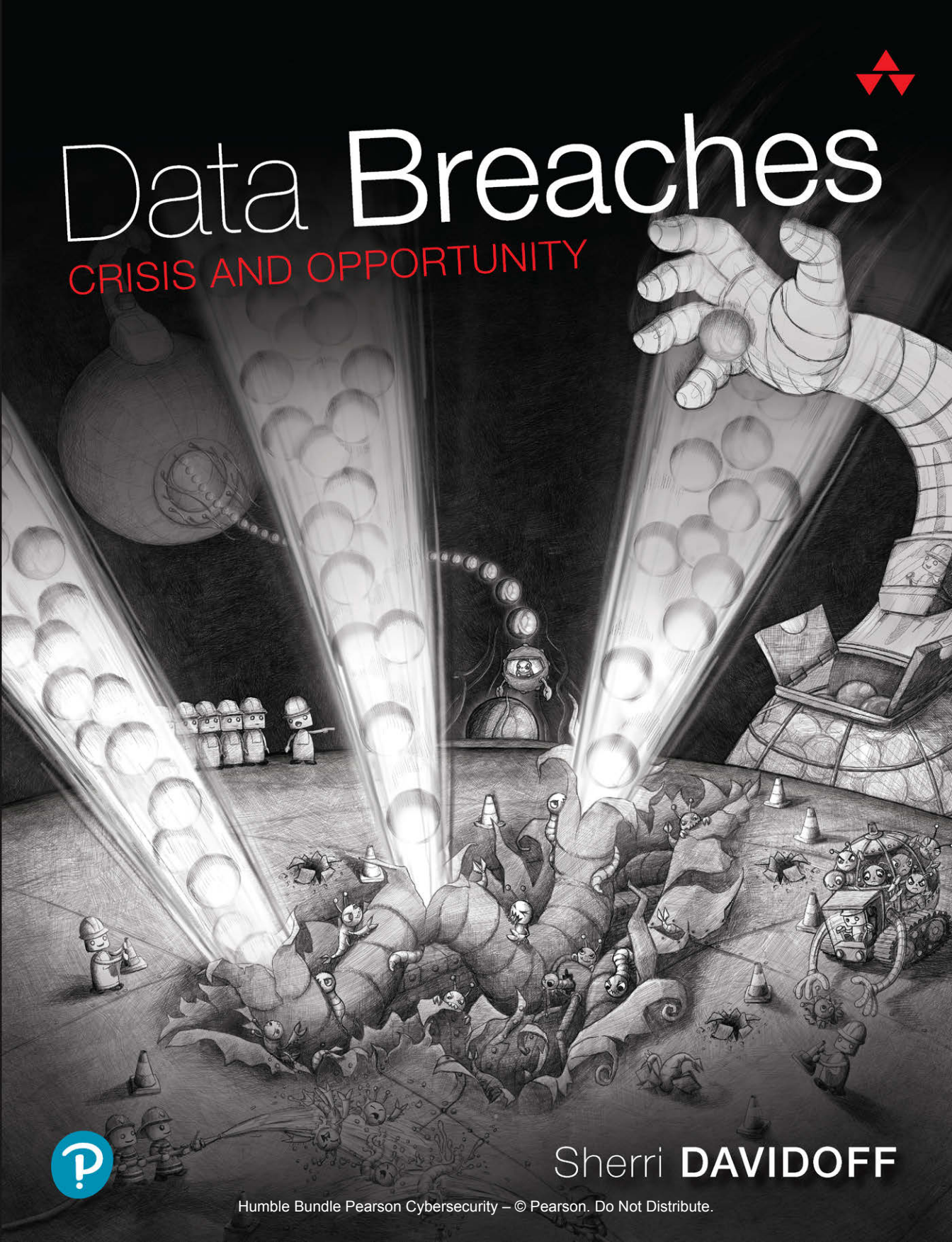
Data Breaches

CRISIS AND OPPORTUNITY



Sherri **DAVIDOFF**

Data Breaches

This page intentionally left blank

Data Breaches

Crisis and Opportunity

Sherri Davidoff

Addison-Wesley

Boston • Columbus • New York • San Francisco • Amsterdam • Cape Town

Dubai • London • Madrid • Milan • Munich • Paris • Montreal • Toronto • Delhi • Mexico City

São Paulo • Sydney • Hong Kong • Seoul • Singapore • Taipei • Tokyo

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2019944293

Cover illustration by Jonah Elgart

ISBN-13: 978-0-13-450678-4
ISBN-10: 0-13-450678-2

ScoutAutomatedPrintCode

For my supergirl, V.
And my awesome little guy, T.
With love always.

This page intentionally left blank

Contents

"Crises precipitate change . . ."
—*Deltron 3030*, "Virus"

This page intentionally left blank

Preface

It's a nightmare: One day, your IT team discovers that you've been hacked. Data has been trickling out of your organization—but for how long? Days? Weeks? Turns out it's been years. All of your most sensitive data has been stolen—databases of personal information, terabytes of email, financial details—and that's only the beginning.

What happens next? What do you do? The decisions you make in the first hours after you discover a data breach are never easy, but they may affect your organization for years to come.

Data has become the lifeblood of our modern society, as well as a huge liability. Big companies and small companies, governments and nonprofits collect and generate increasing amounts of sensitive information—often simply as a by-product of everyday operations. For a while it seemed as though there was no down side to mass data collection, aside from the expense of storage and processing. The more data you had, the better. Why bother getting rid of it?

Over time, the true cost of data collection began to emerge. Stolen credit-card numbers embarrassed merchants and frustrated consumers. Hacked hospitals leaked medical records, frightening patients. Massive electronic data leaks exposed secret government programs and upended presidential campaigns. Questions about security practices caused CEOs to resign, destroyed reputations, and sparked years' worth of litigation.

Entire industries have arisen to manage the fallout from data breaches: identity theft protection companies, digital forensics firms, data breach attorneys, credit monitoring services, and more. New regulations have emerged, like wildflowers after a rainstorm, creating new job responsibilities, reporting requirements, and liabilities. All over the globe, IT staff work through the night applying patches and worrying about vulnerabilities. Data breaches are on the minds and the agendas of boards, CEOs, auditors, legislators, constituents and consumers, in every kind of organization imaginable.

Why do some organizations emerge from a data breach unscathed while others are badly damaged or even go under? How can we all make smart choices to protect our organizations before—and after—a data breach?

The purpose of this book is to shine a light on the unmapped world of data breaches and provide a practical foundation for managing and responding to them. Not only is "data breaches" a new field of study, the term itself did not even exist until 2005. Like scientists watching a volcano rise from the sea, we are challenged both to understand the new environment we are seeing and simultaneously manage the potentially devastating social consequences.

The good news is that there are effective ways of reducing the risk of data breaches. Looking back at landmark cases, we can clearly identify tactics that reduce the damage caused in the wake of a breach. We can also see common mistakes that can cause a data breach to spiral out of control. Our case studies will include published data breaches such as those affecting Equifax, Target, Google, Yahoo, and more, as well as stories and insight from private professionals who have spent years handling data breaches quietly, from the inside. Along the way, we will unveil

a new framework for data breach response and use famous data breaches to illustrate critical turning points and lessons learned.

Who Should Read This Book?

This book will be valuable to any of the following individuals who play a part in breach response:

- Managers, executives, and IT staff concerned about data breaches
- Employees of organizations that have suffered data breaches
- Digital forensic investigators and incident response team members involved in data breach preparation and response
- Information security professionals
- IT consultants involved in cybersecurity incident prevention and response
- Students taking data breach management classes
- Anyone who is worried about getting hacked or has been affected by a data breach

How This Book Is Organized

This book provides a strong, practical foundation for data breach management and response. Here is a summary of each chapter:

- **Chapter 1, "Dark Matters"**: The number of data breaches that actually get reported represents just a small fraction of the number of data breaches that actually occur. Even the definition of a data breach is up in the air, defined differently depending on jurisdiction, industry, and other factors. In this chapter, we will establish a common terminology for discussing data breaches and explore the challenges involved in detecting and measuring the problem.
- **Chapter 2, "Hazardous Material"**: Data is hazardous material. Storing, processing, or transmitting data creates risk for an organization. In order to effectively manage the risk, security professionals must know the specific factors that contribute to the risk of a data breach. Here, we will introduce the five data breach risk factors and discuss how the rise of the modern data economy has caused the risk of a breach to skyrocket. Finally, we will provide high-level tips for reducing risk through minimizing and controlling data.
- **Chapter 3, "Crisis Management"**: Data breaches are crises and should be managed accordingly. The traditional NIST incident response model has limited value when a data breach rears its ugly head. Instead, we introduce a crisis management model and

show how it applies to data breaches. We will use the Equifax breach as a case study to illustrate the importance of crisis communications and discuss strategies for minimizing reputational damage in the event of a breach. Finally, we will examine issues surrounding notification, using the Uber breach as an example, and conclude with a handy list of crisis communication tips.

- **Chapter 4, "Managing DRAMA"**: The term "data breaches" was born in 2005, when the then-infamous ChoicePoint breach burst into the public spotlight. Using the ChoicePoint breach as a case study, we introduce a data breach response model known as DRAMA. This provides a flexible, easy-to-remember framework for data breach response.
- **Chapter 5, "Stolen Data"**: In order to effectively prevent and respond to data breaches, industry professionals need to understand what types of data criminals seek, and why. Fraud and resale (via the dark web) fueled the early epidemic of data breaches and subsequent regulations, which still impact us today. In this chapter, we will explore the inner workings of the dark web, including key technologies such as public key cryptography, onion routing, and cryptocurrency. We will enumerate popular data products that are bought and sold on the dark web, including personally identifiable information, payment card numbers, medical records, passwords, and more.
- **Chapter 6, "Payment Card Breaches"**: Payment card breaches can be very complex and result in years of litigation. The impact is often widespread, affecting merchants, consumers, banks, payment processors, card brands, and the wider community. In this chapter, we will explore the liabilities and impacts of payment card breaches and discuss the influence of the Payment Card Industry (PCI) standards, using the TJX breach as a case study. At the close of this chapter, we will provide important tips for navigating the tricky waters of a payment card breach.
- **Chapter 7, "Retailgeddon"**: The Target breach was one of the most famous in history, largely because it marked a paradigm shift in breach response best practices. Retailers at that time were under siege, and payment card breaches were common. Criminals had developed sophisticated tools for exploiting networks and targeted retailers so they could steal payment card data from point-of-sale systems. We will investigate the lessons learned from the Target breach, both on a technical level and with respect to crisis communications. Finally, we will explore the impacts, including the subsequent rollout of chip (EMV) cards.
- **Chapter 8, "Supply Chain Risks"**: Technology underlies every aspect of our global society, connecting suppliers and their customers in a massive, complex web. Supplier security risks can trickle down to customers, at times resulting in widespread data breaches. In this chapter, we will discuss how risk is transferred as a result of service provider access to customers' IT resources and data. Then, we will analyze the risks introduced throughout the technology supply chain, including software and hardware vendors, and provide tips for minimizing the risk of a breach.
- **Chapter 9, "Health Data Breaches"**: Health information is highly sensitive and prized by criminals, who can use it to commit identity theft, insurance fraud, drug fraud, extortion, and many other crimes. Because of this, healthcare providers and business associates are

subject to some of the most stringent data breach regulations, including HIPAA. In this chapter, we will delve into the relevent parts of the U.S. HIPAA regulations, which define prevention and response requirements for certain types of health-related breaches. Then, we will analyze challenges specific to the healthcare environment, and will discuss the ways data can escape from HIPAA/HITECH regulation or bypass it in the first place. Finally, we'll enumerate the negative impacts of a breach and show how lessons learned from handling medical errors can help us resolve data breaches, too.

- **Chapter 10, "Exposure and Weaponization"**: Data exposure has become a major risk for all kinds of organizations. Stolen data is deliberately exposed for a variety of purposes, including hacktivism, whistleblowing, politics, and more. In this chapter, we will discuss important tactics and technologies that evolved to facilitate exposure. In particular, we will show how WikiLeaks introduced a new model for hosting and distributing large volumes of leaked data, paving the way for "megaleaks." We also outline key response tactics, including verification, identification, data removal, and public relations.
- **Chapter 11, "Extortion"**: Cyber extortion is widespread. Criminals around the world threaten to damage the integrity or availability of information unless they receive a payment or other desirable outcome. In this chapter, we will discuss the four types of cyber extortion (denial, modification, exposure and faux), and provide tips for response.
- **Chapter 12, "Cyber Insurance"**: Cyber insurance has emerged as an important new market—but it is fraught with challenges, both for insurers and consumers. Breach response insurance, in particular, has fundamentally changed industry best practices, giving the insurer an important (and often very beneficial) role. The goal of this chapter is to share a clear description of different types of cyber insurance coverage, provide guidance for selecting cyber insurance, and discuss strategies for maximizing the value of your organization's policy.
- **Chapter 13, "Cloud Breaches"**: The cloud is the emerging battlefront for data breaches. Organizations are migrating sensitive data to the cloud at a rapid pace, while visibility and investigative resources lag behind. In this chapter, we outline common reasons for cloud breaches, including security flaws, permissions errors, lack of control and authentication issues. We delve into key response issues such as lack of visibility, using business email compromise (BEC) breaches as an example. The good news is that if cloud providers improve visibility and access to digital evidence, cloud-based monitoring and breach response has the potential to become highly scalable and efficient.

Stay Up-to-Date

For regular updates and commentary on the latest data breach developments, visit the author's website: **hackeralien.com**.

In the coming pages, we will cover fundamental, root issues in data breach management that will help all of us understand how to better protect ourselves and the communities we serve.

Register your copy of *Data Breaches* on the InformIT site for convenient access to updates and/or corrections as they become available. To start the registration process, go to informit.com/register and log in or create an account. Enter the product ISBN (9780134506784) and click Submit. Look on the Registered Products tab for an Access Bonus Content link next to this product, and follow that link to access any available bonus materials. If you would like to be notified of exclusive offers on new editions and updates, please check the box to receive email from us.

This page intentionally left blank

Acknowledgments

This book was a journey. At first, it seemed so simple: All I had to do was go throw the ring into Mordor—I mean, write a book about data breaches. After I started writing, Yahoo was breached. Equifax was breached. Cyber extortion became an epidemic. Business email compromise cases spread like wildfire. I threw my plan out the window and started again, and again. It was like trying to chart a swiftly moving river while rafting it.

I am so grateful for many people who were part of my journey. First and foremost, for my two wonderful children, who grew so much over the time that I was writing this book! Thank you for your steadfast love and companionship. This book is for you.

There are three amazing women who I am lucky to have in my life on a daily basis: Kaloni Taylor, Karen Sprenger, and Annabelle Winne. Every day, I am thankful for your wisdom and for all that you do. This book literally could not exist without you.

Thanks to the excellent team at Pearson; in particular, my dear editor, Chris Guzikowski, who set me off on this adventure and was there for me with patience and wisdom along the way. Chris Cleveland, my development editor, took the time to slice vast territories off my manuscript and reorient me in the right direction. As painful as it was to have to "kill my darlings," the book is far better because of his direction. Thanks to Haze Humbert, for seeing the writing through its final phases, and for her delicious hot toddy recipe that cured my flu. I am deeply grateful for the work of consultant Louisa Jordan, who meticulously formatted hundreds of footnotes that appear throughout this book.

It is the production team that brings a book to life, and I am thankful for the fantastic crew that brought my words to the page that you are reading now. In particular, many thanks to producer Julie Nahil, project manager Ramya Gangadharan and her team, and copy editor Lisa Wehrle (who checked every single letter of the book—and beyond, since she also edited the formatting and margins!). The immensely talented Jonah Elgart drew the cover art for this book, giving it a striking visual "face" that is creative, quirky, and geeky—exactly the right fit.

Thank you to everyone involved in the review process. My friend and mentor Michael Ford provided advice and feedback on every phase of this process, from pie-in-the-sky early brainstorming sessions to the technical review, during which he read every page of the book and provided extensive comments. Mike Wright and Randy Marchany kindly reviewed the book as well and provided very helpful feedback. I am also grateful to Jeremy N. Smith for providing guidance on the writing process and encouragement along the way, and who (shockingly) edited the entire book *by hand* on paper (and then told me to rewrite it, which I did).

In researching this book, I reached out to dozens of colleagues, whose knowledge and expertise make this book far richer. Many thanks to Brett Anderson, Jay Combs, Heidi DeArment, Sherri Douville, Randy Gainer, Katherine Keefe, Jason Kolberg, Scott Koller, Rob Lee, Dale Leschnitzer, Larry Pierce, Lynne Pizzini, Frank Quinn, Howard Reissner, David G. Ries, Donald Rome, Dave Sande, Shane Vannatta, Neil Wyler, and Anonymous (whoever you are).

I couldn't believe my good fortune when I met attorney Chris Cwalina on a conference call and discovered that he had been the general counsel for the ChoicePoint case—a historic breach. His perspective was invaluable, and I am grateful for the opportunity to share it with readers. In similar fashion, I felt especially fortunate to meet Mike Donovan, the inventor of breach response insurance. Mike took the time to share his experience developing breach response insurance and provided insights on the evolution of risk.

LMG Security's forensics team was instrumental in helping me stay up-to-date on the latest threats and breach response issues. Special thanks to Matt Durrin and Ali Sawyer for taking the time to share their case stories and viewpoints. I would also like to thank the entire team at LMG Security who supported me in so many ways along this journey, including Patrick Burns, Andy Carter, Nate Christoffels, Dan Featherman, Madison Iler, Ben Kast, Ross Miewald, Delaney Moore, Shalena Weagraff, and Ashley Zhinin. Finally, thanks to my colleagues at BrightWise and AMC, especially Michelle Barker, Robin Caddell, Emily Caropreso, Pat Jury, Deb Madison-Levi, Wes Mallgren, Matt Oakley, Mike Powers, Corey Skadburg, and Murray Williams.

My friends and family lifted my heart so many times along the way. I am grateful for your love and support. Special thanks to E. Martin Davidoff, Laura Davidoff, Sheila Davidoff, Debra Shoenfeld, Eileen and Norm Shoenfeld, Brian Shoenfeld, Beth Davidoff, Blake Brasher, Kaylie Johnson, Nadia Madden, Shannon O'Brien, Deviant Ollam, Ben Saunders, Sahra Susman, and Jason Wiener. Last but not least, I would like to thank my wonderful boyfriend Tom Pohl, whose steadfast encouragement helped me reach the end of the road.

About the Author

Sherri Davidoff is the CEO of both LMG Security and BrightWise, Inc. As a recognized expert in digital forensics and cybersecurity, Sherri has been called a "security badass" by the *New York Times*.

Sherri has conducted cybersecurity training for many distinguished organizations, including the FDIC/FFIEC, the American Bar Association, the Department of Defense, and many more. She is a faculty member at the Pacific Coast Banking School, and an instructor for Black Hat, where she teaches her "Data Breaches" course. She is also the coauthor of *Network Forensics: Tracking Hackers Through Cyberspace* (Prentice Hall, 2012), a noted security text in the private sector and a college textbook for many cybersecurity courses.

Sherri is a GIAC-certified forensic examiner (GCFA) and penetration tester (GPEN), and holds her degree in Computer Science and Electrical Engineering from MIT. She has also been featured as the protagonist in *Breaking and Entering: The Extraordinary Story of a Hacker Called "Alien."*

This page intentionally left blank

Chapter 1

Dark Matters

It was the Sunday after Thanksgiving, at a crowded bus station on the east coast. A young man stood in line outside, waiting to purchase a bus ticket from the ticket vending machine so that he could make his way home. He swiped his credit card. The machine spit out a one-way ticket and a receipt. Next.

Unbeknownst to anyone, the machine also recorded the young man's credit card number in a vast and growing database stored there on the sidewalk, along with millions of other credit card numbers. This wasn't supposed to happen.

Years earlier, a coder who worked for the ticketing system's vendor was debugging a tricky problem. The machines weren't processing credit card numbers correctly. He quickly turned on a debugging routine that automatically wrote every credit card number to disk. Aha! He fixed the code—but forgot to turn off the debugging routine. The new version of the software was installed on all new ticket machines deployed around the world. Each ticket machine sat silently on the sidewalk for years saving all the credit card numbers that anyone ever swiped.

Just a few minutes after the young man swiped his credit card, the ticket machine made a web connection to a city employee's home computer. This definitely wasn't supposed to happen.

The city's employees were allowed to work from home and frequently connected their home computers to the city's network in order to access files or check email. At home in the evenings, they also used their computers to download movies, play games, and surf the web. Their teenage kids traded emails and instant messages. Their home computers became infected with viruses and worms. Then, at the start of the workday, they connected their computers to the city's network again. The firewall allowed full access between the employee home computers and the rest of the city's internal network—including the ticket vending machines.

The city's IT staff regularly installed software patches on desktops and servers, which protected them from many viruses and worms—but the ticket vending machines were different. They ran an older version of Microsoft Windows. The ticket machine vendor refused to support the machines if the latest Windows updates were applied, and so the city had to wait until the vendor was ready to apply patches—which happened sporadically and rarely. Nobody wanted to accidentally break the city's bus ticketing infrastructure by applying software patches without the vendor's support. So, the machines sat, unpatched and vulnerable, there on the street.

Meanwhile, the employees' virus-infected home computers frequently probed the entire network for other vulnerable systems—and found the ticket vending machines, which stood quietly on the sidewalk, storing millions of credit card numbers.

Months and years went by. Eventually, the city's IT management realized that the internal firewall rules were wide open and fixed them. Months after that, the vendor notified the city officials of the debugging routine. City officials investigated. Management had one question: Had credit card information been stolen?

This was where I came in, a young digital forensic investigator. I earned my living as a subcontractor in a time when very few people had real-world digital forensics experience.

The city launched a forensic investigation and handed 10 TB of network logs to a third-party forensics firm. The firm called me in to conduct the analysis. At the time, 10 TB of log data was an enormous volume. As soon as the call came in, I rushed out and purchased an expanded storage system with superfast connectors to handle the case. Two days later, the log files arrived on a hard drive via FedEx, and I immediately began the decompression process.

Log files are simply *records of events that happen on a network.* An *event* can be literally anything: a user logging in, or a packet traversing the firewall, or your antivirus software alerting on a Trojan that you accidentally downloaded. This seemingly simple definition belies a deeply challenging problem: When you have hundreds of thousands or even millions of recorded events, how do you find a needle in the haystack? Even more of a challenge: There is no standard format for log files. As a forensic investigator, you never know what information you're going to be handed or what will be left out. Every firewall vendor and IT team sets up its logging system differently. You might simply be handed a file with lots of numbers on every line, and your first job is to figure out what each number means.

At the time I worked the ticket machine case, there were few tools available for analyzing logs, and very little available documentation. Before I could even start to analyze the evidence files, I essentially had to conduct a mini-investigation to understand just what I had been handed; determine what, if any, information would be relevant to the case; and figure out the most efficient way to process all that network-based evidence.

As the evidence files were decompressing, I took a sample of the logs to analyze their format and began writing the custom scripts that would be needed to properly "parse" the evidence.

The logs were full of gaps. Sure, the ticket machines' network activity had been logged—sometimes. There were only ten months of intrusion detection system (IDS) alerts, remote connection records, and firewall log data relating to the ticket vending machines. All of this data was very high level, with only source and destination IP addresses and ports logged, along with the amounts of data transferred. There was no information about specifically what was transferred at any time. The city did not have a data-loss prevention (DLP) system or filesystem monitoring that would have alerted if credit card information specifically was transferred over the network. No operating system logs, no packet contents, and no hard drives were provided for analysis.

The evidence showed that the ticket vending machines had communicated with dozens of systems throughout the city's network, including many employee home computers. The IDS alerts included alarming notices such as "SMB login successful with Guest Privileges," "Server Service Code Execution," "Windows Workstation Service Overflow," and "Outbreak Prevention Signature." The machines had exchanged data with remote servers (often in foreign countries), as well as other computers on the city's network.

The ticket machines were clearly vulnerable, and they had been scanned and probed by infected home computers, which easily could have installed viruses and malware on the unpatched equipment. An attacker that broke in would find huge volumes of credit card

numbers, stored unencrypted on the machines' hard drives. The machines exhibited strange behaviors, such as unexplained communications with foreign countries, at all hours of the day and night. The traffic patterns showed obvious symptoms of malware infection and unauthorized access.

However, there was no smoking gun, no direct evidence that credit card numbers stored on the ticket machines had been stolen by an attacker. How could there be, when there was no network or file monitoring in place that would alert on such activity, and the hard drives weren't provided for analysis? There was no information about the malware's capabilities or exactly what information a criminal may have gained.

In the forensic report, I stated that, due to lack of security controls, there had been ample opportunity for access, but lack of evidence prevented a definitive conclusion on the question of whether credit card data had actually been compromised.

I assumed that the city would publicly disclose the incident. There had clearly been unauthorized access to the ticket machines, and private credit card information was stored on them. It seemed the ethical thing to do. In all likelihood, there was probably sensitive information on the other infected computers within the city's network, as well as employee home computers, which might have been accessed by criminals as well. I knew the city wouldn't disclose the fact that other computers on the network had been compromised (that was an all-too-common occurrence in most organizations), but I hoped the investigation would at least spur a review of its network architecture and logging practices. As a low-level technical analyst, my role ended once the forensic report was delivered, and I was never privy to any further conversations about the incident.

Weeks, months, and years went by. I kept an eye on the news but never saw a public notification. Other forensics cases came in, and I wrote reports with similar conclusions: not enough evidence. Not enough logs. No way to prove a theft beyond the shadow of a doubt. They never made the news, either. Once, I got a phone call from a company that suspected a breach of its point-of-sale system, which processed credit cards. A representative called back five minutes later to say that the company had decided to just format and reinstall the computer, and not investigate at all.

Most of all, I wondered about the calls I didn't get, the cases that were never investigated, and never even detected in the first place.

1.1 Dark Breaches

It's shocking to realize that the number of data breaches that actually get reported represents just a small fraction of the number of data breaches that actually occur. Even the information we do have about data breaches is often skewed, and it certainly doesn't represent any kind of statistically valid sample set from which we can draw scientific conclusions.

"Most businesses that get hacked surely do the right thing and inform customers," reported *BusinessWeek*, naively, in 2002.[1] This reflected a common assumption once held by the general

1. Alex Salkever, "Computer Break-Ins: Your Right to Know," *BusinessWeek*, November 11, 2002.

public that organizations would "of course" report leaks of personal customer information. Experienced security professionals know that reality is much more complex.

Consider that in order for a data breach to be publicized, the following events must occur:

1. **Detection** - Symptoms of a potential data breach must be detected.
2. **Recognition** - The event must be recognized and classified as a data breach.
3. **Disclosure** - Information about the data breach must be disclosed.

Each of these steps sounds fairly straightforward, but reality is often full of technical failures, gray areas, and miscommunications. If an organization's data breach management process fails at any of these three steps—detection, recognition, or disclosure—then the data breach will simply go unreported, and often entirely untracked.

In physics, scientists have for decades inferred the existence of dark matter, as described by CERN:[2]

> [D]ark matter does not interact with the electromagnetic force. This means it does not absorb, reflect or emit light, making it extremely hard to spot. In fact, researchers have been able to infer the existence of dark matter only from the gravitational effect it seems to have on visible matter. Dark matter seems to outweigh visible matter roughly six to one, making up about 27% of the universe. Here's a sobering fact: The matter we know and that makes up all stars and galaxies only accounts for 5% of the content of the universe!

Similarly, "dark breaches" exist. These are breaches in which information may have been compromised, but the incident is never disclosed to any reporter, government agency, or researcher. It may never have been detected in the first place. As with dark matter, there is evidence from which professionals can infer the existence of dark breaches.

1.1.1 What Is a Data Breach?

The question of whether a data breach gets reported is very closely linked to the bigger question: What is a data breach?

"I always say it's defined by the law," says Chris Cwalina, Global Co-Head of Data Protection, Privacy and Cybersecurity at law firm Norton Rose Fulbright. A veteran of the data breach response world, Chris got his start in cybersecurity as the legal "quarterback" in the infamous ChoicePoint data breach back in 2005. One fall evening in Virginia, Chris was kind enough to meet me so that I could pick his brain about data breach response.

Sitting across the table from each other, an attorney and a digital forensics examiner, we each represented key functions of modern incident response—with very different perspectives.

"What a data breach is to somebody like you is different than what it is to lawyers who practice in this space," Chris mused. "When you have an unauthorized actor on your system, it's really important to define 'data breach' carefully, and to say that only your outside legal counsel can make that determination. If you are inside, you should be saying that it is an *incident*. It's

2. CERN, "Dark Matter," CERN, https://home.cern/about/physics/dark-matter (accessed January 5, 2018).

the lawyer's job to determine whether it is a breach, as defined. Lawyers need expert help from IT and IS professionals, but ultimately, the decision comes from applying facts to law. That, unfortunately, is just because of how the laws have evolved."

Security practitioners often refer to cybersecurity "events" and "incidents." Long ago, the National Institute of Standards and Technology (NIST) defined these terms as follows:[3]

> **Event** - Any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
>
> **Computer security incident** (often referred to simply as an "incident") - A violation or an imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

When does an "event" or "incident" become a bona fide data breach? In the United States today, there is no federal definition of a "data breach," or even a federal data breach notification law which applies to all types of organizations. Instead, the United States has a patchwork of state and local laws, often implemented in conjunction with industry-specific federal breach notification laws such as the Health Information Technology for Economic and Clinical Health (HITECH) Act.[4]

"If you look at the state definitions for what a security breach is, they're all pretty close," says Chris Cwalina. Most laws are architected to require "notification" in the event of a "breach of security" of "personal information."

According to the law firm Baker Hostetler, LLP, the most common definition of "breach of security" is:

> the unlawful and unauthorized acquisition of personal information that compromises the security, confidentiality or integrity of personal information.[5]

That means that in order for the general public to find out about a breach, the event must first fit the definitions of both "breach of security" and "personal information," and also meet any other requirements for notification. "The problem is," Chris explained, "some states [require notification upon] unauthorized acquisition or access [of personal information], in some states it's unauthorized access and acquisition (note the 'and' versus the 'or'), in some states it's just access, and in some states it's just acquisition. There should be more consistency with what a data breach *is*."

Many states also have a "harm trigger," Chris elaborated, which modifies the requirement to notify based on an assessment of whether the information has been or is likely to be misused.

---

3. Paul R. Cichonski, Thomas Millar, Timothy Grance, and Karen Scarfone, *Computer Security Incident Handling Guide*, Special Pub. 800-61, rev. 2 (Washington, DC: NIST, 2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

4. HITECH is a U.S. federal regulation established to "promote the adoption and meaningful use of health information technology." Passed in February 2009, HITECH included a game-changing data breach notification provision. For more details, see "HITECH Act Enforcement Interim Final Rule," U.S. Department of Health and Human Services, last revised June 16, 2017, https://www.hhs.gov/hipaa/for-professionals/index.html.

5. Baker Hostetler, "Data Breach Charts," *Baker Law*, July 2018, https://www.bakerlaw.com/files/uploads/documents/data%20breach%20documents/data_breach_charts.pdf.

"Let's say there's access to the data, but you say there's zero likelihood that this information is going to be misused," explained Chris. "Then you can make a determination not to notify. In some cases you have to consult with law enforcement, like in Florida, and then document it, notify the attorney general of your decision, et cetera."

All of these different definitions and laws have led to a great deal of confusion, both regarding what a data breach *is* and how to react when one occurs.

1.1.2 Unprotected Personal Information

When Target was famously hacked in 2013, customers received a notification which stated that "criminals forced their way into our systems and took guest information, including debit and credit card data." Target went on to state that "your name, mailing address, phone number, or email address may also have been taken during the intrusion."

Oddly left out of Target's data breach announcement was a very sensitive topic: your personal shopping history and customer profile. It was left out for a reason—and not because the data didn't exist.

The *New York Times* exposed Target's extensive data collection and analysis practices in 2012, when it ran a story describing how the company leveraged statistics to generate, for example, lists of customers who were pregnant. At the time, Andrew Pole, a statistician hired by Target, revealed that Target assigns each customer a unique "Guest ID" number and ties this to a history of all purchases, as well as a vast array of other personal information. "If you use a credit card or a coupon, or fill out a survey, or mail in a refund, or call the customer help line, or open an e-mail we've sent you or visit our Web site, we'll record it and link it to your Guest ID," Pole said. "We want to know everything we can."

Target also keeps extensive records of your personal details, potentially including sensitive information purchased from data brokers and combined with your customer record. Using this detailed personal information, Target can draw conclusions about your health, needs, and habits, which it can then use for financial gain.

"Also linked to your Guest ID is demographic information like your age, whether you are married and have kids, which part of town you live in, how long it takes you to drive to the store, your estimated salary, whether you've moved recently, what credit cards you carry in your wallet and what Web sites you visit," reported the *New York Times*. "Target can buy data about your ethnicity, job history, the magazines you read, if you've ever declared bankruptcy or got divorced, the year you bought (or lost) your house, where you went to college, what kinds of topics you talk about online, whether you prefer certain brands of coffee, paper towels, cereal or applesauce, your political leanings, reading habits, charitable giving and the number of cars you own."[6]

If data exists, then it can be stolen. When Target was hacked, what happened to all this detailed shopping information and the resulting lists of consumers with health issues or other categorizations? Target took the time to reassure consumers that "there is no indication that PIN numbers have been compromised," but shopping histories weren't mentioned at

6. Charles Duhigg, "How Companies Learn Your Secrets," *New York Times Magazine*, February 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1& r=2&hp.

all—one way or another—in consumer notices. Why would they be, since information of this type—which seems so personal to consumers—is not, in fact, covered by state or federal data breach notification laws?

According to Baker Hostetler, the most common definition of personal information in U.S. state law is:[7]

> an individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state-issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account and generally applies to computerized data that includes personal information. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.

What's left out of this definition? An absolutely enormous array of information that most people consider private, such as:

- Shopping history
- Location information (such as the coordinates of your favorite hangout locations or the route you drive to work, captured by your cell phone or car)
- Health information, including prescription drug records
- Emails
- EZ-Pass, FastLane, or other travel records
- Last name plus Social Security number (SSN) (no first name or first initial)
- And much, much more

Think your health information is protected? Only in certain contexts. In 2016, the U.S. Department of Health and Human Services issued a report outlining the gaps in privacy and security of entities that are not regulated by the Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA (as amended by the HITECH Act in 2009) is the primary federal law that protects personal health information in the United States. It applies to "covered entities," such as healthcare providers, health plans, and healthcare clearinghouses, as well as their "business associates" (persons or entities acting on their behalf, such as billing vendors or IT providers).

Notably, "[t]he wearable fitness trackers, social media sites where individuals share health information through specific social networks, and other technologies that are common today did not exist when Congress enacted [HIPAA]."[8] There are many apps and websites that "allow individuals to enter their health information to monitor blood sugar, eating habits, or

7. Baker Hostetler, "Data Breach Charts."

8. U.S. Department of Health and Human Services, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA* (Washington, DC: US HSS, June 17, 2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

sleeping patterns. Other health data websites may provide information or send out e-mails with information about medications or specific conditions such as allergies, asthma, arthritis, or diabetes. Twenty-seven percent of internet users and 20 percent of adults have tracked their weight, diet, exercise routine, symptoms, or another health indicator online."[9]

Google, which once ran a service called Google Health that enabled users to store health information in the cloud, had an online FAQ that explained:

> Is Google Health covered by HIPAA? Unlike a doctor or health plan, Google Health is not regulated by [HIPAA]. . . . This is because Google does not store data on behalf of health care providers. Instead, our primary relationship is with you, the user.

Due to gaps in the law, certain unauthorized disclosures of health or medical information may not be subject to state or federal breach notification laws. In other words, if your cloud provider gets hacked and loses your health information, it may or may not not be required to tell you.

Definition of a Data Breach

In this book, we will use the term "data breach" loosely to refer to any access or acquisition of confidential information by an unauthorized party. When we refer to "personal information," this includes not only information that is protected by law ("protected personal information") but also any information that a consumer, corporation, or other entity expects to remain private, such as emails, health information, sensitive corporate documents, and more. This definition, far broader than the legal definition, allows us to include in our discussions the vast and untracked volume of cases where the information "breached" is not protected by any existing law.

1.1.3 Quantifying Dark Breaches

From the early days of information security, the U.S. government published reports that clearly illustrated the problem of "dark breaches." There were even some attempts to quantify unreported breaches. In 1996, the GAO issued a report to Congress that described the Defense Information Systems Agency (DISA) Vulnerability Analysis and Assessment Program:[10]

> Since the program's inception in 1992, DISA has conducted 38,000 attacks on Defense computer systems to test how well they were protected. DISA successfully gained access 65 percent of the time. . . . Of these successful attacks, only 988 or about 4 percent were detected by the target organizations. Of those detected, only 267 attacks or roughly 27 percent were reported to DISA.

9. U.S. Department of Health and Human Services, *Examining Oversight*.

10. U.S. General Accounting Office (GAO), *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, Pub. No. B-266140 (Washington, DC: GPO, May 1996), 19, http://www.gao.gov/assets/160/155448.pdf.

Figure 1-1, which is from the 1996 congressional report, illustrates the percentage of attacks that were successful, detected, and reported. As shown, only a very small percentage of successful security breaches were properly reported to DISA.

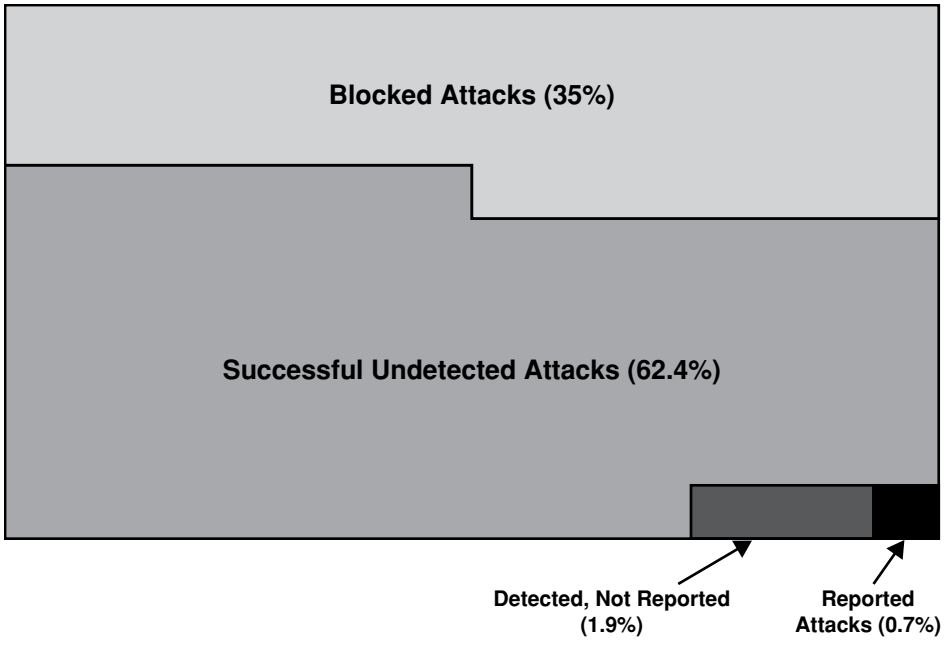


Figure 1-1. Results of DISA vulnerability assessments, 1996. Source: GAO, *Information Security*, 20.

The GAO report went on to state that "DISA estimates indicate that Defense may have been attacked as many as 250,000 times last year," but cautioned that since such a small percentage of breaches was actually detected and reported, the exact number of successful breaches—and therefore the full extent of related damage—was "not known."[11]

"Not known," of course, doesn't mean "nonexistent," as DISA knew all too well. From the GAO report:[12]

> According to Defense officials, attackers have obtained and corrupted sensitive information—they have stolen, modified, and destroyed both data and software. They have installed unwanted files and "back doors" which circumvent normal system protection and allow attackers unauthorized access in the future. They have shut down and crashed entire systems and networks, denying service to users who depend on automated systems to help meet critical missions. Numerous Defense functions have been adversely affected,

11. GAO, *Information Security*, 3.

12. GAO, *Information Security*, 19.

> including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll. . . . While Defense is attempting to react to attacks as it becomes aware of them, it will not be in a strong position to deter them until it develops and implements more aggressive, proactive detection and reaction programs.

1.1.4 Undetected Breaches

Detection is key. By DISA's analysis, the overwhelming number of security breaches (96%) were not reported because they simply weren't detected in the first place. There is evidence to suggest that lack of detection is still a critical issue today. For example, when Yahoo disclosed a major breach of user account data in 2016, the public was shocked to find that it had apparently taken more than two years for the company to fully understand what had occurred.

"For a firm like Yahoo, which is a technology firm no less, you would expect that they would be able to detect and even disclose the breach a little quicker," said cybersecurity professor Rahul Telang, of Carnegie Mellon University. "It was surprising that Yahoo didn't know about it until the user data hit the black market."[13]

But is it really surprising? There are plenty of published reports of data breaches where hackers lurked for well over a year before discovery. For example, the hackers who stole more than 45 million credit card numbers in the infamous "TJ Maxx" breach of the TJX companies were reportedly in the company's systems for 18 months, between July 2005 and December 2006, according to *ComputerWorld*.[14]

After Goodwill's data breach was publicly exposed in 2015 by investigative journalist Brian Krebs, the nonprofit published a statement to customers indicating that "some Goodwill member store locations may have been affected by a data security issue" for more than 18 months. The stolen data included "payment card information—such as names, payment card numbers and expiration dates—of certain Goodwill customers."[15]

Even the U.S. federal government was the victim of long-running compromises. In June 2015, the U.S. Office of Personnel Management (OPM) publicly acknowledged a breach of at least four million personal records that reportedly started over a year earlier.[16] "While the attack was eventually uncovered using the Department of Homeland Security's (DHS) Einstein—the multibillion-dollar intrusion detection and prevention system that stands guard over much

---

13. Tracey Lien, "It's Strange Yahoo Took 2 Years to Discover a Data Breach, Security Experts Say," *Los Angeles Times*, September 23, 2016, http://www.latimes.com/business/technology/la-fi-tn-yahoo-data-breach-20160923-snap-story.html.

14. Jaikumar Vijayan, "TJX Data Breach: At 45.6M Card Numbers, It's the Biggest Ever," *ComputerWorld*, May 29, 2007, https://www.computerworld.com/article/2544306/security0/tjx-data-breach–at-45-6m-card-numbers–it-s-the-biggest-ever.html.

15. Letter from Goodwill Industries International President and CEO Jim Gibbons, September 2, 2014, http://www.goodwill.org/wp-content/uploads/2014/09/Letter.pdf.

16. David E. Sanger and Julie Hirschfield Davis, "Hacking Linked to China Exposes Millions of U.S. Workers," *New York Times*, June 4, 2015, http://www.nytimes.com/2015/06/05/us/breach-in-a-federal-computer-system-exposes-personnel-data.html; Patricia Zengerle and Megan Cassella, "Millions More Americans Hit by Government Personnel Data Hack," *Reuters*, July 9, 2015, https://www.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709.

of the federal government's Internet traffic—it managed to evade this detection entirely until another OPM breach spurred deeper examination."[17]

Why can it take so long to discover a data breach? To the public, it may seem inconceivable that an attacker could walk out with a huge amount of data undetected, like a criminal walking out of a bank branch carrying sacks of cash in broad daylight. But cyber attacks are often less visible and far more pervasive.

For starters, consider the relative sizes of an organization's attack surface in the physical world versus online. Your bank branch is designed to have a limited number of entrances and exits. For modern organizations, however, every employee who surfs the web or checks email represents a potential entry point for malware or an exit via which data may be lost or exfiltrated. The huge attack surface is overwhelming and difficult to monitor or control.

Technology has evolved to automate detection, and it helps—to a point. Organizations with a large enough budget can install cyber intrusion detection systems (IDS) on their networks and computers. These systems monitor for signs of malicious behavior and alert staff when issues are detected. "False positives," where the IDS mistakenly classifies legitimate network traffic as suspicious, add to the noise and make more work for analysts. Conversely, "false negatives," where the IDS fails to alert upon a suspicious event, can result in missed events, with devastating consequences.

Over the years, modern intrusion prevention systems (IPS) evolved to further reduce manual labor. These systems automatically stop suspicious activity, in addition to alerting. However, using an IPS introduces the risk that "false positives" may cause the system to block normal network traffic and therefore possibly interfere with the organization's daily operations.

Malware itself is constantly evolving to avoid detection, with antivirus authors and IDS/IPS vendors struggling to keep up. Dedicated attackers may choose to space out data exfiltration over long periods of time—months or years—so that only a small amount of information is stolen each day. Attackers may also deliberately try to "blend in" with the organization's normal traffic, disguising their activities as web traffic or similar common protocol, and paying careful attention to timing.

Once a breach triggers a cybersecurity system alert, staff need to respond. This can be a challenge, too, because often cybersecurity systems generate far more alerts than staff can handle (hundreds or even thousands for every security staff member each day). In these situations, the cybersecurity logs can represent a liability because the organization has a record of a potential breach but doesn't have the resources to fully investigate or act on it. Even when the volume of alerts is reasonable, humans need to be available 24/7 to respond, which is often not possible given staffing constraints. Many organizations outsource monitoring to third-party managed service providers (usually a smart tactic), but not all organizations have the budget for this specialized service, and those that do may not have the resources to effectively oversee their vendors.

If a cybersecurity alert is reviewed by incident responders and declared an "incident," then responders need to investigate and make decisions such as whether to clean malware off any affected systems and whether to notify any higher-ups or consult with legal counsel. Front-line

17. Sean Gallagher, "Why the 'Biggest Government Hack Ever' Got Past the Feds," *Ars Technica*, June 8, 2015, https://arstechnica.com/information-technology/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/2.

staff members often make the call. If the staff member does not have enough training or experience, or if the organization's incident response policies are unclear or simply not aligned with best practices, then sometimes signs of data breaches can be swept under the rug or misclassified internally without upper management ever knowing. Indeed, when internal IT staff discover evidence of a breach, they may be fearful of blame or simply not recognize the potential implications, and fail to report up the chain.

"Don't expect . . . hackers to alert you to their presence," explained Verizon in their 2018 *Data Breach Investigations Report*. "When [breaches] are discovered it is typically via external sources such as detection as a Common Point of Purchase (CPP) or by law enforcement."[18]

1.1.5 Dark and Darker Breaches

Certain types of data are more likely to be noticed quickly when stolen or detected by third parties because of how the stolen data is used. Payment card information is immediately useful for fraud. When fraud occurs, this is quickly known—and often detected—by card associations such as Visa and Mastercard, issuing banks, or the affected person whose information was stolen.[19] Investigative journalist Brian Krebs, who broke stories on the Target, Home Depot, and Wendy's cardholder data breaches (to name a few), described how he found out about a 2016 breach involving the fast-food restaurant CiCi's Pizza:[20]

> Over the past two months, KrebsOnSecurity has received inquiries from fraud fighters at more than a half-dozen financial institutions in the United States—all asking if I had any information about a possible credit card breach at CiCi's. Every one of these banking industry sources said the same thing: They'd detected a pattern of fraud on cards that had all been used in the last few months at various CiCi's Pizza locations.

The quick and widespread impact of a cardholder data breach, combined with the ability to pinpoint a common point of purchase, means that major breaches of cardholder data tend to be detected very quickly. This is not the case with, say, a breach of internal corporate document repositories.

Mandiant's famous 2013 report, *APT1: Exposing One of China's Cyber Espionage Units*, analyzed the activities of a hacking group it dubbed "APT1," allegedly a unit of China's People's Liberation Army. Mandiant described how the hackers would "periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from

18. Verizon, *2018 Data Breach Investigations Report*, Verizon Enterprise, 2018, 28, https://enterprise.verizon.com/resources/reports/2018/DBIR_2018_Report.pdf.

19. Brian Krebs, "How Was Your Credit Card Stolen?" Krebs on Security, January 19, 2015, https://krebsonsecurity.com/2015/01/how-was-your-credit-card-stolen.

20. Brian Krebs, "Banks: Credit Card Breach at CiCi's Pizza," Krebs on Security, June 3, 2016, https://krebsonsecurity.com/2016/06/banks-credit-card-breach-at-cicis-pizza.

victim organizations' leadership." Rather than immediately monetizing this stolen data, the report claimed that the Chinese government used it for the purposes of gaining long-term economic advantages.[21]

Data breaches of this type are hard to detect because unauthorized recipients of the stolen data can leverage it without revealing that the data was ever stolen.

The same can be true of personal data repositories, such as email accounts or documents stored in the cloud. Bloomberg reported that in the 2016 Yahoo breach, "[h]ackers may have accessed millions of Yahoo accounts for years undetected."[22] Consider for a moment: If your email account was hacked, would you know? Imagine if your username and password were stolen and sold to an organized crime group, which scraped your email account for any information of value. Criminals are all too happy to pay money for your SSN, financial details, and other data that can be used to commit fraud. Marketers will pay money for information about your health issues, marital problems, personal interests, etc. Background-check companies might pay money to know if you smoke pot or have employment issues. How would you even know that this information was stolen at all? If you did find out, how would you know it was stolen from your email account specifically?

Service providers, from IT companies to attorneys, may likewise never detect that customer records have been stolen. Nor do they necessarily have incentive to invest in effective detection systems. For many organizations, plausible deniability is the (perhaps unconsciously) chosen approach.

In January 2013, the Department of Health and Human Services issued an update to HIPAA that changed the definition of a "breach" and related notification requirements. Importantly, the change shifted the *burden of proof*. Now, "[a]n impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised." In other words, data stewards must presume that data has been breached unless there is evidence that indicates otherwise. This fundamental legal shift created incentives for affected organizations to implement effective logging and detection systems, so that they could prove when a breach did *not* happen and accurately determine the number of persons affected when a breach did occur.

This change applies specifically only to HIPAA; most breach notification laws do not yet include this shift in the required burden of proof. As a result, for many organizations, ignorance is still bliss.

1.2 Skewed Statistics

The public is hungry for information about data breaches. What industries are the most targeted? What are the latest causes? What will happen next year, and the year after? Journalists,

21. Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013) https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

22. Jordan Robertson, "Yahoo's Data Breach: What to Do If Your Account Was Hacked," *Bloomberg*, September 22, 2016, https://www.bloomberg.com/news/articles/2016-09-22/yahoo-s-data-breach-what-to-do-if-your-account-was-hacked.

in turn, gobble up reports on the topic and regurgitate them to the public. Any new whitepaper containing "trends" or "statistics" related to the topic is likely to receive a stream of publicity.

The result is a plethora of whitepapers published by corporations and nonprofits, ranging from vendors such as Symantec and Verizon, to the granddaddy Privacy Rights Clearinghouse (a nonprofit) to the Ponemon Institute (a for-profit LLC). Typically these whitepapers are based on public records of data breaches, surveys, or the internal data of corporations involved cybersecurity and breach response.

While journalists love to quote these whitepapers—especially the well-marketed ones—few, if any, are developed with the rigor of a peer-reviewed academic publication. How could they be, when information about data breaches is so limited? Due to the problem of "dark breaches," there is inherent bias in every report. Only rarely is this mentioned in the media.

In this book, I often quote statistics or findings from public sources and some of the more reputable industry whitepapers. While these sources aren't perfect, they are the best we've got at this stage in the development of data breach analysis. Whenever appropriate, I will call attention to inherent biases that likely influence the findings.

As a foundation, let's take a moment to look at common ways that the sources of data and methodology used in these reports can affect the validity of their conclusions.

1.2.1 Public Records

It's tempting to blindly trust studies that are based on public records of data breaches. Government agencies such as the Department of Health and Human Services (HHS) are required by the law to "post a list of breaches of unsecured protected health information"[23] In addition, nonprofit organizations such as the Privacy Rights Clearinghouse (PRC) collect breaches reported through "government agencies or verifiable media sources" and make these lists available online.[24]

But of course, the mere fact that a breach has been publicized means that it is part of a skewed sample set. Once you recognize that published data breaches represent only a subset of the actual numbers (and likely a small one, at that), the inherent limitations of analyzing this data become clear.

As an example, let's critically examine one of the top findings from cybersecurity company Trend Micro, whose 2015 report on data breaches is based exclusively on information from the Privacy Rights Clearinghouse database, which in turn is based on public reports of data breaches:[25] "The healthcare sector was most affected by data breaches, followed by the government and retail sectors."

Media outlets have cited this finding left and right. *DarkReading*, a popular cybersecurity news outlet, released an article with the headline "Healthcare Biggest Offender in 10 Years

23. U.S. Department of Health and Human Services, "Cases Currently Under Investigation," Office for Civil Rights, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (accessed October 14, 2016).

24. Privacy Rights Clearinghouse, *Chronology of Data Breaches: FAQs*, https://www.privacyrights.org/chronology-data-breaches-faq#is-chronology-exhaustive-list (accessed October 14, 2016).

25. Trend Micro, *Follow the Data: Analyzing Breaches by Industry* (San Diego: Privacy Rights Clearinghouse, 2015), https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-analyzing-breaches-by-industry.pdf.

of Data Breaches."[26] *Fortune* magazine reported, "Hackers love to attack the healthcare industry. . . . The healthcare industry leads the way as a hacking target, followed by government and retailers."[27]

But is it really true that the healthcare sector was most affected by data breaches—or does the healthcare industry simply *report* breaches more often? Certainly healthcare providers have more regulatory requirements relating to data breach notification compared with most other industries. The federal HIPAA/HITECH laws mandate that covered entities report data breaches affecting more than 500 persons to the public, and the Office for Civil Rights (OCR) conducts audits and fines entities that do not comply. Likewise, retail companies, by their nature, handle extensive volumes of payment card data, which is easy to detect when used fraudulently—likely resulting in a higher percentage of reported breaches than other types of data.

The Trend Micro report goes on to say: "An increase in the number of reported incidents strongly indicates that the total volume of data breaches has also risen and vice versa."[28]

This is a big assumption—and one that overlooks the impact of major changes in law, insurance coverage, regulation, and technology. In fact, a rise in the volume of *detected* and *reported* breaches can actually signify a good thing. Sure, higher numbers of reported breaches *could* signify a rise in actual breach occurrences—but this trend can also be caused by:

- Improvements in detection systems
- Breach notification laws that are increasingly aligned with public expectations of privacy
- Effective third-party audits and systems to hold organizations accountable for breaches
- Maturation of incident response processes and procedures
- Growth of data breach insurance coverage options

Cybersecurity vendors have incentive to interpret the data as an increase in the number of actual data breaches that occur ("The sky is falling! Buy our product.") In reality, we can only conclude that there has been an increase in the number of *detected* and *reported* data breaches within their sample set—an important distinction.

Another finding of the Trend Micro report was that[29] "[l]ost or stolen physical devices, such as 'portable drives, laptops, office computers, files, and other physical properties' combined were the primary 'breach [method] observed across industries.'"

This generated a spate of news articles with headlines such as "More data breaches caused by lost devices than malware or hacking" (*Network World*)[30] and statements like "Nearly half

---

26. Sara Peters, "Healthcare Biggest Offender in 10 Years of Data Breaches," *DarkReading*, September 22, 2015, http://www.darkreading.com/analytics/healthcare-biggest-o_ender-in-10-years-of-data-breaches/d/d-id/1322292.

27. Jonathan Vanian, "Five Things to Know to Avoid Getting Hacked," *Fortune*, September 25, 2015, http://fortune.com/2015/09/25/five-facts-cyber-security.

28. Trend Micro, *Follow the Data*.

29. Trend Micro, *Follow the Data*.

30. Patrick Nelson, "More Data Breaches Caused by Lost Devices than Malware or Hacking, Trend Micro Says," *Network World*, October 5, 2015, https://www.networkworld.com/article/2988643/security/device-loss-data-breach-malware-hacking-trend-micro-report.html.

of all data breaches occur when ID-theft criminals access information because we lost a device" (*AZWorld*).[31]

But is it really true that more data breaches were caused due to lost or stolen physical devices? All we really know is that there were more *publicly reported* data breaches of this type. An alternative: Could it be that stolen laptop incidents are more straightforward to detect and analyze than a sophisticated spyware infection, leading to higher reporting rates?

Again, cybersecurity vendors and media outlets have clear incentives to produce reports with strong, quotable conclusions, but readers have to take all of these findings with a grain of salt.

1.2.2 Raise Your Hand if You've Had a Data Breach

Due to the often-inaccessible nature of data breach statistics, many publications base their information on surveys. Unfortunately, surveys themselves contain inherent bias and flaws.

In a scathing 2011 report by Microsoft, two researchers ripped apart various survey-based cybercrime and identity theft reports, including the FTC's Identity Theft Survey Reports, the Gartner Phishing Survey, and more.[32] Microsoft's researchers concluded, "Our assessment of the quality of cyber-crime surveys is harsh: they are so compromised and biased that no faith whatever can be placed in their findings . . . our cyber-crime survey estimates rely almost exclusively on unverified user input."[33]

1.2.3 Cybersecurity Vendor Data

You can't throw a rock without hitting a whitepaper on data breaches or cybersecurity "threats" produced by a product or service vendor. Practically every major cybersecurity corporation has recognized the marketing value of coming up with such a report and releasing it for the media to spread. Often, these whitepapers are based on information generated by the vendor's own security products or consulting team.

Over the years, some of these studies—such as Symantec's Internet Security Threat Report (ISTR) and Verizon's Data Breach Investigations Report (DBIR)—have developed into important industry resources with respected methodologies (although they still have limitations). Other vendors simply jump to conclusions. Let's take a look at the evolution of these reports, so that we can better understand both the value and the inherent limitations.

One of the earliest cybersecurity reports was released by a groundbreaking but largely forgotten company called Riptech, Inc. Led by Chief Executive Officer (CEO) Amit Yoran (who later went on to become the president of RSA Security), Riptech was, in 2001, "the only provider of real-time managed security services" (at least according to the company's own press

31. Mark Pribish, "Lost Electronic Devices Can Lead to Data Breaches," *AZ Central*, September 30, 2015, http://www.azcentral.com/story/money/business/tech/2015/09/30/lost-electronic-devices-data-breaches/73058138.

32. Dinei Florêncio and Cormac Herley, "Sex, Lies and Cyber-crime Surveys," 10th Workshop on the Economics of Information Security, Fairfax, VA, 2011, https://web.archive.org/web/20110902055639/http://weis2011.econinfosec.org/papers/Sex,%20Lies%20and%20Cyber-crime%20Surveys.pdf.

33. Florêncio and Herley, "Sex, Lies and Cyber-crime Surveys."

release).[34] In 2002, Riptech released a landmark paper: the Riptech Internet Security Threat Report (ISTR), which was eventually taken over by Symantec.

The inauguaral Riptech ISTR was novel in that it represented the first time that a company engaged in managed security services had leveraged its own collection of data to produce a published report on cybersecurity attack trends. From the inaugural report:[35]

> Riptech analyzes data produced by numerous brands of firewalls and intrusion detection systems (IDSs) used by hundreds of clients throughout the world. Using a sophisticated combination of technology and human expertise to analyze this data, Riptech identifies and investigates cyber attacks that occur on client networks in real-time. A by-product of this daily investigation of Internet attacks is a vast amount of data on cyber threats that can be analyzed to reveal interesting and actionable trends. . . . We believe this study provides a uniquely accurate view of the state of Internet threats.

Riptech's data set could not possibly represent an "accurate view" of the Internet as a whole. Its sample size was approximately 300 companies, more than 100 of which were apparently located in the same netblock, and all of which had taken the highly unusual action (for 2001) of engaging the services of a managed security services provider. However, it was a groundbreaking concept.

When Symantec purchased Riptech later that year, it continued to release the ISTR annually, over time adding Symantec's growing pool of data sources.

By 2016, the Symantec Internet Security Threat Report was all grown up. Symantec stated that the threat data that it used for analysis came from the Symantec Global Intelligence Network, which consists of "more than 63.8 million attack sensors."[36] Of course, even this large sample set is still intrinsically biased, if only because the vast majority of the sources had engaged Symantec as a vendor. Nonetheless, the ISTR is widely considered to be one of the best resources for tracking data breach and cybersecurity trends.

Verizon has also emerged as a key player in data breach investigations and response, with the 2008 inaugural publication of the Verizon Data Breach Investigations Report (VBIR). According to this report, the Verizon Business Investigative Response Team handled "over 500 security breach and data compromise engagements between 2004 and 2007." Staggeringly, the report claimed that Verizon's case load represented "roughly one-third of all publicly disclosed data breaches in 2005 and a quarter of those in both 2006 and 2007 . . . [including] three of the five largest data breaches ever reported."[37]

---

34. Business Wire, "Riptech Unveils Caltarian, a Next-Generation Managed Security Platform," *Free Library*, April 2, 2001, http://www.thefreelibrary.com/Riptech+Unveils+Caltarian,+a+Next-Generation+Managed+Security...-a072584421.

35. Riptech Inc., *Riptech Internet Security Threat Report: Attack Trends for Q3 and Q4 2001* (Alexandria, VA: Riptech Inc., 2001), http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_i.pdf.

36. Symantec, *Internet Security Threat Report* vol. 21 (Mountain View, CA: Symantec, April 2016), 4, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

37. Wade H. Baker, C. David Hylender, and J. Andrew Valentine, *2008 Data Breach Investigations Report*, Verizon Enterprise, 2008, http://www.verizonenterprise.com/resources/security/databreachreport.pdf.

In a notably artistic flourish, the first VBIR prominently highlighted a quote from William R. Maples (*Dead Men Do Tell Tales*):[38]

> That's how I feel about the skeletons in my laboratory. These have tales to tell us, even though they are dead. It is up to me, the forensic anthropologist, to catch their mute cries and whispers, and to interpret them for the living.

Verizon itself was the first to note inherent bias in its data set, since the entire sample consisted of customers who had, obviously, engaged Verizon to investigate a suspected breach. This required a certain level of awareness of cybersecurity within the breached organization, as well as resources available to retain digital forensics and incident response experts.[39]

The company continued to publish the VBIR each year, and as industry response teams diversified, Verizon partnered with a growing population of security companies and incident response teams to enlarge the sample size. To faciliate reporting and analysis of data breaches, Verizon developed the Vocabulary for Event Recording and Incident Sharing (VERIS), which is a publicly available "set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner."[40]

By 2016, the data set was "made up of over 100,000 incidents, of which 3,141 were confirmed data breaches. Of these, 64,199 incidents and 2,260 breaches comprise the finalized dataset that was used in the analysis and figures throughout the report."[41] Certainly an enormous leap from the 500 breaches analyzed in 2008!

1.3 Why Report?

It's tempting to ask the question, "Why aren't data breaches reported?" but perhaps a better question is, "Why *are* breaches reported?"

Organizations that report data breaches suffer potentially devastating consequences, including reputational, operational, and financial impacts. For example, after Target announced its credit card data breach in 2014, its fourth-quarter profits dropped 46%, or $440 million.[42] CEO Gregg Steinhafel resigned a few months later, in a move publicly linked to the breach.[43]

38. Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report."

39. Baker, Hylender, and Valentine, "2008 Data Breach Investigations Report."

40. VERIS: The Vocabulary for Event Recording and Incident Sharing, http://veriscommunity.net (accessed January 5, 2018).

41. Verizon, *2016 Data Breach Investigations Report*, Verizon Enterprise, 2016, 1, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

42. MarketWatch, "Target's Profits Down $440M after Data Breach," *New York Post*, February 26, 2014, https://nypost.com/2014/02/26/targets-profits-down-46-after-data-breach.

43. Antone Gonsalves, "Target CEO Resignation Highlights Cost of Security Blunders," *CSO Online*, May 5, 2014, http://www.csoonline.com/article/2151381/cyber-attacks-espionage/target-ceo-resignation-highlights-cost-of-security-blunders.html.

Home Depot was hit with a painful consumer lawsuit after its data breach, which it finally settled in 2016 for $19.5 million. "The home improvement retailer will set up a $13 million fund to reimburse shoppers for out-of-pocket losses, and spend at least $6.5 million to fund 1-1/2 years of cardholder identity protection services."[44] After the security company RSA was hacked, its parent company, EMC, spent $66 million "on transaction monitoring for its corporate customers who worried that their RSA security tokens—long considered the gold-standard for protecting sensitive data—had been compromised in the attack."[45]

Reputational impact is harder to quantify, but very real. A 2011 Ponemon Institute survey of 843 "senior-level individuals" found that the average "diminished value [of corporate brand] resulting from a data breach of customer data" was 21%. If the breach affected only employee data, the diminshed value of the brand was only 12%.[46]

Data breaches can also have more formal reputational effects. For example, Standard & Poor issued a report in 2015 warning that lenders that suffered data breaches could have their ratings downgraded.[47]

The operational impacts of a data breach can cause direct losses and brand damage, as well. In 2014, *Forbes* and IBM released a joint study showing how business disruptions—caused in part by data breaches—can have deep and lasting consequences for businesses. As summarized by *Forbes*:[48]

> Lost revenues, downtime and the cost of restoring systems can accrue at the rate of $50,000 per minute for a minor disruption. . . . But what about the greater toll a sustained outage or major security breach can take on a company's reputation?
>
> . . . If customers can't log on to your site, you not only lose a sale today, but you also risk losing future business, particularly for retailers. For financial institutions, a security breach can scare away customers and open the door to fraud. A network outage for any telecom or IT company may leave clients wondering why they should trust their own reputation to a vendor who might make them look incompetent.

With all of these negative pressures, and absent clear laws that require reporting or even a clear definition of a "breach," why do organizations report data breaches at all?

---

44. Jonathan Stempel, "Home Depot Settles Consumer Lawsuit over Big 2014 Data Breach," *Reuters*, March 8, 2016, http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z.

45. Hayley Tsukayama, "Cyber Attack on RSA Cost EMC $66 Million," *Washington Post*, July 26, 2011, https://www.washingtonpost.com/pb/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html.

46. Ponemon Institute LLC, *Reputation Impact of a Data Breach: U.S. Study of Executives and Managers* (Research Report Sponsored by Experian, November 2011), https://www.experian.com/assets/data-breach/white-papers/reputation-study.pdf.

47. Roi Perez, "S&P Could Downgrade Lenders to Standard and Poor for Cyber-Security," *SC Media UK*, October 1, 2015, http://www.scmagazineuk.com/standard-and-poor-to-downgrade-banks-credit-rating/article/441892.

48. Hugo Moreno, "Protecting Your Company's Reputation in a Heartbleed World," *Forbes*, April 14, 2014, https://www.forbes.com/forbesinsights/ibm_reputational_IT_risk/index.html.

Data breaches are typically reported to the public for one of three reasons:

- **The data breach is already public or likely to become public.** If you look at most data breach reports that hit the news, you'll notice that they are often first reported by an investigative journalist or involve sensitive information that has been publicly leaked. The affected organizations reported because, well, it's already out there. When investigative journalist Brian Krebs found Home Depot's customer credit card information for sale on the "dark web" in 2014 and published an article about it, Home Depot had little choice but to immediately issue a public statement.
- **There is a clear legal requirement to report, and harm to the organization (such as fines) would occur if the breach improperly went unreported.** For example, the OCR has the ability to impose fines, as well as civil or criminal charges, due to HIPAA violations (which include data breach reporting requirements). That doesn't mean the breached organization *will* notify the public; it just means it has more incentive to do so than in other cases where HIPAA does not apply.
- **The information leaked is at high risk of being misused and the breached organization may be liable for damage**. For example, LastPass, an online password storage application, issued a statement in 2015 notifying users of a breach and encouraging them to "change their master passwords."[49]

Absent one of these motivating factors, there are few (if any) incentives for organizations to publicly disclose the data breach.

Even when breaches are reported to the public, often key details are left out. Symantec highlighted incomplete reporting as a critical issue in the 2016 ISTR:[50]

> [M]ore and more companies chose not to reveal the full extent of the breaches they experienced. Companies choosing not to report the number of records lost increased by 85 percent. . . . The fact that companies are increasingly choosing to hold back critical details after a breach is a disturbing trend. Transparency is critical to security. While numerous data sharing initiatives are underway in the security industry, helping all of us improve our security products and postures, some of this data is getting harder to collect.

1.4 What's Left Unsaid

Who knows what data breaches are happening right now, which we will only hear about in the years to come? The public is flooded with news reports about breaches every day—but oceans

49. Joe Siegrist, "LastPass Security Notice," *LastPass*, June 15, 2015, https://blog.lastpass.com/2015/06/lastpass-security-notice.html.

50. Symantec, "2016 Internet Security Threat Report," *ISTR 21* (April 2016): 6, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

more are never reported. Organizations that detect breaches are faced with an ethical dilemma, in that there is no clear "right" path, and those that disclose may suffer far more than those that keep things quiet. This very fact prevents us from even knowing the true extent of the problem.

Even the very definition of a "data breach" is up for debate. How can we effectively respond to something when we can't even agree on exactly what it *is*?

As a society, we have a lot of work to do. It doesn't benefit anyone if a data breach destroys an organization or sucks resources away that it could have used to support jobs or provide better services to customers. In the years to come, we need to come to a consensus on a definition of "data breach," figure out how to gather data, and develop accurate models. We need more transparency, so that we can analyze the impact of data breaches and identify effective strategies for reducing harm.

We have to decide what we, as a society, want organizations to do in the event of a data breach. Then we have to clearly define that through law, industry standards, and guidelines, and give breached organizations incentives to do the right thing.

Since ancient times of computing (the 1970s), breached organizations have wrestled with the same problems, time and time again. Even the earliest breach cases share many similarities with those we see today. In the next chapters, we'll examine some of the earliest data breaches, see what we can learn, and introduce a new, modern methodology for managing data breach response.

This page intentionally left blank

Chapter 2

Hazardous Material

November 14, 1980 (noon) - The phone rang at a desk at National CSS (NCSS) headquarters in Wilton, Connecticut. A woman answered. On the other end of the line, a voice asked jokingly, "What would you give for the [password] directory?"[1] The caller was referring to the highly sensitive database on NCSS systems that contained all 14,000 customer user IDs and passwords. But it wasn't funny—he really had the data.

At the time, NCSS was a top computer time-sharing company. A predecessor of modern cloud providers, NCSS offered digital storage space and remote processing for approximately 3,100 organizations in banking, government, engineering, finance, utilities, and more. Major customers included Bank of America and Dun & Bradstreet (which had acquired NCSS in 1979).[2]

It is impossible to know precisely what data was on the NCSS systems (and it's unlikely that NCSS knew itself, in much the same way that most of today's cloud providers do not take specific inventory of their customers' data). However, given their massive clientele, the NCSS servers could easily have housed millions of people's Social Security numbers (SSNs), bank account records, payroll information, credit details, and more. An unauthorized person with access to the directory data could read or modify any customer's files, potentially resulting in untold damages.

The Theft

According to FBI's investigative report (revealed nearly 40 years later), the data was stolen by a former NCSS programmer, Bruce Ivan Paul, who had left and gone to a small consulting firm called the Guild. In June 1980, shortly after Paul's departure, a mysterious intruder made multiple unauthorized connections to the NCSS mainframes, attached a backup database that contained the customer passwords, and transferred files to the "GUILD" account on NCSS systems. "The access was accomplished using userids known to Bruce Paul from his work at NCSS," stated the company's internal incident report. "The passwords for these userids may have remained unchanged since the time of his termination. Alternatively they may have been

1. "Event Report as of 1/21/81 08:45:30," FBI file 196A-397 (New Haven), FOIA/PA #1364189-0, E3df34b6cc6c2a9a14ddc71e47c1a18b8d966c57f_Q3702_R343967_D1813129.pdf, January 21, 1981, 48 (obtained under the FOIA from the FBI; received March 2019).

2. IT History Society, *National CSS, Inc. (NCSS),* http://www.ithistory.org/db/companies/national-css-inc-ncss (accessed April 29, 2019).

determined using the DIRPRINT facility" (a command known to NCSS programmers that was used to retrieve passwords).[3]

A month after the passwords were downloaded to the "GUILD" account, Paul transferred the data to the computer system of a company called Mediametrics, based in California. Mediametrics had purchased a mini-computer from NCSS and also hired the Guild to improve its software in exchange for free disk storage space and use of its computer systems. This was a handy arrangement for the Guild, since at the time, computing resources were very limited. Personal computers had not yet become widespread. The Guild's team eagerly took advantage of the Mediametrics disk space.

By November 1980, the relationship between the Guild and Mediametrics had become strained. The Guild was doing "very little work" on Mediametrics projects, yet routinely using the company's computer system. On November 7, the Guild's activities caused Mediametrics' system to crash. In response, Mediametrics informed the Guild that it was no longer allowed to access Mediametrics' computer and changed the Guild's password, expecting that this would lock it out.[4]

It didn't work. Surprisingly, a few days later, a technician at Mediametrics realized that the Guild had once again gained access to the Mediametrics system. The FBI reported that the Guild must have broken in using a default administrator account.

Concerned that the Guild might have stolen proprietary data, too, Mediametrics conducted an inventory of the files in the Guild's disk space.[5] There, it discovered suspicious files that appeared to contain thousands of stolen NCSS customer IDs and passwords, as well as copies of valuable NCSS software. A technician tested three customer passwords and was able to successfully access three NCSS customer accounts. The data was valid.

Triage

Around noon on November 14, 1980, Mediametrics called its contact at NCSS and notified her of the stolen data. She escalated to a manager, who immediately recognized the risk. According to the FBI interview, "[He] explained that, if what [she] said was true, it would have been a most serious breech [*sic*] of security into the National CSS system and would have monumental consequences."[6]

After an internal conference call, NCSS decided to verify that the data was real. An NCSS employee used a terminal to remotely log onto the Guild's account at Mediametrics and began analyzing the files in its disk space. Suddenly, while she was working, a curt message appeared on her screen from "BIPPER" (associated with the Guild's account). "Who the hell is this?"

---

3. Federal Bureau of Investigation, "Prosecutive Report of Investigation Concerning Bruce Ivan Paul; National CSS - Victim; Fraud by Wire - Computer Fraud," FBI file 196A-397 (New Haven), FOIA/PA #1364189-0, E3df34b6cc6c2a9a14ddc71e47c1a18b8d966c57f_Q3702_R343967_D1813131.pdf, October 6, 1981, 12 (obtained under the FOIA from the FBI; received March 2019).

4. Federal Bureau of Investigation, "FD-302," FBI file 196A-397 (New Haven), FOIA/PA #1364189-0, E3df34b6cc6c2a9a14ddc71e47c1a18b8d966c57f_Q3702_R343967_D1813129.pdf, May 29, 1981, 85 (obtained under the FOIA from the FBI; received March 2019).

5. FBI, "Prosecutive Report," 14.

6. FBI, "FD-302," 101.

it read. Minutes later, her connection was forcibly terminated. She reconnected and finished verifying that the data did, in fact, appear to contain valid customer data. (Shortly thereafter, a different NCSS employee received a call from Bruce Ivan Paul, asking who was using the Guild account.)

Having confirmed the validity of the data, NCSS moved into the next phase: damage control. Upon request, Mediametrics agreed to temporarily remove its computer from the network, in order to prevent any further unauthorized access. The following morning, NCSS staff met with Mediametrics onsite and collected system log files, backup tapes, printouts, and other evidence. It was an early example of digital forensic evidence acquisition.

Involving Law Enforcement

Recognizing the potential risks, NCSS attorneys and their management team wrestled with the case. In 1980, there were no computer security incident response manuals, no template breach notification letters, no digital forensics experts, and no "breach coaches" to guide the company. Indeed, the very concept of hosting large quantities of digital data on behalf of another company—and therefore losing it, as well—was relatively new.[7]

Hoping to recover the password files quickly from the suspected thieves, an NCSS attorney made a call he or she probably regretted later—to the FBI.[8] NCSS asked the FBI to "handle the situation quietly" and recover the password data from the suspects.[9]

But the FBI refused to guarantee secrecy and could not take quick action against the suspects to recover the stolen data. "NCSS officials suddenly became defensive and 'uncooperative,' hiding behind a phalanx of corporate lawyers," reported the *New York Times*. In order to move forward with the investigation, the FBI ultimately resorted to threatening NCSS with grand jury subpoenas.[10]

The FBI later told the press it was a "learning experience." It certainly was for NCSS, as well: Once the FBI was notified, the investigation spun out of its control.

The First Customer Breach Notification

NCSS's parent company, Dun & Bradstreet (D&B), stepped in to oversee the response. As one of NCSS's largest customers, the D&B executive team undoubtedly understood the value of the data stored within corporate accounts on NCSS systems and the potential for liability if it were to be misused. According to the *New York Times*, "[T]he traditional D. & B. credit services have become increasingly dependent on NCSS technology and the network. . . . [A]nyone who had obtained the NCSS password directory would have been able to change or erase or create data,

---

7. Harold Feinleib "A Technical History of National CSS," *IT Corporate Histories Collection*, March 4, 2005, http://corphist.computerhistory.org/corphist/documents/doc-42ae226a5a4a1.pdf.

8. Federal Bureau of Investigation, "Complaint Form: FD-71," FBI file 196A-397 (New Haven), FOIA/PA #1364189-0, E3df34b6cc6c2a9a14ddc71e47c1a18b8d966c57f_Q3702_R343967_D1813129.pdf, November 15, 1980, 3 (obtained under the FOIA from the FBI; received March 2019).

9. Vin McLellan, "Case of the Purloined Password," *New York Times*, July 26, 1981, http://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html?pagewanted=1.

10. McLellan, "Case of the Purloined Password."

according to NCSS technicians familiar with the D. & B. software. In other words, temporarily, at least, a thief could create or diminish credit."[11]

Unable to recover the stolen data and faced with the ongoing risk of unauthorized access to customer accounts, D&B made the unprecedented and controversial decision to notify NCSS customers. NCSS liaisons began making phone calls to their customers. The following week, NCSS, under orders of D&B executives, sent what the *New York Times* later dubbed "the first 'broadcast' security alert to the entire customer base of a major timesharing company in the 25-year history of the industry."[12]

As shown in Figure 2-1, the letter was short and sweet, notifying customers of a problem but providing no detail. The November 20 letter included the following statement:[13]

> It has come to our attention that a former employee may have obtained information which could potentially compromise system access security. Although a breach of any customer's data security is highly unlikely, in line with our total commitment to maintain absolute security, we strongly urge that you immediately change all passwords by which you access the National CSS' systems.

This landmark notification letter represented a *minimal disclosure* strategy, with NCSS releasing only the information necessary to minimize the risk of future unauthorized access to customer data. Importantly, NCSS did not *force* a password change, but instead, merely "urged" customers to do so. Forcing a password reset for 14,000 corporate accounts would likely have resulted in interruptions for customers and a high volume of complaints. By notifiying its customer base of the risk (without actually stating outright that the passwords had been stolen), NCSS placed the ball in their court.

Customers understandably expressed frustration at the lack of detail and guarded wording of the notification letter. Frank Logrippo, a manager at the auditing firm Coopers & Lybrand, was told by his customer service representative over the phone that the password directory had been found at another company in California and then received the notification letter the following week. "If the passwords were found at someone else's site," he complained, "it's not 'may be compromised'—it's compromised!"

Rival timesharing firms, too, criticized NCSS's widespread and vague notification. Chester Bartholomew, the "protection and control director" for competitor Boeing Computer Services,[14] said "Everybody in this business has dealt with penetration. Usually, we have enough information to take a rifle shot at it rather than let loose with a shotgun blast."[15] NCSS never indicated when the breach actually occurred, how long the password file had been exposed, or how to tell whether a specific account had been accessed. In response to inquiries, NCSS refused to release any further details, stating that "the matter is still under investigation for potential criminal action."[16]

---

11. McLellan, "Case of the Purloined Password."

12. McLellan, "Case of the Purloined Password."

13. FBI, "Prosecutive Report," 74.

14. Boeing Frontiers, "A Step Back in Virtual Time," *Boeing Frontiers* 2, no. 4 (August 2003), http://www.boeing.com/news/frontiers/archive/2003/august/cover4.html.

15. McLellan, "Case of the Purloined Password."

16. Rita, Shoor. "Firm Avoids Security Breach with Customer Cooperation," *Computerworld*, January 19, 1981, 13.

Dear Customer:

National CSS has always worked to ensure the security of its customers' data and software.

It has come to our attention that a former employee may have obtained information that could potentially compromise system access security.

Although a breach of any customer's data security is highly unlikely, in line with our total commitment to maintain absolute security, we strongly urge that you immediately change all passwords which you use to access National CSS' systems.

To change passwords, issue one of the following CSS commands:

SET LOGPSWD	to change the login password
SET READPSWD	to change the disk read password
SET WRITEPSWD	to change the disk write password

The system will prompt you for: (1) the current login password, (2) the new password, and (3) the new password a second time for validation purposes.

If read/write passwords are different from the login password they should be changed as well.

If you have any problems in implementing this procedure, you may get assistance in the U.S. by calling one of our toll-free numbers:

800-243-6119 (outside Connecticut)
800-882-5575 (Connecticut)

In Europe, call collect:

01-834-2223 (London)
261-56-35 (Paris)

We sincerely regret the inconvenience this will cause, but strongly feel that no other alternative will serve your interests better.

Sincerely,

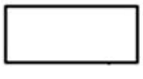


Figure 2-1. The notification letter sent to NCSS customers in November 1980 (obtained under the FOIA from the FBI; received March 2019)

Downplaying Risk

It was not clear what justification, if any, NCSS had for concluding that an actual breach of customer data was "highly unlikely." The company offered no evidence to indicate that customer accounts had *not* been accessed, and the evidence showed that some were. For

example, a later audit uncovered unauthorized access to the systems of Marsh & McLennan, Inc. ("Marsh"), a large insurance company based in San Francisco. The intruder logged in using a default administrator password that came preconfigured on NCSS computers. Upon review, Marsh's team was "unable to determine what the unauthorized user was doing," but they were "99 per cent sure that the unauthorized user did not change any of the files as all things balanced out after the entry."[17]

Although NCSS conducted an audit after the Mediametrics incident, it was very limited in scope. The tools for logging and monitoring account access in 1980 were immature and had not been widely adopted. Detecting unauthorized access was a painstaking and tedious process.

What's more, the risk of widespread account compromise at NCSS was high. At NCSS, customer passwords were accessible to many people and could have been copied and used countless times without discovery. Default passwords were widespread. Customers such as Marsh were not told that the computers they purchased had account passwords that were used on other customer systems and therefore did not consider changing them.[18]

Media Manipulation

Dun & Bradstreet moved quickly to control the media response—and it was clearly well positioned to do so. The popular computer magazine *Datamation* prepared a news report on the incident, but D&B had previously acquired the magazine in 1977 and "vetoed" the article. *Computerworld* magazine published a short piece in January 1981 that perfectly toed the D&B company line with the (misleading) headline "Firm Avoids Security Breach with Customer Cooperation."

"What can be done to prevent a security breach when an employee with access to sensitive information voluntarily leaves the company?" the article queried. According to the article, which quoted only one source (the president of NCSS, David Fehr), customers were "very cooperative about the password change."[19] Problem solved. No mention was made of the fact that the password file was found on a third party's computer system or the possibility that customer files could have been accessed by an unauthorized person.

Somehow, in the public eye, the case of the stolen password file had morphed into a story about how an ordinary employer, faced with an unpreventable "potential security problem," did the right thing and "chose to let all of its timesharing customers in on things" so they could "change the locks."[20]

Reporters, and the general public, didn't know enough about technology to ask the right questions. In 1981, when the *New York Times* article was published, relatively few people had ever used a computer, or even knew what a password *was*. Home computers barely existed. Corporations, government, and research institutions rented space on timesharing servers, and

17. FBI, "FD-302," 92.

18. FBI, "FD-302," 92.

19. Shoor, "Firm Avoids Security Breach."

20. Shoor, "Firm Avoids Security Breach," 13.

only a small percentage of employees logged into the timesharing system to process data. Many people had no clue that their personal details were stored on a computer system at all. People didn't understand what an electronic credit report was or what it could be used for, the concept of "identity theft" didn't exist, and most thought a SSN was good for tax returns and, well, Social Security services.

As a result, the media did not effectively investigate and report on the volume of data that may have been exposed, instead focusing on the theft of the passwords themselves. It was as though the *New York Times* had published an article about an oil tanker hitting an iceberg and thoroughly reported the details of the accident, but failed to investigate whether any oil had actually spilled.

Skeletons in the Closet

The FBI investigation continued. Over time, former NCSS staff members and Department of Justice officials gabbed to the media. Finally, in July 1981, the *New York Times* published a lengthy exposeé ("The Case of the Purloined Password"), and details of the breach finally—and briefly—emerged in the public eye. The *New York Times* article revealed a history of pervasive, and previously unreported, security issues within both NCSS and the timesharing industry as a whole.

Earlier cases from the late 1970s were suddenly exposed, indicating that customers had access to the sensitive NCSS directory—and therefore other customers' passwords—for years. A Bank of America programmer once demonstrated that he could access the NCSS directory from the bank's computers, which had prompted NCSS to conduct a "six-month security review." Around the same time, in the late 1970s, NCSS discovered that a group of their own employees, based in Detroit, had hacked the system in order to routinely gain unauthorized access to customer files for more than a year.

Two NCSS executives also claimed that they had once been offered the password directory of their biggest direct competitor, the Service Bureau Corporation (SBC), for $5,000. Reportedly, SBC officials said they had "no record of the incident."

Industry professionals waved off the problems. "Every timesharing firm in the world has these skeletons in the closet," said Larry Smith, former employee of NCSS.[21] Another professional, interviewed by the FBI, offered his opinion that the theft of the NCSS directory was not done for criminal purposes. "[H]e referred to the term 'hackery' which is known in the business as an attempt by someone to break the system. It was his opinion that the hackery would continue in the computer business as long as security for programs and computer information had loop holes in the design."[22]

What We Can Learn

The NCSS breach of 1980 did not go down in history as the first "mega-breach" to capture the public's attention—but perhaps it should have. Consider the vast troves of data that the NCSS

21. McLellan, "Case of the Purloined Password."

22. FBI, "FD-302," 65.

systems almost certainly housed on behalf of its 3,100 corporate customers, which could have been accessed or modified.

Many of the issues raised in the NCSS case remain relevant in data breaches today. The NCSS breach demonstrates how classic security flaws contribute to the risk of data breaches, including:

- Insider attacks
- Default credentials
- Shared passwords
- Insecure password storage
- Lack of effective monitoring
- Vendor risks

In addition, the response of NCSS and its parent company, Dun & Bradstreet, included nascent elements of a modern breach response, including:

- Digital evidence aquisition
- Law enforcement involvement (clearly a "learning experience" at the time)
- Formal breach notification
- Public relations efforts specifically related to the breach

Above all, the NCSS breach was a landmark case because it illustrated how entrusting other people with data, and holding data on behalf of others, introduces risk for all. On the timesharing system, as in the modern cloud, customers fear that their data may be accessed by unauthorized parties. Hosting providers fear the potential for reputational and legal consequences in the event that a breach occurs. All parties must work together in order to minimize risk system-wide.

As we will see in this chapter, storing data inherently creates risk. As organizations rush to amass large volumes of data, data breaches naturally occur with greater frequency. In the next sections, we will learn about how data collection creates risk and the five factors that influence the risk of a data breach. Finally, we will show how understanding these five factors can help security professionals effectively assess and manage the risk of a breach.

2.1 Data Is the New Oil

In March 1989, the massive *Exxon Valdez* oil spill devastated pristine Alaskan waters, immediately killing hundreds of thousands of animals and causing untold long-term damage to the marine environment. It was one of the worst environmental catastrophes ever caused by humans.

Ironically, just one month before the *Exxon Valdez* spill, Dun & Bradstreet executive George Feeney enthusiastically likened information to oil:[23]

> In the oil business you start off exploring for oil, you move on to producing and refining it, and only then do you worry about marketing and distributing it. . . . Well, think of the information business like the oil business. In the 1970's and early 1980's, we gathered data, processed it and refined it. Now the critical technology is making it available to customers.

Like early auto mechanics, the people who stored, used, and disposed of electronic data during the 1970s and 1980s did so without any thought of negative consequences. Indeed, it didn't seem like there could be much of a downside to accumulating data; on the contrary, there was enormous potential. Published stories of computer break-ins were few and far between. There were no laws or regulations surrounding data storage or breach notification requirements. The term "data breach" didn't even exist.

It turned out that, much like oil, data could spill and escape the confines of its containers. And spill it did.

Data = Risk

Storing, processing, or transmitting data creates risk for an organization. Treat sensitive data as hazardous material. You wouldn't allow large volumes of oil, natural gas, or other chemicals to be stored willy-nilly throughout your physical facilities, with no safety standards or checks. That would be a recipe for disaster. In the same manner, identify sensitive information throughout your organization and assess and manage the risks associated with it. Make sure that data is stored securely and in compliance with regulations, regularly check on your security systems, and dispose of data promptly and properly when you no longer need it.

2.1.1 Secret Data Collection

There are indications that some companies purposefully hid their data collection practices from the public, understanding that it would make people uncomfortable. For example, in 1981, the *Los Angeles Times* published an article called "TRW Credit-Check Unit Maintains Low Profile—and 86 Million Files." While today this wouldn't be considered news at all, at the time, the company's business model was absolutely eye-opening for readers. The article began much like an exposé:[24]

> There are no windows facing the street, no corporate signs on the side, no markings to indicate what's going on inside. There is virtually nothing to attract the glance of a passing

23. Claudia H. Deutsch, "Dun & Bradstreet's Bid to Stay Ahead," *New York Times*, late ed. (East Coast), February 12, 1989, A1.

24. Tom Furlong, "TRW Credit-Check Unit Maintains Low Profile—and 86 Million Files," *Los Angeles Times*, September 18, 1981.

> motorist. The facade is no accident. Housed within are super-sensitive financial and credit records of virtually every Californian who has charged a washing machine at Montgomery Ward & Co., bought a meal on MasterCard or purchased an airline ticket with Visa.

The article goes on to explain to concerned and curious public readers how credit reports were collected, used, and updated. While credit reporting had existed for decades on a small scale, operating within specific geographic regions and industries, by the early 1980s, advancements in computer and communications technology allowed them to expand dramatically. "Histories that were once read over the phone to an inquiring business were now transmitted electronically. . . . [Credit reporting companies transformed] themselves from 'local associations' or 'bureaus' that clipped wedding announcements from newspapers to 'efficient integrated systems serving an entire society."[25]

By 1981, TRW stored "about 500 million lines of information on consumers, 25 times what it was 10 years ago, and 22 million lines on businesses, up from nothing five years ago. . . . The very existence of such a large data bank is somewhat Orwellian to those who worry the data will be misused." No wonder the company kept a low profile.

2.1.2 The TRW Breach

The public's fears appeared justified when TRW burst into the spotlight on June 21, 1984. "The credit ratings of the 90 million people tracked by TRW Information Services have been exposed to credit card thieves armed with simple home computers," reported Lou Dolinar of *Newsday*.[26] A password used by Sears to check customer credit reports had been stolen and posted to an electronic bulletin board, reportedly for as long as two and a half years.[27]

Unlike the *New York Times* reporter in the NCSS case just a few years earlier, Dolinar connected the dots. Only one TRW customer password was exposed, and yet he recognized that this password was the key to accessing all consumer data on the system—90 million records in total. The 1984 headline, "Computer Thieves Tamper with Credit," immediately grabbed the attention of consumers. In contrast, the 1981 headline in the NCSS breach, "The Case of the Purloined Password," held little meaning for the majority of the audience.

In fact, Dolinar's conclusion—that the theft of the password "exposed" all of TRW's consumer information to prospective thieves—represented the first time that the media held a company accountable due to the *potential* for unauthorized access to millions of accounts. TRW had the burden of proving that the accounts weren't actually inappropriately accessed.

TRW denied that consumer data could have been exposed. "There is no evidence . . . that anyone used the code to break into the records stored in the computer, which include credit card numbers and other information on more than 100 million people throughout the nation," said a TRW spokesperson. "All we know for sure is that the (secrecy of the) password was violated."[28]

---

25. Mark Furletti, "An Overview and History of Credit Reporting," Federal Reserve Bank of Philadelphia, June 2002.

26. Lou Dolinar, "Computer Thieves Tamper with Credit," *Morning News* (Wilmington, DE), June 21, 1984, 9.

27. Christine McGeever, "TRW Security Criticized," *InfoWorld*, August 13, 1984, 14.

28. Marcida Dodson, "TRW Investigates 'Stolen' Password," *Los Angeles Times*, June 22, 1984.

The hackers themselves disagreed. "I'm the one that did it," a hacker called "Tom" told *InfoWorld* magazine. He added that TRW's response was "a lie to keep themselves clean."[29]

A spokesperson for Sears confirmed that TRW had notified the company and changed the password. However, this fact did nothing to reassure consumers, who were the subjects of the "exposed" records and had not themselves been notified of the security breach.

Later referred to as "the first identity theft-related breach [to catch] the media's eye" by security expert Lenny Zeltser,[30] the TRW breach illustrated the risks of large-scale data accumulation. Regardless of whether all 90 million records had actually been stolen, the public held TRW accountable for the security of every record.

In direct response to the TRW breach, Representative Dan Glickman of the U.S. House added an amendment to the pending Counterfeit Access Device and Abuse Act of 1984, which made it "a federal crime to obtain unauthorized computer access to information protected by the Privacy Act and the Fair Credit Reporting Act."[31] The focus of regulation in the 1980s remained squarely on punishing the hackers, rather than holding organizations accountable for implementing appropriate computer security measures to protect against data breaches. *It would take two more decades before U.S. lawmakers passed regulations aimed at holding data custodians accountable.*

Even as the volume of data collection and processing continued to increase, measures for securely storing data lagged behind. Data was stored in poorly secured containers and transported over unencrypted communications lines. Measures for detecting and responding to "data spills" were virtually nonexistent. Data breaches became a systemic, widespread, and pervasive problem.

2.2 The Five Data Breach Risk Factors

Data is hazardous material. The more you have, the greater your risk of a data breach. In order to effectively manage the risk, you must understand the factors that contribute to the risk of a data breach.

There are five general factors that influence the risk of a data breach. These risk factors are:

1. **Retention:** The length of time that the data exists
2. **Proliferation:** The number of copies of data that exist
3. **Access:** The number of people who have access to the data, the number of ways that the data can be accessed, and the ease of obtaining access
4. **Liquidity:** The time required to access, transfer, and process the data
5. **Value:** The amount the data is worth

29. McGeever, "TRW Security Criticized," 14.

30. Lenny Zeltser, "Early Discussions of Computer Security in the Media," *SANS ISC InfoSec Forums*, September 10, 2006, https://isc.sans.edu/forums/diary/Early+Discussions+of+Computer+Security+in+the+Media/1685.

31. Mitch Betts, "DP Crime Bill Toughened," *ComputerWorld*, July 2, 1984.

The evolution of technology has increased the risk in each of these five areas, as we will see in the next sections.

2.3 The Demand for Data

Today, many types of organizations—and individuals—acquire sensitive personal data. These organizations fuel the market for data. Key players include advertising agencies, media outlets, data analytics firms, software companies, and data brokers. Data from your organization may end up in their hands, either through legitimate transactions or as the result of theft and data laundering.

Understanding how sensitive data is used, and why it is valuable, will help you evaluate the risk of storing, processing, or transferring a data set. In this section, we will examine key players in the data market and analyze how their demand for sensitive data influences the risks of a data breach.

2.3.1 Media Outlets

Media outlets create strong incentives for data leaks. Many will quietly pay for confidential information, even when those providing it are breaking the law. For example, in 2008 Lawanda Jackson, an administrative specialist at UCLA Medical Center, was convicted of selling medical information about high-profile patients to the *National Enquirer*, including information regarding the treatment of Britney Spears, Farrah Fawcett, Maria Shriver, and others. Prosecutors said that the *National Enquirer* "deposited checks totaling at least $4,600 into her husband's checking account beginning in 2006."[32]

The *National Enquirer* was caught only because celebrity Farrah Fawcett essentially set up a sting. Details about Fawcett's medical treatment were repeatedly reported in the *National Enquirer*. Eventually, she became convinced that they were being leaked from the UCLA healthcare facility itself, where she was treated. When she experienced a resurgence of cancer, she spoke with her doctor and agreed that they would withhold the news from family and friends. "I set it up with the doctor," said Fawcett. "I said, 'OK, you know and I know.' . . . I knew that if it came out, it was coming from UCLA." Days later, the *Enquirer* ran a story about Fawcett's latest medical diagnosis. "I couldn't believe how fast it came out," she said.[33]

The hospital employee was tried and convicted—but what were the consequences for the *National Enquirer*? Before Fawcett died, she made it clear that she wanted to see the magazine charged: "They obviously know it's like buying stolen goods. They've committed a crime. They've paid her money," she said.[34]

32. Shaya Tayefe Mohajer, "Former UCLA Hospital Worker Admits Selling Records," *San Diego Union-Tribune*, December 2, 2008, http://www.sandiegouniontribune.com/sdut-medical-records-breach-120208-2008dec02-story.html.

33. Charles Ornstein, "Farrah Fawcett: 'Under a Microscope' and Holding On to Hope," *ProPublica*, May 11, 2009, https://www.propublica.org/article/farrah-fawcett-under-a-microscope-and-holding-onto-hope-511.

34. Ornstein, "Farrah Fawcett."

The *Enquirer* defended its actions in a statement, saying, "[Fawcett's] public discussion of her illness has provided a valuable and important forum for awareness about the disease."[35] Both Fawcett and Jackson died before charges were filed against the tabloid.[36]

The Farrah Fawcett case was not an isolated incident—far from it. In another case, Dawn Holland, a former employee to the Betty Ford clinic, confessed that media outlet TMZ paid her $10,000 for information and a copy of a report that detailed an internal incident involving Lindsay Lohan. Patient confidentiality at the Betty Ford clinic is protected under state and federal regulation, according to clinic document.[37] TMZ apparently took steps to cover up the flow of money. According to the *New York Times*, "TMZ paid [Holland] through a bank account of her lawyer at the time, Keith Davidson, who has other clients who have appeared on TMZ. . . . She said that TMZ had called her incessantly after the incident, and that she finally agreed to talk after the treatment center suspended her."[38]

The public's lust for personal details of celebrities' lives, including health and medical information, creates an unyielding revenue stream for magazines, websites, and TV shows that provide data. "An analysis of advertising estimates from those outlets shows that the revenue stream now tops more than $3 billion annually, driving the gossip industry to ferret out salacious tidbits on a scale not seen since the California courts effectively shut down the scandal sheets of the 1950s."[39]

Where do media outlets get the juicy tidbits that fuel their businesses? A whole support industry has sprung up to harvest data about celebrities and other newsworthy people, generating quick cash for suppliers of sensitive data. "This new secrets exchange has its own set of bankable stars and one-hit wonders, high-rolling power brokers and low-level scammers, many of whom follow a fluid set of rules that do not always comport with those of state and federal law, let alone those of family or friendship," reported the *New York Times*.[40]

"We pay CA$H for Valid, Accurate, Usable Tips on Celebrities," advertised one gossip data broker, Hollywoodtip.com.[41] Lured by the promise of easy money, low-wage healthcare employees like Jackson and Holland (who made only $22,000/yr) are enticed to spill the beans.

In the days after pop star Michael Jackson's death (in June 2009), the Los Angeles County Coroner's Department found itself under siege. "[T]he offer for pictures of Michael Jackson in our building was worth $2 million the day after he died," said Deputy Coroner Ed Winter.

---

35. Ornstein, "Farrah Fawcett."

36. Jim Rutenberg, "The Gossip Machine, Churning Out Cash," *New York Times*, May 21, 2011, http://www.nytimes.com/2011/05/22/us/22gossip.html.

37. Patient confidentiality is federally protected by Alcohol and Drug Abuse Patient Records, 42 C.F.R. pt. 2; and/or HIPAA Privacy Regulations, 45 C.F.R. pts. 160, 164. See Hazelden Betty Ford Foundation, *Authorization to Disclose Medical Records*, https://www.hazelden.org/web/public/document/privacy-notice.pdf (accessed May 12, 2019).

38. Rutenberg, "Gossip Machine."

39. Rutenberg, "Gossip Machine."

40. Rutenberg, "Gossip Machine."

41. Rutenberg, "Gossip Machine."

"We had to shut down public access to our building. We had people literally climb the back fence trying to break in and get what they could."

Law enforcement officials do investigate celebrity data breach cases, with limited success. The Department of Justice has "conducted a wide-ranging investigation into illegal leaks of celebrity health records and other confidential files," including cases involving Fawcett, Spears, and Tiger Woods. However, since payments for data are often made in cash, often through intermediaries, they are difficult to track. The emergence of intermediary data brokers that support media has made it even more challenging for law enforcement to determine how a leak occurred, let alone prosecute. "Sometimes I think we're losing," said one investigator.[42]

2.3.2 Big Advertising

Marketing agencies can find enormous value in personal data, whether they serve retailers, entertainment, healthcare, or another industry. "Name a condition—Alzheimer's disease, a weak heart, obesity, poor bladder control, clinical depression, irritable bowel syndrome, erectile dysfunction, even HIV—and some data brokers will compile a list of people who have the condition, and will sell the list to companies for direct marketing," says Adam Tanner, author of *Our Bodies, Our Data*, an exposé on the medical data market.[43]

Retailers want to lure consumers who have specific needs, such as pregnancy products or diabetes support. Healthcare providers will pay for lists of potential patients, so that they can target advertising based on their specialties. Pharmaceutical companies have direct incentive to advertise to persons who suffer from illnesses that their products can treat—as well as their doctors. Attorneys engaged in class-action lawsuits might want to send a notification to persons with a specific ailment related to their case. Media providers may want to place targeted ads for films or shows that appeal to people with certain interests, as well as health-related data such as sexual orientation.

Today, health data is combined with consumer profile databases from big data brokers such as Acxiom to produce frighteningly comprehensive profiles on consumers. What's more, data analytics firms can use propensity modeling to predict a subject's ailments or health-related interests based on consumer profile data. Intimate consumer data is leveraged using digital advertising and analytics, which in turn are also used to augment and improve consumer profiling.

One former IMS Health executive, Bob Merold, casually described how consumer medical data is used to target online advertising: "Companies like IMS are selling 'Here [are] four million patients with erectile dysfunction and here [are] their profiles,' and then Google puts it into their algorithms so that the Viagra ads show up when you are searching fishing or whatever the heck the things are that correlate."[44]

---

42. Rutenberg, "Gossip Machine."

43. Adam Tanner, *Our Bodies, Our Data: How Companies Make Billions Selling Our Medical Records* (Boston: Beacon Press, 2017), 130.

44. Tanner, *Our Bodies, Our Data*, 135–36.

2.3.3 Big Data Analytics

Big data analytics is a burgeoning industry. Organizations within the healthcare ecosystem have an incentive to leverage data from all facets of patients' lives, in order to more efficiently and effectively diagnose and serve patients, and make money. Big data analytics has created enormous advances in clinical operations, medical research and development, treatment cost predictions, and public health management, to name a few areas.

"McKinsey estimates that big data analytics can enable more than $300 billion in savings per year in U.S. healthcare, two thirds of that through reductions of approximately 8% in national healthcare expenditures. Clinical operations and R & D are two of the largest areas for potential savings with $165 billion and $108 billion in waste respectively."[45]

Many other types of organizations can likewise gain advantages by leveraging health data and derived products, including advertising firms, entertainment vendors, and retailers. This expanding marketplace has increased the value of personal health data and created new incentives for selling, trading, processing, and hoarding it. As technology advances and data mining becomes increasingly sophisticated, raw data is much like crude oil: unrefined and full of potential.

Health data analytics relies on stores of personal health data, such as:

- Prescription records
- Lab test results
- Sensor data, such as heart rate, blood pressure, insulin levels
- Doctor's notes
- Medical images (X rays, CAT scans, MRIs, etc.)
- Insurance information
- Billing details

In addition, personal health data can be augmented with other types of personal information, such as:

- Social media activity
- Web search queries
- Shopping history
- Credit card transactions
- GPS location history
- Demographic records
- Interests and characteristics derived from other sources

45. Wullianallur Raghupathi and Viju Raghupathi, "Big Data Analytics in Healthcare: Promise and Potential," *Health Information Science and Systems* 2, no. 1 (2014): article 3, doi: 10.1186/2047-2501-2-3.

"You may soon get a call from your doctor if you've let your gym membership lapse, made a habit of picking up candy bars at the check-out counter or begin shopping at plus-sized stores," reported Bloomberg News in 2014.[46] At the time, Carolinas HealthCare System had just purchased consumer data on 2 million people, including shopping histories and credit card transactions.

Carolinas HealthCare used the data to assign a risk score to patients and ultimately planned to regularly share patient risk scores with doctors and nurses, so they could proactively reach out to high-risk patients.[47] The Affordable Care Act increasingly tied healthcare reimbursements to quality metrics and clinical outcomes, giving hospitals increased incentive to invest in big data analytics that could help them to reduce readmission rates and improve overall patient health.

Of course, injecting new kinds of consumer data into the healthcare ecosystem increases the amount of sensitive data and therefore the risk of a potential data breach.

2.3.4 Data Analytics Firms

Big data analytics is increasingly conducted by specialized data analytics firms, which collect data from a variety of sources and produce derivative data products to be purchased or leveraged by clients. Processing data on a large scale requires a proportional investment in hardware and software for processing, as well as raw collections of data assets to be used for training and development purposes. Analytics firms typically have a complex web of relationships including data sources, customers, data brokers, and other analytics firms. Personal data flows through this web, often winding up in unexpected places.

Truven Health System is a medical data analytics firm. According to the company's quarterly SEC report, in 2013 Truven held approximately 3 PB of data, which included "20 billion data records on nearly 200 million de-identified patient lives."[48] Where did Truven's patient lives come from? Originally started as MedStat Systems, the company collected and analyzed insurance claims from large enterprises, including General Electric, Federal Express, and others.[49] It offered clients free analytics products in exchange for the right to resell their anonymized data. In 1994, the company was sold to Thomson, which later merged with Reuters.

Adam Tanner, the author of *Our Bodies, Our Data*, was a journalist working for Thomson-Reuters in 2007, when the companies merged. "We journalists felt complete surprise when we learned our new combined company now had an insurance database with tens of millions of patient histories," Tanner reflected.[50]

---

46. Shannon Pettypiece and Jordan Robertson, "Hospitals Soon See Donuts-to-Cigarette Charges for Health," *Bloomberg*, June 26, 2014, https://www.bloomberg.com/news/articles/2014-06-26/hospitals-soon-see-donuts-to-cigarette-charges-for-health.

47. Shannon Pettypiece and Jordan Robertson, "Hospitals, Including Carolinas HealthCare, Using Consumer Purchase Data for Information on Patient Health," *Charlotte Observer*, June 27, 2014, http://www.charlotteobserver.com/living/health-family/article9135980.html.

48. U.S. Securities and Exchange Commission (SEC), "Truven Holding Corp./Truven Health Analytics, Inc.," Form 10-K, 2013, https://www.sec.gov/Archives/edgar/data/1571116/000144530514001222/truvenhealthq410-k2013.htm.

49. Tanner, *Our Bodies, Our Data*, 69.

50. Tanner, *Our Bodies, Our Data*, 69.

Explorys was another health data analytics firm that emerged as a leader in the mid-2000s. A spinoff of the Cleveland Clinic, Explorys amassed a database containing 50 million patient lives, collected from 360 hospitals.[51]

Today, tech companies such as IBM purchase patient "lives" in bulk, to fuel the next generation of artificial-intelligence-driven medical diagnostic tools. In 2015, IBM launched IBM Watson Health, a cloud-based health analytics platform driven by the Watson artificial intelligence system. Subsequently, IBM invested heavily in building its collection of health data. By April 2016, it had acquired four health data companies, including Explorys (for an undisclosed sum) and Truven ($2.6 billion and 215 million patient lives).

All told, by the end of 2016 IBM Watson had amassed more than 300 million patient lives. The company touted its "HIPAA-enabled" cloud, enticing more healthcare providers to upload their data to the system and partner with the tech giant. IBM also strategically partnered with Apple, releasing a ResearchKit for developers that enabled health apps on the AppleWatch or iPhone to store and analyze personal health data using the Watson Health cloud as the back end. The first app, SleepHealth, was released in 2016.[52]

Big data analytics holds enormous potential. Like any powerful tool, it can be harnessed for the benefit of society or cause great damage if not carefully controlled. The newly emerging industry has incentivized retention, fueled proliferation, expanded access, increased data liquidity, and increased value of personal health data—all five factors that increase the risk of data breaches.

2.3.5 Data Brokers

Data brokers, according to the Federal Trade Commission (FTC), are "companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud."[53]

Data brokers are a key part of the data supply chain, which incentivizes and perpetuates data breaches simply as a natural result of its existence. For example, data such as a purchase history may be generated by consumers shopping in a store; collected by the retailer; sold to a data broker, who in turn analyzes it and categorizes the user as, say, an expectant mother. That data broker sells it to a larger data broker, which merges it with credit reports to generate a list of low-income expectant mothers. This list, in turn, is purchased by a marketing firm, who uses it to advertise on behalf of a diaper manufacturer.

To support their business model, data brokers amass a vast and varied trove of consumer data, including purchase histories, health issues, web browsing activity, financial details,

51. Rajiv Leventhal, "Explorys CMO: IBM Deal Will Fuel New Predictive Power," *Healthcare Informatics*, April 15, 2015, https://www.healthcare-informatics.com/article/explorys-cmio-ibm-deal-will-fuel-new-predictive-power.

52. Laura Lorenzetti, "IBM Debuts Apple ResearchKit Study on Watson Health Cloud," *Fortune*, March 2, 2016, http://fortune.com/2016/03/02/ibm-watson-apple-researchkit.

53. Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* (Washington, DC: FTC, 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

employment records, daily habits, ethnicity, and more. The FTC conducted a study of nine data brokers in 2014 and found that "[d]ata brokers collect and store a vast amount of data on almost every U.S. household and commercial transaction. . . . [O]ne data broker's database has information on 1.4 billion consumer transactions and over 700 billion aggregated data elements; another data broker's database covers one trillion dollars in consumer transactions; and yet another data broker adds three billion new records each month to its databases."[54]

This data is analyzed and distilled to create data products, such as those designed to facilitate decision making (background checks, credit scores), marketing, and more. Brokers therefore maintain not only stores of raw data collected from many sources; they also maintain neatly packaged data products that include inferences derived using data analytics. These products are valuable for a variety of reasons. "[W]hile data brokers have a data category for 'Diabetes Interest' that a manufacturer of sugar-free products could use to offer product discounts, an insurance company could use that same category to classify a consumer as higher risk." [55]

No one knows exactly how many data brokers exist. Pam Dixon, executive director of the World Privacy Forum, estimated in 2013 that it included between 3,500 to 4,000 companies.[56] The data-driven marketing economy (DDME) (which includes the subset of data brokers that help businesses select and market to consumers) was valued at $202 billion in 2015.[57]

By purchasing, selling, and sharing information, data brokers increase the number of copies of data, as well as the number of people who have access to a given piece of information. Data brokers distill huge, complex data sets into concise, highly liquid snippets of structured data, designed for easy transfer to other organizations. Many retain data "indefinitely" to facilitate future analysis or for the purposes of identity verification.[58] And of course, the data broker's goal is to maintain and increase the value of the data it holds, since of course data is its product.

In short, data brokers, like other key players in the nascent data economy, inherently increase all five of the data breach risk factors.

Data Decay

There is a time value of data, which is often discussed in the context of big data analytics or sales data. Over time, most types of information lose value. For example, databases of contact information gradually lose value as people change jobs, move home addresses, or pass away.

(*Continues*)

54. Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (Washington, DC: FTC, 2014), iv, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

55. FTC, *Data Brokers*, vi.

56. U.S. Senate, *What Information Do Data Brokers Have on Consumers, and How Do They Use It?* (Washington, DC: GPO, 2013), 75, https://www.gpo.gov/fdsys/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf.

57. John Deighton and Peter A. Johnson, "The Value of Data: 2015," Data and Marketing Association, December 2015, https://thedma.org/wp-content/uploads/Value-of-Data-Summary.pdf.

58. FTC, *Data Brokers*, vi.

(*Continued*)

Credit card numbers expire after so many years or change due to lost wallets and fraud. Medical records are useful to data analytics companies such as IBM that seek to use artificial intelligence to better predict treatment, but these, too, become outdated as treatment options evolve over time.

In security, data decay can be a *good* thing. A stolen trove of intellectual property data dated from 1970 may be worthless today. Many organizations horde records for 20, 30, or 40 years (or more), simply because they have no clear mandate to destroy the data. Given the emergence of data breach laws and liability, this can result in an enormous accumulation of risk. Fortunately, the natural decay in the value of data can help to offset some of this risk.

One of the reasons that SSN theft remains such a big problem is because SSNs retain their value—both to consumers and to criminals. Since SSNs are rarely changed, they remain useful for many years.

When preparing for a data breach, it is important for organizations to accurately assess the type and volume of data stores. Consider, also, the rate of data decay for the various types of information that your organization stores. Data that retains value to criminals represents a greater risk, and yet may not be needed for your business operations after a certain period of time. Compare the rate of data decay with the usefulness to your organization over time in order to prioritize data disposal efforts.

2.4 Anonymization and Renonymization

It is common practice for organizations to "anonymize" data sets, removing explicit identifiers such as names and SSNs, and often replacing them with individual identifiers such as numeric codes. This is also known as de-identification. The goal is to reduce the risk associated with data exposure, while retaining valuable data that can been mined. By removing identifying characteristics, data custodians theorize, individuals cannot be harmed by data exposure. Regulations such as HIPAA and other laws take anonymization into account; typically security and breach notification requirements do not apply to anonymized data.

Often, data custodians assume that if a data set is "anonymized," it is safe to share and publish without risk of harm. Unfortunately, this is not the case. Anonymization is often reversible. To the naked eye, an anonymized data set might seem impossible to map back to the individual named subjects, but in many cases, such a task can be rendered trivial. How? Even anonymized data contains information that can be unique to an individual, such as the timing of hospital visits, specific combinations of "lifestyle interests," and personal characteristics. By mapping these unique details to other data sources, such as a voter registration list, purchase histories, marketing lists, or other data sets, it is possible to link databases and ultimately identify individuals.

This means that even anonymized data carries a risk of causing a breach. To demonstrate this, in 1997 Harvard University researcher Latanya Sweeney famously identified Governor

William Weld's hospital records in a de-identified database released by the Massachussetts Group Insurance Commission (GIC). As described by law professor Paul Ohm:[59]

> At the time GIC released the data, William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In response, then-graduate student Sweeney started hunting for the Governor's hospital records in the GIC data. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code. In a theatrical flourish, Dr. Sweeney sent the Governor's health records (which included diagnoses and prescriptions) to his office.

Some methods of anonymization leave more residual risk than others. The risk depends on precisely what information remains in the data set after anonymization. Data custodians must decide which details to remove and which to leave in the data set. If too much information remains and the data set is exposed, then it can cause a breach (at least, as defined by the public, if not the law).

2.4.1 Anonymization Gone Wrong

Netflix discovered the hard way that ineffective anonymization can lead to data exposure, public relations crises, and lawsuits. In 2011, as a publicity stunt, the company ran a contest to see who could create the best algorithm for predicting user film ratings, based on each user's previous film ratings. In support of this, Netflix released an "anonymized" data set containing 100 million movie ratings from more than 480,000 subscribers. Each entry in the data set included a numeric identifier unique to each subscriber, details of each movie rated, the date it was rated, and the subscriber's rating.

Researchers Arvind Narayanan and Vitaly Shmatikov weren't as interested in film predictions as they were in privacy. They analyzed the Netflix data set and found that they could re-identify users by comparing the entries to a small sample of publicly available information from the website IMDB. As a proof-of-concept, the researchers re-identified two Netflix subscribers, by cross-correlating the movie review data with public IMDB movie ratings posted on the web. Due to IMDB's terms of service, the researchers used only a small subset of the available public reviews. Based only on the dates and content of the movie reviews, the researchers were able to link two IMDB reviewers who also appeared in the Netflix data set and identified them based on their IMDB profiles.

"Jane Doe," who watched movies in Netflix's "Gay and Lesbian" categories, was among those whose movie-rating history was made public in the Netflix Prize dataset. She initiated

59. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57 (2010): 1701, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (accessed January 18, 2018).

a class-action lawsuit against Netflix, claiming that if her sexual orientation were to become known, "it would negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children's' ability to live peaceful lives within Plaintiff Doe's community."[60] As a provider of audiovisual recordings, Netflix was regulated under the Video Privacy Protection Act of 1988, which was established after U.S. Supreme Court nominee Robert Bork's video rental history was leaked to the press.

In court documents, the plaintiffs described what they called "The Brokeback Mountain Factor": essentially, the concept that a person's movie-watching history can reveal far more than just a person's entertainment preferences. "A Netflix member's movie data may reveal that member's private information such as sexuality, religious beliefs, or political affiliations. Such data may also reveal a member's personal struggles with issues such as domestic violence, adultery, alcoholism, or substance abuse"[61] Netflix, under pressure from the FTC and the public, ultimately settled the lawsuit and canceled the Netflix Prize contest.[62]

Renonymization

"Renonymization" isn't in the dictionary (yet), but it was defined in 2009 by commentator David S. Isenberg as follows:[63]

> To discover, using data from an "anonymized" data set (a data set from which the explicit identifying data has been removed) which specific individuals generated the data.

Renonymization is typically conducted by combining deanonymized data sets with other data sources, such as voter registration lists, hospitalization records, shopping history, and more.

2.4.2 Big Data Killed Anonymity

Data brokers, which store billions of pieces of data on millions of consumers, have access to big databases that can easily facilitate renonymization and linking of disparate data sets. In fact, data brokers frequently link data sets procured from different sources and offer products designed to connect online consumers with their offline activities. Data brokers may purchase

60. Jane Doe v. Netflix, Inc., 2009, San Jose Division, CA, https://www.wired.com/images_blogs/threatlevel/2009/12/doe-v-netflix.pdf.

61. Jane Doe v. Netflix.

62. Steve Lohr, "Netflix Cancels Contest after Concerns are Raised about Privacy," *New York Times*, March 12, 2010, http://www.nytimes.com/2010/03/13/technology/13netflix.html.

63. David S. Isenberg, "Word of the Day: renonymize," *isen.blog*, May 28, 2009, http://isen.com/blog/2009/05/word-of-the-day-renonymize/.

anonymized data sets from different sources and use automated tools to connect the dots if it suits their business needs.

The National Security Agency (NSA)—one of the world's largest data aggregators—was able to identify pseudonymous Bitcoin creator Satoshi Nakamoto using stylometry, combined with access to an enormous database of writing samples.

"By taking Satoshi's texts and finding the 50 most common words, the NSA was able to break down his text into 5,000 word chunks and analyse each to find the frequency of those 50 words," explained entrepreneur Alexander Muse. The NSA then compared the "fingerprint" of Satoshi's writing style with intelligence databases containing trillions of writing samples, including the PRISM and MUSCULAR programs. "[T]he NSA was able to place trillions of writings from more than a billion people in the same plane as Satoshi's writings to find his true identity. The effort took less than a month and resulted in positive match."[64]

In short, the bigger the data broker, the easier it is to pick you out of a supposedly "anonymized" data set.

2.5 Follow the Data

Driven by the huge potential for efficiency gains and profit, organizations of all kinds have amassed computerized data at a tremendous pace. Handwritten records have been entered into databases; file cabinets have been scanned and ultimately emptied in the shift to electronic records. Freed of physical constraints, organizations had the capacity to store more data. What's more, they could analyze more data, too, now that data retrieval times were measured in milliseconds rather than minutes. Data became more *liquid*—easier to transfer—due to digitization and the emergence of structured data formats. This made it easier to share and trade, leading to even greater proliferation and the emergence of data markets.

In this section, we will trace the flow of data through an example supply chain, in order to better understand how the risk of data breaches has expanded over the years. We will focus on personal health data for this illustration, since it is a good example that shows the complex data processing relationships within the modern economy.

2.5.1 Pharmacies: A Case Study

In the late 1970s and early 1980s, pharmacies all over the United States began to install computer systems. Voluminous file cabinets containing personal information, insurance details, and prescriptions were digitized. This enabled pharmacists to process orders much faster, detect errors, save time on billing (which was highly complex due to insurance reimbursements), and identify fraud. Customers enjoyed added perks such as the ability to fill prescriptions at multiple locations in a chain—a strong competitive advantage.

64. Alexander Muse, "How the NSA Identified Satoshi Nakamoto," *Medium*, August 26, 2017, https://medium.com/cryptomuse/how-the-nsa-caught-satoshi-nakamoto-868affcef595.

Soon, pharmacists discovered that they could leverage their computerized databases to make extra money. For example, Thomas Menighan, owner of the Medicine Shoppe in West Virginia, installed a computer system in 1978. He was quickly approached by a company called IMS Health, which "offered to pay him fifty dollars a month to copy his prescription files onto an eight-inch floppy disk and send it in by mail."[65] Excited about the revenue, Menighan copied his pharmacy's database to the disk, mailed it in, and received $50. "I thought I was making out like a bandit!" the pharmacist exclaimed.

Patients might have agreed. Very few realized that their prescription data was shared outside the pharmacy, and fewer still knew that it was used to help pharmaceutical companies target doctors in sophisticated data-driven marketing and sales programs.

IMS Health, founded in 1954, was an early data broker. It provided market intelligence information to pharmaceutical companies and other organizations. By collecting detailed prescription and sales records from pharmacies, the company could provide drug manufacturers with reports about what products were actually moving off pharmacies' shelves.[66]

"Look, you are creating data as a by-product. It's an exhaust from your system," said IMS executive Roger Korman, describing how the company convinced sources to share their data. "Why don't you take that thing and turn it into an asset and sell it?"[67]

IMS reports included medication and amounts dispensed, as well as the patient's age and other characteristics. Individual names were typically (though not always) removed before the data was sent to IMS. Importantly, the prescribing *doctor's* name was included. This "doctor-identified data" enabled IMS Health to sell detailed reports of doctors' prescription histories to drug manufacturers, who then targeted individual doctors in sophisticated sales and marketing programs. Doctors were the gatekeepers to the market, drug manufacturers recognized. "Research has shown that winning just one more prescription per week from each prescriber, yields an annual gain of $52 million in sales," advertised IMS. "So, if you're not targeting with the utmost precision, you could be throwing away a fortune."[68]

Drug manufacturers flocked to purchase IMS reports. Today, a large pharmaceutical company might pay $10 to $40 million per year for IMS products and services, according to Adam Tanner. "Drug companies have to have them," he writes, "whatever the cost—and the price is certainly high."[69]

Pharmacy chains, in turn, now routinely plan for revenue from the sale of their databases. "Pretty much everyone who is in the business has some sort of supply arrangement for de-identified prescription data," said CVS Health executive Peter Lofberg. "CVS Caremark is one of the providers of data into that marketplace. On the retail side of the business, they also have pretty extensive data collection ranging from loyalty cards and that sort of thing to track people's shopping patterns. Also on the retail pharmacy side, like most retailers, they will sell certain types of data to market research companies and so on."[70] According to Tanner, today's

65. Tanner, *Our Bodies, Our Data*, 14.

66. Tanner, *Our Bodies, Our Data*, 14.

67. Tanner, *Our Bodies, Our Data*, 71.

68. Tanner, *Our Bodies, Our Data*, 43.

69. Tanner, *Our Bodies, Our Data*, 48–49.

70. Tanner, *Our Bodies, Our Data*, 16.

pharmacies can generate about one cent for each prescription, which can add up to millions of dollars for large chains.[71]

2.5.2 Data Skimming

As organizations began to leverage third-party software providers, software vendors suddenly realized the value of the data that they could access—and decided that they, too, could profit from it. The result was that sensitive data that once resided within an organization was collected and mined by third-party providers, which leveraged it and sold data products to even more organizations. Data proliferated and spread, increasing risk of a breach for all parties in the data supply chain.

"W[e] are getting tons of data in real time!" thought Fritz Krieger, who was hired in 1998 to manage data sales on behalf of a company called Cardinal Health. Cardinal Health was a drug wholesaler that also offered a service called ScriptLINE, which helped pharmacists maximize and manage their insurance reimbursements. That meant it had instant access to each transaction as it was processed. Cardinal teamed up with CVS, Wal-Mart, Kmart, and Albertson's to create an online product called "R(x)ealTime," which provided real-time sales data to subscribers.[72]

Cardinal Health was just one of many software providers that profited from the data that flowed through their products. "As more insurance plans covered prescription drugs, a layer of data processors called clearinghouses, or switches, emerged," explains Tanner. "Those companies route claims from the pharmacy or doctor's office to those paying the bills such as the insurance company or . . . Medicare. Entrepreneurs running switches and pharmacy software programs learned that they could make extra cash by selling their expertise to the secondary market."[73] Often, pharmacists themselves did not even know who was selling "their" data.

As the realization dawned that software providers were "skimming" data from electronic transactions, pharmacists pushed back. In 1994, two Illinois pharmacies sued a small software company, Mayberry Systems, alleging that the software provider sold their prescription data without authorization ("misappropriation of trade secrets"). The lawsuit was later expanded to include IMS Health, a purchaser of the data, and certified as a class action to include all 350 pharmacies that were Mayberry customers. Later, in 2003, two pharmacies sued IMS Health and 60 software providers that they purchased data from, alleging that they "misappropriated the trade secrets (i.e., prescription data) of thousands of pharmacies in the United States and used this information either without authorization or outside the scope of any authorization." IMS settled both lawsuits in 2004 for approximately $10.6 million, and continued its work.[74]

The maturation of AllScripts took medical data skimming to a whole new level. Developed as a service for doctors to electronically send prescriptions to pharmacies, AllScripts expanded

71. Tanner, *Our Bodies, Our Data*, 16.

72. Biz Journals.com, "Cardinal Health, Others Form Prescription-Data Analysis Firm," *Columbus Business First*, July 30, 2001, https://www.bizjournals.com/columbus/stories/2001/07/30/daily2.html.

73. Tanner, *Our Bodies, Our Data*, 17.

74. U.S. Securities and Exchange Commission (SEC), "IMS Health Incorporated 2004 Annual Report to Shareholders," Exhibit 13, https://www.sec.gov/Archives/edgar/data/1058083/000104746905006554/a2153610zex-13.htm (accessed May 12, 2019).

to include electronic medical records, thereby gaining access to in-depth patient records from nearly one in three doctors' offices and half of all hospitals in the United States.[75] There was profit to be made from harvesting, mining, and selling patient data. In 2000, IMS invested $10 million in AllScripts. Glen Tullman, former CEO of AllScripts, said, "Today, if you look at AllScripts, the data business is the only thing that is driving the growth of bottom-line earnings there. That's a key jewel in the world today, and that's data coming from electronic health records."[76]

Practice Fusion, a web-based electronic health records (EHR) system, now offers its software free to healthcare providers. The company generates revenue by selling ads and sharing data with third parties. "[Practice Fusion] crunches 100 million patient records it has stored remotely in an online database to alert providers when treatments or tests might be needed," reported the *Wall Street Journal* in 2015. "Some of those messages are sponsored, letting marketers deliver the ultimate nudge: a subtle pitch to the right doctor, about the right patient, at the right moment."[77]

Even the biggest EHR players are getting in on the action: Cerner, the market leader in the $28 billion electronic medical record system market, sells access to its patient database. According to Senior Vice President David McCallie Jr., Cerner provides access using "data enclaves," which allow customers to remotely analyze the data without downloading the full database.[78] Cerner's website advertises, "Our strategic analytics solutions offer the ability to discover new insights by providing pre-built content and [a] variety of analytic visualization tools."[79]

The emergence of "data skimming" created a whole new market for medical data. At the same time, it dramatically increased the risk of data breaches. Sensitive data proliferated and spread to many more organizations. Those that already had sensitive data discovered that they could monetize it in new ways, which gave them incentives to collect even more.

2.5.3 Service Providers

Service providers, likewise, discovered that when they received data in order to provide a service, they could often reuse that data for wholly different purposes in order to make a profit. This fuels data proliferation, creates incentive for giving more people access to sensitive data, and increases the value of the raw data used to create data products.

Laboratories are a prime example. When a patient's test results are ready, the lab can share the outcome not just with the doctor, but also with customers that pay to receive reports of results. The patient's identifying information is typically removed in accordance with HIPAA, but doctor-identified data remains. That means drug companies know which doctors have patients with relevant diagnoses. Sales reps can immediately reach out to the doctor to convince

75. Tanner, *Our Bodies, Our Data*, 72.

76. Tanner, *Our Bodies, Our Data*, 72.

77. Elizabeth Dwoskin, "The Next Marketing Frontier: Your Medical Records," *Wall Street Journal*, March 3, 2015, https://www.wsj.com/articles/the-next-marketing-frontier-your-medical-records-1425408631.

78. Tanner, *Our Bodies, Our Data*, 142.

79. Cerner, *Analytics: Uncover the Value of Your Data*, https://www.cerner.com/solutions/population-health-management/analytics (accessed January 8, 2018).

him or her that their drug is the right treatment option, even before the doctor has a chance to see the patient again.

Prognos is a leading broker for laboratory records, boasting that its registry contains more than "11 billion clinical diagnostics records for 175 million patients across 35 disease areas." Where does the data come from? Quest Diagnostics, LabCorp, Cigna, and Biogen have all been publicly named as "collaborators." The company's main product, Prognos DxCloud, "ingests all payer lab data, including connecting and extracting from new lab sources to achieve expanded lab data coverage. . . . The result is actionable member health insights available to payers through robust, secure data connectivity access and web services ensuring delivery of lab data to the right person at the right time."[80] Prognos DxCloud is used for insurance risk assessment and cost analyses, treatment decision making, research, and more.

2.5.4 Insurance

Insurers, too, are in on the action. Blue Health Intelligence, a spin-off of Blue Cross Blue Shield, advertises that it is "[t]he nation's largest health information analytics data warehouse," based on "over 10 years of claims experience from over 172 million unique members nationwide." Other insurers, including Anthem and UnitedHealth, offer similar services.

In 2012, IMS excitedly announced that in collaboration with Blue Health Intelligence, it was releasing a product called PharMetrics Plus. The database contains "fully adjudicated pharmacy, hospital and medical claims at the anonymized patient level, sourced from commercial payers covering over 100 million enrollees from 2007 to present."[81] According to the product advertisement, the data includes:

- Diagnoses
- Procedures
- Diagnostic & lab tests ordered (no lab values)
- Enrollment
- Adverse events
- Hospitalizations
- Office visits
- ER visits
- Home care
- Cost & data of treatment
- On/off formulary status
- Co pays/deductibles
- Complete medical and pharmacy costs

IMS additionally advertises that "data from disparate sources can be linked upon request (e.g., from Electronic Medical Record, Registries, Laboratory data) to provide additional clinical detail]."[82] Potential purchasers might include drug companies, marketing firms, researchers, healthcare facilities, and other analytics companies.

---

80. Marketwired, "New AI Cloud Platform by Prognos Transforms Member Lab Data to Address Business Challenges for Payers," press release, May 10, 2017, http://markets.businessinsider.com/news/stocks/New-AI-Cloud-Platform-by-Prognos-Transforms-Member-Lab-Data-to-Address-Business-Challenges-for-Payers-1002000305.

81. B.R.I.D.G.E. To_Data, *QuintilesIMS Real-World Data Adjudicated Claims: USA [QuintilesIMS PharMetrics Plus]*, https://www.bridgetodata.org/node/824 (accessed January 8, 2018).

82. B.R.I.D.G.E To_Data, *QuintilesIMS*.

Bill Saunders, executive at Kaiser Permanante, explained that insurance companies routinely share de-identified claims data with analytics companies, for direct profit or trade of services. "The Blues plans are the largest supplier of claims data. . . . There are a lot of small insurance companies that supply data to them as well so that they can get free analytical services in exchange for their claims data."[83] Analytics companies such as Milliman, Ingenix, and others process data on behalf of insurers and provide them with risk scores based on factors such as age and gender, utilization benchmarks, service cost projections, and more. According to Saunders, Kaiser does not provide claims information to data brokers.

Insurers also provide fully identifiable claims information to employers and groups. Employers running self-funded groups typically hire the insurance company to administer claims. In this case, since the employer owns the claims data, the insurer must provide it with fully identified claims records. That means employers with self-funded insurance policies have access to employee prescription records, medical procedures, and more. All too often, enterprise security professionals in these organizations are unaware that such granular health data exists on their network, until a breach occurs.

The U.S. government group also demands detailed claims information, and Saunders said, "we are not de-identifying the data at their mandate." Saunders also said that insurers are required to provide detailed, identified claims information to state programs. "Hopefully they have good security systems to manage it and keep it confidential."

Of course, insurers aren't the only source of claims data. "The same claim form actually exists in at least three locations," said Zach Henderson, senior vice president of Health Care Markets. "[They exist] in the system that created the claim (the provider), the clearinghouse that moved the claim and the entity that paid the claim (payer or PBM)."[84] Any or all of these entities can mine the data and share the results with others, further increasing the risk of data exposure.

2.5.5 State Government

State governments collect extensive details regarding prescription and hospitalization records, and they often sell or share this data with corporations or researchers. Security professionals who work in these environments (or those who have access to the data) should be aware of the extent of the data collected, as well as the limitations of de-identification techniques.

According to Harvard University researchers Sean Hooley and Latanya Sweeney, "[t]hirty-three states release hospital discharge data in some form, with varying levels of demographic information and hospital stay details such as hospital name, admission and discharge dates, diagnoses, doctors who attended to the patient, payer, and cost of the stay." State governments are exempt from HIPAA regulations, and each state is free to decide what level of de-identification is sufficient.[85]

In Washington State, hospitals are required to share hospitalization details with the state, including "age, sex, zip code and billed charges of patients, as well as the codes for their

83. Personal conversation between the author and Bill Saunders, June 2017.

84. Tanner, *Our Bodies, Our Data*, 179.

85. Sean Hooley and Latanya Sweeney, "Survey of Publicly Available State Health Databases" (whitepaper 1075-1, Data Privacy Lab, Harvard University, Cambridge, MA, June 2013), https://thedatamap.org/1075-1.pdf.

diagnoses and procedures." Washington State now has a database of hospitalization records from 1987 to the present, which it makes available to the public.[86]

In 2013, Sweeney purchased the Washington State hospitalization database for $50 and attempted to match medical records to news reports. She found that 43% of the time, "[n]ews information uniquely and exactly matched medical records in the State database," enabling her to quickly and easily re-identify the records. "Employers, financial organizations and others know the same kind of information as reported in news stories," Sweeney concluded, "making it just as easy for them to identify the medical records of employees, debtors, and others."[87]

Commercial data brokers and analytics firms IMS Health, Milliman, Ingenix, WebMD Health, and Truven Health Analytics are among the top purchasers of state hospital discharge data, according to a 2013 *Bloomberg* report.[88] In this roundabout manner, sensitive medical information can enter the data supply chain, where it can then be combined with other data sources (such as purchase records, web surfing activity, and more) to create shockingly detailed records of individual lives. Exposure of this data is often not considered a breach under state or federal law, depending on the precise details, contractual obligations, and specific jurisdictions.

2.5.6 Cost/Benefit Analysis

Data has become a precious resource, as well as a valuable commodity. The expansion of computing power and digital storage space has led organizations to integrate sensitive data into everyday business processes, in order to increase efficiency and productivity. The development of data analytics tools has sparked the rise of the data brokerage industry and created strong, direct financial incentives for collecting and sharing data. This has resulted in a global increase in the volume of sensitive data that organizations collect, store, process, and transmit.

At the same time, regulations have lagged. As we will see in the following chapters, data breach laws and standards are typically applied to organizations that most visibly collect sensitive data (such as healthcare clinics and merchants that collect payment card data), while less-visible organizations that exchange data (such as analytics firms and data brokers) are largely unregulated. What's more, the information protected by existing data breach laws and standards is very limited compared with the wide spectrum of sensitive data that is currently bought, sold, and leveraged.

Historically, relatively few organizations have been held accountable for their data spills. All too often, the costs of a data breach are borne by the data subjects themselves or society as a whole. This is slowly changing, however, as the public becomes savvier, regulations evolve, and the media digs deeper to follow the trail of sensitive data.

As more organizations bear the cost of their data spills, the cost/benefit ratios of storing data change, and reducing the risk of a data breach becomes more important.

---

86. Washington State Department of Health, *Comprehensive Hospital Abstract Reporting System (CHARS)*, https://www.doh.wa.gov/DataandStatisticalReports/HealthcareinWashington/HospitalandPatientData/HospitalDischargeDataCHARS (accessed January 9, 2018).

87. Latanya Sweeney, "Matching Known Patients to Health Records in Washington State Data" (Data Privacy Lab, Harvard University, Cambridge, MA, June 2013), https://dataprivacylab.org/projects/wa/1089-1.pdf.

88. "Who's Buying Your Medical Records?," Bloomberg, https://www.bloomberg.com/graphics/infographics/whos-buying-your-medical-records.html (accessed January 9, 2018).

2.6 Reducing Risk

As with any kind of hazardous material, the quickest and cheapest way for an organization to reduce the risk of a data breach is to minimize the volume of data stored. This requires a fundamental shift in the approach to data collection and transfer for most modern organizations, which have spent the last few decades stockpiling as much data as feasible and then storing it in loosely controlled locations. Any sensitive data that an organization does choose to retain needs to be carefully tracked, stored in a controlled manner, and properly disposed of when it is no longer needed.

2.6.1 Track Your Data

The first step to reducing and then securing sensitive data is to identify what you have and keep track of it. To accomplish this, you must establish a data classification program, take an inventory, and create a data map. Along the way, pay close attention to the places that data can escape from your control.

2.6.1.1 Data Classification

A data classification scheme is the foundation of every strong cybersecurity and breach response program. Typically it is advisable to classify data into three to five categories. Table 2-1 shows a sample data classification scheme with four categories: Public, Internal, Confidential, and Private (which, in this case, includes personally identifiable information and patient health information).

2.6.1.2 Inventory Your Data

Next, take the time to create a detailed inventory of your organization's sensitive information. Depending on the kinds of data that your organization holds, you may wish to be more or less granular. Small organizations with limited sensitive information may be able to reasonably maintain this inventory in a spreadsheet; organizations with more complex needs should consider leveraging enterprise data management software.

How much data do you have? For each type of sensitive information, estimate the volume of data. Certain types of information, such as SSNs, payment card data, or driver's license numbers can be measured in *number of records*. Other data, such as customer accounts or medical files, can be measured by *number of individuals*. For more complex data sets, such as legal files, it may be most useful to measure simply by *volume of data* (i.e., terabytes). Finally, data such as intellectual property (i.e., Coca-Cola's secret recipe) may be most effectively measured by *value*, in dollars or other measure of currency.

Most organizations tend to underestimate the amount of sensitive data that they store. When I conduct an initial interview for a cyber insurance policy review, I normally ask how many records my client maintains. The client will typically say something like, "Well, we have 40,000 customers, so about 40,000 people's records." Then I ask, "How long do you retain customer information?" More often than not, the answer is "forever," or the client is unsure. Suddenly, 40,000 records balloon into hundreds of thousands because the organization has actually retained data of all previous customers over 20 to 30 years.

Table 2-1 Sample Data Classification Scheme

Type	Definition	Examples
Public	Data that anyone may access.	Press announcements Website home page Marketing materials
Internal	Data that may be accessed by anyone internal to the organization. Public release would not cause significant harm to the organization or individuals.	Internal website General employee communications
Confidential	Access is restricted to authorized users. Disclosure could have serious adverse impact on the organization, a business partner, or the public through financial harm, reputational damage, or delay/failure of normal operations.	Proprietary or sensitive research Financial details Audit results Passwords
Private	Information that identifies and describes an individual, where unauthorized disclosure, modification, destruction, or use could cause breach of regulation or contract, and/or serious harm to the individual or organization.	SSNs Payment card data Driver's license numbers Medical information

2.6.1.3 Map the Flow

Once you have a comprehensive list of the types of sensitive information present in your organization, map the flow of information so you understand where it lives. You may find it helpful to create a *data flow diagram*, which is a visual representation of the flow of information.

Many data loss prevention (DLP) systems include automated discovery of sensitive data throughout your network and can produce reports or visual maps of the information flow. Certain cloud providers also offer built-in DLP and data inventory tools. For example, Office365 includes built-in data loss prevention capabilities, which enable you to "discover documents that contain sensitive data throughout your tenant."[89]

89. *Form a Query to Find Sensitive Data Stored on Sites*, Microsoft, https://support.office.com/en-us/article/Form-a-query-to-find-sensitive-data-stored-on-sites-3019fbc5-7f15-4972-8d0e-dc182dc7f836 (accessed January 19, 2018).

The Enterprise/Personal Interface

In my home state of Montana, we often talk about how to manage risks in the *wildland-urban interface*: the "zone of transition between unoccupied land and human development." People like to live near forests, grasslands, and other undeveloped areas, and yet also have the conveniences of society. Homes and structures built in these zones are at elevated risk of damage due to wildfire and other dangers, and should take special precautions to reduce the risk of a crisis.[90]

Similarly, the "enterprise/personal interface" poses special risks that should be consciously managed. What is the "enterprise/personal interface"? It is the *zone of transition between your enterprise technology and personal assets*. Do you allow employees to check email from their personal devices or work from home? If so, your data may flow onto personal devices and out of your control. Employees sometimes also try to forward enterprise data to their personal accounts, often so that they can bypass technical controls preventing them from working at home. This is a common risk that can lead to regulatory violations and data breaches.

While DLP systems can reduce this risk (if they are based on strong technology, carefully tuned and monitored), there is no panacea. Carefully define the "enterprise/personal interface" for your organization, and use administrative and technical controls to keep your data under control.

2.6.2 Minimize Your Data

Minimizing data is the quickest way to reduce your risk. Once you have a good handle on where data lives within your organization, you can then minimize it using one of three strategies: dispose of it, devalue it, or abstain from collecting it in the first place.

2.6.2.1 Disposal

Carefully weigh the risks and benefits for each type of data that you choose to retain, and consciously set limits. Regularly remove data from your systems when it is no longer needed. It's important to have a formal policy that defines your data retention period and removal process, so that everyone in your organization is on the same page. Organizations typically store data in a variety of formats (paper, CDs, bits and bytes on a server, tape), and the best practices for disposal vary depending on the format. Some methods are more secure than others. Create your process and then regularly audit and report to ensure that it is being followed.

2.6.2.2 Devalue

Often, you can reap the benefits of storing data and reduce the risk. One method is through "tokenization"—the process of replacing sensitive data fields with different, less sensitive values.

90. National Wildfire Coordinating Group, *Wildland Urban Interface Wildfire Mitigation Desk Reference Guide* (Boise: NWCG, May 2017), 4, https://www.nwcg.gov/sites/default/files/publications/pms051.pdf.

Using tokenization, you can remove information that is valuable to criminals on the dark web, but still retain the content that is useful for your purposes.

For example, until the early 2000s, many health insurance companies used the SSN as a policyholder's identifier, and it was printed on health insurance cards. Over time, insurers replaced SSNs with a completely different identifier that could not be exploited or used for fraud as easily.

2.6.2.3 Abstain

Carefully review your data collection processes. Do you need all the data you collect? Is the value of the data that you retain worth the risk? If not, don't collect it! By abstaining from data collection, you avoid the costs of security, as well as the risk of a breach.

2.7 Conclusion

Data has emerged as a powerful new resource, driving new markets and spurring efficiency and productivity. At the same time, it is hard to control and can easily leak out. Data breaches have increased in frequency, causing reputational and financial damage to organizations and consumers.

In this chapter, we have presented this important principle:

Data = Risk: Treat data as you would any hazardous material.

We also introduced the five factors that influence the risk of a data breach. These factors are:

1. **Retention:** The length of time that the data exists
2. **Proliferation:** The number of copies of data that exist
3. **Access:** The number of people who have access to the data, the number of ways that the data can be accessed, and the ease of obtaining access
4. **Liquidity:** The time required to access, transfer, and process the data
5. **Value:** The amount the data is worth

Finally, we discussed techniques for minimizing sensitive data in your environment, which will inherently reduce your risk of a data breach.

Chapter 3

Crisis Management

On September 7, 2017, Equifax, one of the "big three" consumer credit reporting agencies, announced a massive data breach affecting 143 million U.S. consumers—almost half the population of the entire United States. By the time the dust had settled, the company announced that 146.6 million U.S. consumers were impacted, as well as approximately 15 million U.K. citizens and 19,000 Canadians.[1]

According to Equifax's press release, "[T]he information accessed primarily includes names, Social Security numbers (SSNs), birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed."[2]

Nearly half of all SSNs had been exposed in one fell swoop. "This is about as bad as it gets," said Pamela Dixon, executive director of the World Privacy Forum. "If you have a credit report, chances are you may be in this breach. The chances are much better than 50 percent."[3]

Equifax had quietly spent six weeks investigating its breach and had the luxury of planning its own disclosure. In preparation for the public announcement, it had:

- Put together a polished press release.
- Retained cybersecurity attorneys from the firm King & Spalding LLP.
- Hired the forensics firm Mandiant to investigate.
- Reported the incident to the FBI.
- Set up a website, www.equifaxsecurity2017.com, which (in theory) allowed consumers to check whether they were affected and to register for the remedial package if so.
- Set up call centers to assist consumers. According to Chief Executive Officer Rick Smith, this involved hiring and training thousands of customer service representatives in less than two weeks.

1. Equifax, "Equifax Announces Cybersecurity Incident Involving Consumer Information," *Equifax Announcements*, September 7, 2017, https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information.

2. Equifax, "Equifax Announces Cybersecurity Incident."

3. T. Siegel Bernard, T. Hsu, N. Perlath, and R. Lieber, "Equifax Says Cyberattack May Have Affected 143 Million in the U.S.," *New York Times*, September 7, 2017, https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

- Developed a "robust package of remedial materials," which, according to Smith, included "(1) monitoring of consumer credit files across all three bureaus, (2) access to Equifax credit files, (3) the ability to lock the Equifax credit file, (4) an insurance policy to cover out-of-pocket costs associated with identity theft, and (5) dark web scans for consumers' social security numbers."[4]

It looked good on paper—but it all went terribly wrong.

Immediately following the breach notification, Equifax's stock prices took a nosedive. Shortly thereafter, the chief information officer (CIO) and chief security officer (CSO) resigned. Within a few weeks, CEO Rick Smith would resign as well (although he was later called to testify before Congress, where his statements fueled public outrage).

Within two months of the breach, Equifax was facing more than 240 consumer class-action lawsuits, as well as lawsuits filed by financial institutions and shareholders. The company reported in its quarterly SEC 10-Q filing that it was "cooperating with federal, state, city and foreign governmental agencies and officials investigating or otherwise seeking information and/or documents . . . including 50 state attorneys general offices, as well as the District of Columbia and Puerto Rico, the Federal Trade Commission (FTC), the Consumer Finance Protection Bureau (CFPB), the U.S. Securities and Exchange Commission (SEC), the New York Department of Financial Services, as well as other regulatory agencies in the United States, the United Kingdom, and Canada.[5]

By the time Equifax released its first-quarter report for 2018, the company had spent $242.7 million in response to the breach. In July 2019, Equifax agreed to pay up to $700 million as part of a settlement with the FTC, the CFPB, and 50 U.S. states and territories.

The breach shone a spotlight on the "underregulated" data brokerage industry. A flurry of new legislation was proposed in Congress, such as bills to support national data breach notification, credit report error correction, and even the "Freedom from Equifax Exploitation (FREE) Act," which would give consumers more control over credit report freezes and fraud alerts. There was even a proposed "Data Broker Accountability and Transparency Act," which would "press data broker companies, including recently breached credit report company Equifax, to implement better privacy and security practices."[6]

"Equifax will not be defined by this incident, but rather, by how we respond," said CEO Rick Smith valiantly, on the day the breach was announced. It was true. While the Equifax breach itself was bad, what turned it into an utter disaster was the company's *response*, as we will see.

---

4. *Hearing on "Oversight of Equifax Data Breach: Answers for Consumers" Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy and Commerce*, 115th Cong. (October 3, 2017), https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf (prepared testimony of Richard F. Smith, former Chairman and CEO, Equifax).

5. U.S. Securities and Exchange Commission (SEC), "Equifax Inc.," Form 10-Q, 2017, https://www.sec.gov/Archives/edgar/data/33185/000003318517000032/efx10q20170930; Hayley Tsukayama, "Equifax Faces Hundreds of Class-Action Lawsuits and an SEC Subpoena over the Way It Handled Its Data Breach," *Washington Post*, November 9, 2017, https://www.washingtonpost.com/news/the-switch/wp/2017/11/09/equifax-faces-hundreds-of-class-action-lawsuits-and-an-sec-subpoena-over-the-way-it-handled-its-data-breach.

6. Joe Uchill, "Dems Propose Data Security Bill after Equifax Hack," *Hill*, September 14, 2017, http://thehill.com/policy/cybersecurity/350694-on-heels-of-equifax-breach-dems-propose-data-broker-privacy-and-security.

In its immediate response to the breach, Equifax made choices that destroyed the public's trust by undermining the perception of its competence, character, and caring. This led to a reckoning not just for Equifax but for the data brokerage industry as a whole.

3.1 Crisis and Opportunity

According to crisis management expert Steven Fink:[7]

> A *crisis* is a fluid and dynamic state of affairs containing equal parts danger and opportunity. It is a turning point, for better or worse. The Chinese have a word for this: *wei-fi*.

As any experienced cybersecurity professional will tell you, most data breaches are "a fluid and dynamic state of affairs" (which is part of why is it so challenging to plan your response ahead of time). Every data breach (or suspected data breach) involves inherent danger. There is, of course, the obvious risk that a criminal will acquire and misuse sensitive information. There is the risk of outrage and loss of goodwill of customers, shareholders, and employees. There is the danger of lawsuits and fines. There is the risk of symbolic and unnecessary firings or reorganizations that damage morale and business operations. There is potential for direct financial, reputational, and operational damage.

And yet, data breaches can present enormous opportunities. When you are caught in the midst of a crisis, it can be hard to focus on the positive, but doing so can reap rewards. Data breaches happen for a reason (in fact, like car accidents, they are usually the result of multiple failures). In response to a data breach, we have seen organizations suddenly engage customers, employees, and shareholders more effectively than ever before, taking great pains to listen, understand, and react. Data breaches can quickly oust ineffective leaders and spur much-needed management changes. They can inspire management to appropriately prioritize and invest in modern computer technology, which increases both security and efficiency. They can be catalysts that propel organizations and even whole industries to become stronger in the long run: more secure, more organized, and more effective communicators.

The outcome of a crisis depends on how you react. Unfortunately, relatively few organizations plan for data breaches as a potential crisis, and therefore don't have the necessary resources in place to effectively manage data breaches that escalate to this level. Much like organizations that handle hazardous waste, any organization that stores, processes, or transmits a significant volume of sensitive data should be prepared to handle a data breach crisis.

3.1.1 Incidents

Today, the majority of organizations that plan for data breaches include it as part of their cybersecurity *incident response* program, which is typically developed within the IT department. This is largely for historical reasons and not because it is the best strategy. In the early 2000s,

7. Steven Fink, *Crisis Communications: The Definitive Guide to Managing the Message* (New York: McGraw-Hill, 2013), xv.

virulent worms such as Blaster, Slammer, and MyDoom wreaked havoc across networks, infecting hundreds of thousands of computers and causing network outages. Information security teams prepared by implementing antivirus, network monitoring, intrusion detection, patching, and reimaging mechanisms. It was clear that the community needed a model for planning and responding to these types of threats.

In January 2004, the National Institute of Standards and Technology (NIST) released its first *Computer Security Incident Handling Guide*. What is an "incident"? According to NIST: "A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."[8]

The classic NIST model breaks a cyclical incident response process into four high-level phases, shown in Figure 3-1:

1. Preparation
2. Detection and Analysis
3. Containment, Eradication, and Recovery
4. Post-Incident Activity

Theoretically, responders move through these phases of response in roughly linear cycle, returning to previous phases repeatedly as needed.

The NIST incident response lifecycle model actually worked very well when applied to the most widespread cybersecurity incidents of the early 2000s. When a virus or worm was detected, it was analyzed and then "contained" using network throttling or antivirus. The infected system was cleaned or reimaged ("eradication"); data was restored ("recovery"); and finally the incident was documented and (if necessary) discussed at a postmortem meeting.

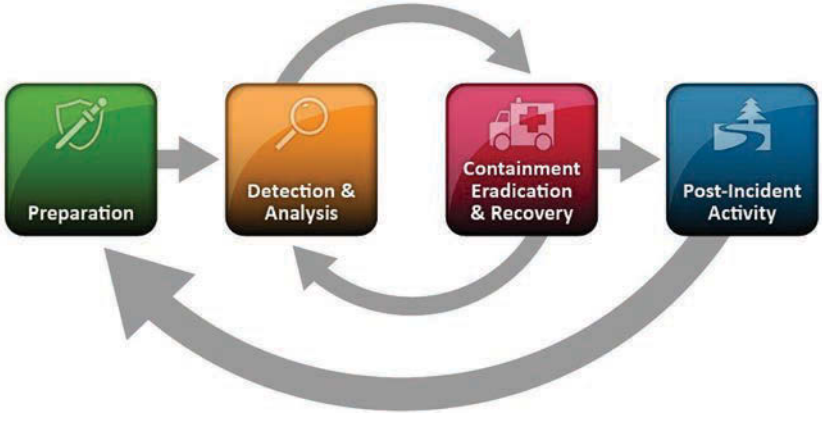


Figure 3-1. The NIST incident response lifecycle. Source: NIST, *Computer Security Incident Handling Guide*.

8. Paul R. Cichonski, Thomas Millar, Timothy Grance, and Karen Scarfone, *Computer Security Incident Handling Guide*, Special Pub. 800-61, rev. 2 (Washington, DC: NIST, 2012), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Since then, organizations throughout the nation have used it as the basis for planning and managing cybersecurity incident response, including data breaches. And therein lies the problem: While the NIST guide is very helpful for managing many kinds of *computer security incidents*, as we will see, a data breach is typically not just an *incident* and therefore must be managed differently.

3.1.2 Data Breaches Are Different

Where in the NIST incident response lifecycle is the part where regulators fine your organization for negligence? Where does the CEO make a public statement? Where are the notification letters, the phone calls to insurers, the class-action lawsuits?

The NIST model can supposedly apply to "loss of data confidentiality," but frankly, the tidy NIST model isn't all that useful when managing a data breach. Most organizations include data breaches in cybersecurity incident response plans, but when an actual data breach occurs, the playbook goes out the window.

The biggest mistake of data breach management and response is the assumption a data breach is a computer security *incident*. It is usually much more than that. A data breach is a *crisis* and must be treated accordingly.

3.1.3 Recognizing Crises

Crisis management expert Ian Mitroff carefully differentiates between an *incident* and a *crisis* as follows:

- An *incident* is "a disruption of a component, a unit, or a subsystem of a larger system, such as a valve or a system generator in a nuclear plant. The operation of the whole system is not threatened and the defective part is merely repaired."
- A *crisis* is "a disruption that . . . affects a system as a whole."[9]

Steven Fink further defines a crisis as "any prodromal situation that runs the risk of":

1. Escalating in intensity.
2. Falling under close media or government scrutiny.
3. Interfering with the normal operations of business.
4. Jeopardizing the positive public image presently enjoyed by a company or its officers.
5. Damaging a company's bottom line in any way.[10]

Data breaches, by their very nature, create risks in all five of Fink's categories above.

9. T. Pauchant and I. Mitroff, *Transforming the Crisis-Prone Organization* (San Francisco: Jossey-Bass, 1992), 12.

10. Steven Fink, *Crisis Management: Planning for the Inevitable*, rev. ed. (Bloomington, IN: iUniverse, 1986), 23–24.

3.1.4 The Four Stages of a Crisis

The NIST incident response lifecycle is very useful for certain types of incidents. However, the purpose of having a model is to help us to better understand a situation and respond more effectively. When it comes to data breaches, Fink's crisis management model is a more useful tool for understanding data breach management and response, as we will see throughout this book.

According to Fink, every crisis moves through four stages. These stages are:[11]

- **Prodromal** - The "precrisis" phase, in which there are warnings or precursors that, if acted upon, can enable responders to minimize the impact of the crisis.
- **Acute** - The "time when chaos reigns supreme," according to Fink. At this stage, the crisis has become visible outside the organization, and leadership must address it.
- **Chronic** - During this stage, "litigation occurs, media exposes are aired, internal investigations are launched, government oversight investigations commence." As the name implies, the chronic stage can last for years.
- **Resolution** - The crisis is settled and normal activities resume.

These stages apply neatly to data breaches, which typically do include a prodrome (such as an intrusion detection system alert), followed by an acute phase (such as an intense media scandal). This results in lawsuits, public outcry, internal investigations, etc., as described in the chronic phase. Finally, the breached organization may reach the resolution stage, typically after undergoing changes to processes and procedures. It can take years to get there.

The goal of crisis management is to "manage the prodrome so successfully that you go from prodrome to resolution without falling into the morass of the acute and chronic stages."[12] The same is true of data breaches: the best way to manage a data breach is to prevent it from occurring in the first place. If that is not possible, the next best technique is to rely upon a strong detection and response program, so that your response team can identify the earliest signs of an intrusion and react quickly enough to minimize the risk of data exposure. Effective network instrumentation, logging, and alerting are key elements of a strong detection and response program. Finally, if a data breach reaches the acute crisis phase, then it is important to have a strong crisis management and crisis communications program in place. This latter piece—crisis communications—is critical. It is not enough to manage the data breach crisis itself; you must also take care to manage the *perception* of the crisis.

3.2 Crisis Communications, or Communications Crisis?

When planning for data breaches, many organizations emphasize the technical aspects of the response effort: modifying firewall rules on the fly, cleaning spyware and rootkits off endpoint

11. Fink, *Crisis Communications*, 46.

12. Fink, *Crisis Communications*, 47.

systems, preserving evidence. This is part of the organization's *crisis management* strategy, which addresses the "reality of the crisis."[13]

If there is one area that is overlooked more than any other in data breach planning, it is crisis communications. Time and time again, we see organizations turn data breaches into reputational catastrophes due to classic communications mistakes.

"Crisis communications is managing the perception of that same reality," explains Fink. "It is telling the public what is going on (or what you want the public to know about what is going on). It is shaping public opinion."[14] In a data breach crisis, a poor or nonexistent communications strategy can cause far more long-lasting damage than any actual harm caused by the breach itself. While a full exploration of effective crisis communications is outside the scope of this book, we will point out clear communications mistakes in the data breaches we study and share commonly accepted "rules of thumb" that can help your crisis communications go more smoothly.

When a data breach occurs, communications with key stakeholders such as customers, employees, shareholders, and the media are often developed on the fly. Sometimes multiple staff members talk to the press, leading to mixed messages. Other times, the organization goes radio silent, and the public is left with no answers, no reassurance, and a sense of distrust. In the next sections, we will break down why crisis communication is so important and provide reader with clear strategies for a strong response.

3.2.1 Image Is Everything

When a data breach crisis occurs, organizations face a significant threat to their image. "Image" is the perception of an organization in the mind of a stakeholder. Far from being a superficial matter, an organization's image is vital.

A damaged image can impact customer relations, as well as investor confidence and stock values. Image is also critical for defining the organization's relationship with law enforcement, regulators, and legislators. In a data breach, damage to an organization's image can trigger consumer lawsuits, cause increased fines and settlement costs, and even affect the content of laws that are passed as a result of the crisis. It can impact hiring, morale, and employee retention. If image repair is fumbled, key executives may be forced to step down as a result of a breach, as Equifax's CEO shockingly discovered.

The impact of a data breach on an organization's image depends on many factors. Image repair expert William L. Benoit says that a threat to one's image occurs when the relevant audience believes that:[15]

1. An act occurred that is undesirable.
2. You are responsible for that action.

13. Fink, *Crisis Communications*, 8.

14. Fink, *Crisis Communications*, 8.

15. William L. Benoit, *Accounts, Excuses, and Apologies*, 2nd ed. (Albany: SUNY Press, 2014), 28.

Data breaches can damage the relationship between stakeholders and the organization. There is a risk that the organization will be perceived as responsible for the undesirable act (the breach). This, in turn, creates a threat to the organization's image.

3.2.2 Stakeholders

Fundamentally, a corporate image is the result of a relationship that the organization develops with each stakeholder. To use Equifax as an example, key stakeholders include:

- Consumers
- Shareholders
- Employees
- Regulators
- Board of Directors
- Legislators
- And more

These categories of stakeholders have different concerns in the wake of a breach.

3.2.3 The 3 C's of Trust

A data breach can injure the relationship between stakeholders and the organization. Specifically, it damages trust. Military psychologist Patrick J. Sweeney conducted a study of enlisted soldiers in 2003 and found that three factors were central to trust:[16]

- **Competence** - Capable of skillfully executing one's job
- **Character** - Strong adherence to good values, including loyalty, duty, respect, selfless service, honor, integrity, and personal courage
- **Caring** - Genuine concern for the well-being of others

As we will see, these three factors apply as well in the context of trust between stakeholders and an organization.

3.2.4 Image Repair Strategies

Throughout this book, we will see that breached organizations work hard to preserve and repair their images. Here, we will introduce a model for analyzing different strategies, in order to evaluate their effectiveness.

16. Michael D. Matthews, "The 3 C's of Trust," *Psychology Today*, May 3, 2016, https://www.psychologytoday.com/blog/head-strong/201605/the-3-c-s-trust.

Benoit lists five categories of image repair strategies:[17]

1. *Denial* - The accused denies that the negative event happened or that he or she caused it.
2. *Evasion of Responsibility* - The accused attempts to avoid responsibility, such as by claiming the event was an uncontrollable accident or that he or she did not have the information or ability to control the situation.
3. *Reducing Offensiveness* - The accused attempts to reduce the audience's negative feelings through one of six variants:
   - Bolstering - Highlighting positive actions and attributes of the accused
   - Minimization - Convincing the audience that the negative event was not as bad as it appears
   - Differentiation - Emphasizing differences between the event and similar negative occurrences
   - Transcendence - Placing the event in a different context
   - Attacking one's accuser - Discrediting the source of accusations
   - Compensation - Offering remuneration in the form of valued goods and services
4. *Corrective Action* - The accused makes changes to repair damage and/or prevent similar situations from occurring in the future.
5. *Mortification* - The accused admits that he or she was wrong and asks for forgiveness.

All of these image repair strategies can, and have, been employed in data breach responses, some to greater effect than others.

3.2.5 Notification

Notification is perhaps the most critical part of data breach crisis communications, and it can have an enormous impact on public perception and image management. Key questions include:

- **When should you notify key stakeholders?** Rarely, if ever, are all the facts about a data breach known up front. On the one hand, a quick notification can signal that you care and are acting in good faith. On the other hand, it may be the case that by waiting, you find out more information that reduces the scope of the notification requirements. There is no "right" time, and crisis management teams have many tradeoffs to consider.
- **Who should be notified?** There are internal notifications (e.g., upper management, legal) In some cases, it may be appropriate to bring in law enforcement. Certain states require notification to an attorney general or other parties. Depending on the type of data exposed, it may be necessary to alert consumers or employees.

17. Benoit, *Accounts, Excuses, and Apologies*, 28.

- **How should you notify?** Paper mailings, email notification, a web announcement, or phone calls are all common options. Your notification requirements vary depending on the type of data exposed, the number of data subjects affected, the geographic location of the data subjects, and other factors. Notification can be expensive, and often cost is a limiting factor. Today, many organizations take a multipronged approach, which includes email or paper individual notifications, supported by a website FAQ and a call center where consumers can get more information.
- **What information should be included in a notification?** On the one hand, you want to build trust and appear transparent. It's also important to give data subjects enough information to reduce their risk, whenever that is possible. At the same time, current laws are not in line with the public's expectations of privacy. Typically information that is not specifically regulated (such as shoppers' purchase histories or web surfing habits) are not explicitly mentioned in data breach announcements, even if it is likely that information has been exposed.

In this section, we highlight some of the key challenges that breach response teams face when determining when, who, and how to notify.

3.2.5.1 Regulated vs. Unregulated Data

Data breach investigations are typically conducted to evaluate the risk that data regulated by a breach notification law or contractual clause was inappropriately accessed or acquired. Modern breach response teams are often led by an experienced attorney who acts as the "breach coach," guiding the investigation and coordinating the participants. Digital forensic investigators take direction from the attorney, gathering and analyzing the evidence that the attorney needs to determine whether a notification statute or clause has been triggered.

Data breach notification laws emerged in the United States during a simpler time. Many state laws were created in response to the 2005 ChoicePoint breach (discussed in more detail in Chapter 4, "Managing DRAMA"), when financial fraud had captured the media's attention. Credit monitoring and identity theft protection emerged during this period as well and became a part of the cookie-cutter breach response process.

State breach notification laws do not require organizations to make a full confession to consumers, detailing every single data element that may have been stolen. Rather, the laws are designed to protect a specific, limited subset of "personal information." Recall from Chapter 1 that most of the time, "personal information" includes:[18]

> [a]n individual's first name or first initial and last name plus one or more of the following data elements: (i) Social Security number, (ii) driver's license number or state- issued ID card number, (iii) account number, credit card number or debit card number combined with any security code, access code, PIN or password needed to access an account.

18. Baker Hostetler, "Data Breach Charts," *Baker Law*, November 2017, https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

What about web surfing history, purchase history, "lifestyle interests," salary information, and more? "As long as it doesn't contain any of the data elements that would trigger notification such as Social Security Number or financial account information, then no, it would not trigger a notification obligation," says data breach attorney and certified computer forensic examiner M. Scott Koller, of Baker Hostetler. Even in cases where regulated data elements are involved, breached organizations are not required to notify subjects about other, nonregulated elements that may have been accessed. "In my practice, I generally will include additional information so [affected persons] have a better sense of what occurred," says Koller. "For example, if a real estate agent was breached, I would say that the information includes name, address, Social Security Number, and other information submitted with your application." Koller cites mailing address as a common piece of information that may not be protected by statute but is often included in notification letters.

3.2.5.2 Left Out

Digital forensic analysis is often a painstaking, time-intensive, and expensive process. Reconstructing a picture of precisely what data elements were accessed, and when, can involve hundreds if not thousands of hours of labor, particularly if the organization did not retain good logs. Even breached organizations have limited budgets (and so do their insurers, who may be footing the bill). And again, there is the time pressure that comes from crisis communications needs.

As a result, data breach investigations often do not include the full range of an attacker's activities. Rather, investigations normally focus on the regulated data elements and leave out systems that are not needed for complying with data breach notification requirements. Computers that don't contain *regulated* data elements may not be included in digital evidence preservation at all.

For example, at Equifax, intruders reportedly first gained access to personal information in May 2017, after exploiting a vulnerability in a public-facing Equifax web server. Once the attackers gained a foothold, they explored the company's internal network. They crawled through the network for more than two months before they were finally discovered on July 29. Bloomberg Technology later published an investigative report that revealed that criminals "had time to customize their tools to more efficiently exploit Equifax's software, and to query and analyze dozens of databases to decide which held the most valuable data. The trove they collected was so large it had to be broken up into smaller pieces to try to avoid tripping alarms as data slipped from the company's grasp through the summer."[19]

Unregulated data such as web surfing activity, shopping history, or social connections may be stolen by an attacker, but data brokers would not be required to report that to the public, or even check to see whether anything was stolen in the first place. Equifax likely held extensive volumes of this type of data because it offers digital marketing services, including "Data-driven Digital Targeting" designed to track consumers and target advertisements. Exactly which Equifax databases did the attackers access? The public will likely never know. Equifax, like

19. Michael Riley, Jordan Robertson, and Anita Sharpe, "The Equifax Hack Has the Hallmarks of State-Sponsored Pros," *Bloomberg*, September 29, 2017, https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

other data brokers, has amassed troves of sensitive consumer and business data, but only a small percentage is regulated by state and federal data breach notification laws.

Attorneys, forensics firms, the media, and the public are all focused on the potential exposure of SSNs and the risk of identity theft, just as they were a decade ago—but it is increasingly clear that technology and data analytics have changed the game. "There's a trend toward expanding what qualifies as 'personal information,' and that trend has continued year after year," says Koller. "So far, expansion is where people are sensitive . . . people are sensitive to medical information, sensitive to biometric information, usernames and passwords, because there's harm to that." In the coming years, data breach responders will need to stay up-to-date on the changing regulatory requirements, as well as key stakeholders' (often unspoken) expectations.

3.2.5.3 Overnotification

Overnotification is when an organization alerts people to a potential data breach when it was not truly necessary. Since a data breach can cause reputational, financial, and operational damage, obviously overnotification is something to avoid. When it occurs, it is usually due to lack of evidence or easy access to log data.

Think of all the "megabreaches" you've read about in the news. Headlines announce that hundreds of thousands of patient records or millions of credit card numbers were exposed. Behind the scenes, there is often no proof that hackers actually acquired all of that data. Instead, the organization simply wasn't logging *access* to sensitive information, and as a result there was no way for investigators to tell what data had *actually* been acquired and what remained untouched. Absent evidence, some regulations require organizations to assume that a breach occurred.

Today, cheap and widely available tools exist that will create a record of activities, such as every time a file is uploaded (or downloaded), every time a user logs in (or out), or every time a user views customer records. These log files can be absolutely invaluable in the event of a suspected breach.

Imagine that you are faced with a case where a hacker broke into a database server that housed 50,000 customer records. Upon reviewing the log files, your investigative team finds that only three customer records were actually accessed by the criminal. Intead of sending out 50,000 customer notifications, you send out three. Worth it? Definitely!

Every organization's logging and monitoring system is unique and should be tailored to protect its most sensitive information assets. This reduces the risk of overnotification and can save an organization from a full-scale disaster.

3.2.5.4 Delays in Notification

Breach response teams are under enormous pressure to decide who needs to be notified as quickly as possible. As the public becomes savvier and more aware of the potential harm that can be caused by data breaches, they are less tolerant of delayed notifications. Even a lag of as little as a week can incur consumer wrath.

In the case of Equifax, the company reportedly spent six weeks investigating its data breach and preparing notifications. Forensic investigators, law enforcement agents, data breach attorneys, and other professionals involved in data breach management know that six weeks is

a common notification window (certainly well within HIPAA's 60-day period, for example)—but this was not your average breach. The theft of 145.5 million SSNs meant that organizations throughout the United States could no longer rely on SSNs as a means of authenticating consumers. (Of course, as outlined in Chapter 5, "Stolen Data," much of the data was already stolen anyway, but until the Equifax breach occurred, most U.S. citizens maintained a healthy denial.) From the public's perspective, every day that Equifax waited to disclose was one more day that affected individuals did not have the opportunity to protect themselves from potential harm.

When the notification delay stretches to years, you have a lot of explaining to do, and the delay may be far more damaging than the breach itself—as Yahoo discovered in 2016 when its data breach was finally uncovered.

"If a breach occurs, consumers should not be first learning of it three years later," said Senator Mark Warner of Virginia, in response to Yahoo's breach notification. "Prompt notification enables users to potentially limit the harm of a breach of this kind, particularly when it may have exposed authentication information such as security question answers they may have used on other sites."[20] This reflected a notable advancement in the public's demonstrated understanding of data breaches: By the end of 2016, many people recognized that the compromise of their account credentials from one vendor could enable attackers to gain access to other accounts as well.

3.2.6 Uber's Skeleton in the Closet

Woe to the company that keeps a data breach secret—and then eventually is unmasked.

Uber is one such company. In 2016, Uber fell victim to cyber extortion—and made a bad choice. An anonyous hacker (who called himself "John Dough") emailed the company, claiming to have found a vulnerability and accessed sensitive data. It turned out that he had gained access to the company's cloud-based repository at GitHub, where he found credentials and other data that enabled him to break into Uber's Amazon web servers, which housed the company's crown jewels—source code and data on 57 million customers and drivers (including approximately 600,000 driver's license numbers).

The hacker politely but firmly demanded a payoff for the discovery of the "vulnerability." At the time, Uber had a bug bounty program, managed by the speciality company HackerOne. After verifying the hacker's claims, Uber discussed payment for the hacker's report. Rob Fletcher, Uber's product security engineering manager, informed John Dough that the bug bounty program's typical top payment was $10,000. The hacker demanded more.

"Yes we expect at least 100,000$," the hacker wrote back. "I am sure you understand what this could've turned out to be if it was to get into the wrong hands, I mean you guys had private keys, private data stored, backups of everything, config files etc. . . . This would've heart [*sic*] the company a lot more than you think."[21]

---

20. Hayley Tsukayama, "It Took Three Years for Yahoo to Tell Us about Its Latest Breach. Why Does It Take So Long?" *Washington Post*, December 19, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/12/16/it-took-three-years-for-yahoo-to-tell-us-about-its-latest-breach-why-does-it-take-so-long.

21. "Uber 'Bug Bounty' Emails," Document Cloud, https://www.documentcloud.org/documents/4349230-Uber-Bug-Bounty-Emails.html (accessed March 19, 2018).

Uber acquiesced and arranged for payment of $100,000. It turned out that there were actually two hackers—the original "John Dough," based in Canada, and a second person—a 20-year-old man in Florida who had actually downloaded Uber's sensitive data. According to reports, "Uber made the payment to confirm the hacker's identity and have him sign a nondisclosure agreement to deter further wrongdoing. Uber also conducted a forensic analysis of the hacker's machine to make sure the data had been purged."[22]

Internally, the case was managed by Uber's CSO, John Sullivan, and the company's internal legal director, Craig Clark. Reportedly, Uber's CEO at the time, Travis Kalanick, was briefed. Uber's team made the decision that notification was not required, and the case was closed—or so they thought.

3.2.6.1 Housecleaning

The case probably would have stayed closed forever, but in 2017, Uber's CEO resigned amid a growing scandal that revealed pervasive unethical and in some cases illegal behavior at the company. The new CEO took the reins in September 2017. The company's board initiated an internal investigation of the security team's activities, enlisting the help of an outside law firm. As part of this investigation, the unusual $100,000 "bug bounty" payment was uncovered—and investigated. The company also hired the forensics firm Mandiant to take an inventory of the affected data.

Cleaning the skeletons out of the closet was very important for Uber's new leadership team. In order to rebuild trust with key stakeholders and the public, they needed to demonstrate openness and honesty. Any scandals that remained hidden could come back to haunt the new leadership team, which they did not want to risk. This was especially important given Uber's rocky financial footing; were the company to be sold, the breach might well have come out during a cyber diligence review later. Exposing Uber's dirty secrets all at once allowed Uber's new team the opportunity to control the dialogue, point the finger at the old management, and continue on with a clean(ish) slate. As a result, Uber's data breach case was cracked wide open.

On November 21, 2017, Uber's new CEO, Dara Khosrowshahi, released a statement disclosing the company's "2016 Data Security Incident." In this statement, he revealed that the names and driver's license numbers for 600,000 drivers had been downloaded, in addition to "personal information of 57 million Uber users around the world." Khosrowshahi specifically called out Uber's failure to notify data subjects or regulators as a problem, and announced that the company's CSO John Sullivan and attorney Craig Clark had been fired, effective immediately.[23]

"None of this should have happened, and I will not make excuses for it," he wrote. "While I can't erase the past, I can commit on behalf of every Uber employee that we will learn from our mistakes."[24]

---

22. Joseph Menn and Dustin Volz, "Exclusive: Uber Paid 20-Year-Old Florida Man to Keep Data Breach Secret: Sources," *Reuters*, December 7, 2017, https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C.

23. Menn and Volz, "Exclusive."

24. Dara Khosrowshahi, "2016 Data Security Incident," Uber, November 21, 2017, https://www.uber.com/newsroom/2016-data-incident.

3.2.6.2 Fallout

Angry riders and drivers immediately took the company to task on social media—not just for the breach itself, but for the way it was handled. Days later, two class-action lawsuits were filed against the ride-sharing company. Washington State, as well as Los Angeles and Chicago, filed their own lawsuits. Attorneys general from around the country began investigating, and in March 2018, Pennsylvania's state attorney general announced that he was suing Uber for violating the state data breach notification law.

"The fact that the company took approximately a year to notify impacted users raises red flags within this committee as to what systemic issues prevented such time-sensitive information from being made available to those left vulnerable," said U.S. Representative Jerry Moran (R-KS).[25]

Uber's chief information security officer, John Flynn, was called to testify before Congress about the breach. A large part of his testimony was in defense of the bug bounty program, which had come under fire due to its role in the cover-up. "We recognize that the bug bounty program is not an appropriate vehicle for dealing with intruders who seek to extort funds from the company," Flynn said. "The approach that these intruders took was separate and distinct from those of the researchers in the security community for whom bug bounty programs are designed. . . . [A]t the end of the day, these intruders were fundamentally different from legitimate bug bounty recipients."

3.2.6.3 Effects

The Uber case rocked the boat for third-party breach response teams, who frequently based decisions of disclosure on a risk analysis. Many breach coaches and security managers would have reached the same conclusions as Sullivan and Clark. After all, the hacker had signed an NDA, and the company had conducted a forensic analysis of his laptop. For many attorneys, this would have been considered sufficient evidence to conclude that there was a low risk of harm.

Deferring to outside counsel may have helped. There is no public evidence that Sullivan and Clark called upon an outside cybersecurity attorney for legal assistance in this case. Involving outside counsel allows internal staff to defer to an experienced third party with regards to disclosure decisions, providing significant protection for the internal team in the event that the decision is later questioned. Given the complex state of cybersecurity regulation and litigation, it is always safest to involve outside counsel. Had Uber's investigative team chosen to involve outside counsel, they may well have reached a different conclusion.[26]

As shocking as the Uber disclosure was, one has to question whether it was truly outside the norm. It's safe to say that if Uber had not chosen to report the 2016 breach, it most likely never would have been revealed. How many companies today have similar skeletons in the closet that may never be uncovered?

---

25. Naomi Nix and Eric Newcomer, "Uber Defends Bug Bounty Hacker Program to Washington Lawmakers," *Bloomberg*, February 6, 2018, https://www.bloomberg.com/news/articles/2018-02-06/uber-defends-bug-bounty-hacker-program-to-washington-lawmakers.

26. Louise Matsakis, "Uber 'Surprised' by Totally Unsurprising Pennsylvania Data Breach Lawsuit," *Wired*, March 5, 2018, https://www.wired.com/story/uber-pennsylvania-data-breach-lawsuit.

3.3 Equifax

Now that we've introduced the principles of crisis communications and image repair, let's analyze the Equifax breach response. Recall the "3 C's of Trust":

- **Competence** - Capable of skillfully executing one's job
- **Character** - Strong adherence to good values, including loyalty, duty, respect, selfless service, honor, integrity, and personal courage
- **Caring** - Genuine concern for the well-being of others

As we will see, Equifax's response caused stakeholders to question all three of these factors, which badly damaged Equifax's image and exacerbated the crisis.

3.3.1 Competence Concerns

After announcing the breach on September 7, 2017, Equifax was immediately off on the wrong foot. Consumers rushed to freeze their credit, only to find that Equifax's freeze request page was unresponsive.[27]

Equifax also set up a website that consumers could visit to find out whether their data was exposed, but as investigative journalist Brian Krebs reported, the site was "completely broken at best, and little more than a stalling tactic or sham at worst."[28]

The site asked consumers to submit the last six digits of their SSNs in order to determine whether they were affected. Consumers who did enter their information received vague and often conflicting results. Krebs reported that "[i]n some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones."[29] Krebs himself did not receive a yes-or-no answer, but rather "a message that credit monitoring services we were eligible for were not available and to check back later in the month." These responses were infuriating for consumers, who were anxious and frustrated that the promised corrective action was not available.

Tensions were further inflamed when consumers discovered that in order to sign up for Equifax's free TrustedID credit monitoring service, the terms of use required them to forfeit their rights to participate in a class-action lawsuit (language that Equifax later said had been included inadvertently). Equifax quickly changed the language following public outcry.[30]

Ironically, many web browsers flagged the breach information site as a phishing attack in the first few hours after the announcement. To make matters worse, the site was riddled with

27. Brian Krebs, "Equifax Breach: Setting the Record Straight," Krebs on Security, September 20, 2017, https://krebsonsecurity.com/2017/09/equifax-breach-setting-the-record-straight.

28. Brian Krebs, "Equifax Breach Response Turns Dumpster Fire," Krebs on Security, September 8, 2017, https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire.

29. Krebs, "Equifax Breach Response."

30. Mahita Gajanan, "Equifax Says You Won't Surrender Your Right to Sue by Asking for Help After Massive Hack," *Time*, September 11, 2017, http://time.com/4936081/equifax-data-breach-hack.

security holes. "[V]ulnerabilities in the site can allow hackers to siphon off personal information of anyone who visits."[31] While building a brand-new, interactive website may have been nice in theory, Equifax's developers—reportedly associated with the outside public relations firm Edelman—clearly did a rush job.[32]

"Talk about ham-handed responses. . . . This is simply unacceptable," said U.S. Representative Greg Walden.[33]

Right away, Equifax appeared incompetent. This negative image was exacerbated days later, when the media discovered that Equifax's official Twitter account had accidentally tweeted the link to a phony phishing site, securityequifax2017.com, four times during the response. "When your social media profile is tweeting out a phishing link, that's bad news bears," said security professional Michael Borohovski, cofounder of Tinfoil Security.[34]

As details of Equifax's cybersecurity issues were exposed, it painted an increasingly ugly picture. Just days after the breach was announced, Krebs reported a ridiculous vulnerability in a portal used by Equifax Argentina employees for credit dispute management: the portal was "wide open, protected by perhaps the most easy-to-guess password combination ever: 'admin/admin.'"[35]

Two days later, Equifax confirmed in a statement that the megabreach had been caused when hackers broke into a web server, exploiting a well-known vulnerability in the Apache Struts framework. The vulnerability had been announced in March 2017, and Equifax was hacked in May—meaning that the company had more than two months to patch the system but didn't.[36] Equifax announced the cause only after a research firm published an uncited report implicating the Apache Struts vulnerability, which sparked rumors.[37] The day after the statement was released, the company's chief information officer and chief security officer stepped down.

Equifax's CEO later blamed an employee for not installing the patch and said a subsequent security scan did not detect the issue. Consumers didn't buy the excuse, if it was one.

Senator Elizabeth Warren tweeted: "It's outrageous that Equifax—a company whose one job is to collect consumer information—failed to safeguard data for 143M Americans."[38]

---

31. Zack Whittaker, "Equifax's Credit Report Monitoring Site Is also Vulnerable to Hacking," *ZD Net*, September 12, 2017, http://www.zdnet.com/article/equifax-freeze-your-account-site-is-also-vulnerable-to-hacking.

32. Krebs, "Equifax Breach Response"; Lily Hay Newman, "All the Ways Equifax Epically Bungled Its Breach Response," *Wired*, September 24, 2017, https://www.wired.com/story/equifax-breach-response.

33. Alfred Ng, "Equifax Ex-CEO Blames Breach on One Person and a Bad Scanner," *CNET*, October 3, 2017, https://www.cnet.com/news/equifax-ex-ceo-blames-breach-on-one-person-and-a-bad-scanner.

34. Newman, "All the Ways."

35. Brian Krebs, "Ayuda! (Help!) Equifax Has My Data!" Krebs on Security, September 12, 2017, https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data.

36. Lily Hay Newman, "Equifax Officially Has No Excuse," *Wired*, September 14, 2017, https://www.wired.com/story/equifax-breach-no-excuse.

37. Robert W. Baird & Co., "Equifax Inc. (EFX) Announces Significant Data Breach; -13.4% in After-Hours," *Baird Equity Research*, September 7, 2017, https://baird.bluematrix.com/docs/pdf/dbf801ef-f20e-4d6f-91c1-88e55503ecb0.pdf.

38. Brad Stone, "The Category 5 Equifax Hurricane," *Bloomberg*, September 11, 2017, https://www.bloomberg.com/news/articles/2017-09-11/the-category-5-equifax-hurricane.

3.3.2 Character Flaws

The integrity of Equifax, as a corporation, as well as its leadership team, was called into question immediately due to the length of time taken before notifying. "Equifax waited six weeks to disclose the breach," wrote reporter Michael Hiltzik in the *Los Angeles Times* the day following the company's announcement. "That's six weeks that consumers could have been victimized without their knowledge and therefore left without the ability to take countermeasures. Equifax hasn't explained the delay."[39] It wasn't just the public that was kept in the dark; CEO Smith also waited 20 days to inform the company's board, despite the massive scale of the breach.[40]

The delay triggered deep suspicion. "New York Attorney General Eric Schneiderman wants to know when the company learned about the breach and how exactly it happened," *Bloomberg* reported. Questions of integrity grew when it became known that three senior Equifax executives had sold shares in the company worth nearly $2 million in the days following the breach discovery.

Making Money Off Data Breaches

Ironically, in the long term Equifax stood to profit handsomely from the breach, given that it was in the business of providing credit monitoring services. In a scorching U.S. Senate committee hearing the month following the breach, Senator Elizabeth Warren pointed out that "[f]rom 2013 until today, Equifax has disclosed at least four separate hacks in which it compromised sensitive personal data. In those four years . . . [Equifax's profit has] gone up by more than 80 percent over that time."[41]

The reasons were plain: By early October, 7.5 million people had signed up for Equifax's credit monitoring service. While the service was free for the first year for affected consumers, anyone who continued using the service after that would have to pay $17/month, potentially netting Equifax hundreds of millions of additional revenue per year. After the Equifax breach, the identity theft protection company Lifelock also reported a tenfold increase in enrollments. Lifelock purchased its credit monitoring service from Equifax—meaning that profits were passed along as well.

Once Equifax's conflict of interest was revealed, it further fueled mistrust and triggered more scrutiny of the data brokerage industry as a whole. "So the breach of your system has actually created more business opportunities for you," snarled Warren to former CEO Rick Smith in a Senate banking committee hearing. "Equifax did a terrible job of protecting our data, because they didn't have a reason to protect our data. . . . The incentives in this industry are completely out of whack."[42]

---

39. Michael Hiltzik, "Here Are All the Ways the Equifax Data Breach Is Worse than You Can Imagine," *Los Angeles Times*, September 8, 2017, http://www.latimes.com/business/hiltzik/la-fi-hiltzik-equifax-breach-20170908-story.html.

40. Liz Moyer, "Equifax's Then-CEO Waited Three Weeks to Inform Board of Massive Data Breach, Testimony Says," *CNBC*, October 2, 2017, https://www.cnbc.com/2017/10/02/equifaxs-then-ceo-waited-three-weeks-to-inform-board-of-massive-data-breach-testimony-says.html.

41. Daniel Marans, "Elizabeth Warren Scorches Former Equifax CEO for Profiting from Data Breaches," *HuffPost*, October 4, 2017, https://www.huffpost.com/entry/elizabeth-warren-equifax-ceo_n_59d503ace4b06226e3f55c83.

42. Marans, "Elizabeth Warren Scorches."

3.3.3 Uncaring

In the aftermath of the breach announcement, Equifax's call centers couldn't come close to handling the flood of phone calls. Consumers were infuriated. The lack of two-way communication contributed to a growing sense that Equifax did not actually care about the consumer.

Later, in his congressional testimony, former CEO Smith apologized:[43]

> We were disappointed with the rollout of our website and call centers, which in many cases added to the frustration of American consumers. The scale of this hack was enormous and we struggled with the initial effort to meet the challenges that effective remediation posed. The company dramatically increased the number of customer service representatives at the call centers and the website has been improved to handle the large number of visitors. Still, the rollout of these resources should have been far better, and I regret that the response exacerbated rather than alleviated matters for so many.

Smith closely integrated his personal image with Equifax's breach response. On the same day as the breach announcement, Equifax released a video featuring Smith—presumably in an attempt to humanize the company. It didn't do them any favors. Smith essentially read the company's statement out loud with a wooden expression, looking like a deer in headlights. Although Equifax wisely included an explicit apology in the message, it was buried halfway through the video, and the words were not enough to overcome Smith's strained, unemotional demeanor.[44]

The Equifax breach quickly exploded into a "dumpster fire" (as Krebs put it). Smith was forced to resign after a 12-year tenure, just weeks after the breach was announced.

3.3.4 Impact

Equifax's communications following its breach left stakeholders with the following impressions:

- **Incompetent** - Smith did not oversee Equifax's cybersecurity program effectively, as evidenced by the breach and gross fumbles with technology in the company's response.
- **Lack of Character** - Equifax's delayed notification, along with rumors of an executive stock dump during the breach investigation, caused the public to question the integrity of the company and its leadership.
- **Uncaring** - Smith's wooden performance in Equifax's public relations video, combined with the call center frustrations, left the strong impression that Equifax did not care about consumers.

As a result, the breach badly damaged Equifax's image and destroyed trust that key stakeholders had in the company's leadership.

Throughout the acute phases of the crisis, Equifax's stock value clearly changed based on the company's communications. Stock prices fell from $142.72 on the day of the announcement

43. U.S. Comm. on Energy and Commerce, *Prepared Testimony of Richard F. Smith*.

44. Equifax, "Rick Smith, Chairman and CEO of Equifax, on Cybersecurity Incident Involving Consumer Data," *YouTube*, September 7, 2017, https://www.youtube.com/watch?v=bh1gzJFVFLc.

to a low of $92.98 a week later on September 15, 2017, as shown in Figure 3-2. Things started to pick up with the resignation of the CIO and CSO; clearly shareholders began to rebuild confidence with a change of management. With Smith's resignation, Equifax's stock rose yet again. By the end of the year, share prices were still down, but slowly recovering.

Figure 3-2. Equifax's stock price before, during, and after the acute phase of the data breach. Source: Yahoo Finance, https://finance.yahoo.com.

3.3.5 Crisis Communications Tips

There are many lessons to be learned from the Equifax breach, but perhaps none are so well illustrated and so poignant as those relating to crisis communications. In today's day and age, many CEOs—too many—will find themselves in much the same position as Smith.

In those first few hours, days, and weeks, keep in mind the following priorities:

- **Maintain Trust with Your Stakeholders.** Remember the 3 C's: Competence, Character, and Caring.
- **Tell It Early, Tell It Yourself.** Maintain a congenial relationship with the media. By providing a quote when contacted by the press, you send the message that you are not trying to hide.
- **Tell the Truth.** If you tell the truth, you won't have to suffer the consequences of a scandalous lie.
- **Make It a "One-Day" Story.** Few data breach stories are ever really one day, but get as close as you can by consolidating announcements and responding to the press as quickly as possible. Don't give journalists incentive to "dig."

- **Take Responsibility.** This is the foundation for rebuilding trust.
- **Apologize Clearly and Quickly.** A sincere apology diffuses anger and shows respect for your stakeholders.
- **Listen!** Prepare your staff to listen to stakeholders. For example, you might consider opening a call center in response to the breach, so that members of the public can quickly speak with a real human. Likewise, shareholders, regulators, and other stakeholders need a point of contact who can listen to their concerns and diffuse strong emotions.
- **Make Sure Your Tools Work.** Too often, when a breach occurs, breached companies offer services to the public, such as a hotline or credit monitoring, but the technology or processes to support them are broken or not immediately available. This further inflames sentiments.
- **Make Amends.** Use image repair tactics such as compensation or corrective action to restore your organization's image.

3.4 Conclusion

In this chapter, we showed how data breaches are typically *crises* and introduced Steven Fink's four stages of a crisis. We also showed how the "3 C's of Trust" relate to crisis communications and discussed the fundamentals of image repair theory. Finally, we analyzed the Equifax breach and showed how flaws in the company's crisis communications strategy turned its crisis into a public relations "dumpster fire."

Now that we understand how the fundamentals of crisis management relate to data breaches, let's use this to devise a model for our response.

This page intentionally left blank

Chapter 4

Managing DRAMA

Thirty-five thousand strange and unexpected letters silently landed in mailboxes across California in February 2005. Like the first signs of an oil spill washing up on shore, the messages were a quiet harbinger of a massive crisis that was about to bubble up.

Sixty-one-year-old California resident Mary Chapman opened the letter. It was from a company she had never even heard of before: ChoicePoint, Inc. The letter read:

> I'm writing to inform you of a recent crime committed against ChoicePoint that MAY have resulted in your name, address, and Social Security number being viewed by businesses that are not allowed access to such information. We have reason to believe your personal information may have been obtained by unauthorized third parties, and we deeply regret any inconvenience this event may cause you.
>
> . . . We believe that several individuals, posing as legitimate business customers, recently committed fraud by claiming to have a lawful purpose for accessing information about individuals, when in fact, they did not.[1]

Chapman was furious—and not just because of the fraud. "I'm angry that a company is out there selling my personal information for monetary gain. Yes, I'm angry. I'm very angry," said Chapman.[2]

She was not alone. What was ChoicePoint, and why was it selling people's personal information? At the time, ChoicePoint was the nation's leading provider of background checks—but because its customers were businesses and governments, few consumers had heard of the company. "Although not a household name, it maintains what it claims is the largest collection of court records, addresses and other public data on people in the country—some 19 billion

1. "ChoicePoint's Letter to Consumers Whose Information Was Compromised," *CSO*, May 1, 2005, http://www.csoonline.com/article/2118059/data-protection/choicepoint-s-letter-to-consumers-whose-information-was-compromised.html.

2. Sarah D. Scalet, "The Five Most Shocking Things About the ChoicePoint Data Security Breach," *CSO*, May 1, 2005, https://www.csoonline.com/article/2118134/compliance/the-five-most–shocking-things-about-the-choicepoint-data-security-breach.html.

records in all."[3] The company was spun off from Equifax in 1997, reportedly in part to enable it to sell data without being subject to the regulation of a financial services firm.[4]

"Even though you might not have heard of ChoicePoint, they've heard of you," said Daniel Solove, a professor at George Washington University, after the theft was announced. "They are playing a role in . . . people's lives whether they know it or not."[5]

The notification letters sparked a massive national investigation and public response. By the time the crisis was resolved:

- 163,000 consumers were notified that their personal details had been sold to criminals.
- At least 800 cases of identity theft resulted from the breach, according to the FTC.
- ChoicePoint paid $10 million to settle a class-action lawsuit by consumers.
- The Federal Trade Commission (FTC) fined ChoicePoint $15 million (consisting of a $10 million fine and a $5 million fund to help consumers). At the time, this was "the largest civil penalty over data security in the agency's history."[6]
- Forty-four attorneys general formed a coalition and sued the company in a case that dragged on for years (ultimately the parties settled for $500,000 and agreement that ChoicePoint would implement better security for all consumer records, not just those protected under the Fair Credit Reporting Act).
- ChoicePoint was subjected to a consent decree requiring it to implement stronger security measures for protecting consumer data under the Fair Credit Reporting Act and undergo regular third-party security audits until 2026.
- ChoicePoint voluntarily announced that it would limit its sales of sensitive consumer information.[7]
- ChoicePoint purchased credit reports and one year of credit monitoring for affected consumers (after significant public outcry).
- The Securities and Exchange Commission (SEC) conducted a three-year investigation into ChoicePoint executives' sale of company stock shortly before the breach was announced.[8]

---

3. Joseph Menn, "Fraud Ring Taps Into Credit Data," *Los Angeles Times*, February 16, 2005, http://articles.latimes.com/2005/feb/16/business/fi-hacker16.

4. Paul N. Otto, Annie I. Antón, David L. Baumer, "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information," *North Carolina State University Technical Reports*, TR-2005-18, p. 2, https://repository.lib.ncsu.edu/bitstream/handle/1840.4/922/TR-2006-18.pdf?sequence=1&isAllowed=y (accessed May 14, 2019).

5. Bob Sullivan, "Database Giant Gives Access to Fake Firms," *NBC News*, February 14, 2005, http://www.nbcnews.com/id/6969799/print/1/displaymode/1098.

6. Bob Sullivan, "ChoicePoint to Pay $15 Million over Data Breach," *NBC News*, January 26, 2006, http://www.nbcnews.com/id/11030692/ns/technology and science-security/t/choicepoint-pay-million-over-data-breach/.

7. "ChoicePoint Stops Selling 'Sensitive Consumer Data,' Confirms SEC Investigation," *Chief Marketer*, March 6, 2005, http://www.chiefmarketer.com/choicepoint-stops-selling-sensitive-consumer-data-confirms-sec-investigation.

8. "ChoicePoint Stops Selling."

- ChoicePoint's chief executive officer (CEO) and chief operating officer (COO) were grilled by Congress.
- Twenty-two states enacted data breach notification laws before the end of the year, with more to follow in subsequent years.
- ChoicePoint was widely labeled the "poster child for data-loss incidents,"[9] a title that it owned for years until the 2007 TJ Maxx and later 2013 Target breaches overshadowed it.

Why did the ChoicePoint breach, in particular, generate such an intense public reaction? The answer lies in ChoicePoint's *response* to the breach, particularly in the early phases. From the outside—media reports, congressional testimony, FTC and SEC investigations—ChoicePoint leadership appeared incompetent at best and downright criminal at worst. (This is not to say they were, but appearances matter.) Inside, there is evidence that the organization was staffed by people who were intelligent, well meaning, and caring—yet woefully unprepared for the crisis.

In this chapter, we will analyze the ChoicePoint crisis in the context of Steven Fink's four phases: prodromal, acute, chronic, and resolution (see § 3.1.4). Traditionally, data breaches have been managed as *incidents* rather than *crises*, leading to response plans that get thrown aside when a real breach occurs.

Instead, we will introduce a new model for managing data breaches, based on the concept that a breach is a crisis. The result is a useful model that summarizes the overarching response goals at each phase:

- **Develop** your data breach response function.
- **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
- **Act** quickly, ethically, openly, and empathetically to minimize the impact of a breach.
- **Maintain** data breach response efforts throughout the chronic phase, and potentially long-term.
- **Adapt** proactively and wisely in response to a potential data breach.

All of these capabilities must exist simultaneously, although specific functions tend to be used more at certain phases of the data breach crisis.

The acronym for our data breach response model is "DRAMA," which is easy to remember since it is designed to help us manage (and hopefully reduce) drama! Throughout this chapter, we will step through the ChoicePoint breach and tie each phase to our DRAMA response model.

4.1 The Birth of Data Breaches

There had been other breaches, bigger breaches, even around the same time period. "That same month, February, saw stories that had bigger numbers (Bank of America, 1.2 million

9. Dan Kaplan, "ChoicePoint Settles Lawsuit over 2005 Breach," *SC Media US*, January 28, 2008, https://www.scmagazine.com/choicepoint-settles-lawsuit-over-2005-breach/article/554149.

names and Social Security numbers [SSNs]) and more sex appeal (T-Mobile, Paris Hilton) than the predictable details of the ChoicePoint case," commented Sarah Scalet of *CSO* magazine. "Thousands of victims, compromised SSNs, an arrest on charges of identity theft. Yada yada yada. But somewhere along the way, the ChoicePoint saga became the spark that caused an explosion."[10]

ChoicePoint was arguably the first modern "megabreach"—not because of the volume or type of data that was exposed, but because of how the company responded.

4.1.1 Data Breaches: A New Concept Emerges

"I certainly wasn't thinking of the words 'cyber' and 'security' at the time. Those words weren't forefront on my mind."

Attorney Chris Cwalina sat across the table from me, sipping sparkling water on a warm fall evening in Virginia. Chris was not just a veteran of data breach industry—he was one of the first attorneys to help manage a modern data breach crisis. Chris had been hired by the general counsel of ChoicePoint shortly after the breach became public to act as ChoicePoint's "quarterback," helping to manage the ensuing litigation and investigations, together with a large team of experts.

Before the ChoicePoint case, *data breaches* didn't exist, at least not as a concept defined by law separate from other types of accidents or security incidents. "I was thinking these were bad guys who fraudulently deceived the company into giving them valuable information," recalled Chris. "This was like a *theft*, a successful theft."

That changed on February 17, 2005, just days after the ChoicePoint "theft" was announced. The *Los Angeles Times* printed a landmark article quoting U.S. Senator Dianne Feinstein: "Data breaches are becoming all too common, and current federal law does not require notification to consumers." It was possibly the first time that any legislator had been quoted in the mainstream media using the term "data breach."[11] Indeed, it was one of the first times that the term had ever been used at all in any publication, anywhere, save for a few isolated instances, typically used in headlines as a shortened version of "cardholder data breach."[12]

In the same article, Beth Givens, founder of the Privacy Rights Clearinghouse (PRC), stated: "A data breach affecting ChoicePoint is akin to the pot of gold at the end of the rainbow." There it was again! The new term, "data breach," went viral shortly thereafter, popping up in hundreds of publications over the coming months.

4.1.2 The Power of a Name

Once the concept was given a name, suddenly the public had the power to talk about the problem—and to track it. The PRC created its popular online database, "A Chronology of

10. Scalet, "Five Most Shocking Things."

11. Joseph Menn and David Colker, "More Victims in Scam Will Be Alerted," *Los Angeles Times*, February 17, 2005, http://articles.latimes.com/2005/feb/17/business/fi-hacker17.

12. L. Kuykendall, "BJ's Case Shows Issuers' Data-Breach Cost Fatigue," *American Banker*, August 26, 2004.

Data Breaches," which lists all "reported data breaches from 2005 to present."[13] What most people don't realize is that the database was *originally* named "A Chronology of Data Breaches Reported Since the ChoicePoint Incident."[14] A simple introduction on the website stated:

> The data breaches noted below have been reported because the personal information compromised includes data elements useful to identity thieves, such as Social Security numbers, account numbers, and driver's license numbers. The catalyst for reporting data breaches to the affected individuals has been the California law that requires notice of security breaches, the only state in the nation to have such a law at this time.

Yes! The ChoicePoint case literally inspired people to begin tracking this newly defined thing, the "data breach." Since that time, the PRC updated the database to include data breaches from January 1, 2005, onwards.

Effectively, 2005 is "Year 0" for data breaches. In this book, we consider January 1, 2005, the beginning of "data breaches" as an event tracked distinctively from other cybersecurity-related incidents.

4.2 A Smoldering Crisis

Crisis management experts often talk about two kinds of crises: *sudden* and *smoldering*. Sudden crises are what they sound like: "unexpected events in which the organization has virtually no control and perceived limited fault or responsibility." The Tylenol product tampering case from 1982 is a good example of a sudden crisis, in which no one reasonably foresaw that a murderer would insert poison into packages of painkillers. Johnson & Johnson emerged from the crisis with the reputation of a good corporate citizen that took quick action when a murderer struck.

The ChoicePoint breach, on the other hand, is an example of a smoldering crisis. These start out as "small, internal problems within a firm, become public to stakeholders, and, over time, escalate to crisis status as a result of inattention by management." Smoldering crises "are generally perceived as the responsibility and fault of a firm's leadership."[15]

For more than two years, criminals used stolen identities to acquire fake business licenses and then faxed their applications to ChoicePoint from Kinko's stores and similar locations. Since the stolen identities had no criminal backgrounds, the scammers sailed through ChoicePoint's own application background check process. Researchers later reported that once a ChoicePoint customer received account credentials, "that individual or business enjoyed

13. *Chronology of Data Breaches: FAQs*, Privacy Rights Clearinghouse, https://www.privacyrights.org/chronology-data-breaches-faq#is-chronology-exhaustive-list (accessed October 14, 2016).

14. *A Chronology of Data Breaches Reported Since the ChoicePoint Incident*, Privacy Rights Clearinghouse, April 20, 2005, http://web.archive.org/web/20050421104632/http://www.privacyrights.org/ar/ChronDataBreaches.htm.

15. Erica H. James and Lynn P. Wooten, "Leadership in Turbulent Times: Competencies for Thriving Amidst Crisis," (Working Paper No. 04-04, Darden Graduate School of Business Administration, University of Virginia, 2004), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=555966.

largely unsupervised and unfettered access to the wealth of information inside ChoicePoint's databases. The major hurdle appears to have been the initial identity verification, which was easily bypassed using stolen identities."[16] Identity theft led to more identity theft.

In this section, we will discuss how the emerging crime of identity theft, ChoicePoint's own rush to accumulate personal information, and the increasing use of data as "access devices" laid the groundwork for what would soon become ChoicePoint's crisis.

4.2.1 The Identity Theft Scare

At the time that the ChoicePoint breach occurred, Americans were already reeling with the growing epidemic of "identity theft," bombarded with nightmarish stories of people like Michael Berry, an average citizen who found himself wanted for murder because a criminal had created a fake driver's license in his name.[17] A news story in the *New York Times* highlighted another example, that of Brent James of Arizona, who suddenly began receiving calls from a collections agency, harrassing him about defaulted loans he had never taken out. James discovered that "someone had entered into two cellphone contracts and bought a car in his name. And though Mr. James and his wife have owned a home since 2000, he also has 'multiple personal judgments against [him]' by landlords suing over a broken lease."[18]

The *Washington Post* reported that the ChoicePoint breach "comes at a time when identity fraud and theft are on the rise, with as many as 10 million Americans a year falling victim to criminals who charge goods in their names or empty their bank accounts."[19] According to the FTC, in 2005 identity theft was the top consumer concern for the sixth year in a row.[20]

4.2.2 The Product Is . . . You

At the same time, entrepreneurs were beginning to recognize the massive potential value of personal information within the "legitimate" economy. As ChoicePoint had, companies could sell personal information to creditors, insurance companies, employers, and the federal government.

The *Wall Street Journal* reported that ChoicePoint and its peers allowed federal agencies to do an "end run" around the domestic privacy protections of the 1974 U.S. Privacy Act. "ChoicePoint and its rivals specialize in doing what the law discourages the government from doing on its own—culling, sorting and packaging data on individuals from scores of sources, including credit bureaus, marketers and regulatory agencies."[21]

---

16. Otto, Antón, and Baumer, "ChoicePoint Dilemma," 2.

17. Center for Investigative Reporting (CIR), "Identity Crisis," *CIR Online*, August 9, 2003, https://web.archive.org/web/20150526053835/http://cironline.org/reports/identity-crisis-2085.

18. Gary Rivlin, "Purloined Lives," *New York Times*, March 17, 2005, http://www.nytimes.com/2005/03/17/business/purloined-lives.html?%20r=0.

19. Robert O'Harrow Jr., "ID Data Conned from Firm: ChoicePoint Case Points to Huge Fraud," *Washington Post*, February 17, 2005, http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html.

20. Otto, Antón, and Baumer, "ChoicePoint Dilemma," 2.

21. Glenn R. Simpson, "FBI's Reliance on the Private Sector Has Raised Some Privacy Concerns," *Wall Street Journal*, April 13, 2001, http://www.wsj.com/articles/SB987107477135398077.

4.2.3 Valuable Snippets of Data

ChoicePoint accumulated personal information because it was useful for many kinds of business purposes: employee background checks, customer credit verification, and more. The reason this was so dangerous is because at the same time, some of these little snippets of personal information (names, SSNs, phone numbers, etc.) were increasingly used as keys to facilitate access to various accounts and valuable assets.

In the United States, the SSN is a prime example: a simple nine-digit number that has been used far beyond its original design purpose. According to the Social Security Administration:[22]

> The Social Security number (SSN) was created in 1936 for the sole purpose of tracking the earnings histories of U.S. workers, for use in determining Social Security benefit entitlement and computing benefit levels. Since then, use of the SSN has expanded substantially. Today the SSN may be the most commonly used numbering system in the United States. As of December 2008, the Social Security Administration (SSA) had issued over 450 million original SSNs, and nearly every legal resident of the United States had one. The SSN's very universality has led to its adoption throughout government and the private sector as a chief means of identifying and gathering information about an individual.

Today, U.S. citizens use SSNs to:

- Gain access to bank accounts over the phone
- Get approved for a credit card
- Obtain a tax refund
- Gain access to medical records
- Verify identity and gain access to a wide variety of sensitive information and accounts

Criminals can use stolen SSNs for much the same purposes. "Together with other basic information, like name and date of birth, the Social Security number is a passport to a person's identity," wrote *Bloomberg* columnist Suzanne Woolley in 2017.[23]

4.2.4 Knowledge-Based Authentication

What makes the SSN so powerful? The SSN is often used, either implicitly or explicitly, to *authenticate* a person. *Authenticate* means to *verify a person's identity*.

22. Carolyn Puckett, "The Story of the Social Security Number," *Social Security Bulletin* 69, no. 2 (2009), https://www.ssa.gov/policy/docs/ssb/v69n2/v69n2p55.html.

23. Suzanne Woolley, "Your Social Security Number Now Looks Like a Time Bomb. It Is," *Bloomberg*, June 1, 2017, https://www.bloomberg.com/news/articles/2017-06-01/identity-theft-feeds-on-social-security-numbers-run-amok.

Cybersecurity professionals like to say that you can authenticate a person in one of three ways, using:

1. *Something you know*, such as a password or confidential personal information
2. *Something you have*, such as a driver's license number or hardware token
3. *Something you are*, such as your fingerprint or iris pattern

(There are other methods, such as *somewhere you are* or *something you can do*, but the three methods above are by far the most common.)

When I call my bank and the receptionist asks for my name and SSN, she *authenticates* me, or verifies my identity, using that special piece of data—an example of type 1 authentication (something you know), also known as knowledge-based authentication.

4.2.5 Access Devices

Your SSN, of course, is hardly the only example of a sensitive piece of data that is used to access valuable assets. Payment card information, driver's license numbers, and even passwords are used similarly. This concept is reflected in U.S. law, which defines the general term "access device" (18 U.S.C. §1029(e)(1)).

> [T]he term "access device" is used in the statute and is defined broadly as any "card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds. . . ." The only limitation, i.e., "other than a transfer originated solely by paper instrument," excludes activities such as passing forged checks.[24]

Your SSN has great potential: You can use it to gain access to your bank account or your medical records, to get approved for a credit card, to obtain your tax refund. By nature, any data classified as an "access device" has this potential utility and is therefore a valuable asset. And where there are valuable assets, there is crime.

Your SSN Has Already Been Stolen

Unfortunately, there is ample evidence that most, if not all, SSNs have already been stolen (and already were, long before the infamous 2017 Equifax breach). Consider just the following two data breach cases:

(*Continues*)

24. U.S. Department of Justice, "1030. Definitions," *Criminal Resource Manual*, https://www.justice.gov/usam/criminal-resource-manual-1030-definitions (accessed January 8, 2018).

(*Continued*)

Court Ventures (Experian subsidiary) (October 2013, 200 million records): Experian subsidiary Court Ventures, Inc., was outed in 2013 for giving a major identity theft ring "direct access to personal and financial data on more than 200 million Americans."[25] The ringleader, Hieu Minh Ngo, purchased consumer data from Court Ventures and routinely paid for it using overseas cash wire transfers.

Anthem (February 2015, 78.8 million records): Anthem announced that it had been the victim of a targeted cybersecurity attack, and eventually disclosed that the theft included 78.8 million people's records, including—you guessed it—SSNs, as well as "names, birthdays, medical IDs, street addresses, email addresses and employment information, including income data."[26]

Between just these two cases, approximately 278.8 million SSNs were exposed. The current U.S. population is estimated at 325 million people,[27] approximately 250 million of which are adults.[28] That means that the volume of SSNs exposed in these two breaches alone exceeds the number of adults in the United States.

Of course, there is no way for us to know how many of those numbers were duplicated across the data sets exposed or how many records were exposed to risk but never used by criminals. On the flip side, there have also been many other breaches exposing SSNs.[29] Prior to 2003, there was no law that required an organization to report a SSN theft at all—and those numbers are still in use.

"[T]he United States has a big problem," wrote reporter Lily Hay Newman of *Slate* magazine, in the aftermath of the Equifax breach. "It seems that no one's Social Security number is safe; if yours hasn't been compromised yet, it probably will be soon, given the high rate of large-scale data breaches."[30]

4.3 Prodromal Phase

The ChoicePoint breach unfolded slowly over a long period. Along the way, there were many signs—large and small—that could have alerted ChoicePoint staff that something was amiss,

25. Brian Krebs, "At Experian, Security Attrition Amid Acquisitions," *Krebs on Security* (blog), October 8, 2015, https://krebsonsecurity.com/tag/court-ventures.

26. Anthem, "Attention Providers in Virginia: Important Message from Joseph Swedish," *Network eUpdate*, February 5, 2015, https://www11.anthem.com/provider/va/f1/s0/t0/pw_e231507.pdf.

27. U.S. Census Bureau, U.S. *and World Population Clock*, https://www.census.gov/popclock (accessed January 8, 2018).

28. U.S. Census Bureau, *Quick Facts: United States*, https://www.census.gov/quickfacts/table/PST045216/00 (accessed January 8, 2018).

29. *Data Breaches*, Privacy Rights Clearinghouse, https://www.privacyrights.org/data-breaches (accessed January 8, 2018).

30. Lily Hay Newman, "The Social Security Number's Insecurities," *Slate*, July 10, 2015, http://www.slate.com/articles/technology/future_tense/2015/07/opm_anthem_data_breaches_show_the_insecurity_of_the_social_security_number.html.

but in hindsight it was clear that the organization simply did not have processes in place to recognize, escalate, and investigate suspicious activity. What's more, ChoicePoint's information control practices had major gaps, but management did not notice.

In this section, we will step through the prodromal phase of the ChoicePoint crisis and highlight ways that ChoicePoint could have caught the crisis before it exploded into the acute phase.

4.3.1 The Smoldering Crisis Begins . . .

Criminals began setting up fraudulent customer accounts as early as September 2003, more than two years before management became aware of the suspicious accounts. Were the fraudsters extremely sophisticated or stealthy? No. According to a subsequent FTC complaint, ChoicePoint didn't detect the fraudulent application "because it had not implemented reasonable procedures to verify or authenticate the identities and qualifications of prospective subscribers."[31]

The FTC provided specific examples of ChoicePoint's failure to detect and report suspicious activity, such as:[32]

> . . . b. ChoicePoint accepted for verification purposes documentation that included facially contradictory information, such as different business addresses on federal tax identification documents and utility statements, without conducting further inquiry to resolve the contradiction;
>
> c. ChoicePoint accepted other forms of facially contradictory or illogical application information, such as articles of incorporation that reflected that the business was suspended or inactive, and tax registration materials that showed that the business' registration was cancelled a few days prior to the date the application was submitted to ChoicePoint . . . ;
>
> . . . e. ChoicePoint approved, without further inquiry, the applications of subscribers notwithstanding the fact that the applicant left critical information, such as business license number, contact information, or applicant's last name, blank on the application;
>
> f. ChoicePoint accepted applications transmitted by facsimile from public commercial locations, and accepted multiple applications for putatively separate businesses from the same facsimile numbers . . . ;
>
> g. ChoicePoint accepted and approved, without further inquiry, the applications of subscribers notwithstanding the fact that ChoicePoint's own internal reports on the applicant linked him or her to possible fraud associated with the Social Security number of another individual.

Each of these examples includes a prodrome—a warning sign that, if recognized, could have allowed the company to avert the acute phase of the crisis. Really, one of the most shocking

31. United States v. ChoicePoint Inc., CA No. 1:06-CV-0198 (N.D. Ga. 2006), https://www.ftc.gov/sites/default/files/documents/cases/2006/01/0523069complaint.pdf.

32. United States v. ChoicePoint, CA No. 1:06-CV-0198, at 5–6.

things about the ChoicePoint breach was that it consisted of many repeated individual frauds, which occurred over and over during a period of years, without any response.

4.3.2 Isn't It Ironic?

Despite the growing concern about identity theft and fraud, ChoicePoint didn't seem to treat its massive database of sensitive consumer data like hazardous material that needed careful control. After the breach was announced, the news ran story after story with examples of ChoicePoint's lax information control practices. The *Wall Street Journal* reported, "[O]ne could even buy ChoicePoint background-check kits at Sam's Club for $39.99, though ChoicePoint says it required buyers to prove valid business purposes for using them."[33]

Unfortunately, ChoicePoint itself did not appear to make smart decisions about approving customer applications. This was all the more damning because, according to ChoicePoint's chairman and CEO, Derek V. Smith, "ChoicePoint's core competency [was] verifying and authenticating individuals and their credentials."[34] During his tenure as CEO of ChoicePoint, Smith authored two books about information security and risk. When the company was spun out from Equifax in 1997, it "took the name of ChoicePoint, signaling that it would help clients make smart decisions when they reach a 'choice point.'"[35]

The irony was not lost on the media, which raked ChoicePoint over the coals for it. "ChoicePoint has just thrust itself into the nation's consciousness as a conglomerate hoist by its own petard," wrote the *New York Times*. "The outfit that sells the ability to anticipate suspicious activity; that provides security to the nation's security services; that claims it protects people from identity theft—has been easily penetrated by a gang that stole its dossiers on at least 145,000 people across the country."[36]

4.3.3 A Suspicious Phone Call

ChoicePoint, as an organization, only began to realize there was a serious problem in September 2004, when a staff member received a suspicious phone call. The *Wall Street Journal* later reported:[37]

> The company said a caller with a distinctive foreign accent, identifying himself as James Garrett of MBS Collections, applied for an account that would give him access to ChoicePoint data. In another phone call, what sounded like the same man identified himself as John Galloway of Gallo Financial, also applying for an account. Faxed driver's licenses for both applicants arrived, with photos that, like the voices, seemed identical.

---

33. Evan Perez and Rick Brooks, "For Big Vendor of Personal Data, a Theft Lays Bare the Downside," *Wall Street Journal*, May 2, 2005, https://www.wsj.com/articles/SB111507095616722555.

34. Bruce Schneier, "ChoicePoint," *Schneier on Security* (blog), February 23, 2005, https://www.schneier.com/blog/archives/2005/02/choicepoint.html.

35. Evan Perez and Rick Brooks, "For ChoicePoint, a Theft Lays Bare the Downside," *Pittsburgh Post-Gazette*, May 3, 2005, http://www.post-gazette.com/business/businessnews/2005/05/03/For-ChoicePoint-a-theft-lays-bare-the-downside/stories/200505030214.

36. William Safire, "Goodbye to Privacy," *New York Times*, April 10, 2005, https://www.nytimes.com/2005/04/10/books/review/goodbye-to-privacy.html.

37. Perez and Brooks, "For Big Vendor."

ChoicePoint staff alerted the Los Angeles sheriff's department, which immediately opened an investigation. "When 'James Garrett' called again, the firm, at a detective's instruction, told him to go to a Copymat store on Sunset Boulevard to pick up a fax. There, investigators confronted a man named Olatunji Oluwatosin. He dropped to the ground ChoicePoint applications that bore both the MBS and Gallo business names."[38] Oluwatosin was arrested. A Nigerian citizen, he ultimately pled no contest to identity theft and was sentenced to 16 months in prison. Later, investigators determined that Oluwatosin was part of a larger identity theft crime ring, which sold stolen identities on the black market for "$2,000 to $7,000 each."[39]

Evidence gathered from Oluwatosin's apartment indicated that he had been regularly accessing ChoicePoint's databases for an extended period without sending up any red flags. "On Mr. Oluwatosin's kitchen counter, detectives found printouts from ChoicePoint databases, showing that ChoicePoint accounts had been used to make 17,000 searches," according to an L.A. sherriff's detective.[40]

A *Wall Street Journal* reporter was apparently able to review the customer applications dropped by Oluwatosin on the day of his arrest. "The applications . . . suggest how much ChoicePoint depended on the honor system in deciding whom to let see its trove of personal information. A one-page form asked the applicant for basic data such as phone and fax numbers, a business-license number and an email address. In a field asking for the proposed business use for the databases, 'James Garrett' and 'John Galloway' wrote, 'We use the services for collecting debt.'"[41]

4.3.4 Hiding in Plain Sight

A data breach can affect the organization as a whole, right down to the very valuation of an entire company. Therefore, it's not enough for a small group of people within one or two departments to *detect* and *analyze* the event. An individual team siloed in a single department may not have the visibility to independently assess the potential risk to the organization as a whole or the reach to take the cross-organizational actions necessary to respond appropriately.

Organizations need to have a process in which first responders *recognize an event as a potential data breach* and *escalate* it to the appropriate decision makers for further guidance. Then, appropriate personnel need to *investigate* and gather input from potentially many areas of the organization—such as IT, compliance, legal, public relations—and evaluate it all together in order to understand the *scope* of the problem and determine the best next steps for the organization.

This process—recognition, escalation, investigation, and scoping—is all part of a larger phase of the incident response process in which the organization *realizes* that the data breach exists. According to the *Oxford English Dictionary*, "realize" means "to become fully aware of (something) as a fact; understand clearly." The different activities (recognition, escalation, investigation, and scoping) tend to overlap, and multiple activities occur simultaneously.

---

38. Perez and Brooks, "For Big Vendor."

39. Perez and Brooks, "For Big Vendor."

40. Perez and Brooks, "For Big Vendor."

41. Perez and Brooks, "For Big Vendor."

Realizing that a potential data breach exists and working to understand it as clearly as possible require cross-organizational efforts, typically conducted with input at all levels from first responders to the executive team (and nowadays, even the board of directors).

4.3.5 Recognize

According to a former ChoicePoint executive, Mimi Bright Ribotsky, ChoicePoint staff often talked about how difficult it was to verify the legitimacy of customers, but did not fully appreciate the potential impact of the problem. "I didn't think people realized what could happen as far as information getting into the wrong hands," she said.[42]

Therein lies much of the issue: Often, front-line staff members notice a suspicious event, a gap in process, or a vulnerability, but do not recognize the potential for catastrophic impact on the organization. And why would they, without the high-level view? In order for front-line staff members to recognize an issue as a potential data breach, the organization first needs to develop a process and provide tools and training to assist staff in recognizing symptoms.

4.3.6 Escalate

Someone within ChoicePoint alerted law enforcement—that we know. However, he or she apparently didn't alert ChoicePoint executives. "ChoicePoint's vice president testified in the Senate that he was the first executive to learn of the data breach, finding out in mid-November."[43] CEO Derek Smith was reportedly "in the dark about the exposure for two months after it was detected last fall." Smith reported that he was first informed of the crime in "January, or perhaps 'late December.'"[44]

That meant even as law enforcement carried reams of paper with ChoicePoint data out of rooms belonging to a Nigerian identity thief, executives apparently were going about their days, thinking everything was business as usual. As a result, the executive team was not involved in the first weeks (perhaps even months) of the breach response. During those crucial weeks while the crisis was building, ChoicePoint was unable to strategize, gather information, or take action at that executive level. The CEO was later blindsided by the extent of the problem and had to make critical decisions under enormous pressure.

If the executive team had been informed immediately of the suspected crime, ChoicePoint may well have been in a better position. Derek V. Smith himself was a thoughtful CEO. Before ChoicePoint's breach was discovered, he wrote in a book: "What keeps me awake is the knowledge that so many of the tragedies—small and large—that we see every day could have been prevented or reduced if only the right well-meaning person had the right information at the precise moment they needed to make a well-informed decision."[45]

---

42. Perez and Brooks, "For Big Vendor."

43. Otto, Antón, and Baumer, "ChoicePoint Dilemma."

44. Otto, Antón, and Baumer, "ChoicePoint Dilemma."

45. Derek V. Small, *Risk Revolution: The Threat Facing America and Technology's Promise for a Safer Tomorrow* (Lanham, MD: Taylor Trade, 2004).

Indeed! If only ChoicePoint's front-line staff had known to reject fraudulent applications or, at least after the fact, escalate to the executive team immediately so they could make a "well-informed decision."

"The escalation path is actually harder than it seems," said Chris Cwalina. "When we do exercises, [we often find that] what the incident response team thought was an appropriate level of escalation [is different from] the expectations of senior management and the board-level people. Characterization and severity level designation can be equally challenging."

For example, your board members might expect to hear about a suspected data breach in a very early phase, whereas IT staff might be inclined to wait and escalate only after there is solid proof that a breach occurred. It's critical to involve staff at every level of the organization in the data breach planning process and tabletop exercises, to ensure everyone is on the same page.

4.3.7 Investigate

> From the airline ticket agent who allowed the September 11th terrorists onto airplanes to the minister who allowed a convicted sex offender to lead Sunday School and Scout groups—seemingly minor decisions made without the benefit of modern information tools can go terribly awry.[46]—Derek V. Smith, CEO of ChoicePoint, 2004.

(Not to mention the decision made by the ChoicePoint clerk who approved Oluwatosin's customer application . . . You just can't make this stuff up!)

The executives at ChoicePoint were deeply aware that knowledge is power and that "modern information tools" enabled organizations to make smarter decisions. This was the core of their business model, their sales pitch. And yet, somehow they appeared to have forgotten this when it came to management of their own company's operations.[47] When the breach hit, ChoicePoint struggled to understand exactly what had happened because it had limited information about access to its own crown jewels. As the *Wall Street Journal* reported:[48]

> ChoicePoint Inc. has 19 billion data files, full of personal information about nearly every American adult. In minutes, it can produce a report listing someone's former addresses, old roommates, family members and neighbors. The company's computers can tell its clients if an insurance applicant has ever filed a claim and whether a job candidate has ever been sued or faced a tax lien.
>
> But last October, after its databases were accessed by a man bent on identity theft, there was one thing ChoicePoint struggled to do: Figure out just what records had been stolen.
>
> "They said it was a huge task and they didn't have the staff to do it," says Lt. Robert Costa, head of the Los Angeles County sheriff's department identity-theft squad. "Apparently their technology wasn't built so you were able to find the electronic footsteps these guys left."

---

46. Derek V. Small, *Risk Revolution: The Threat Facing America and Technology's Promise for a Safer Tomorrow* (Lanham, MD: Taylor Trade, 2004).

47. Perez and Brooks, "For Big Vendor."

48. Evan Perez and Rick Brooks, "For Big Vendor of Personal Data, a Theft Lays Bare the Downside," *Wall Street Journal*, May 3, 2005, https://www.wsj.com/articles/SB111507095616722555?mg=id-wsj.

4.3.7.1 Got Logs?

To this day, lack of available evidence remains one of the most critical challenges in data breach investigations. "*Logging and forensic artifacts* is the biggest issue we have as lawyers [working on a data breach case]," Chris Cwalina confided. "More often than not, we don't have the logs or the evidence we wish we had."

What are "logs," and why are they so important? A log is simply *a record of an event*. There are many types of logs—logs that track when someone signs on to a computer, logs that record the size of a packet that traversed a firewall, logs that indicate when antivirus software detected malicious code. Logs can help you determine whether an attacker stole one person's or 10,000 people's health information.

Unfortunately, in many organizations, logs are sparse or nonexistent. "More often than not the log capability was there, but it either wasn't turned on . . . or not retained long enough," said Chris.

All too often, logs "roll over" or are automatically deleted after a short time (days or weeks), based on a specific date or log volume. Sometimes, the response team doesn't realize they need a log until several months into the investigation, and by the time they look, it is gone. This is why it's critical to *preserve* any records you think you might possibly need right at the beginning of the investigation. Remember, preservation is relatively cheap. Analysis is typically far more resource intensive. You don't have to analyze every piece of evidence you collect, but if you decide down the road that you need something, you won't have the opportunity to go back in time and preserve it. Cast a wide net early on.

"I can only speak to the cases I worked on," said Chris. "But in a lot of these big notification cases that we've seen, my guess is the lawyers were left with nothing definitive to hang their hat on. On the one hand, you might have IT people saying, 'Well, we can't rule it out. We can't rule it out.' And then on the other hand, the lawyers saying, 'Well, if access or acquisition can't be ruled out, then we can't rule out misuse, so it might be best to notify everybody, in an abundance of caution.'" In other words, Chris suspects that in a number of incidents individuals whose information was not really at risk were notified anyways. "If you had the logs you might be able to learn that actually a lot of the data didn't get out of the door. 'Logs' is something that should be in bold with exclamation points."

4.3.7.2 Logs!!

At ChoicePoint, the team collected both physical and digital evidence and had to correlate data from multiple sources in order to piece together the puzzle. "The bad guys had used the printer [at their facilities]. In some instances they had set up actual offices," described Chris. "Law enforcement found storage rooms with the paper. There was a federal and state law enforcement investigation that was very thorough and very good. They tracked down and found the culprits and found caches of documents. We literally found boxes of documents."

The criminals had accessed the records online, logging in with usernames and passwords, and then ran searches and printed the results. Since the material was accessed online, ChoicePoint also had some electronic records. "We had logs of username and password access. . . . There were many accounts that were fraudulent," described Chris. "We were trying to determine, based on our access logs, what was the scope of information that [the criminals] potentially had access to? As you can imagine, that was a lengthy, complicated process."

Why so complicated? Simply having logs is not enough. You also have to understand exactly what they mean—a process that seems more straightforward than it really is. All too often, response teams find themselves reviewing logs for the first time during the data breach crisis. It's not always clear what each field means, and there's often little or no documentation about the record format. This seemingly simple problem can lead to errors or delays that ultimately can destroy a company's reputation.

In the case of ChoicePoint, the public wanted answers. Whose records were accessed?

Senior management wanted answers, too. "They wanted to make sure we had all the details right, that all of the affected individuals were notified," reminisced Chris. But getting the details right wasn't so simple. "With any investigation, especially related to IT, the facts change," said Chris. "That's the nature of the beast with IT-related incidents. It was very frustrating for senior management that things would change, numbers would change."

Chris gave an example in which the investigative team might find one set of logs and conclude that a line item indicated an HTTP "GET" request, which meant that a customer had accessed a record. Later, the investigative team would correlate that first log with another set of logs and realize that the line item actually meant that the person didn't access the records at all but merely clicked to the next page.

Lack of familiarity with internal logs is one of the biggest factors that slows down a data breach response—along with a lack of access to the logs to begin with. At ChoicePoint, the organization apparently had some logs, but they weren't easy for the response team to understand, and there was no preestablished process for interpreting them.

As a result, ChoicePoint's investigative team would provide executive leadership with a preliminary number and then, a few days later, the team would have to revise it after further analysis. This made public relations very, very difficult.

"Know your logging capabilities," Chris advised. "Think about it now, in advance of an incident. Think about what you currently retain and why. And really think that through with the right people."

4.3.8 Scope

"Senior management was very involved with the investigation," remembered Chris. "They wanted to know [the] scope."

Scoping is a critical (and all-too-often-overlooked) component of data breach response, in which you determine exactly what data, computer systems, physical facilities, or other aspects of the organization are involved in a breach. Basically, you define the area at risk as best you can.

"How did [the criminals] get the data? What data did they get? Do we know what the box is?" Chris gestured, drawing a box in the air with his fingers.

The first step of scoping a data breach is to define the key questions that need to be answered, based on the risks to the organization caused by the potential data breach. Common questions include:

- What type(s) of information may potentially have been exposed?
- Who is affected by the exposure of this information? How many people?

- How much data may have been exposed?
- What laws, regulations, and/or contractual obligations relate?
- What jurisdictions do the affected parties reside in?

In the case of ChoicePoint, the decision makers desperately needed to know precisely whose records were accessed by the criminal. Why was this important? In 2003, California enforced the nation's first security breach notification law. S.B. 1386 "requires any company that stores customer data electronically to notify its California customers of a security breach to the company's computer system if the company knows or reasonably believes that unencrypted [personal] information about the customer has been stolen."[49] The law applied to any company that does business with a California resident, even companies based outside of California. To provide incentive for compliance, California allowed injured customers to "institute civil actions to recover damages."[50]

In other words, if ChoicePoint had exposed any records relating to a California resident, then it was *legally required* to notify the affected person. Since the criminal, Oluwatosin, was living in the Los Angeles area, ChoicePoint (an Atlanta-based company) worked with the local Los Angeles sheriff's office, which instructed ChoicePoint to notify affected consumers in accordance with the new, widely publicized law.[51]

For ChoicePoint, the seemingly simple question of scope took a very long time to answer, due to the issues with its logging process. Initially, the company sent notifications only to residents of California—approximately 30,000 in total. After a massive public outcry from the rest of the country, ChoicePoint conceded that another 110,000 consumers around the nation were affected and would be notified as well. The Los Angeles sheriff's department told the media that criminals could have downloaded records relating to as many as 4 million people. "ChoicePoint disputes that estimate but says the number of victims may grow higher than the 145,000 it has so far acknowledged," responded the beleaguered corporate spokespersons.[52] Even months after the breach was announced, the actual tally of affected persons remained unknown.

If only ChoicePoint could have easily created a report listing all accesses to consumer records! The technology was available, but the company had not deployed it. The fact that it took months and months for executives to understand the actual scope of the breach dramatically impacted their ability to respond and damaged the company's image, as we will see in the next sections.

---

49. FindLaw®, *California Raises the Bar on Data Security and Privacy*, http://corporate.findlaw.com/law-library/california-raises-the-bar-on-data-security-and-privacy.html (accessed January 7, 2018).

50. Official California Legislative Information, *Bill No. SB 1386*, http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html (accessed January 7, 2018).

51. Charles Gasparino, "When Secrets Get Out," *Newsweek*, March 13, 2005, http://www.newsweek.com/when-secrets-get-out-115027.

52. Perez and Brooks, "For Big Vendor."

Realize

During the prodromal phase, your primary response goal is to *realize* that an indicator is a potential warning sign of an impending data breach crisis. "Realize" is the second phase in our DRAMA breach response model. This phase typically requires the following actions:

- **Recognize** the prodromes of a data breach.
- **Escalate** to the data breach response team.
- **Investigate** by preserving and analyzing available evidence.
- **Scope** the breach.

4.4 Acute Phase

Things went from bad to worse very quickly for ChoicePoint as soon as its first consumer notification letters were received in mid-February.

"If the prodromal phase alerts you to the fact that a hot spot is brewing, the acute crisis phase tells you that it has erupted," writes Steven Fink. "One of the major difficulties for managing a crisis during the acute phase is the avalanchelike speed and intensity that often accompany and characterize this phase."[53]

When ChoicePoint's data breach crisis exploded into the public eye, the company made it worse by clamming up, failing to provide clear information, and ultimately failing to manage the public perception of the crisis in a timely and effective manner.

4.4.1 Ain't Nobody Here But Us Chickens

"The man who wrote the book on information security has been conspicuous in his absence this week," reported Bill Husted of the *Atlanta Journal-Constitution*. "Alpharetta-based ChoicePoint faces a public relations nightmare after it sold personal data about consumers to identity thieves posing as legitimate business customers. . . . But since news of the crisis broke, Smith has made no public statements and declined interview requests. That strategy dumbfounds crisis management and marketing experts contacted Friday."[54]

"If it's a national issue, the CEO must be involved. Otherwise he's saying he doesn't care," said crisis management expert Jonathan Bernstein.[55]

53. Steven Fink, *Crisis Management: Planning for the Inevitable* (Lincoln, NE: iUniverse, Inc. 2002), 22.

54. Bill Husted, "Boss Keeps Low Profile Amid Crisis Experts Rap Strategy of ChoicePoint," *Atlanta Journal-Constitution*, February 19, 2005.

55. Husted, "Boss Keeps Low Profile."

"You have to take responsibility publicly," concurred public relations consultant Al Ries of Atlanta. "The CEO should come forward immediately, get on radio and TV and apologize." Instead, Smith disappeared.

4.4.2 Just California . . . Really

The company had initially sent notifications to consumers on February 8, 2005—but only to California residents, the one state in the nation with a law requiring organizations to alert consumers when their "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[56] A ChoicePoint spokesman said, "California is the focus of the investigation and we don't have any evidence to indicate at this point that the situation has spread beyond California."[57]

Few people believed that. Instead, most people assumed that ChoicePoint had notified only Californians because it was not legally required to notify affected individuals in other states. "Right now you've got people in Massachusetts saying, 'Hey, why am I less important than people in California?'" said Matt Stevens, the chief technical officer (CTO) of Network Intelligence.[58]

4.4.3 . . . Oh, and Maybe 110,000 Other People

On the very same day that ChoicePoint said "we don't have any evidence to indicate . . . that the situation has spread beyond California," it posted an announcement on its website stating that "[a]dditional disclosures will be forthcoming to approximately 110,000 consumers outside of California whose information also may have been accessed."[59]

"The number of people being notified that they may have been caught in a massive identity-theft scam quadrupled . . . to 145,000," reported the *Los Angeles Times*. "The company took the step after criticism that it was sending warning letters only to 35,000 possible victims in California, where state law requires such disclosure."[60]

4.4.4 The Explosion

Nineteen state attorneys general released an open letter to the company "demanding that the company respond immediately with details about how it will notify their residents."[61] State and

---

56. Baker Hostetler, "Data Breach Charts," *Baker Law*, November 2017, 25, https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf.

57. Rachel Konrad, "Californians Warned that Hackers May Have Stolen their Data," *USA Today*, February 16, 2005, http://usatoday30.usatoday.com/tech/news/computersecurity/hacking/2005-02-16-choicepoint-hacked_x.htm.

58. Associated Press, "Big ID Theft in California," *Wired*, February 16, 2005, http://web.archive.org/web/20050217193946/http://wired.com/news/business/0,1367,66628,00.html.

59. ChoicePoint, *ChoicePoint Update on Fraud Investigation*, February 16, 2005, https://web.archive.org/web/20050217071222/http://www.choicepoint.com/news/statement_0205_1.html.

60. Menn and Colker, "More Victims."

61. Rachel Konrad, "Data Firm Allowed 700 Identity Thefts: Half-Million Still at Risk at Credit Broker with No Federal Regulation," *Pittsburgh Post-Gazette*, February 19, 2005.

federal legislators took action. Senator Dianne Feinstein used the ChoicePoint case as political capital to push for hearings on a federal data security and breach notification bill.[62]

The public was outraged by the fact that ChoicePoint staff had discovered the fraud in September 2004 but waited until February 2005 to notify victims. During that time, affected consumers were exposed to higher risk of identity theft, but were not aware and could not take appropriate action to reduce their risk of fraud (such as freezing their credit). The longer ChoicePoint waited, the greater the risk was to affected consumers.

According to the *Atlanta Journal-Constitution* "[t]he firm set up no special phone line to handle consumer inquiries."[63] Within a week, the media reported that ChoicePoint had set up a toll-free number to answer questions related to the incident but that it was dysfunctional. For example, NBC News, which broke the story on February 14, 2005, reported that California resident Elizabeth Rosen called the number but was quickly frustrated about the lack of information provided. "[W]hen I called, the person just read from a script . . . they said disclosing too many details may hurt an ongoing investigation," Rosen said. "I'm not happy about this. I didn't even know who ChoicePoint was."[64]

4.4.5 The Blame Game

ChoicePoint representatives blamed law enforcement for the delay in notification, saying that it occurred because police officers had "requested that notification not take place, so as not to compromise the investigation." In response, the Los Angeles County sheriff's office stated that it had told ChoicePoint in November that the company was legally required to notify California residents.[65] Furthermore, police indicated that "ChoicePoint did not appear willing to quickly share information about the case." Robert Costa, lead investigator for the Southern California High Tech Task Force's identity theft detail, told the media, "We've been following up on leads while waiting for ChoicePoint."[66]

As the media storm ensued, ChoicePoint emphasized that it had been the victim of a crime, conceding no wrongdoing. "We're not to blame," said ChoicePoint spokesperson James Lee. The company's unsympathetic letter provided little help for the recipients, recommending only that they "place a fraud alert on [their] credit report[s] by calling the toll-free number of any one of the three credit bureaus listed below," carefully review their credit reports for errors, and contact the credit card companies directly if they notice any suspicious activity.

"The way the letter sounds, it was totally an incident against them, and an 'inconvenience' to us," said Chapman about the notification letter from ChoicePoint. "I'm going to have to watch my back for the rest of my life."[67]

---

62. Menn and Colker, "More Victims."

63. Husted, "Boss Keeps Low Profile."

64. Bob Sullivan, "Database Giant Gives Access to Fake Firms," *NBC News*, February 14, 2005, http://www.nbcnews.com/id/6969799/print/1/displaymode/1098.

65. Evan Perez, "ChoicePoint Is Pressed for Explanations to Breach," *Wall Street Journal*, February 25, 2005, http://www.wsj.com/articles/SB110927975875763476?mg=id-wsj.

66. Robert O'Harrow Jr., "ID Data Conned from Firm: ChoicePoint Case Points to Huge Fraud," *Washington Post*, February 17, 2005, http://www.washingtonpost.com/wp-dyn/articles/A30897-2005Feb16.html.

67. Scalet, "Five Most Shocking Things."

4.4.6 That New Credit Monitoring Thing

Eventually, ChoicePoint's response team did get organized, make clear public statements, and take thoughtful action to compensate consumers. On February 25, ChoicePoint sent a follow-up letter to affected consumers, with a remarkable offer:[68]

> We assure you we understand the inconvenience this incident may cause you and have therefore partnered with Experian, one of the three national credit reporting companies, to provide you, at our cost, with the resources that will help you monitor and protect the use of your personal information.
>
> One of these resources is the credit monitoring service provided by Experian. Reviewing your credit report frequently for inaccuracies is one way of helping prevent against potential identity theft. . . . This credit monitoring service will allow you to have unlimited access to your Experian credit report and will provide you with daily monitoring and email alerts of key changes to your Experian credit report.

For thousands of people, this was the first time they had ever heard of "credit monitoring" as a service, let alone received it. A decade later, offers of credit monitoring in these situations are so commonplace that many consumers now have "free credit monitoring" three or four times over due to different breaches that exposed their information. Back then, it was a new idea, and wholly appropriate given the type of information accessed and the public concerns of identity theft.

4.4.7 Act Now, While Goodwill Lasts

It might seem obvious, but once you realize a data breach crisis may have occurred, you must *act*. This is especially important if you are already in the acute phase. You must act to manage the crisis itself, as well as the perception of the crisis. This requires a two-pronged approach: crisis management and crisis communications.

The delayed response from ChoicePoint's executive team at the start of the acute phase is understandable, but it cost them. The executive team undoubtedly felt ashamed and vulnerable. They didn't know what to do. They didn't have the information they needed. They weren't prepared to manage the crisis. In all likelihood, they were fearful that taking responsibility or making strong public statements would place them at greater risk of liability. So they clammed up. Even though eventually they did take proactive response measures, their early delays enraged the public and stoked the flames.

What kinds of actions should you take? Here are a few examples:

Crisis Management:

- Quarantine infected systems to stop the spread of malware.
- Secure your systems by purging malware, removing attacker accounts, and tightening firewall rules.

68. EPIC.org, ChoicePoint letter dated February 25, 2005, https://epic.org/privacy/choicepoint/cp_letter_022505.pdf (accessed January 7, 2018).

- Devalue stolen data if possible by changing passwords or other mutable information.
- Implement additional controls to reduce harm, such as fraud monitoring for stolen credit card numbers.

Crisis Communications:

- Notify consumers.
- Provide a statement to the media.
- Hold press conferences.
- Set up a call center.
- Provide compensation, if appropriate.

The biggest mistake organizations make during the acute phase is that they don't take quick and immediate action. Frequently, data breach response teams get mired in internal legal discussions or try to wait until the scoping is fully complete before communicating with affected stakeholders or taking action. This last mistake is extremely common: In cases where the organization is unprepared and log collection and analysis is slow and painstaking, the scoping phase can take a long time, and often you simply can't afford to wait until you have all the answers.

As we will see throughout this book, the longer you wait to act, the greater the risk that stolen data will be misused, and the more you have to worry about negative press and reputational damage. That's not to say that you should rush a response (there is a balance), but prioritize action. Remember, laws and regulations are only part of what guides your response. Maintaining trust and goodwill with your stakeholders is of the utmost importance. This requires clear, timely, and honest action.

4.5 Reducing Harm

Data breaches create risk for multiple parties. These can include:

- Individuals whose personal information has been exposed
- The breached organization itself (due to the potential for unauthorized access, lawsuits, financial and reputational damage, etc.)
- Third parties such as banks, credit card companies, hospitals, government agencies, and any entity offering an asset that the stolen data is used to access

If you act quickly in response to a breach, it is possible to reduce risk of harm to key stakeholders. Here are three common strategies for reducing harm:

1. Devalue the data
2. Monitor and respond
3. Implement additional access controls

We will examine each of these strategies in turn.

4.5.1 Devalue the Data

Digitized data is a beautiful thing. An inherent benefit of digitized data is that, in theory, it is easy to distribute, easy to change, and easy to access remotely. These are all qualities that can help us reduce risk quickly in the event that a data breach is discovered.

4.5.1.1 Passwords

When passwords are exposed, what can be done to reduce the risk of harm? Change the passwords in your authentication system, of course. Then the exposed data can no longer be used to access the assets for which the passwords were originally created. To minimize risk, passwords should be changed as soon as possible following discovery of a suspected breach. The downside of changing passwords, of course, is that it is an irritation and an inconvenience to users, who often have a choice of what services they use. The process can also create additional burdens on customer or employee IT support staff.

4.5.1.2 Payment Card Numbers

Payment card numbers, too, can be changed—although they are not as ephemeral as a password. Since payment card numbers are, literally, embossed onto a card and distributed to cardholders, it costs money to buy card stock, and takes time and effort to imprint new cards and get them to consumers. Again, the issue of customer irritation is significant, as is cost. There is also the issue of data dependencies. Many consumers have set up autopays, for example, that rely on a static payment card number. When the card number changes, it causes work and annoyance for consumers who must reconfigure their bill payment methods. For all of these reasons, banks and card brands often choose not to change card numbers, even when they know a card number has been exposed or stolen.

4.5.1.3 Stuck with a Stolen SSN

SSNs represent the epitome of data dependencies. Most Americans have the same SSN for their entire lives. Even if you know your SSN has been stolen, the Social Security Administration (SSA) will not change it if there is "no evidence that someone is using your number." Even if you are one of the rare persons who successfully lobbies for a new SSN, the SSA cautions:[69]

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.

69. U.S. Social Security Administration, *Identity Theft and Your Social Security Number*, (Pub. No. 05-10064 (Washington, DC: SSA, June 2017) https://www.ssa.gov/pubs/EN-05-10064.pdf.

In other words, **there is no effective way to change your SSN throughout the entire information ecosystem, and therefore, there is no way to fully devalue the data if it is stolen.**

Equifax painfully illustrated the fatal flaw of SSNs: They could not be changed on a large scale. The U.S. government did not have the infrastructure to change 145.5 million SSNs. This meant that the risk resulting from the theft remained largely uncontrolled.

"I feel very strongly that the Social Security number has outlived its usefulness," said Rob Joyce, the White House cybersecurity coordinator. "Every time we use the Social Security number, you put it at risk."[70]

In his congressional testimony, former Equifax CEO Risk Smith came to the same conclusion. "If there's one thing I would love to see this country think about, it's the concept of a Social Security number in this environment being private and secure. I think it's time as a country to think beyond that," he said. "What is a better way to identify consumers in our country in a very secure way? I think that way is something different than an SSN, a date of birth and a name."[71]

When it comes to data breaches, SSNs are a perfect storm: They proliferate with use, many people have access to them, they are highly *liquid* due to their compact size and structured format, and they remain unchanged over the course of a person's lifetime (and beyond).

4.5.1.4 Alternate Forms of Authentication

Much of the harm from data breaches stems from a widespread reliance on knowledge-based authentication. When secret keys are spilled, it creates risk. Fortunately, recent advances have made other forms of authentication far more convenient, for users and organizations. Modern technology now enables us to use one-time PINs, mobile apps, thumbprints, facial expressions, voiceprints, or small hardware tokens as keys to log in to computer accounts. Critically, the key itself does not need to be revealed during the authentication process. Instead of sending a copy of your thumbprint over the Internet, advanced cryptography is used to prove that your thumbprint was valid, without revealing the actual thumbprint itself. Apple iPhones and iPads include a built-in thumbprint reader and an application programming interface (API) that allows apps to leverage the TouchID authentication feature. Windows 10 builds in the Windows Hello functionality, which is designed to support biometric authentication.

More than 95% of Americans have cell phones, enabling two-factor authentication based on SMS (text) messages. A whopping 77% of U.S. adults own a smartphone, facilitating the deployment of two-factor authentication—based mobile apps.[72]

---

70. Nafeesa Syeed and Elizabeth Dexheimer, "The White House and Equifax Agree: Social Security Numbers Should Go," *Bloomberg*, October 4, 2017, https://www.bloomberg.com/news/articles/2017-10-03/white-house-and-equifax-agree-social-security-numbers-should-go.

71. *House Energy and Commerce Subcommittee Hearing on "Equifax Data Breach" Before the Subcomm. on Digital Commerce and Consumer Protection of the H. Comm. on Energy and Commerce, 115th Cong.* (October 3, 2017), https://www.c-span.org/video/?434786-1/lawmakers-grill-equifax-ceo-data-breach&start=9971 (prepared testimony of Richard F. Smith, former Chairman and CEO, Equifax).

72. Pew Research Center, "Mobile Fact Sheet," *Pew Internet and Technology*, January 12, 2017, http://www.pewinternet.org/fact-sheet/mobile.

Slowly, the world is moving away from knowledge-based authentication, reducing the value of sensitive personal information for use in fraud and other crimes. This reduces risk for both consumers and organizations.

4.5.2 Monitor and Respond

A second option is to monitor accounts or assets that may be accessed using stolen data and develop a system for detecting and responding to fraudulent use. When a data breach happens today, free credit monitoring is perhaps the most common form of compensation provided to victims, as illustrated in the ChoicePoint case.

Credit agencies such as Experian, TransUnion, and Equifax collect records of lending and payment activity on mortgages, loans, credit cards, bills, and other financial accounts. From this, they produce your credit report and calculate your credit score (really, multiple scores) that are designed to convey information about your creditworthiness to other lenders.

When a criminal sets up a new account using a victim's stolen personal information or abuses an existing account, a record of this activity will typically show up on the victim's credit report. The consequences of identity theft can include unpaid credit card bills that the victim didn't even know existed, repeated credit inquiries by new lenders, and other results that negatively impact the victim's credit. For the victim, this can result in a nightmare scenario where he or she is denied credit or charged exhorbitant interest rates due to a damaged credit rating.

Enter *credit monitoring*: a service where a third party, such as the Big Three credit agencies (Experian, Equifax, and TransUnion), or vendors such as AllClear or LifeLock, monitor the victim's credit reports and provide alerts when there are any suspicious changes. These may include changes in your credit score, address, new accounts, delinquencies, credit inquiries, and other factors that might affect your credit score.

Credit monitoring provides some value to consumers by helping to detect issues with their credit report quickly. It's also a way for the credit bureaus to make extra recurring revenue: They typically charge consumers $15 to $20 a month. Card brands are in on the action, too: "The monitoring business is profitable enough that big credit card companies, including Capital One and Discover, now partner with Experian to sell private-label versions of the monitoring service directly to their customers, taking a cut of the fees and giving the rest to Experian."[73]

The FTC's Sing-Along Credit Report Videos

Consumers historically had a hard time detecting identity theft quickly, in part because of lack of access to their own credit reports. Initially, consumers had no right to see the data that credit bureaus collected on them and had to purchase their credit reports if they wanted to view them. Most consumers would have no idea there was a mistake on their credit report until a lender rejected them. That changed in 2003, when Congress passed the Fair and Accurate Credit

(*Continues*)

73. Ron Lieber, "A Free Credit Score Followed by a Monthly Bill," *New York Times*, November 2, 2009, http://www.nytimes.com/2009/11/03/your-money/credit-scores/03scores.html.

(*Continued*)

Transactions Act (FACTA), an amendment to the Fair Credit Reporting Act. Among other provisions, FACTA required each credit bureau to give consumers free access to their credit report once each year. The primary website for the program is AnnualCreditReport.com.

The credit bureaus, however, found a way to profit off the new requirement. Experian had previously purchased a company that owned the domain freecreditreport.com. The credit bureau began heavily marketing FreeCreditReport.com as a means for consumers to obtain their "free" credit reports. "Smelling opportunity, Experian bought ads on Google and other sites that diverted some people looking for their legally mandated credit reports," reported the *New York Times*, years later.[74]

Experian produced a series of catchy commercials featuring a young guitar-playing protagonist singing about different ways that his credit score was damaged. If only he had gone to FreeCreditReport.com, the guitarist laments![75]

What consumers didn't realize was that once they signed up, they were automatically enrolled in a credit-monitoring program that charged them $79.95 if they did not cancel within 30 days.

In 2005, the FTC fined Experian $950,000 for deceptive marketing practices and later forced the company to "give up [an additional] $300,000 in ill-gotten gains" as a result of violations of the initial settlement.[76]

Then, in one of the FTC's most inspired moments, the government agency released its own videos spoofing Experian's original ads.[77] "Despite the musical claims of some TV commercials, the only authorized source to get your free annual credit report under federal law is AnnualCreditReport.com," stated the agency in a 2009 press release. "To reinforce this message, the Federal Trade Commission is featuring two new videos with their own catchy tunes."[78]

4.5.2.1 Credit Monitoring for Victims

Many organizations purchase free credit monitoring on behalf of affected victims. The idea is to offer victims something of value that will also reduce their risk of identity theft. This ties in with classic image repair theory, combining two strategies: *compensation* and *corrective action*. Table 4-1 shows examples of each, as described by image repair expert William L. Benoit:[79]

73. Lieber, "Free Credit Score."

74. Gerard Dalbon, "FreeCreditReport.com All 9 Commercials," *YouTube*, 4:38, min, posted October 3, 2009, https://www.youtube.com/watch?v=tloVHJtrJ_k.

75. Federal Trade Commission (FTC), "FTC Releases Spoof Videos with a Serious Message: AnnualCreditReport.com is the Only Authorized Source for Free Annual Credit Reports," press release, March 10, 2009, https://www.ftc.gov/news-events/press-releases/2009/03/ftc-releases-spoof-videos-serious-message-annualcreditreportcom.

76. FTC, "FTC Releases Spoof Videos."

78. FTC, "AnnualCreditReport.com Restaurant: Federal Trade Commission," *YouTube*, 0:50 min, posted March 9, 2009, https://www.youtube.com/watch?v=xZ0xsF5XWfo (accessed January 9, 2018).

79. William L. Benoit, *Accounts, Excuses, and Apologies*, 2nd ed. (New York: SUNY Press, 2014), 28.

Table 4-1 Examples of "Compensation" and "Corrective Action" Image Repair Strategies. Source: Benoit, *Accounts, Excuses, and Apologies*, 28.

Strategy/Tactic	Example
Compensation	*Because the waiter spilled a drink on your clothes, we'll give you dessert for free.*
Corrective Action	*Because the waiter spilled a drink on your suit, we'll pay to have it dry cleaned.*

How useful is credit monitoring for victims of a breach? "Credit monitoring is only helpful if your social security number has been stolen, notifying you if someone applies for an account in your name," writes Kathleen Burke of MarketWatch. "It doesn't track fraudulent credit card charges."[80] For breaches involving healthcare data, credit monitoring doesn't address potential embarrassment or discrimination that can come as a result of exposed medical details.

After a breach, organizations often have only enough budget to offer credit monitoring a year, and the providers sometimes monitor credit reports from only one major credit bureau, not all three. "Hackers can use stolen information to apply for credit at any of these three bureaus and after any amount of time," adds Burke.

After the health insurer Anthem was breached, the company offered victims two years of free credit monitoring, twice as long as most organizations. Jairo Angulo and his wife previously had health insurance through Anthem and were notified that their personal information was stolen in the breach. For Angulo, two years of free credit monitoring was "not nearly enough."[81]

"If your Social Security number and other information is out in the world, it's out there forever," said Angulo. "Anthem should be paying for my credit monitoring for the rest of my life."[82] (The Anthem breach will be discussed in more detail in Chapter 9, "Health Data Breaches.")

Over the years, both data breaches and the free credit monitoring offer have become such a common response tactic that many consumers have received free credit monitoring three, four, five, or more times as a result of different breaches. This has reduced the value of credit monitoring as a compensatory strategy; for consumers who already have the service, it doesn't provide significant value. On the flip side, if it is not offered, consumers notice.

4.5.2.2 Internal Fraud Monitoring

In the payment card industry, banks and card brands have developed sophisticated systems for detecting potential fraudulent use of card data. Often, these are based on a behavioral profile of the cardholder: For example, if the cardholder is based in Boston, the system might alert and block a sudden attempted purchase in Des Moines. What modern cardholder hasn't gotten off an airplane, only to find that their first purchase in a new city is declined?

---

80. Kathleen Burke, "'Free Credit Monitoring' after Data Breaches is More Sucker than Succor," *MarketWatch*, June 10, 2015, http://www.marketwatch.com/story/free-credit-monitoring-after-data-breaches-is-more-sucker-than-succor-2015-06-10.

81. David Lazarus, "So What Does a Corporation Owe You after a Data Breach?" *Los Angeles Times*, May 10, 2016, http://www.latimes.com/business/lazarus/la-fi-lazarus-security-breaches-20160510-snap-story.html.

82. Lazarus, "So What Does a Corporation Owe You."

Of course, it can be expensive and labor intensive for banks and card brands to implement effective monitoring systems, and false positives cost merchants business and damage their relationship with consumers. "[T]wo-thirds of cardholders who were declined during an e-commerce (electronic) transaction or m-commerce (mobile) transaction reduced or stopped their patronage of the merchant following a false-positive decline, versus 54 percent for all declined cardholders," stated an Internal Revenue Service (IRS) whitepaper on fraud.[83]

The IRS itself has been subject to rampant tax refund fraud, due to stolen taxpayer personal information, including W-2 forms. To combat this, the IRS has developed "a complex and multifaceted" program to "address identity theft and detect and prevent improper fraudulent refunds." This includes employing filters, data analytics and manual analysis to flag potentially fraudulent returns before refunds are issued. In addition, "the IRS began employing additional filters known as the Identity Theft business rules in January 2009. The business rules are applied to any return filed with a Social Security number (SSN) associated with an identity theft indicator. These returns are not allowed to post to taxpayers' accounts (these are called 'unpostable' returns) until the IRS can review the returns and accounts, and determine that they belong to the valid SSN owners." As described by the Taxpayer Advocate Service in the 2016 Annual Report to Congress, the IRS's fraud detection processes have a high false positive rate—up to 91%! This resulted in 1.2 million delayed returns for the calendar year 2016 (through September) and caused taxpayer refunds to be delayed by approximately two months.

Taxpayers whose returns are delayed due to possible identity theft are instructed to call the IRS's Taxpayer Protection Program hotline, which had an abysmal level of service of 31.7% and an average wait time of 11 minutes in fiscal year 2016.[84] The high rate of false positives also erodes employee morale within the IRS, in addition to the fact that the program as a whole is undoubtedly expensive—costs that ultimately come out of the taxpayers' pockets.

4.5.3 Implement Additional Access Controls

SSNs, payment card numbers, passwords, and many other types of data are called "access devices" for a reason: because they facilitate access to valuable information or assets. If such an access device is stolen, it may be costly, difficult, or impossible to devalue the data entirely. However, in many cases, organizations can implement additional access controls to reduce the risk of unauthorized access. These controls are often combined with additional monitoring efforts.

For example: if customer passwords are exposed, but the breached organization does not force a password reset immediately due to, say, concern about irritated customers, the organization may choose to implement an additional check to determine whether the device or IP address used to log in to the customer account has been used in the past. If so, the organization may allow the login to proceed. Otherwise, the user may be subjected to additional

83. Taxpayer Advocate Service, "Most Serious Problems: Fraud Detection," *Annual Report to Congress* 1 (2006): 151–60. https://taxpayeradvocate.irs.gov/Media/Default/Documents/2016-ARC/ARC16_Volume1_MSP_09_FraudDetection.pdf.

84. "Level of service" is a measure of "the relative success rate of taxpayers who call the toll-free lines seeking assistance from customer service representatives." Taxpayer Advocate Service, "Most Serious Problems: IRS Toll-Free Telephone Service Is Declining as Taxpayer Demand for Telephone Service Is Increasing," *Annual Report to Congress* 1 (2009): 1, 5, https://www.irs.gov/pub/tas/msp_1.pdf.

verification procedures, such as a text or call to the phone number on file. From a technical perspective, this is riskier than forcing an immediate password reset across the board, but management may decide that the business risk associated with the potential for widespread customer irritation outweighs the risk of unauthorized account access.

This type of additional check is common for payment cards: Often banks or card brands are aware that a consumer's card number has been stolen. However, rather than spending money to replace cards in bulk and risk widespread customer anger, financial institutions may choose to selectively implement additional controls such as callbacks when they detect deviations from the cardholder's normal spending patterns.

The challenge comes when sensitive information is used to access systems outside the breached organization, often in many different places. The SSN is a perfect example of this—your SSN may have been stolen from a hospital and used to procure a cell phone from Verizon. The hospital has no control over Verizon's sales cycle, and their security teams do not communicate. Indeed, the hospital may never suffer any direct damage due to a breach of personally identifible information (it may not even be detected!) and yet many outside organizations and the victims themselves may experience financial damage.

4.5.3.1 The Credit Freeze Band-Aid

Experts agree that one of the most effective ways for consumers to protect themselves against identity theft is to "freeze" their credit—essentially, preventing credit reporting agencies from releasing their credit reports. Since most lenders pull a consumer's credit before approving a new account, this effectively prevents fraudsters from opening new accounts in a victim's name.

In 2003, legislators began to craft laws that would make it easier for consumers to freeze their credit. Over the next few years, the Consumer Data Industry Association (CDIA), which represents the Big Three credit bureaus, fought back. "[C]redit freezes could . . . cut deeply into the credit bureaus' core business," reported *USA Today* in 2007. "The CDIA has been scrambling . . . to get federal lawmakers to defuse the onrush of state laws empowering consumers to freeze access to their credit histories to prevent identity theft."[85]

It was a losing battle for the CDIA: Across the country, laws passed in 49 states and the District of Columbia allowing consumers to freeze their credit. States also introduced mechanisms for a "quick thaw," which would allow consumers to quickly unfreeze their credit reports using a PIN so that they could process legitimate credit applications.

A credit freeze is a form of additional access control that consumers can implement following a breach. For personally identifiable information, which is used by an endless variety of organizations all over the map, it is perhaps the best way to control unauthorized use. Credit freezes are, however, a rudimentary tool. Consumers cannot limit access to their credit reports to specific, authorized entities. Instead, the access control is based on timing: either a report is frozen or unfrozen. If a criminal happens to apply for a loan at the same time that a victim has unfrozen his or her credit for legitimate reasons, then the criminal may well succeed. Also, a credit freeze reduces the risk of only specific types of identity theft that involve a creditor pulling a consumer's report.

---

85. Byron Acohido and Jon Swartz, "Credit Bureaus Fight Consumer-Ordered Freezes," *USA Today*, June 25, 2007, https://usatoday30.usatoday.com/money/perfi/credit/2007-06-25-credit-freeze-usat_n.htm.

4.5.3.2 Debit Card Lock

In response to debit card thefts, banks introduced a "debit card lock" feature, which allows customers to "turn off" their debit cards using their mobile phone or online banking web application.[86] The *New York Times* published a report on the debit card lock in early 2016. "In an informal test, a reporter locked a Bank of America debit card using a mobile phone; the card was then rejected by an A.T.M. (The machine spit out the card and displayed a message stating, 'This card is not valid.') Then, moments later, while at the A.T.M., the user unlocked the card using the mobile phone. The machine immediately accepted the card and dispensed cash."[87]

In advertisements, the debit card lock is typically featured as a way for consumers to "turn off" their card if they notice it is physically missing. However, the tool can be used to reduce risk of payment card fraud in general. By giving consumers the ability to activate and deactivate a card number in seconds, banks have deployed a time-based security control.

Consumers now have the ability to leave card numbers "locked" most of the time, unlocking a card number for only the few minutes it takes to conduct a transaction. This, in turn, gives attackers a small window of opportunity, which dramatically reduces the value of the card number. Of course, many consumers will not take advantage of this feature, but for those who do, it is a powerful tool.

4.5.3.3 Identity Theft Protection Rackets

Identity theft protection services are an extension of credit monitoring, designed to help consumers detect identity theft. Many forms of identity theft protection services today also offer support for members who are victims of identity theft, including assistance with payment and identification card replacement, credit report clean-up, and similar services.

LifeLock, which was founded in 2005 after the publicity wave of the ChoicePoint breach, is one of the most well-known identity theft protection providers. The company has been plagued with controversy regarding the effectiveness of its services, as well as its ability to keep its own members' data secure.

"I'm Todd Davis, CEO of LifeLock. My social security number is 457-55-5462," stated a 2006 LifeLock advertisement, plastered with Davis's photo. "Yes, that really is my social security number. No I'm not crazy. I'm just sure our system works. Just like we have with mine, LifeLock will make your personal information useless to a criminal. And it's GUARANTEED."

LifeLock ran a similar television ad campaign, featuring a truck that was painted with Davis's SSN. The advertising campaign took off—but probably not in the way LifeLock's marketing team had hoped. Over the next few years, Davis's identity was stolen at least 13 times, by criminals who took out loans in his name, opened utility accounts, and even ran up a fraudulent $2,390 cell-phone bill with AT&T. Davis filed police reports and involved law enforcement to attempt to find and prosecute the criminals.

---

86. Richard Burnett, "Debit Card 'On/Off' Switch Helps Keep Security Intact," *Wells Fargo Stories*, April 28, 2017, https://stories.wf.com/debit-card-onoff-switch-helps-keep-security-intact.

87. Ann Carrns, "A Way to Lock Lost Debit Cards, from a Big Bank," *New York Times*, February 3, 2016, https://www.nytimes.com/2016/02/04/your-money/a-way-to-lock-lost-debit-cards-from-a-big-bank.html.

"Davis' publication of his Social Security number created more victims than just himself," reported the *Phoenix New Times* online magazine, which interviewed the frustrated Albany, Georgia, police department upon discovery of the AT&T fraud.[88]

In 2010, LifeLock "agreed to pay $11 million to the Federal Trade Commission and $1 million to a group of 35 state attorneys general to settle charges that the company used false claims to promote its identity theft protection services, which it widely advertised by displaying the CEO's Social Security number on the side of a truck."[89]

FTC Chair Jon Leibowitz made a damning statement about the company in an official FTC press release, saying that "[w]hile LifeLock promised consumers complete protection against all types of identity theft, in truth, the protection it actually provided left enough holes that you could drive a truck through it."[90]

In addition, the FTC asserted that LifeLock did not take appropriate measures to secure customer information, exposing consumers who signed up for LifeLock's services to additional risk.[91]

Act

Once you realize a data breach may have occurred, *take action* to reduce risk to affected stakeholders and manage communications. "Act" is the third phase in our DRAMA breach response model. This might sound simple, but in the acute phase of a crisis it can be tempting to clam up!

Activate both your *crisis management* and *crisis communications* plans immediately. To preserve your reputation, act:

- **Quickly**
- **Ethically**
- **Empathetically**

Managing a data breach during the acute phase is a lot like riding a motorcycle around a steep curve when you're going a little too fast. Your instinct may be to tap on the brakes, slow down. This can be disastrous. Instead, to achieve stability, you have to stay cool, lean in, and press the accelerator.

88. Kim Zetter, "LifeLock CEO's Identity Stolen 13 Times," *Wired*, May 18, 2010, https://www.wired.com/2010/05/lifelock-identity-theft.

89. Federal Trade Commission (FTC), "LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False," press release, March 9, 2010, https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states.

90. FTC, "LifeLock Will Pay $12 Million."

91. Federal Trade Commission v. Lifelock Inc., 2:10-cv-00530-MHM (D. Ariz. 2010), https://www.wired.com/images_blogs/threatlevel/2010/03/lifelockcomplaint.pdf.

4.6 Chronic Phase

"It is during [the chronic] stage that the carcass gets picked clean," writes Fink. "If there is to be a congressional investigation, or an audit, or a newspaper expose, or a long period of interviews and explanations and mea culpas, this is when such malignancies settle in."[92]

4.6.1 Call in the Experts

ChoicePoint faced a multitude of investigations and legal actions. "The SEC had an investigation, the FTC had an investigation, [there was a] coalition of forty-four Attorney Generals . . . chaired by Vermont, Illinois and California. . . . We had lawsuits, a consumer class action, a derivative class action, 401(k) litigation," Chris Cwalina rattled off the players one by one. "The coalition actually made things a little bit more manageable frankly, because at first we got inquiries from all these AGs, and then there was a coalition formed where we just then had the one sort of entity that we had to respond to on behalf of all of them. . . . [Congress] called a hearing, so we had executives that had to testify, PR, crisis management, external communications dealing with the press, dealing with class actions, dealing with the various regulators."

"What did you learn from managing the ChoicePoint breach?" I asked.

"Dealing with a [data breach] adequately requires a large number of subject matter experts," he responded immediately. Certainly by the time the ChoicePoint crisis reached the chronic phase, the company had pulled together an organized, well-managed response effort. It hired subject matter experts for each area of the breach response, with Chris as the "quarterback," coordinating the various efforts.

"Privacy and cyber security practices didn't exist back then," said Chris. "So the company hired lawyers with expertise dealing with [attorneys general], or lawyers with expertise dealing with the FTC, or lawyers with expertise dealing with consumer class actions. Then we coordinated all those law firms, plus the factual investigations and the internal stuff."

Times have changed since ChoicePoint's breach. Today, when an organization suspects a breach, there are law firms with specialized data breach practices that maintain all the subject matter experts that you would need in-house. "Part of my idea for going into private practice was to go to a place where I could get as close to one stop shop as I could, be at a firm where I could have all the pieces necessary for a company [that] had a breach," said Chris.

Quite often, the chronic phase of a data breach crisis lingers, much like a chronic cough. Executive teams might expect things to return to normal any day, while in reality customer relationships continue to need repairing, regulators need responses, and various other aspects of the crisis management must continue for long after the acute phase has passed. During the chronic phase, the key goal of the crisis management team is to *maintain* the response effort.

92. Fink, *Crisis Management*, 23–24.

Don't expect the response to end when the acute phase is over. The organization needs a long-term plan for managing all aspects of the potential ripple effects of the crisis, including:

- Lawsuits
- Increased scrutiny by regulators
- Consumer relationship repair
- Image repair campaigns
- Media and public investigations

In the wake of a breach, you may need to budget long-term resources for staff to rebuild customer relationships, manage compensation programs, handle investigations and lawsuits, or execute other programs that you put in place.

4.6.2 A Time for Introspection

The chronic phase "is also a period of recovery, of self-analysis, of self-doubt, and of healing," writes Fink.[93] Indeed, much of the "opportunity" of a data breach comes from the natural introspection and subsequent investment in better practices that many organizations undertake after a breach.

In the ChoicePoint breach, the introspection happened for many affected parties, from the company itself, to consumers, to the industry of data brokers, to the U.S. legislature. "The security breach that ChoicePoint discovered last fall in California has caused us to go through some serious soul searching," said ChoicePoint CEO Derek Smith.[94] The United States as a nation examined this new industry, data brokers, in order to understand the risks to consumers and push for greater transparency. The spotlight of the ChoicePoint crisis made the public much more aware of the growing new market—as well as the risks.

"[T]he very existence of these vast information stockpiles—vulnerable to both error and poaching—has spawned a new area of worry and risk," wrote the *Wall Street Journal*, echoing popular sentiment.[95]

4.6.3 Testifying before Congress

Amid growing concerns that information brokers were not effectively self-regulating, the Senate Judiciary Committee initiated an inquiry. The executives of ChoicePoint, as well as competitors from Acxiom and LexisNexis, testified before Congress at a hearing on April 15, 2005, on

93. Fink, *Crisis Management*, 24.

94. Jonathan Peterson, "Data Collectors Face Lawmakers," *Los Angeles Times*, March 16, 2005, http://articles.latimes.com/2005/mar/16/business/fi-choice16.

95. Perez and Brooks, "For Big Vendor."

"Securing Electronic Personal Data." In this hearing, Senator Feinstein grilled the executives to determine whether the California law had an impact on breach disclosure. Below is an excerpt of the transcript from that historic hearing:[96]

> *Senator Feinstein*. . . . The California law went into effect in 2003. I would like to ask each of the people here representing companies to indicate if, prior to 2003, you had a breach and did not notify people. Mr. Sanford?
>
> *Mr. Sanford [LexisNexis]*. I believe there were security breaches in the business that I acquired that I mentioned, Seisint. I believe there may have been a security breach in LexisNexis prior to 2003, that may have involved personally identifiable information, and we did not make notice prior.
>
> *Senator Feinstein*. Thank you. I appreciate the honesty. Mr. Curling?
>
> *Mr. Curling [ChoicePoint]*. Yes, ma'am, I previously indicated there was a breach that we didn't notify them.
>
> *Senator Feinstein*. Thank you. Ms. Barrett?
>
> *Ms. Barrett [Acxoim]*. The breach that we had in 2003 did span the enactment of the law in July. Our obligation as a provider since the breach did not involve our—
>
> *Senator Feinstein*. My question is, did you have a breach prior to the 2003 law going into effect?
>
> *Ms. Barrett*. Yes, the breach that we had did span it, but we did provide notice to our clients.
>
> *Senator Feinstein*. Thank you. This is my point: If it weren't for the California law, we would have no way of knowing breaches that have occurred. It is really only because of that law that we now know. We in no way, shape or form are able to pierce the depth of what has happened in this industry.

Maintain

During the chronic phase of the data breach, make sure to *maintain* your response efforts. This can be tricky! "You have to manage the breach and carry on business at the same time," points out Karen Sprenger, chief operating officer (COO) of LMG Security. "It's not like the world stops and waits for you to handle your breach."

(*Continues*)

96. C-SPAN, "Securing Electronic Personal Data," *C-SPAN*, video, 2:32:49 min, posted April 13, 2005, https://www.c-span.org/video/?186271-1/securing-electronic-personal-data.

(*Continued*)

"Maintain" is the fourth phase in our DRAMA breach response model. Here are a few quick tips for effectively maintaining your response efforts (and your sanity):

- Enumerate potential short- and long-term risks to your organization as a result of the breach, such as loss of customer trust, third-party investigations, or increased scrutiny from regulators.
- Develop short- and long-term plans to mitigate these risks.
- Assign responsibility for managing ongoing response efforts over time.
- Budget for resources such as tools, staff, and consultants who are engaged in ongoing response efforts.
- Recognize signs of burnout in staff who are part of the ongoing crisis response efforts, and ensure that additional staff are hired as appropriate to manage new workloads.
- Document your organization's goals, and specify points at which certain ongoing response efforts can be dialed back or completed.

4.7 Resolution Phase

The "resolution" stage is when "the patient is well and whole again," says Fink. He cautions, however, that "crises historically evolve in cyclical fashion, and a crisis sufferer almost never has the luxury of dealing exclusively with one crisis at a time."[97] Data breaches often involve multiple "crises," which tend to stem from similar deficiencies.

4.7.1 The New Normal

When a data breach occurs, what does it mean to be "well and whole"? Things will never be exactly the way they were before the breach. Your organization will be different after a breach. You can't control that fact; but you can control, to a certain extent, *how* it evolves and what it becomes. ChoicePoint itself went through a major adaptation process—something that it had not done effectively after suffering earlier breaches. In Senate hearings, ChoicePoint's president admitted that "between 45 and 50" similar breaches had occurred previously.[98] The media

97. Fink, *Crisis Management*, 28.

98. Evan Perez and Rick Brooks, "For ChoicePoint, a Theft Lays Bare the Downside," *Pittsburgh Post-Gazette*, May 3, 2005, http://www.post-gazette.com/business/businessnews/2005/05/03/For-ChoicePoint-a-theft-lays-bare-the-downside/stories/200505030214 (accessed January 7, 2018).

reported that ChoicePoint had suffered an earlier, similar breach in 2002, perpetrated by a pair of Nigerian criminals.[99]

According to the FTC, even though law enforcement alerted ChoicePoint multiple times to these earlier breaches, the company failed to "monitor or otherwise identify unauthorized activity." The company simply had not learned from prior breaches—likely because it was not required to notify consumers, and therefore there was no great public outcry.

ChoicePoint's failure to adapt after the 2002 breach left it vulnerable in the years to come, as the risks of identity theft and data breaches continued to intensify.

4.7.2 Growing Stronger

When the 2005 crisis hit, ChoicePoint was finally forced to adapt, due to pressures from the public, regulators, shareholders, and others. The company launched an internal reorganization, creating a "chief credentialing, compliance and privacy officer" position, which reported directly to the board of directors. It even changed its business model—to an extent. "At ChoicePoint, damage control eventually kicked in. The company announced that it would 'discontinue the sale of information products that contain sensitive consumer data, including Social Security and driver's license numbers, except where there is a specific consumer-driven transaction or benefit' or law enforcement purpose."[100] As per the consent decree that it was eventually subjected to, the company was required to implement stronger security measures and conduct routine third-party security audits.

The company was also financially damaged by the data breach. On the day of the announcement, "its stock price fell 3.1% on the day the breach was reported, and then continued to fall." Two years later, shares were still worth only 80% of the pre-breach value.[101] Unlike other companies, ChoicePoint might not have had to worry as much about brand damage since it was not a consumer-facing company, because (as Chris Cwalina pointed out) "not a lot of people knew who ChoicePoint was in the first place."

Ultimately, ChoicePoint moved past its data breach crisis. According to Gartner, the company "transformed itself from a poster child of data breaches to a role model for data security and privacy practices."[102]

This is consistent with Chris Cwalina's view of what occurred. "ChoicePoint senior leaders and employees really came together to turn a challenging event into a positive force," he mused. "They put a lot of resources into improving and further building a compliance and privacy function. They brought in a lot of new people and relied on an existing large group of really talented employees to improve. I think that they did a really good job in that regard. It was not like senior execs said, 'This is no big deal. We're not going to bother with this.' Everyone

99. "ChoicePoint Reported to Have Had Previous ID Theft," *Insurance Journal*, March 3, 2005, http://www.insurancejournal.com/news/national/2005/03/03/52108.htm.

100. Scalet, "Five Most Shocking Things."

101. Khalid Kark, "The Cost of Data Breaches: Looking at the Hard Numbers," *Tech Target*, March 2007, http://searchsecurity.techtarget.com/tip/The-cost-of-data-breaches-Looking-at-the-hard-numbers.

102. Jon Swartz and Byron Acohido, "Who's Guarding Your Data in the Cybervault?" *TechNewsWorld*, May 17, 2007, http://web.archive.org/web/20070517203855/http://www.technewsworld.com/story/56709.html.

involved actually cared quite deeply about what occurred, and put a lot of time, effort and resources into it."

ChoicePoint was acquired in 2008 for $4.1 billion by Reed Elsevier, the parent company of LexisNexis.

4.7.3 Changing the World

Security expert Bruce Schneier pointed out that the economics did not incent data brokers to protect consumer data. "The hundreds of millions of people in ChoicePoint's databases are not ChoicePoint's customers. They have no power to switch credit agencies. They have no economic pressure that they can bring to bear on the problem. . . . ChoicePoint doesn't bear the costs of identity theft, so ChoicePoint doesn't take those costs into account when figuring out how much money to spend on data security. In economic terms, it's an 'externality.'"[103]

The ChoicePoint case illustrated to the U.S. public and legislators that:

- Absent laws, information brokers did not effectively protect consumer information from exposure.
- Information brokers would not notify consumers of a data breach out of the goodness of their hearts, but instead required clear legal and/or financial incentives.
- Breach notification legislation *worked*, at least in some cases.

"Responsible handling of such records is every bit as important a public safety issue as is the proper disposal of hazardous waste," wrote Atlanta pundit Scott Henry in the aftermath of the ChoicePoint breach. "If it turns out that ChoicePoint's gross negligence doesn't violate current law, the laws are clearly inadequate. It's encouraging that legislators in Georgia and around the country are already drafting laws that would help prevent—or at least provide reasonable notification of—a similar security breach."[104]

As a result of the ChoicePoint breach, laws across the United States were enacted to hold organizations accountable for notifying consumers of a breach, therefore also indirectly providing incentive to reduce breaches. By June 2005, 35 states had introduced data breach notification laws, and at least 22 states had enacted laws by October of that same year.[105]

The World Privacy Forum later called ChoicePoint "the *Exxon Valdez* of privacy." While many breaches have been compared to *Exxon Valdez* crisis, the ChoicePoint case is perhaps its closest equivalent. Like the *Exxon Valdez* spill, ChoicePoint wasn't the first disaster of its type or the biggest (not even close). It was, however, the most visible to the American public and resulted in the creation of new laws and greater oversight. The ChoicePoint breach helped the public understand that organizations require clear incentives in order to act in the best interest of the public.

---

103. Schneier, "ChoicePoint."

104. Scott Henry, "ChoicePoint," *Creative Loafing*, February 23, 2005, http://www.creativeloafing.com/news/article/13017248/choicepoint.

105. Milton C. Sutton, *Security Breach Notifications: State Laws, Federal Proposals, and Recommendations* (Moritz College of Law, Ohio State University, 2012), 935, http://moritzlaw.osu.edu/students/groups/is/files/2012/02/s-sutton.pdf.

In other words, the ChoicePoint breach didn't just change ChoicePoint. It changed the data brokerage industry and the world.

Adapt

"A data breach can't be undone," says Karen Sprenger, an 18-year veteran of the digital forensics industry. The best you can do is learn from it. "Adapt" is the final phase of our DRAMA breach response model.

Your organization will almost certainly change as a natural process following the breach. You can also put your organization in a better position by *consciously* adapting in proactive ways, such as:

- Implement more effective security procedures, including both technical and policy changes.
- Improve logging and monitoring infrastructure.
- Obtain comprehensive data breach insurance.
- Build better crisis management and crisis communications plans.

By adapting proactively and wisely, you can maintain the value of your organization and reduce the risk of future breaches. When your organization emerges, it can be "well and whole"—but it will be different.

4.8 Before a Breach

Now that we've analyzed a data breach crisis from beginning to end, inside and out, let's go back to the beginning. What could ChoicePoint have done to handle its breach more effectively?

Data breaches represent crises, which by their nature are often fast moving and unpredictable. "You need to be ready in advance and take time to prepare with a multidisciplinary team," said Chris Cwalina. For ChoicePoint, a major failing was simply that it had not developed any crisis management plans for recognizing or responding to a potential data breach. As a result, it stumbled over and over—particularly in the prodromal and acute phases, which require a quick response.

"The lack of a plan or the infrastructure to handle a data breach created problems in disseminating information and handling public relations," observed researchers from North Carolina State University who analyzed the ChoicePoint breach.[106]

But where does planning start? The fundamental problem at ChoicePoint—and indeed, in many organizations—is that no one had been tasked with oversight for data breach crisis planning in the first place.

106. Otto, Antón, and Baumer, "ChoicePoint Dilemma."

4.8.1 Cybersecurity Starts at the Top

The data breach crisis planning process is most effective when it is driven from the executive level, and managed by a risk officer or chief information security officer (CISO), outside of IT. Ideally, it should be integrated with an enterprise crisis management effort.

It turned out that ChoicePoint had never assigned responsibility for managing information holistically, throughout the enterprise. As a result, ChoicePoint's team was not only forced to create response procedures on the fly; they even created whole positions that, in retrospect, should already have existed. For example, the notification letter that ChoicePoint sent to consumers was signed "J. Michael de Janes, Chief Privacy Officer."

CSO magazine pointed out that de Janes was "actually the general counsel for ChoicePoint. His description of responsibilities on the ChoicePoint website does not include privacy. It seems that ChoicePoint just needed a privacy officer, and fast."[107]

The company *did* have a very accomplished CISO at the helm: Rich Baich, who had been named "Information Security Executive of the Year in Georgia" during 2004, "in recognition of his accomplishments in the realm of information security."[108] He was a Certified Information Systems Security and Privacy Professional (CISSP) and also a Certified Information Security Manager. His book, *Winning as a CISO*, (ironically) was published in June 2005, while the ChoicePoint crisis still burned.

When the ChoicePoint data breach erupted, Baich was publicly roasted and called a "fraud and discredit to the position of the CISO." He responded by pointing out that the breach was not a "hack," arguing that issues with customer vetting processes were not his responsibility.

"Look, I'm the chief information security officer. Fraud doesn't relate to me."[109]

And indeed, it didn't. Despite the fancy title ("Chief,") ChoicePoint's CISO was siloed inside the IT department, which was fully separate from the unit of business that handled customer vetting and access policies. Although on paper ChoicePoint had someone who might appear to be "in charge" of information security, in reality, due to Baich's placement within the organization, it was not possible for him to manage information security or coordinate a breach response across all business units, as was truly necessary.

Cybersecurity incident response teams have traditionally been built and led from within the IT department. This might have made sense when most cybersecurity incidents were handled by IT staff, without major risk to the organization as a whole. Viruses, spam, inappropriate use, equipment loss—all of these cases were once handled within IT, with little planning or involvement from other departments.

Over the years, as data breaches have become more of a concern, organizations have started to realize that planning for data breaches must be a coordinated effort involving stakeholders from across the organization. While your IT department may be perfectly capable of managing the *technical* aspects of a data breach, it is rarely the case that an IT manager is in a position to effectively plan for or manage an enterprise-wide crisis response strategy, which typically

---

107. Scalet, "Five Most Shocking Things," 29.

108. "ChoicePoint CISO Named Information Security Executive of the Year in Georgia 2004," *Business Wire News*, March 19, 2004, https://www.businesswire.com/news/home/20040319005030/en/ChoicePoint-CISO-Named-Information-Security-Executive-Year.

109. Scalet, "Five Most Shocking Things."

involves a diverse team such as representatives from legal, public relations, human resources, risk management, executive management, and other departments. Furthermore, since data breaches often expose flaws within IT (including process deficiencies, resource allocation issues, and more), it is often most effective to have data breach planning managed by a team outside the IT department, thereby reducing the potential for conflict of interest.

"Information Security should [not] necessarily be under IT," said Chris Cwalina. "Incident response is in essence a risk management function. And an incident response team should have appropriate support and visibility in the organization or it will be difficult to make progress. Also, it is so important for legal to be part of the incident response function and investigative process. Security analysts and lawyers need to spend a lot of time together and learn to speak one another's language. This is critical."

"[T]he CISO can't just work in the tech space," said Michael Assante, chief security officer (CSO) of American Electric Power. "They have to start looking at business processes."[110]

"[T]he extent to which fingers are pointed at [Baich] speaks volumes about how broadly CISOs have come to be regarded as protectors of information, no matter the threat," wrote *CSO* magazine. "[W]hat happened reflected a wholesale failure of ChoicePoint's approach to security governance."[111] ChoicePoint had never fully evaluated or addressed the risks of a data breach at a holistic, enterprise level. This gap stemmed directly from the fact that ChoicePoint had never assigned responsibility for doing so *to a person who had an appropriate breadth of access within the organization*. Despite *CSO* magazine's damning assessment of ChoicePoint's information security program, this failure is repeated over and over in organizations everywhere, even to this very day.

In order to successfully manage cybersecurity, and its sister, data breach response, an executive-level person needs to be engaged, with oversight by the board of directors or other top stakeholders. All too often, we give a person responsibility for "information security," but it cannot truly be meaningful unless that person is placed high enough in the organization to actually oversee information management *across the whole enterprise*.

Within a month of ChoicePoint's breach notification, the company announced that it had hired Carol DiBattiste, former deputy administrator of the U.S. Transportation Security Administration, to take on the new role of "chief credentialing, compliance and privacy officer" for the company. This new role reported directly to the board of directors. "[W]e need a strong voice outside the day-to-day business that is responsible for customer credentialing, compliance and privacy," said John Hamrem, chair of ChoicePoint's privacy committee. "Having a person of Carol's stature join us is vital to our efforts to have the kind of policies, procedures and compliance programs that build confidence as well as set a standard for the industry."[112]

---

110. Scalet, "Five Most Shocking Things."

111. Scalet, "Five Most Shocking Things."

112. Associated Press, "ChoicePoint Names DiBattiste Chief Credentialing, Compliance and Privacy Officer," *Atlanta Business Chronicle*, March 8, 2005, https://www.bizjournals.com/atlanta/stories/2005/03/07/daily6.html.

4.8.2 The Myth of the Security Team

Cybersecurity and data breach response aren't solo efforts. Large organizations typically have an information security team, which is tasked with both proactive cybersecurity and incident response.

Data breaches, however, are crises that reverberate throughout the organization—and beyond. They cannot be designed or executed solely by the "information security team," however convenient that might seem. Response planning efforts must reflect the crisis itself and involve stakeholders throughout the organization and out into the broader ecosystem, such as:

- Legal
- Public relations
- Customer relations
- IT
- Cybersecurity team
- Insurance
- Human resources
- Physical security
- Finance
- Executive team
- Board of directors
- Forensics firms
- Customers
- Former IT staff
- Key vendors/suppliers

When developing a data breach crisis response function, management must engage all of the key stakeholders regularly. The frequency and depth of involvement varies for each stakeholder, but in order for crisis response plans to be effective, this involvement must be ongoing throughout the lifespan of the organization.

Develop

The great military strategist Sun Tsu said, "Win first, then do battle." This maxim is as true for data breaches as it is for war. "Develop" is the very first phase of our DRAMA breach response model, and it encompasses the activities that must occur before a breach happens. Organizations need to develop and maintain data breach response plans in order to minimize the negative impacts of a breach. Make sure your data breach crisis plan is initiated at the executive level and includes all key stakeholders throughout the enterprise.

4.9 Conclusion

ChoicePoint was a catalyst for change. From a historical perspective, the crisis was game changing, resulting in a dramatic shift in public perception, new laws, and even the birth of the term "data breach."

The ChoicePoint breach also demonstrates the importance of developing your data breach crisis management function in advance and ensuring that it is aligned with your organization's key risks. The breach was far more explosive and impactful because of the company's lack of response, particularly in the early stages of the crisis. At the same time, the company did, suddenly, adapt midcrisis and was able to manage the chronic phase effectively, which helped to restore confidence and value.

In this chapter, we analyzed the ChoicePoint breach in the context of Steven Fink's four stages of a crisis:

- Prodromal
- Acute
- Chronic
- Resolution

We also reviewed the capabilities that your organization needs to have in place in order to manage our data breach crisis:

- **Develop** your data breach response function.
- **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
- **Act** quickly, ethically, and empathetically to manage the crisis and perceptions.
- **Maintain** data breach response efforts throughout the chronic phase, and potentially long-term.
- **Adapt** proactively and wisely in response to a potential data breach.

The ChoicePoint crisis teaches us that, as the name implies, we have choices at each stage of the crisis. An organization, however, is not an individual, and it requires coordination and planning in order to ensure that smart decisions are made and acted upon.

Chapter 5

Stolen Data

Christmas Day, 1999. A teenage Russian hacker who went by the pseudonym "Maxus" sat in his dimly lit bedroom, hunched over a keyboard. Outside, wind whirled across the frozen nighttime wasteland. He checked his email one more time and shook his head. Nothing. He was bored.

No more waiting! It was time.

Weeks before, Maxus had stumbled across a security flaw in the website of CD Universe, a popular online music store. Exploring, he found he was able to download customer usernames, passwords, and even credit card numbers from the site: nearly 300,000 records in total. Normally, he would have sold the credit card numbers to criminals on Internet chat rooms, but this time, he had felt a little more creative. Instead, he faxed the company a ransom note that read, "Pay me $100,000 and I'll fix your bugs and forget about your SHOP FOREVER.....or I'll sell your cards and tell about this incident in news." CD Universe did not respond. Maxus waited, then emailed. Then he waited some more.[1]

Now, he had waited long enough.

Maxus quickly created a text file with some HTML code, and a hastily coded Perl script. He uploaded these both to his web server.[2] "MAXUS credit card datapipe," he named his new site, shown in Figure 5-1. "Hello, my name is Maxus. I would like to present you a credit cards datapipe. If you press the button you will get a real credit card directly from the biggest online shop database. No kidding."

For good measure, he added a link to one of his own music mixes: "listen to DJ Maxus music, click HERE." Then he added a guestbook and wrote a first message: "Hello carders! Maxus Stone."[3]

Maxus yawned. It was late—already early morning on December 26, 1999. The site was up. That'll show them. Time for a break.

Two weeks later, more than 300,000 credit card numbers had been stolen through Maxus's "credit card datapipe." Maxus emailed InternetNews.com with samples of the stolen data (notifying the news, as promised), and a media storm ensued. Elias Levy, chief technology

1. "John Markoff, "Thief Reveals Credit Card Data When Web Extortion Plot Fails," *New York Times*, January 10, 2000, http://www.nytimes.com/2000/01/10/business/thief-reveals-credit-card-data-when-web-extortion-plot-fails.html.

2. PC-Radio.com, *MAXUS Credit Cards Datapipe*, https://web.archive.org/web/20010417150341/http://www.pc-radio.com/maxus.htm (accessed April 24, 2016).

3. Mike Brunker, "CD Universe Evidence Compromised," *ZD Net*, June 8, 2000, http://www.zdnet.com/article/cd-universe-evidence-compromised.

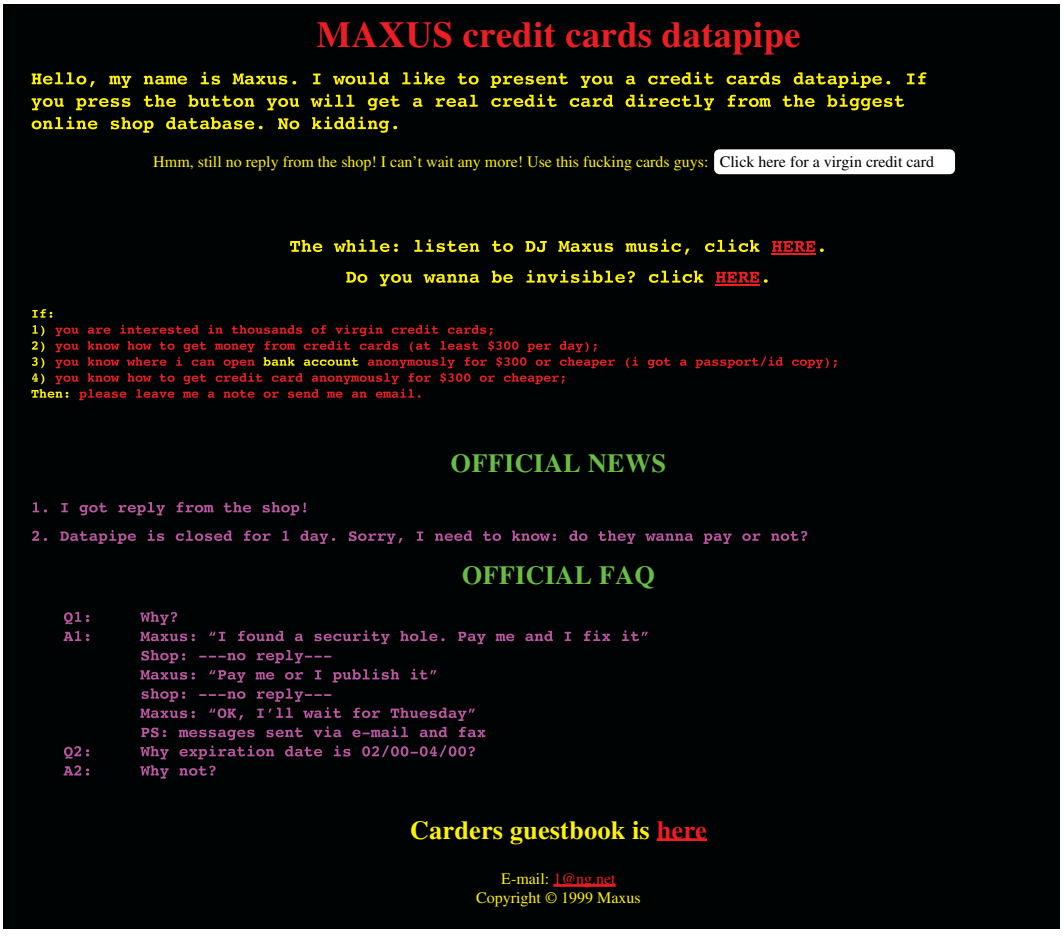


Figure 5-1. Representation of the carding site created by Maxus in the 2000 CD Universe breach. Source: PC-Radio.com, *MAXUS Credit Cards Datapipe*.

officer (CTO) of SecurityFocus.com, said the theft "is very disturbing. It realizes the fears people have about online commerce."[4]

The FBI opened an investigation, but six months later, the press reported, "U.S. authorities have been unable to find the thief. And even if they do, they are unlikely to be able to successfully prosecute the case because electronic evidence collected from the company's computers was not adequately protected."[5]

4. Brian McWilliams, "Failed Blackmail Attempt Leads to Credit Card Theft," *InternetNews.com*, January 9, 2000, http://www.internetnews.com/bus-news/print.php/278091; Editorial, "A New Threat to Your Credit," *Kiplinger's Personal Finance* 54, no. 4 (April 2000): 34.

5. Brunker, "CD Universe Evidence Compromised."

In an unusual move for the time, American Express and Discover replaced cards. A spokesperson for Discover said that it was "the only time she remembers the company recalling its cards."[6] While today, replacing cards is commonplace, at the time it was a novel—and expensive—move.

5.1 Leveraging Breached Data

When breached data is exploited, it is typically used for one of the following purposes:

- *Fraud* - Data is leveraged by an attacker to gain money, goods, or services.
- *Sale* - Data is sold on the dark web or to a direct buyer for immediate profit.
- *Intelligence* - Data is used by an opponent to gain a strategic advantage in military, diplomatic, economic, or even personal matters. (Revealing that data has been leaked or stolen may reduce the value of the information or damage future prospects for obtaining covert intelligence.)
- *Exposure* - Data is revealed to the world, thereby damaging the target's reputation, unmasking illicit or objectionable activities, or reducing the value of an information asset.
- *Extortion* - An attacker threatens to transfer data to an opponent or expose it to the world, unless the target gives in to demands (often a monetary payment).

Anyone—individuals, businesses, governments—can leverage breached data in these ways, in order to gain an advantage or damage another entity. In some cases, there are multiple ways that the data can be leveraged. For example, in the Maxus case, pilfered payment card data was used for attempted extortion, exposure, and, ultimately, fraud.

In this chapter, we will explore how data can be used for fraud or sold on the dark web. (In later chapters, we will address intelligence, exposure, and extortion.) Fraud and the dark web fueled the epidemic of data breaches and subsequent regulations that emerged during the first decade of the twenty-first century and that still impact us today. Along the way, we will highlight key technological advancements that led to the creation of the dark web, which facilitates resale of stolen data and also supplies tools and techniques for breaking into computers and accounts.

5.2 Fraud

Criminals often steal or purchase data in order to commit fraud. Common types of fraud that relate to data breaches include:

- **Payment card fraud** - Stolen payment card numbers are used to create fake cards or purchase goods.

6. Editorial, "AmEx, Discover Forced to Replace Cards over Security Breach," *CNET*, January 19, 2000, https://web.archive.org/web/20150402113747/http://news.cnet.com/2100-1017-235818.html.

- **Insurance fraud** - Misuse of a victim's health insurance data to obtain insurance coverage for medical services. This is especially common in the United States, where gaps in insurance coverage create need and the distributed insurance network makes it difficult to detect and respond to fraud.
- **Prescription drug fraud** - Misuse of a victim's prescription records, medical records, and/or insurance coverage specifically to obtain prescription drugs.
- **W-2 fraud** - Theft of personal information is used to file fake tax returns so that criminals can fraudulently receive the victim's tax refund.
- **Wire transfer fraud** - Victims are tricked into initiating a wire transfer to a bank account controlled by criminals, often in the context of a vendor payment or real estate transaction.
- **Identity theft** - A general term that refers to the misappropriation of a victim's personal information (name, address, Social Security number (SSN), insurance details, payment card number, etc.) for the purposes of committing fraud. All of the specific types of fraud listed above are examples of identity theft.

5.2.1 From Fraud to Data Breaches

Fraud, of course, is nothing new, but it has evolved dramatically with the shift to online business activities and the emergence of the dark web. In the late twentieth century, criminals focused on stealing valuable data locally, from consumers or businesses, and typically resold it to contacts who were physically nearby. As the Internet blossomed, it opened up new avenues for fraud and led to the emergence of data breaches on a massive scale.

"ConMan" was one such criminal. Today, ConMan is a respected security professional at a major corporation—but as a teenager on Long Island in the 1990s, he made money stealing new, unsigned credit cards out of people's mailboxes and selling them to his mafia contacts for a fraction of the card limit.

Since ConMan's uncle was a computer programmer, he was exposed to the Internet early on. This gave him a "great business idea": If he could break into the credit card companies online, he would be able to steal or create as many cards as he wanted. There would be no need to physically steal mail at all.

With guidance from his friends on Bulletin-Board Systems, ConMan eventually broke into a credit card company via a modem, gaining access to a database that enabled him to read details on existing cards or create new credit cards with arbitrary names and numbers. He then mailed these to abandoned homes in Long Island and ultimately sold them to his mafia contacts.

"I'd go to my mafia contact and sell this $5k card for $500 dollars," ConMan explained. "I would take 10% and they would say 'absolutely!' and they would go out and use it. I never used one myself."

Wisely, ConMan never used his home Internet connection to break into the credit card company. Instead, he co-opted his neighbors' Internet connections. (Long before the days of stealing wireless connectivity, ConMan "stole wired.") "I had a laptop—well, it was actually giant and ridiculous in the late 90s—and I took this beast of a machine along the side of a house somewhere and hook up, [so I could] actually get online," he explained. "I'd just unscrew the

box, and I'd hook the wire to the house, I'd run it across the lawn. I was using their line to dial out in the middle of the night . . . or I'd ride my bike 4 blocks over and I'd do it from some [random] house where there was an abandoned house next door. Every once in a while your connection would drop because somebody in the house picked up the phone."

ConMan wasn't alone. During the 1990s, many early hackers "aged out" of mischievous activities and began to focus more on criminal activities for profit, essentially becoming professional black-hat hackers. For example, teenage hacker Albert Gonzalez (or "soupnazi" to his online friends) led a group called the "Keebler Elves" that was known for defacing websites. However, Albert and his cohorts soon discovered that breaking into a website gave them easy access to databases of credit card numbers, SSNs, identification information, and more.

Hackers who started off as innocent explorers turned to crime, and criminals turned to hackers for data. "Black hats" like Albert became less interested in defacing websites and more interested in quietly harvesting valuable data. "I've told the Keebler members that I'm not a big fan of defacing pages," Albert went on to say. "I'd rather have root [complete access] to someone's account."[7]

Albert leveraged his access to quietly steal credit card numbers, identification data, and other information that he could monetize. "[Albert] was . . . purchasing clothing and CDs online with stolen credit-card numbers," reported the *New York Times*, years later. "He ordered the merchandise delivered to empty houses in Miami, and then had a friend drive him to pick it up during lunch period."[8] Much like ConMan, Albert learned to leverage abandoned houses for delivery of ill-gotten goods.

5.3 Sale

Stolen data can be used to commit fraud, but often hackers (like ConMan) do not want to take the risk of committing fraud themselves. Instead, criminals that specialize in breaching digital data repositories may choose to sell their ill-gotten goods to other criminals, who in turn specialize in committing fraud. Once upon a time, this required having personal connections with organized crime groups such as the mafia. However, as legitimate data markets expanded, so too did the underground trade in stolen data.

Specific technological developments such as carding shops, onion routing, and cryptocurrency paved the way for the dark web: a network of underground e-commerce sites that facilitate the trade of stolen data and tools to support hacking and fraud (among other nefarious activities).

The dark web fueled data breaches. Criminals could monetize stolen data far more easily and with less risk. They now had a forum to dump all kinds of stolen data, including competitive intelligence, passwords, and medical records, even if they had no clear path for leveraging

7. Robert Lemos, "Does the Media Provoke Hacking?" *ZD Net*, July 6, 1999, http://www.zdnet.com/article/does-the-media-provoke-hacking.

8. James Verini, "The Great Cyberheist," *New York Times Magazine*, November 10, 2010, http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

the data directly. Instead of stealing just payment card data or personal information from a compromised system, criminals had incentive to gather up what data they could and place it online for prospective buyers to browse. The more data, the more profit.

By understanding how the dark web works, enterprise security professionals can more accurately assess risk and anticipate future threats. Today's security professionals may also be called upon to access the dark web in order to evaluate a potential data breach or conduct threat intelligence. In this section, we will showcase the key technologies that underly the dark web, including dark e-commerce sites, onion routing, and cryptocurrency.

5.3.1 Selling Stolen Data

The turn of the twenty-first century brought with it a wave of criminal discussion forums, how-to guides for committing fraud, and tools for counterfeiters. The Counterfeit Library, which came out in 2000, was an early site that was popular with identification thieves and carders (payment card thieves). Thousands of contributers primarily from the English-speaking world joined in the conversations, swapping detailed information about identity theft, credit card fraud, fake degrees, doctors' letters, and many other forms of document fraud and theft.[9]

By 2001, the Russian-speaking criminal world had established CarderPlanet.com, which facilitated the exchange of stolen digital goods, from credit card numbers to "fullz" (a collection of information about a person, such as the victim's name, address, Social Security number, driver's license number, mother's maiden name, and potentially other details that would be useful for a fraudster). The site also sold physical products to support fraud, such as blank plastic cards with magnetic stripes (for copying stolen card numbers onto).[10]

Payment card data was no longer simply a tool to be used for converting credit to cash. Instead, it had become a product. The same was true for identification details and other personal data. Sites like CarderPlanet created an efficient and widely accessible marketplace for these products and, in the process, gave hackers around the world new incentive—and tools—to break into networks and steal the data.

5.3.1.1 Shadowcrew

The English-speaking world wanted in on the action. In 2002, the "Shadowcrew" site was established by a former mortgage broker in New Jersey and a part-time student in Arizona. Shadowcrew was an "archetypal criminal cyberbazaar" that brought the sophisticated features of CarderPlanet to the English-speaking world.[11] Figure 5-2 is a screenshot of the Shadowcrew home page, as of October 2004.

Thousands of users flocked to Shadowcrew in order to read tutorials on everything from "how to use a stolen credit card number, forge a driver's license, defeat a burglar alarm, or silence a gun." The site's forums and tutorials helped to perpetuate knowledge about hacking, typically for the purposes of stealing credit and debit card numbers and other valuable data. Shadowcrew also provided a marketplace for buying and selling credit and debit card "dumps":

9. Kevin Poulsen, *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground* (New York: Crown, 2011), 74.

10. Poulsen, *Kingpin*, 75.

11. Verini, "Great Cyberheist."

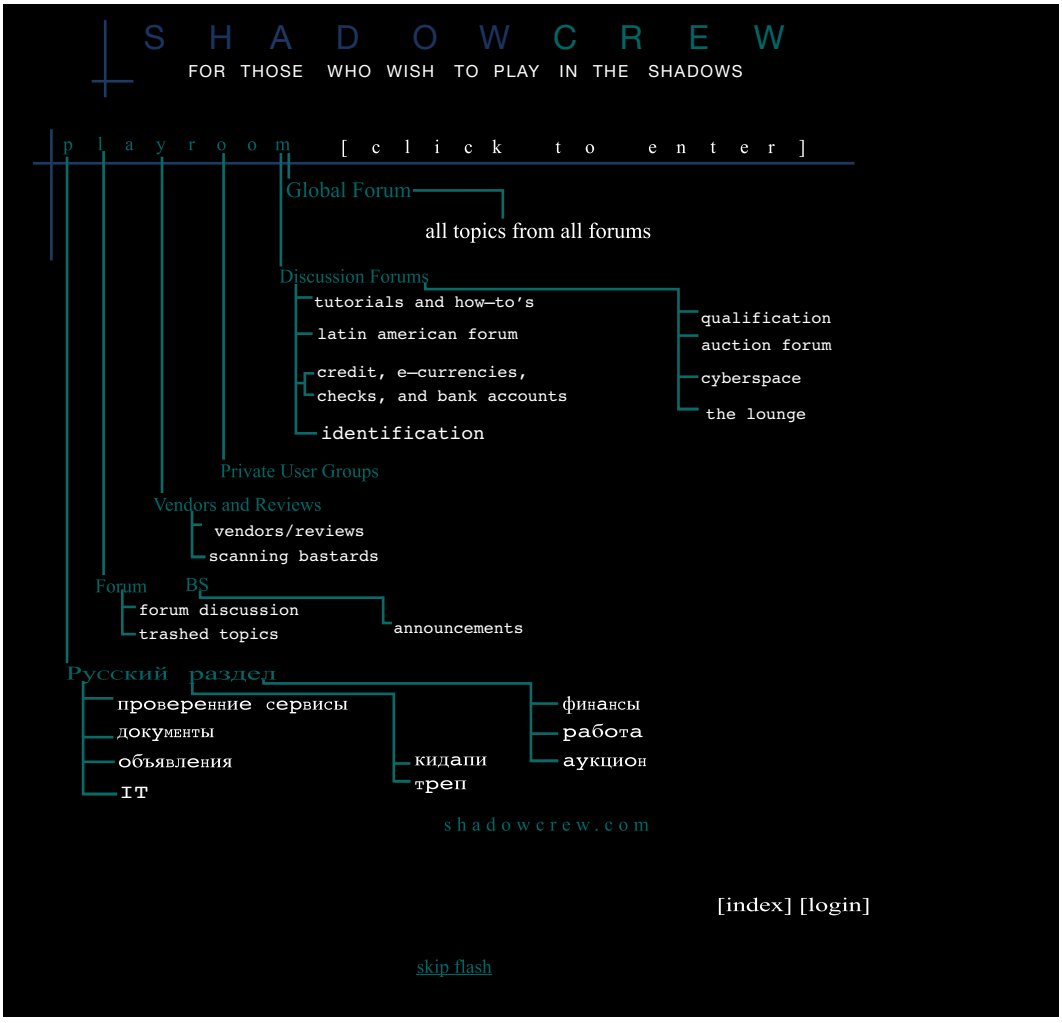


Figure 5-2. Representation of the Shadowcrew home page, circa October 2004. Source: https://web.archive.org/web/20041019024632/shadowcrew.com.

files containing data from cards' magstripes, typically sold in dumps with tens, hundreds, or even thousands of records. The dumps were purchased by criminals who would resell the data or convert it to cash or goods, typically by overwriting the magnetic stripe on gift cards or card blanks with the stolen data using a magnetic strip encoder (also available on Shadowcrew) or by using the stolen data for card-not-present (CNP) transactions with retailers.[12]

12. Brad Stone, "Global Trail of an Online Crime Ring," *New York Times*, August 11, 2008, http://www.nytimes.com/2008/08/12/technology/12theft.html.

Vendors from around the world applied to sell their goods and, once approved, provided "a dizzying array of illicit products and services: credit reports, hacked online bank accounts, and names, birth dates, and Social Security numbers of potential identity theft targets."[13] Vendors wishing to sell their products on Shadowcrew were required to go through a formal vetting process. The prospective vendor would send a sample of his or her product to a designated Shadowcrew member, who would evaluate it and write a review. Vendors who scammed members were shunned and could be punished. In one case, Shadowcrew organizers punished a "scamming bastard" known as "CCSupplier" by publishing his real name, home address, and phone number on the site.[14] One federal prosecutor later referred to Shadowcrew as "an eBay, Monster.com and MySpace for cybercrime."[15]

Shadowcrew was easily accessible to anyone who could type the easy-to-remember URL "shadowcrew.com." (The dark web of the modern world didn't yet exist.) On the one hand, this low barrier to entry made it easy for Shadowcrew to attract new buyers and sellers. On the other hand, it also enabled law enforcement to easily visit the site, apply for accounts, set up sting operations, and track down the administrators—ultimately leading to Shadowcrew's demise.

5.3.1.2 Shadowcrew Takedown

As Shadowcrew and similar sites expanded, credit card fraud rose quickly. In the United States, federal investigators struggled to track down the perpetrators. They got their lucky break one night when hacker Albert Gonzalez was nabbed "cashing out" stolen payment card data at an ATM in New York.

Busted!

Cybercriminal Albert Gonzalez carefully glued on a costume nose ring, donned a long, scraggly women's wig, and packed his pockets full of more than 75 debit cards. It was a warm summer night in New York. Shortly before midnight, the 22-year-old Cuban-born hacker walked into a Chase Manhattan ATM on the Upper West Side of the city. He had timed his visit carefully. Pulling a debit card out of his pocket, he fed it into the ATM and collected the cash. Then he pulled out another and did the same. And another. As soon as the clock struck midnight, the withdrawal limits on the debit cards would reset, and he planned to do the same thing all over again. Albert was "cashing out."

There was another person in the Chase ATM that night, watching him closely. Unbeknownst to Albert, a plainclothes NYPD detective had followed him into the ATM that night. The detective was on the hunt for car thieves in the area and thought Albert looked suspicious. Watching Albert

(*Continues*)

13. Poulsen, *Kingpin*.

14. Sarah Hilley, "Case Analysis: Shadowcrew Carding Gang," Bank Info Security, April 3, 2006, http://www.bankinfosecurity.com/case-analysis-shadowcrew-carding-gang-a-136.

15. Stone, "Global Trail."

(*Continued*)

feed card after card into the ATM, the detective concluded that, although Albert wasn't stealing cars, he was probably "stealing something."[16] *He arrested Albert and brought him into custody.*

No one knew it at the time, but Albert's arrest would ultimately lead to the downfall of the Shadowcrew site. It was also just the beginning of Albert's incredible career as one the greatest data thieves the world has ever seen—all the more shocking given that, at the same time, he was employed by the U.S. Secret Service.

When Albert Gonzalez was caught in July 2003, the New York/New Jersey Secret Service was knee-deep in investigating carders—particularly those "cashing out" in the area—without much success. Although the Secret Service is perhaps best known for protecting the president of the United States, the agency is also responsible for investigating financial crimes. Due to the increasing technical sophistication of financial fraud rings, the agency created the New York Electronic Crimes Task Force (ECTF) in 1995. It was expanded to a national program in 2001 as part of the U.S. Patriot Act.

Albert, they found, was exactly what they needed—polite, smart, and deeply embedded in criminal card fraud rings. Under the nickname of "Cumbajohnny," Gonzalez was a moderator and "rising star" on the online carder marketplace, Shadowcrew. After his arrest, law enforcement discovered millions of card numbers on his home computer in New Jersey and offered him a deal: If he helped the Secret Service take down other fraudsters, it wouldn't prosecute him.[17]

Albert agreed. He was the thread that would ultimately unravel Shadowcrew and lead to the indictment of 19 of the site's members—but oddly enough, for Albert, it was just the beginning of his career as a cybercriminal mastermind. First a double agent and then eventually a double-double agent, Gonzalez helped Secret Service operatives infiltrate the carding underground forums and take down his fellow carders—while at the same time stealing millions of payment card numbers from retailers and managing an international money-laundering ring.

"In the beginning, he was quiet and reserved, but then he started opening up. He started to trust us," said a Secret Service agent who worked closely with Albert.[18] Albert not only shared details about how Shadowcrew and card fraud worked—he also became the "lynchpin" of "Operation Firewall," the Secret Service's year-long investigation and takedown of the Shadowcrew organization. In exchange, the Secret Service paid him an annual salary of $75,000/year (cash, so as to not create a paper trail).[19]

"Gonzalez worked alongside the agents, sometimes all day and into the night, for months on end. Most called him Albert. A couple of them who especially liked him called him Soup,

16. James Verini, "The Hacker Who Went into the Cold," *New York Times Magazine*, November 14, 2010, 44–51, 60, 62–63.

17. Verini, "Great Cyberheist."

18. Verini, "Hacker Who Went into the Cold," 44–51, 60, 62–63.

19. Kim Zetter, "Secret Service Paid TJX Hacker $75,000 a Year," *Wired*, March 22, 2010, https://www.wired.com/2010/03/gonzalez-salary.

after his old screen-name soupnazi."[20] Working out of an Army garage in Jersey City, Albert slowly gained the trust of Shadowcrew's leadership and rose in their ranks.

By the spring of 2004, Albert had convinced the Shadowcrew leadership to move their communications over to a virtual private network (VPN) that he maintained. The VPN offered Shadowcrew leaders assurance that their emails, instant messages, and other communications would be encrypted and kept safe from the prying eyes of Internet service provider (ISP) security teams or law enforcement. Secretly, the Secret Service monitored all of the VPN traffic and collected detailed evidence of Shadowcrew members' illegal activities. As described later in the book, *Kingpin*:

> There were deals every day and every night, with a weekly surge in trading Sunday evenings. The transactions ranged from the petty to the gargantuan. On May 19, agents watched Scarface transfer 115,695 credit card numbers to another member; in July, APK moved a counterfeit UK passport; in August, Mintfloss sold a fake New York driver's license, an Empire Blue Cross health insurance card, and a City University of New York student ID card to a member in need of a full identification portfolio.

On the night of October 26, 2004, Albert sat at a keyboard at Secret Service Headquarters in Washington, D.C. His job: to lure the unsuspecting targets of Operation Firewall into chat sessions before Secret Service agents busted them. The timing was carefully coordinated: agents placed in more than eight U.S. states and six countries barged down doors beginning at 9 p.m. The goal was to arrest as many targets as quickly as possible before Shadowcrew members had time to alert each other. Getting the members to converse in a chat session as the arrests occurred provided key evidence connecting their real-life identities with their online personas.

The *New York Times* later reported that "it was by some estimates the most successful cybercrime case the government had ever carried out."[21] Nineteen people were indicted, and many more were spooked. Figure 5-3 shows the Shadowcrew home page after the Secret Service takedown. A note at the bottom of the page urged members to "CONTACT YOUR LOCAL UNITED STATES SECRET SERVICE FIELD OFFICE....BEFORE WE CONTACT YOU!!"

Shadowcrew's demise taught cybercriminals a lesson: They needed to carefully protect the anonymity of buyers, sellers, and site administrators.

5.3.2 Asymmetric Cryptography

Asymmetric cryptography, popularly known as public key cryptography, is a fundamental security concept used both by defenders to protect their data and attackers to evade detection and identification. Asymmetric cryptography is the foundation of both onion routing and cryptocurrency, two important technologies that we will study in the next sections. Asymmetric cryptography can be used for good: for example, to keep emails secure even after a hacker has broken into your inbox. It can also be used by cybercriminals to facilitate quick and anonymous

20. Verini, "Great Cyberheist."

21. Verini, "Great Cyberheist."

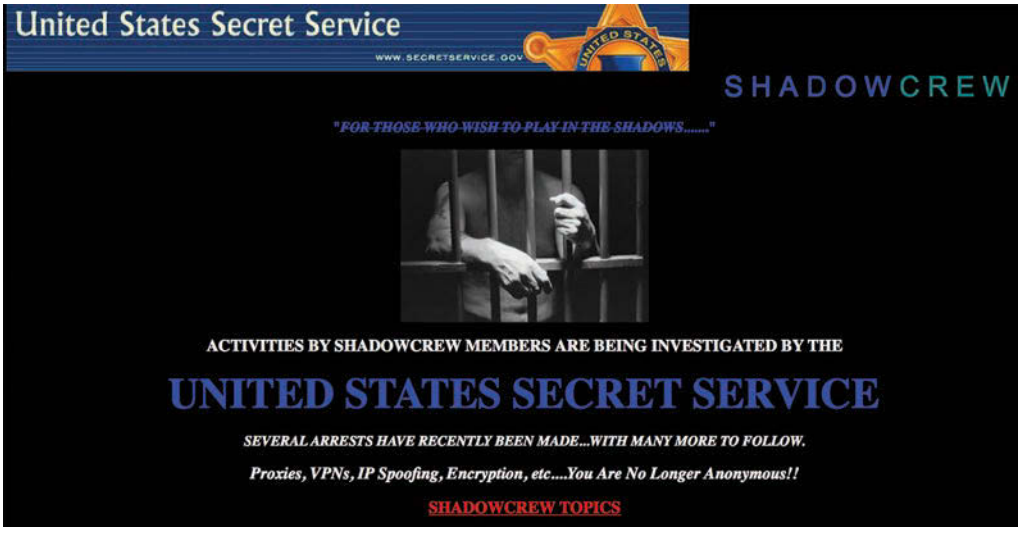


Figure 5-3. The Shadowcrew home page, as seen on October 30, 2004. Source: U.S. Secret Service, October 30, 2004, http://web.archive.org/web/20041030015234/http://shadowcrew.com/.

ransom payments or to keep buyers and sellers on the dark web anonymous. And it can be used for so much more.

Every professional involved in data breach prevention, preparation, response, or investigation should be familiar with the fundamental principles of asymmetric cryptography because it is a factor in almost every modern data breach. Here are the most important technical concepts:

Encryption is the process of scrambling information so it cannot be accessed by anyone except authorized parties. There are two basic types of encryption: *symmetric* and *asymmetric* encryption. (A "key" is simply a long, randomized string of numbers, typically stored in a file, which is used as input when you encrypt or decrypt a file.) With symmetric key encryption, the *same* key is required to encrypt or decrypt the message. This means that the person who has the key can scramble or recover the original message, but no one else can. Symmetric encryption is useful when you want to, say, encrypt a laptop so that a thief could not access the contents.

With *asymmetric* (also known as *public key*) encryption, there are two different keys, which together form a *key pair*. What one key encrypts, the other key decrypts. Among other benefits, this makes it easy to send and receive confidential messages over the Internet. Each person publishes one key so the whole world can view it (the public key) and keeps the corresponding *private key* hidden. To send a confidential message, you would look up the recipient's public key and encrypt the message with it. Only the private key can decrypt the message, so you can happily send the message across the big wide Internet, knowing that only the person with the corresponding private key (the recipient) will be able to decrypt the message. This concept is also fundamental to onion routing, as we will see.

Let's say you want to verify that a specific person really did send a message and the message was not altered in transit. Asymmetric key cryptography can also be used for this purpose. The

sender would use his or her private key, plus the message, as input to a mathematical algorithm that then produces a *digital signature*. The digital signature is appended to the message when it is sent. The recipient can then look up the sender's public key and feed this plus the message itself into a signature verifying algorithm, which is designed to produce a result that indicates whether the sender and message combination is authentic.

The effectiveness of asymmetric cryptography relies upon the secrecy of the private key. For this reason, private keys have become a common target of data breaches. Criminals routinely break into computers and specifically scan for private keys used for cryptocurrency, file encryption, communications security, and more. These data elements, too, can be bought and sold for a profit on the dark web. With this in mind, let's examine how asymmetric encryption facilitated the creation of the dark web in the first place.

5.3.3 Onion Routing

Onion routing, a technique for anonymizing network traffic, is the core technology that now defines the dark web. The concept of onion routing was invented in the mid-1990s by scientists at the U.S. Naval Research Laboratory, further developed by Defense Advanced Research Projects Agency (DARPA), and then popularized in the early 2000s. Onion routing is also used for making anonymous submissions to sites like WikiLeaks, which are used to expose leaked data (we will discuss this more in Chapter 10, "Exposure and Weaponization").

To understand how onion routing works, let's first look at an ordinary visit to an Internet website. Normally, a user's web traffic is sent to a web server, and the web server receives the source IP address of the requesting computer along with the content of the request. Any intermediary (such as an ISP) that can view a web server's traffic can gather a list of its visitors (again, based on the source IP address). Law enforcement can work with ISPs to map IP addresses to customer names and addresses. This can be tricky, of course, when cybercriminals are spread out across the globe, but today, it is done routinely.

Onion routing protects users' traffic by wrapping their messages in layers of encryption, so that the ultimate source and destination cannot be seen by anyone. To understand how onion routing works, imagine a network of computers, each of which can pass along messages from other computers. When a user wants to anonymously surf to a website, his or her computer selects a route through the network and encrypts the message route information in layers. Each layer of encryption can be opened only by the corresponding computer along the path (because it is encrypted using that computer's public key) and when decrypted, reveals the address of the next computer in the path.

As the message travels through the network, each computer decrypts the current layer of encryption, reads the address of the next computer, peels off the current layer, and passes the remaining message to the next computer in the path. This next computer similarly decrypts the current layer of encryption, reads the address of the next computer, peels off the current layer, and passes the remaining message along. This process continues until the message reaches its final destination.

In this manner, messages can be transferred through the network, but no intermediary ever sees both the source and destination addresses. Onion routing is based on the principle of minimal privilege, meaning that it reveals only the information necessary to get the message where it needs to be. Each computer can know the address of the previous computer in the path and the address of the next computer, but that's it.

Tor is one popular example of onion routing software, which was developed by scientists Paul Syverson, Roger Dingledine, and Nick Mathewson. Tor has many different uses: Law enforcement uses it to collect evidence from dark websites anonymously; intelligence agents use it to hide their communications in foreign countries; cybercriminals use it to conceal their identities; and everyday people use it to preserve their privacy on the web. Dingledine smiles when he points out that Tor is perhaps the only project funded by both the Department of Defense and the Electronic Frontier Foundation (EFF). "The United States government can't simply run an anonymity system for everybody and then use it themselves only," he explains. "Because then every time a connection came from it people would say, 'Oh, it's another CIA agent.' If those are the only people using the network."[22]

Importantly, Tor includes a way for users to offer "onion services" (also known as "hidden services,") such as websites and chat rooms. Anyone wishing to offer a service can register in the Tor network and obtain an "onion service descriptor," which is a 16-character name followed by ".onion". Visitors can access the service by typing the onion service descriptor into a Tor browser. (There are also Tor plug-ins for popular web browsers.) They are then routed via preconfigured paths to the service. Note that unlike ordinary web services, hidden services can be hosted behind a firewall because the server's IP address does not need to be publicly routable.

Today, carding shops and other dark websites are often set up as hidden services in Tor, where sellers peddle stolen data and buyers browse the myriad of offerings.

5.3.4 Dark E-Commerce Sites

As Tor grew in popularity, cybercriminals discovered that they could use it to market stolen goods over a network that inherently protected the anonymity of buyers and sellers and was not accessible to the general public. This dramatically reduced the risk of selling illegal data, drugs, and other wares online. Hidden services on Tor expanded, fueling trade in stolen data and incentivizing criminals to hack. The result? More data breaches.

But early dark web e-commerce sites still had a problem: payment. Onion routing made it difficult to trace buyers and sellers using network forensics. Law enforcement still had another ace up their sleeves, and that was the lack of a truly anonymous digital payment method. Buyers on the dark web had some options for paying for stolen goods. For example, buyers could physically mail cash, but there was always the risk that it would get stolen in transit, and of course physical packages could be inspected and traced by law enforcement. Checks and credit cards were far too easily tracked, and sellers did not want to worry about payments being reversed or seized by legitimate banking institutions. In the early days of the dark web, PayPal was popular, as were fast money transfer services such as Western Union. Services such as Libery Reserve (a "digital currency" backed by gold) sprang up, offering criminals a method for transferring funds with relative anonymity—but these services were often shady and would on occasion disappear, along with everyone's money.[23] Law enforcement had multiple avenues for tracing payments through any of these systems, which typically required the user to provide an email address, at minimum.

---

22. Yasha Levine, "Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government," *Pando*, July 16, 2014, https://pando.com/2014/07/16/tor-spooks.

23. "Liberty Reserve Digital Money Service Forced Offline," *BBC News*, May 27, 2013, https://www.bbc.co.uk/news/technology-22680297.

The Farmer's Market was an example of a popular early dark e-commerce site that ultimately was shut down due to the lack of anonymous payment and linked email accounts. Like legitimate e-commerce sites of the time, it had a user-friendly web order form and features such as discussion forums, vendor screening, and customer support. The site supported a variety of payment systems, including cash, Western Union, PayPal, iGolder, and Pecunix.[24] "The Farmer's Market . . . was like an Amazon for consumers of controlled substances," wrote Dan Goodin for *Ars Technica*, which reported that the market had approximately 3,000 customers in 35 countries.[25]

Onion routing wasn't enough to protect the ringleaders of the Farmer's Market from arrest and takedown. In 2012, the U.S. federal government unsealed an indictment of eight people involved in the Farmer's Market, including both site administrators and customers. Based on evidence presented in the indictment, law enforcement agents appeared to have traced electronic payments through financial services vendors such as PayPal and Western Union.[26]

5.3.5 Cryptocurrency

In order for cybercriminals to truly obtain anonymity, they needed a more secure payment system. This was delivered, modestly and precisely, on Halloween in 2008. On this day, an unidentified person (or group of individuals) that went by the name "Satoshi Nakamoto" sent an email that would change the world. "I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party," began the email, which was sent to a popular cryptography mailing list. The message included a link to the author's new paper, "Bitcoin: A Peer-to-Peer Electronic Cash System."[27]

Initially scrutinized by academics, Bitcoin changed the dark web—and the field of data breaches—within a few short years. Dark web e-commerce sites such as the Silk Road relied upon it for transactions. Bitcoin and other cryptocurrencies have several features that are important for buyers and sellers on the dark web:

- Anonymous payments
- No middleman
- Nonreversible

In traditional online payment systems brokered by financial institutions, suspicious or disputed transactions can be traced or reversed by the intermediary financial institutions. Bitcoin's invention and subsequent global adoption gave cybercriminals, for the first time, the ability to conduct anonymous, irreversible financial transactions, outside the scrutiny of the legitimate banking infrastructure. This dramatically reduced risk to buyers and sellers, paving the way for a dramatic expansion of the dark markets.

---

24. Kim Zetter, "8 Suspects Arrested in Online Drugs Market Sting," *Wired*, April 16, 2012, https://www.wired.com/2012/04/online-drug-market-takedown.

25. Dan Goodin, "Feds Shutter Online Narcotics Store That Used TOR to Hide Its Tracks," *Ars Technica*, April 12, 2016, https://arstechnica.com/tech-policy/2012/04/feds-shutter-online-narcotics-store-that-used-tor-to-hide-its-tracks.

26. United States v. Marc Peter Willems, CR-11-01137 (C.D. Cal. 2011), https://www.wired.com/images_blogs/threatlevel/2012/04/WILLEMSIndictment-FILED.045.pdf.

27. Email in author's inbox, received on October 31, 2008, via the mailing list "cryptography@metzdowd.org".

Data breach responders and security professionals should know, at a fundamental level, how cryptocurrency works since the technology facilitates the sale of stolen data and is used in ransomware and extortion cases, cryptojacking, and other cases. Here are a few important things to know about cryptocurrency.

- Cryptocurrency is a digital asset, in which cryptography is used to regulate the creation of new units and transfer funds. (Bitcoin was the first cryptocurrency.)
- Transactions are recorded in a distributed digital ledger known as the *blockchain*.
- The blockchain is just a collection of files, which anyone in the world can download or share with others.
- Users have "public/private key pairs" that are stored in a *wallet*. These are used to faciliate funds transfers and verify transactions. (See section 5.3.2 for a summary of asymmetric key encryption.)
- Wallets do not store coins. They store public/private key pairs.
- To send cryptocurrency to another person, you create a message that contains (among other things) the amount you are sending, the public key of the recipient, and a digital signature that you create using your own private key. Then you send that out to all the other computers in the cryptocurrency network. Every other computer can use your corresponding public key to verify that your payment message is authentic.
- "Miners" are computers that earn cryptocurrency either by processing other people's transactions or by discovering a brand new block in the blockchain. Both of these activities require significant computing power, which represents an investment in equipment, electricity, and time.
- To discover a new block, a miner must guess the answer to a very hard math puzzle. When a miner finds a valid answer, it places it in a message that is digitally signed with its private key and sends that to the cryptocurrency network. The first miner to discover a new block is rewarded with a specific, predetermined amount of cryptocurrency, and a new block that includes the answer, the amount, and the successful miner's public key is added to the blockchain.
- In most types of cryptocurrency, the blockchain is public, meaning that anyone can view the sender address, recipient address, and amount of any transaction. (Monero is a notable exception, since it obfuscates much of the public transactional data.) However, public/private key pairs do not need to be linked to a specific person's identity, and so it is possible to conduct transactions anonymously.[28]
- Since there is no central bank and no one organization controls the blockchain, it is not possible for a third party to reverse a transaction.

28. Studies have shown that it is possible to analyze the public Bitcoin ledger and derive information about the *relationships* between wallet addresses, which can potentially lead to identification. See Dorit Ron and Adi Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Israel, 2012, https://pdfs.semanticscholar.org/93ba/e7155092c8ba1ae1c4ad9f30ae1b7c829dd7.pdf.

Cybercriminals routinely use cryptocurrency to buy and sell stolen data on the dark web. Cryptocurrency also plays an important role in cyber extortion cases (which are often data breaches), as discussed in Chapter 11, "Extortion." Extortionists threaten to hold data hostage or expose it to the world unless paid in cryptocurrency. Cryptocurrency enables criminals to demand quick, anonymous payments over the Internet. At the same time, criminals are protected because the ransom payments are difficult if not impossible to trace or reverse.

Since cryptocurrency is a digital asset, it has also become a target of data breaches. New strains of malware now scan an infected host for cryptocurrency, steal it, and delete it. As cryptomining operations multiply and financial institutions begin to experiment with using cryptocurrency for interbank transfer,[29] data breaches involving cryptocurrency are likely to become increasingly common.

Finally, cryptojacking is a new type of cyberthreat that often results in a legally declared data breach (regardless of whether any data was actually stolen). Cryptojacking is a breach where an attacker gains unauthorized access to a computer and installs cryptocurrency mining software. In this way, criminals can reap the rewards of cryptocurrency mining, without the investment in equipment or electricity.

5.3.6 Modern Dark Data Brokers

The emergence of onion routing and cryptocurrency changed the game for cybercriminals. Suddenly, anyone in the world could buy and sell stolen data online, with relatively little risk of being tracked down if they were careful. E-commerce sites quickly sprang up on the dark web, offering many of the same features as mainstream e-commerce sites: user-friendly interfaces, payment escrow, vendor feedback, and more.

The Silk Road was the first darknet market to leverage both Tor and Bitcoin. Launched by self-taught programmer Ross Ulbricht (later known as "Dread Pirate Roberts") in early 2011, the site eventually grew to include nearly a million users, facilitating more than $1 billion of sales.[30]

"Silk Road has emerged as the most sophisticated and extensive criminal marketplace on the Internet today," explained FBI Special Agent Christopher Tarbell, in a criminal complaint against Ulbricht filed on September 27, 2013. "The site has sought to make conducting illegal transactions on the Internet as easy and frictionless as shopping online at mainstream e-commerce websites."[31]

The cutting-edge marketplace featured a Bitcoin escrow system, as well as a Bitcoin "tumbler" to provide extra transaction security for users. The tumbler "sends all payments through a complex, semi-random series of dummy transactions, . . . making it nearly impossible

29. Anthony Coggin, "Singapore Central Bank to Use Blockchain Tech for New Payment Transfer Project," *Cointelegraph*, June 9, 2017, https://cointelegraph.com/news/singapore-central-bank-to-use-blockchain-tech-for-new-payment-transfer-project.

30. Joshuah Bearman, "The Rise & Fall of Silk Road," *Wired*, May 2015, https://www.wired.com/2015/04/silk-road-1.

31. United States v. Ross William Ulbricht, 13-MAG-2328 (S.D.N.Y. 2013), https://krebsonsecurity.com/wp-content/uploads/2013/10/UlbrichtCriminalComplaint.pdf.

to link your payment with any coins leaving the site."[32] This means that even if both the buyer's and seller's Bitcoin addresses are known, they are not directly linked to a shared transaction in the blockchain, which makes it very difficult to follow the money.

The Silk Road also featured a popular discusson forum, as well as a private messaging system, so that users would not have to rely on third-party communications systems such as Hushmail, which had been the downfall of many cybercriminals. Like legitimate e-commerce enterprises, the site was supported by a team of administrators who received regular Bitcoin payments ranging from $1,000 to $2,000 per week. It was shut down in October 2013, in a dramatic FBI raid that led to Ulbricht's arrest. Less than a month later, Silk Road 2.0 was launched (though it, too, shut down in November 2014). As of the time of this writing, Silk Road 3.1 is currently operational and offers a dizzying array of stolen data dumps, hacking tools, drugs, and other contraband.

Modern darknet markets provide a clear path for exchanging—and therefore quickly monetizing—stolen data. As a result, specialized roles have emerged in the hacker economy. For example, different criminals might:

- Launch phishing attacks and build "botnets" for resale
- Scan compromised "bots" for potentially valuable data and then harvest, sort, and resell it
- Create hacker tools such as exploit kits that other criminals use to hack efficiently
- Run a "darknet market" used to exchange stolen data, tools, and other contraband

There are many other specialized roles in the hacker economy, and new roles constantly develop as technology evolves.

5.4 The Goods

The dark web facilitates data breaches by providing ways for criminals to quickly and easily monetize stolen data. It also does more: It provides criminals with tools and information that help them hack into accounts and break into computers, leaving even more data breaches in their wake.

Conversely, data breaches influence the dark web. When criminals breach a computer, they often find themselves with access to vast troves of data. Some types of data do not (yet) have a clear path for monetization. Like legitimate entrepreneurs, creative and enterprising criminals develop new schemes for leveraging different kinds of stolen data. As a result, new, specialized darknet markets emerge (such as specialized W-2 shops). By monitoring the dark web, it is possible to detect data breaches and anticipate emerging types of attacks.

In this section, we will review common types of data breach-related goods sold on the dark web. These include personally identifiable information, payment card numbers, W-2 forms, account credentials, medical records, and remote access to computers. Along the way, we will

32. United States v. Ross William Ulbricht.

discuss how criminals leverage these goods. This will help defenders understand what to protect today and how to anticipate future threats.

5.4.1 Personally Identifiable Information

Stolen identities have been exchanged online for decades. "Personally identifiable information" (PII), such as names, addresses, birth dates, and SSNs, are valuable because they're useful for committing identity theft and financial fraud. Today, criminals often bundle stolen personal information and sell it as a package called "fullz," which typically sell for around $30 per record. Prices can vary, with higher prices reserved for victims who have strong credit scores or higher credit card balances. [33]

5.4.2 Payment Card Numbers

Payment card numbers are widely sought after—and supplied. Stolen payment card numbers typically sold for $10 to $20 per record in 2019, according to Gemini Advisory, a firm that monitors the dark web.[34]

5.4.2.1 W-2 Forms

W-2 fraud rose to epidemic proportions in the past decade, fueled in large part by the widespread availability of stolen PII and copies of W-2 forms themselves. Criminals use stolen PII, including SSNs, names, addresses, and wages, to file fraudulent tax returns in order to claim victims' refunds. Refund fraud reached a whopping $5.2 billion in 2010.[35] Fortunately, the IRS implemented techniques to detect and prevent W-2 fraud, and refund fraud declined, but as of 2017 the Taxpayer Advocate Service estimated that it still "cost the government (and thus, taxpayers) more than one billion dollars each year."[36]

Specialized e-commerce shops sprung up on the dark web, peddling W-2 forms. Journalist Brian Krebs has published screenshots of a shop where visitors could select individual W-2 forms based on the victim's name, address, wage, or SSN. Forms were priced based on the

33. Keith Collins, "Here's What Your Stolen Identity Goes for on the Internet's Black Market," *Quartz*, July 23, 2015, https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market; Brian Stack, "Here's How Much Your Personal Information Is Selling For on the Dark Web," *Experian*, December 6, 2017, https://web.archive.org/web/20180220093122/https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

34. Brian Krebs, "Data: E-Retail Hacks More Lucrative Than Ever," *Krebs on Security* (blog), April 30, 2019, https://krebsonsecurity.com/2019/04/data-e-retail-hacks-more-lucrative-than-ever/.

35. Treasury Inspector General for Tax Administration, "Efforts Continue to Result in Improved Identification of Fraudulent Tax Returns Involving Identity Theft; However, Accuracy of Measures Needs Improvement, Reference Number: 2017-40-017," U.S. Department of the Treasury, February 7, 2017, https://www.treasury.gov/tigta/auditreports/2017reports/201740017fr.pdf.

36. Taxpayer Advocate Service, "Most Serious Problems: Fraud Detection," *Annual Report to Congress* 1 (2016): 151–60, https://taxpayeradvocate.irs.gov/Media/Default/Documents/2016-ARC/ARC16_Volume1_MSP_09_FraudDetection.pdf.

wage, with higher wage earners fetching a greater price. The interface is intuitive; customers simply click a button to add a W-2 form to their shopping cart and then check out.[37]

5.4.2.2 Medical Records

Medical records are a gold mine for criminals. Healthcare clinics collect extremely comprehensive records on individuals, including PII, billing details, and health information. As a result, stolen medical records can be used for a wide variety of fraudulent purposes. "[Y]ou can use those profiles for normal fraud stuff," advertised one criminal, who was selling medical records online.[38]

By stealing a victim's health insurance information, criminals can file false insurance claims or obtain medical care using the victim's benefits. In the United States, where health insurance coverage is inconsistent, medical fraud is estimated to cost between $80 and $230 billion per year.[39] "Fraud involving the Medicare program for seniors and the disabled totaled more than $6 billion in the last two years, according to a database maintained by Medical Identity Fraud Alliance."[40] Criminals can also leverage a victim's identity to obtain prescriptions for drugs such as opiods and resell them to people who don't have prescriptions or need to feed addictions.

Medical data can be useful in all kinds of ways that aren't immediately apparent. In 2011, thousands of patient X rays were stolen from Beth Israel Deaconess hospital in Boston. Beth Israel's chief information officer, John Halamka, said that "the scans are often sold to Chinese nationals who can't pass health exams for travel visas."[41]

Importantly, when it comes to the value of health data, there isn't much solid research to go on. Current reports on the value of healthcare records are not based on statistically valid sample sets but observations of individual transactions that happen to be accessible to a researcher. Sometimes they are even just rumors, quoted and requoted, originating with an off-the-cuff remark by an executive or a security professional years earlier. An oft-referenced quote by Pam Dixon, executive director of the World Privacy Forum, is that "medical records files command a very high price—they can sell for $50 on the black market." Her 2008 statement is still referenced by reporters today.

One thing is certain: Bulk theft and sale of medical data is becoming more visible. In 2016, TheDarkOverlord extortion gang offered electronic health records in bulk on the black market for approximately $1 to $2 per record. Reporters and security professionals took note of the apparent price drop; a research report by security firm TrapX speculated that it was an issue of

---

37. Brian Krebs, "W-2 2016 Screenshot," *Krebs on Security* (blog), 2017, https://krebsonsecurity.com/wp-content/uploads/2017/01/w2shop-140.png.

38. Jennifer Schlesinger, "Dark Web is Fertile Ground for Stolen Medical Records," *CNBC*, March 11, 2016, http://www.cnbc.com/2016/03/10/dark-web-is-fertile-ground-for-stolen-medical-records.html.

39. Laura Shin, "Medical Identity Theft: How the Health Care Industry is Failing Us," *Fortune*, August 31, 2014, http://fortune.com/2014/08/31/medical-identity-theft-how-the-health-care-industry-is-failing-us.

40. Caroline Humer and Jim Finkle, "Your Medical Record is Worth More to Hackers than Your Credit Card," *Reuters*, September 24, 2014, http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924.

41. Nsikan Akpan, "Has Health Care Hacking Become an Epidemic?" *PBS News Hour*, March 23, 2016, http://www.pbs.org/newshour/updates/has-health-care-hacking-become-an-epidemic.

supply and demand. "So many millions of health care records have been stolen that, incredibly, the value of a health care record being sold on the 'dark web' appears to have decreased in 2016."[42]

"The volume of medical data for sale in the criminal underground is increasing, leading to very low prices for individual records," concurred Vitali Kremez, a senior analyst at Flashpoint.[43] At the same time, the increasing maturity of the markets has made it easier for criminals to sell the data in the first place, leading to greater proliferation of stolen medical data.

5.4.2.3 Account Credentials

Username and password combinations sell like hotcakes on the dark web. These can be used directly by criminals to perpetrate new data breaches, in order to steal more data for resale, commit fraud, access bank accounts, or all of the above.

In 2017, researchers from Google published a landmark paper in which they described their monitoring of stolen credentials sales on the dark web for one year (March 2016 to March 2017). They found more than 1.9 *billion* credentials for sale. Many of the passwords were stolen in large, highly publicized data breaches, including Myspace, Adobe, LinkedIn, Dropbox, Tumblr, and others.[44]

Early on, bank account credentials were commonly traded. Pricing was typically set based on a percentage of the account balance. Later, the market for hacked email and social media accounts developed. Email accounts, in particular, are gold mines for sensitive data. With access to your email account, criminals can:

- **Reset passwords for sites like Amazon, PayPal, your online banking website, and more.** These accounts are effectively purchasing tools; criminals can easily use them to buy goods or services, or even transfer cash.
- **Commit wire transfer fraud.** Criminals search email accounts for requests for wire transfers, such as those that result from real estate closings, insurance payouts, or vendor payments. Then, they intercept messages and send fraudulent requests (sometimes from a different account) designed to initiate wire transfer to accounts that they control.
- **Hack your colleagues, clients, friends, and family.** Criminals can use your account to send an email to any of your contacts, which may in turn infect their computers.
- **Steal confidential information, which can be used or resold.** Email contains a treasure trove of data, which can range from copies of tax returns to business trade secrets to patient health information, and more.

---

42. Trapx Labs, *Health Care Cyber Breach Research Report for 2016* (San Mateo, CA: Trapx Security, 2016), 4, https://trapx.com/wp-content/uploads/2017/08/Research_Paper_TrapX_Health_Care.pdf.

43. Chris Bing, "Abundance of Stolen Healthcare Records on Dark Web is Causing a Price Collapse," *Cybersecurity*, October 24, 2016, https://www.cyberscoop.com/dark-web-health-records-price-dropping.

44. Kurt Thomas et al., "Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (Dallas, October 30-November 3, 2017), 1422 https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46437.pdf.

Social media accounts are similarly useful for criminals. For example, in May 2016, a hacker named "Peace" was spotted on TheRealDeal market selling a database containing account information for 167 million LinkedIn users. The database included email addresses and encrypted passwords for 117 million users. The price? Five bitcoin, or approximately $2,200 at the time.

Why would criminals want your LinkedIn password? First, because many people reuse credentials for multiple accounts. Using the stolen LinkedIn passwords, criminals might be able to break into victims' email accounts, bank accounts, or other attractive targets. Social media accounts are also useful for targeting new victims since criminals can use them to spread malicious links or send crafted scam messages. "A Twitter account costs more to purchase than a stolen credit card because the former's account credentials potentially have a greater yield," reported the RAND National Security Research Division in 2014.[45]

Password data breaches became so common that in 2013, security researcher Troy Hunt released the "Have I Been Pwned" web service, which enables users to check to see whether their credentials have been exposed in a previous data breach.[46] Despite the rash of stolen credentials, passwords continued to remain the most widely adopted means of securing cloud accounts. The result has been a widespread epidemic of "business email compromise" (BEC) and other cloud account breaches, which will be discussed more in Chapter 13, "Cloud Breaches."

5.4.2.4 Your Computer

Computers themselves are worth money—and we're not talking about selling the physical hardware on eBay. Criminals on the dark web buy and sell remote access to computers. An infected computer may be grouped with dozens or even hundreds of other "bots" (hacked computers). These botnets (groups of hacked computers) are then sold (or rented by the hour) to other criminals. On one dark market site, captured by Dancho Danchev of Webroot, 1,000 U.S. bots are sold for $200. Criminals can use this access to harvest sensitive data, attack other computers, or lock up data and hold it for ransom.[47]

5.4.3 Data Laundering

The dark web isn't the only place where stolen data can be sold. Certain types of stolen data—such as PII, health information, behavioral analytics, and more are commonly traded in legitimate markets, as discussed in Chapter 2, "Hazardous Material." While reputable firms typically do not intentionally purchase data from criminals, the lack of transparency and

45. Selena Larson, "Google Says Hackers Steal Almost 250,000 Web Logins Each Week," *CNN Tech*, November 9, 2017, http://money.cnn.com/2017/11/09/technology/google-hackers-research/index.html.

46. Troy Hunt, "Introducing 306 Million Freely Downloadable Pwned Passwords," Troyhunt.com, August 3, 2017, https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords; "Have I Been Pwned?" Pwned Passwords, https://haveibeenpwned.com/Passwords (accessed March 19, 2018).

47. Pierluigi Paganini, "Botnets for Rent, Criminal Services Sold in the Underground Market," Security Affairs, February 14, 2013, http://securityaffairs.co/wordpress/12339/cyber-crime/botnets-for-rent-criminal-services-sold-in-the-underground-market.html; "New Underground Service Offers Access to Thousands of Malware-Infected Hosts," *Webroot*, (blog) February 12, 2013, http://www.webroot.com/blog/2013/02/12/new-underground-service-offers-access-to-thousands-of-malware-infected-hosts.

regulation has made it possible for stolen information to flow into legitimate markets, which can in turn incentive breaches.

Stolen data can reenter the legitimate supply chain through a complex web of data brokers. In 2014, the Federal Trade Commission (FTC) conducted a survey of nine major data brokers and found that they "obtain most of their data from other data brokers rather than directly from an original source. Some of those data brokers may in turn have obtained the information from other data brokers. Seven of the nine data brokers in the Commission's study provide data to each other." Legitimate data brokers are reticent to reveal their sources. In response to an inquiry by the Senate Committee on Commerce, Science, and Transportation, three major data brokers (Acxiom, Experian, and Epsilon) refused to reveal their data sources (or customers, for that matter). "[A] number of the queried brokers perpetuate this secrecy by contractually limiting customers from disclosing their data sources," the committee reported.[48]

The complexity of the data brokerage marketplace, as well as the lack of oversight and transparency, increases the risk that stolen data can reenter the legitimate data market.[49] Many types of stolen data are not easily traceable, like unmarked cash. For example, SSNs may be issued centrally by the federal government, but from that point on there is no central organization that tracks their proliferation and use. It's likely that SSNs have been breached, sold, and resold so many times that a single number may have been stolen from many different places and passed through many unauthorized hands. Similarly, health information, prescription data, web surfing, and GPS location data can be collected in many different ways and from many different places—sometimes legally and sometimes not.

The result is that criminals can steal virtually any kind of data today and find a buyer who will not ask too many questions. As legitimate data analytics and brokerage firms continue to invent new data products, they drive the market for raw data sources. Absent careful vetting, that can include stolen data, further fueling the data breach epidemic.

Reacting to Stolen Data

It can be shocking to discover that data from your organization is on the dark web—but there are ways that you can react to protect yourself and any individuals involved. Here are a few tips:

- Determine the scope of data that may have been stolen as quickly as possible. It can take a long time to complete a full data breach investigation, but in the meantime, you can develop a preliminary working model based on the available evidence.
- Keep in mind that the data may have been stolen from a supplier or partner that you rely upon. Your organization's network may not have been breached.

(*Continues*)

48. U.S. Senate Comm. on Commerce, Science, and Transportation, *A Review of the Data Broker Industry* (Washington, DC: U.S. Senate, 2013), 6, http://educationnewyork.com/files/rockefeller_databroker.pdf.

49. Rob O'Neil, "Cybercriminals Boost Sales Through 'Data Laundering'," *ZD Net*, March 16, 2015, http://www.zdnet.com/article/cyber-criminals-boost-sales-through-data-laundering.

(*Continued*)

- Take steps to reduce harm as quickly as possible:
  - Notify affected individuals as soon as practical, so that they have the opportunity to take action.
  - Devalue the data whenever possible, such as by changing passwords.
  - Monitor any accounts or assets that may be accessed using stolen data.
  - Implement additional access controls, such as two-factor authentication or credit freezes, depending on the type of data exposed.
- Be prepared for media inquiries. As we will see in the coming chapters, once data is exposed on the dark web, journalists may see it as a juicy story.

Some organizations hire professional firms to monitor the dark web and provide alerts if any of their data appears to be for sale. This increasingly popular service is known as "dark web scanning." While no single company has full access to the dark web, some have extensive access to popular darknet markets. This type of service can help organizations proactively detect data breaches and minimize surprise media attention.

5.5 Conclusion

In this chapter, we discussed common ways that stolen data is leveraged. We also showed how fraud and the darknet markets evolved symbiotically and explained the core technologies (such as onion routing and cryptocurrency) that reappear in many different types of data breach cases. Now that we have established this foundation, we will analyze cases where payment card data is stolen, used to commit fraud, and peddled on the dark web.

This page intentionally left blank

Chapter 6

Payment Card Breaches

In March 2008, Cissy McComb, owner of Cisero's Ristorante, called the Park City, Utah, police department. She had just received a letter from Elavon, her restaurant's payment processor, notifying her that "payment cards used at Cisero's may have been accessed, counterfeited and fraudulently used elsewhere." Visa had identified the restaurant as a "common point-of-purchase" for a group of stolen cards and notified the bank. Cisero's was a mom-and-pop Italian restaurant located on Main Street in Park City. Steve and Cissy McComb had opened the restaurant in 1985 and ran it for 30 years. During the summertime Sundance Festival, Cisero's was packed with flashy stars and visiting tourists. The owners bragged that Robert Redford, Sandra Bullock, and Russell Crowe had dined there. Sidney Poiter once set his menu on fire by accidentally touching it to the flickering table candle. The rest of the year, Cisero's was a local staple.[1]

Now, Mrs. McComb was worried. After calling the Park City police department, Mrs. McComb drove to her local branch of U.S. Bank, which in 2001 had arranged for its affiliated payment processor, Elavon, to handle the restaurant's credit card processing. None of her local branch's staff knew anything about a suspected breach.

In June, Mrs. McComb received another worrisome letter. Elavon notified the couple that they would be fined $5,000 for the breach and would need to provide a certificate of "PCI compliance" in approximately a month, or they would face additional fines. Subsequently, U.S. Bank "unilaterally" deducted $5,000 from the restaurant's account. The McCombs submitted an attestation of PCI compliance and paid approximately $41,000 to upgrade their point-of-sale (POS) systems.

Behind the scenes, the couple later discovered that Visa had sent U.S. Bank a letter stating: "If Cisero's Ristorante and Nightclub does not demonstrate . . . compliance within 30 days from the date of this letter, U.S. Bank will be assessed a monthly fine of $5,000." The fines would increase to $10,000 or more per month after 90 days. Although U.S. Bank had the right to appeal these fines, the bank would have had to pay a nonrefundable $5,000 fee to Visa just to submit an appeal, which would have been added to the restaurant's accrued liability.

1. Bubba Brown, "Cisero's Ristorante, a Park City Mainstay, Closes Doors," ParkRecord.com, July 22, 2016, https://www.parkrecord.com/news/business/ciseros-ristorante-a-park-city-mainstay-closes-doors.

The McCombs also received notice from Elavon that they were required to conduct a forensic investigation, at their own expense. Elavon provided them with a list of six forensics companies that were approved by Visa and Mastercard to conduct the investigations. The McCombs selected a firm named Cybertrust. Cybertrust investigated and found that there was "no concrete evidence" of a security breach, and "no evidence of intrusive, malicious, or unauthorized activity." The McCombs hired a second forensics firm as well, which reached similar conclusions.[2]

Nonetheless, U.S. Bank deducted more than $5,000 from the McCombs' bank account again, without their consent, after Mastercard reported that issuers including Chase and RBS had reported fraudulent charges and were seeking to recover damages. According to news reports, "Visa determined that the total cost of the liability for Cisero's noncompliance was $1.33 million, but ultimately set the fine at $55,000. . . . MasterCard stated that although it could have imposed a fine of up to $100,000 for the violation of storing card data, it decided to impose a fine of only $15,000."

The McCombs quickly closed their bank account to avoid any further deductions. Elavon sued for approximately $82,600 in additional fines. The McCombs fought back, filing a countersuit. "It's just like Visa and MasterCard are governments," said the couple's attorney, Stephen Cannon. "Where do they get the authority to execute a system of fines and penalties against merchants?"[3]

After a burst of media attention, the case was settled quietly out of court.

6.1 The Greatest Payment Card Scam of All

Payment card breaches can be very complex and result in years of litigation. They can damage a merchant's reputation with consumers and even drive a business *out* of business. In a payment card breach, consumers' credit or debit card numbers are exposed. The card numbers are often distributed through the dark web or other channels, and then criminals monetize them by making card-not-present purchases or by creating fake cards, which they can then use or resell for a percentage of the balance.

Over the years, payment card information has consistently ranked at the top of data compromise charts (topped only by the more generic "personal information" such as name, Social Security number (SSN), etc).[4] This is for two reasons: First, payment card information is at extremely high risk of theft; and second, when a cardholder data breach occurs, it is very likely to be detected (more so than other types of breaches).

2. Elavon, Inc. v. Cisero's Inc., Civil No. 100500480 (3d Jud. Dist. Ct., Summit Cty., 2011), https://www.wired.com/images_blogs/threatlevel/2012/01/Cisero-PCI-Countersuit.pdf.

3. Kim Zetter, "Rare Legal Fight Takes on Credit Card Company Security Standards and Fines," *Wired*, January 11, 2012, https://www.wired.com/2012/01/pci-lawsuit.

4. *2016 Data Breach Investigations Report*, Verizon Enterprise, 2016, 44, https://enterprise.verizon.com/resources/reports/2016/DBIR_2016_Report.pdf.

Why does cardholder data present such a high risk of a data breach? It is because payment card security is obviously broken, in that it relies upon a shared secret that, really, isn't much of a secret at all. Your card number is essentially the "key" to your account. In order to keep your account secure, you must keep this long number very very secret—but in order to actually *use* it, you have to share it with many people. This system is fundamentally flawed.

Payment card numbers are small and compact—very liquid. They proliferate with use. Many people have access to them, from waiters to billing clerks to IT administrators. They are valuable on the black market, for obvious reasons. Often organizations choose to store payment card data for extended periods of time, to facilitate autopay and speed transactions. In short, all five of the data breach risk factors apply: retention, proliferation, access, liquidity, and value.

Today, there are far more secure ways to conduct payment transactions. Mobile devices and advances in cryptographic authentication have the potential to render the risky payment card number obsolete. Without payment card numbers, there would be no cardholder data breaches. That would mean merchants would not need to worry about securing vast volumes of sensitive payment card numbers that pass through their systems. Banks would not have to invest (as much) in fraud monitoring or reissuing of cards. Consumers would not have to pay the price of cardholder data breaches, in the form of increased fees and prices.

Given the high rate of data breaches and resulting fraud, why do we still rely on insecure payment card numbers? While some progress has been made over the years, a complete overhaul of the system would require a huge investment from card brands, payment processors, merchants, and every entity involved. In the meantime, the more powerful players (card brands and banks) have developed "Band-Aids" (mechanisms for detecting fraud early and recouping losses after a breach), sometimes at the expense of less-powerful entities.

Behind the scenes, the card brands in particular have amassed enormous control over the process of sorting out liability and have effectively pitted other key players against each other. The payment card industry is self-regulated with respect to cybersecurity, and it has implemented contractual obligations that can feel to participants like governmental regulations (even though they are not). Card brands—such as Visa, Mastercard, Discover, and American Express—write the rules for their payment networks. Based on their contracts, banks and merchants are responsible for absorbing the majority of the losses, rather than the card brands themselves. Merchants, payment processors, and others who handle payment cards have no choice but to follow the card brands' rules, lest they be denied the ability to accept payment cards—the lifeblood of our modern economy.

The result is that when a cardholder data breach happens, merchants—even small ones—can be left holding the bag. Banks are caught in the middle, torn between their allegience to customers and their own bottom line. Even forensics firms that investigate cardholder data breaches are subtly controlled: They must answer to the card brands in order to be "qualified" to investigate payment card breaches.

In this chapter, we will explore the different players involved in a payment card breach and the deep network of factors that influences their actions. Along the way, we will specifically examine how the standards established by the Payment Card Industry Security Standards Council (PCI SSC) affect various parties before and after a breach. We will step through the TJ Maxx and Heartland data breaches, which established strong precedents for determining liability, and show how compliance with the PCI SSC's standards affect breach response best practices.

6.2 Impact of a Breach

Fraud is rampant, and no one wants to be stuck covering the losses. This fundamental issue is at the heart of payment card data breach response. Many different participants are affected by a payment card breach, including:

- Consumers
- Banks
- Payment processors
- Merchants
- Card brands

In this section, we will discuss the impact of payment card breaches on each of these participants.

6.2.1 How Credit Card Payment Systems Work

In order to understand who foots the bill for a credit or debit card data breach, you first have to understand, at a high level, how payment card networks work. Different card brands have slightly different setups: typically a "three-party scheme" or "four-party scheme."

Visa and Mastercard use four-party schemes, as illustrated in Figure 6-1. In four-party schemes, each transaction involves four participants: the cardholder, the issuer (the cardholder's bank), the acquirer (the merchant's bank), and the merchant. In between, card brands and payment processors help to communicate transaction data and move funds. In the Cisero's v. Elavon countersuit, the four parties were eloquently defined as follows:[5]

- ***Cardholder.*** A cardholder is a consumer who makes a purchase from a merchant using an electronic payment card.
- ***Merchants.*** When a cardholder makes an in-person transaction, the cardholder's credit or debit card is swiped at a merchant's POS terminal.
- ***Acquirers.*** Acquirers are merchant's banks, such as U.S. Bank, that "acquire" transactions by providing merchants with access to the payment networks and maintaining amounts due to the merchant. Acquiring banks usually contract with a processor, such as Elavon, to provide merchants with authorization, clearance, and settlement transaction services.
- ***Issuers.*** Issuers are cardholders' banks, such as Bank of America or Wells Fargo, that issue credit and debit payment cards to retail customers.

5. Elavon v. Cisero's.

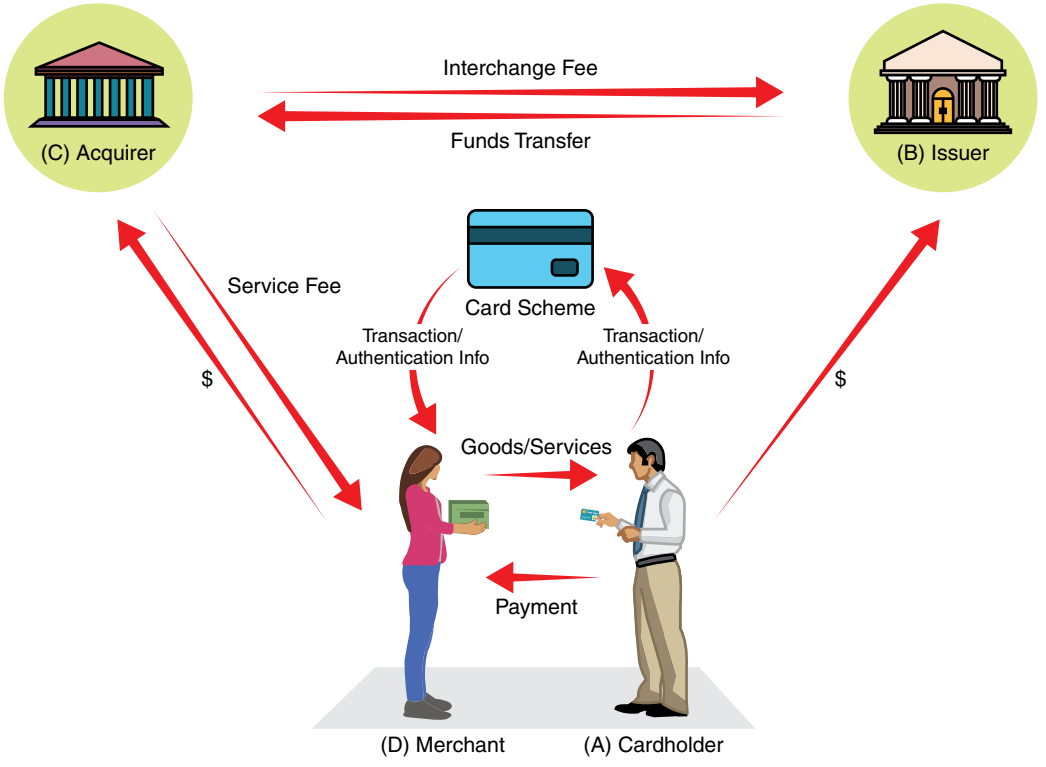


Figure 6-1. The four-party payment system.

Let's walk through a typical transaction. When a cardholder (A) purchases a product or service using his card, the issuing bank (B) authorizes the transaction. Once authorization is received, the acquirer (C) transfers money to the merchant (D), minus a service fee. The issuing bank sends money to the acquirer (minus any interchange fee) and debits the cardholder's account.

Three-party schemes, such as those used by American Express and Discover, are similar except that the issuer and the acquirer are the same brand. This is why your local bank may issue you a Visa- or Mastercard-branded card, but not an American Express or Discover card.

6.2.2 Consumers

Consumers, naturally, are impacted by payment card fraud when money is stolen from their accounts or charged to their credit cards. This can have a chilling effect, making consumers

more reticent to hand their card number to merchants. Payment card breaches are bad for business—and therefore bad for everyone in the payment processing chain. "When someone hacks a site, it raises a lot of questions to the consumer," commented Chris Merritt, a consultant for retailers.[6]

To protect the public, the United States passed a federal law that mandates that consumers are liable only for the first $50 of fraudulent charges.[7] Some card associations took that even further: Visa, for example, instituted a "zero-liability" policy, to reassure consumers. Credit card companies "tout[ed] antifraud campaigns" and promised that "cardholders won't have to pay a dime" if their cards were used fraudulently.[8]

"Zero-liability" didn't stop consumer horror stories from hitting the news. In one feature, consumer Karen Jones purchased music online from CD Universe before her credit card number was exposed by Maxus's credit card data pipe. While Jones wasn't responsible for the financial loss, she said that the theft had "caused her a considerable amount of grief," estimating that she had spent approximately 10 hours a week for months "corresponding with credit card companies and dozens of merchants and vendors to get more than $4,000 in fraudulent charges removed from her account." Over the years, banks invested heavily in fraud prevention systems to minimize the impact on consumers even after card numbers were stolen.

If consumers aren't liable for the fraudulent charges, who is? Clearly, the money has to come from somewhere. Criminals aren't giving it back.

6.2.3 Poor Banks

The issuing banks often bear the brunt of losses due to cardholder data breaches. When a credit or debit card number is stolen and a criminal makes a fraudulent charge, the issuing bank typically bears the responsibility for making the cardholder whole again. The issuer can try to recover the money from the merchant's bank (the acquirer), which in turn can attempt to recoup the costs from the merchant. (In some cases, there are other payment facilitators in the chain, which may bear some responsibility.) This system has led to many conflicts between the issuers and merchants, as the case of Cisero's illustrated.

When a cardholder data breach is detected, the issuer has a choice: to cancel the card and reissue it, or to allow the card to remain active and monitor it for fraud. Both options are costly. If the bank chooses to reissue, cardholders are often annoyed because their card may suddenly not work, and they may need to provide new card numbers to merchants with whom they have set up autopay. If the bank does not reissue, then a fraudster may attempt to use the card number, resulting in losses. Given the prevalence of cardholder data breaches, banks

6. Paul A. Greenberg, "Online Credit Card Security Takes Another Hit," January 20, 2000, *E-Commerce Times*, https://www.ecommercetimes.com/story/2291.html.

7. United States Code, *15 U.S.C. 1643: Liability of Holder of Credit Card* (Washington, DC: GPO, 2006) https://www.gpo.gov/fdsys/granule/USCODE-2011-title15/USCODE-2011-title15-chap41-subchapI-partB-sec1643.

8. Paul Beckett and Jathon Sapsford, "A Tussle over Who Pays for Credit-Card Theft," *Wall Street Journal*, May 1, 2003, https://www.wsj.com/articles/SB105173975140172900.

often choose the latter approach: They simply monitor affected accounts for fraud and have additional controls in place to minimize risk.

6.2.4 Poor Merchants

Merchants who experience a cardholder data breach may be on the hook for thousands if not millions of dollars. When cardholder data is stolen from a merchant's network or POS system and subsequently used for fraud, the banks may attempt to recover losses from the merchant. As we will see from the TJ Maxx breach later in this chapter, they are often successful. Typically the banks still lose money; the amounts that they recover from the merchant's bank don't cover the cost of reissuing cards, or customer goodwill, or even the entire amount of fraudulent charges in many cases.

What's more, the card brands may levy steep fines against the merchant's acquiring bank, particularly if there is evidence that they were not compliant with industry security standards. As in the case of Cisero's, the acquirer may then charge the merchant for these fines. The acquirer has the right to do this because of its contract with the merchant.

Merchants also lose out when they process fraudulent transactions due to stolen payment card numbers. For example, Gary Howell, the owner of a mail-order auto-parts business in West Virginia, discovered that a remote customer had bought $4,200 in car parts—using a stolen American Express card. He was told that the loss was his responsibility. When he called American Express asking for help tracking down the fraudster, an American Express spokesperson said the company had a "no prosecute" policy and refused to help.[9] All over the globe, merchants who send goods or provide services in exchange for a fraudulent credit card transaction risk losing the value of whatever it was they provided.

6.2.5 Poor Payment Processors

Payment processors are intermediaries that facilitate communication between merchants, card brands, and banks. When a customer provides a merchant with a payment card, a payment processor will manage tasks such as determining whether the customer has sufficient credit to make a charge ("authorization") or directing the banks to debit the customer's account and release funds to the merchant ("settlement" and "funding").

Much like merchants, payment processors can be victims of cardholder data breaches, in which case they may be liable for resulting losses. Later in this chapter, we will study the Heartland payment processor breach, which was a landmark case.

Payment processors also take a hit when they unknowingly process fraudulent transactions, in the form of fees that are charged by the card brands. For example, Website Billing Inc., a company that processed payments on behalf of online retailers, got in a major public battle with Visa over transaction fees. According to Website, Visa required it to pay $15 for every fraudulent transaction that the company processed. On top of that, "when fraudulent purchases exceeded 5% of all its international transactions, Visa began slapping on an additional $100 penalty

9. Beckett and Sapsford, "Tussle."

for each bogus transaction." Website took Visa to federal court over the fines. Ultimately, the parties settled, and Website was required to pay Visa more than $1 million.[10]

6.2.6 Not-So-Poor Card Brands

Card brands have a leg up: They write the rules for their payment networks. Contractually, banks and merchants are responsible for absorbing the majority of the losses rather than the card brands.

In addition, card brands can levy fines against the other parties in the system and charge extra fees to cover the cost of fraud. Card associations argue that their extra fees are designed to "cover the cost of processing bogus transactions, much like banks charge for bounced checks."[11]

Some parties have speculated that card brands such as Visa and Mastercard even turned a profit from the extra fees. "Their response [to credit card fraud] has been very slow because they have been able to pass the cost along to merchants and in the process levy fines that lead to a net gain for banks in the system," said an attorney for Website, Michael Chesal.

Mastercard's chief executive officer (CEO) responded, pointing out that "I don't think anybody cavalierly sits back and says, 'We can poison the well from which the industry drinks.'"[12]

Over the years, the card brands have developed a complex set of cybersecurity standards that all the other parties in the system must follow. As we will see, these standards effectively place the responsiblity for security (and losses) on merchants, payment processors, banks, and the other participants in the system.

6.2.7 Poor Consumers, After All

As merchants and banks continued to suffer escalating losses due to data breaches and fraud, they passed the costs along to consumers, via price hikes and transaction fees. While consumers may have "zero liability" for specific fraudulent transactions, ultimately, they bear the costs.

6.3 Placing Blame

Everyone knows payment card fraud is rampant—but whose fault is it? This question is critical for determining (a) who should be liable for the losses, and (b) who is responsible for fixing the problem.

6.3.1 Bulls-Eye on Merchants

When cardholder data is stolen, it is typically through one of the following methods:

- **Internal network breach:** Hackers break into a merchant's or payment processor's network and capture payment card data as it is stored, processed, or transmitted. Often, POS

10. Beckett and Sapsford, "Tussle."

11. Beckett and Sapsford, "Tussle."

12. Beckett and Sapsford, "Tussle."

systems on a merchant's internal network are specifically targeted and compromised. The risk of an internal network breach is compounded by the fact that merchants often store credit card data for extended periods of time, unwittingly stockpiling troves of hazardous material.

- **E-Commerce website hack:** Many e-commerce websites have vulnerabilities, which enable criminals from around the world to subvert their payment systems and, in some cases, gain remote access to sensitive internal servers and databases as well.
- **Physical theft:** Criminals place "skimmers" on top of legitimate card readers to capture the encoded information from the magnetic stripe or simply copy card data when it is handed over by a consumer (e.g., as in the case of a waiter or retail clerk). Physical theft is relatively low volume compared with the enormous databases that can be exposed through other methods.

The place where the payment card data is breached is, of course, the most visible and the most obvious point of failure. Merchants in particular are at very high risk of a breach, for the following reasons:

- Merchants collectively handle extensive volumes of payment card data.
- Merchants' payment processing systems are exposed to the public and therefore to criminals. For example, local merchants have open stores where people physically walk through and interact directly with POS systems. E-commerce sites are, by nature, directly connected to the Internet.
- Merchants are not in the security business (or, not usually)! They simply want to process payments. In fact, many merchants are mom-and-pop businesses with limited IT support and few funds to invest in security.

For these reasons, merchants represent a very high-risk point in the payment card system.

6.3.2 Fundamentally Flawed

Merchants can increase or decrease the risk depending on how well they secure their environments, but ultimately, they cannot fix what is a fundamentally insecure system.

The current payment card system places merchants in a particularly risky position. It's important to recognize that this is not the only possible system; there are other payment methods that are far less risky for merchants, with respect to data breaches. New forms of payment systems have emerged, such as PayPal and ApplePay, which do not require merchants to handle payment card numbers at all. Transactions *can* be authenticated without static card numbers, rendering the very concept of payment card data breaches obsolete.

However, none of these new solutions has become as widely adopted as traditional magnetic-stripe cards encoded with a very long number. "The technology needed to support [stronger authentication] is available and can be implemented fairly easily . . . but few banks appear to be doing so," observed Gartner analyst Aviva Litan.[13]

13. Kim Zetter, "That Big Security Fix for Credit Cards Won't Stop Fraud," *Wired*, September 30, 2015, https://www.wired.com/2015/09/big-security-fix-credit-cards-wont-stop-fraud.

Merchants undoubtedly would prefer a system that reduces their risk, but they are participants in a much bigger system that they did not architect and do not control. It is unlikely that the card brands will drive fundamental changes to the payment system security model so long as the losses they incur do not exceed the cost of a major system overhaul. The result is that payment card data breaches will continue, perhaps gradually fading away as alternate payment systems emerge over time.

Investing in Alternate Payment Technologies

Payment card breaches do not have to exist. They occur because our current payment system relies on shared secrets that are then widely distributed—an obviously insecure model. As payment technology evolves, merchants, banks, and other participants would be wise to invest in technologies that do not rely on static payment card numbers, such as ApplePay, PayPal, and other alternative payment methods.

6.3.3 Security Standards Emerge

As payment card data breaches proliferated, card associations and banks were quick to highlight the risk at the endpoints, such as online retailers. In response, merchants and payment processors began to push back on the card associations, complaining that they did not provide appropriate support to entities using their systems.

Pressure mounted on the payment card industry to stop the bleeding. Clearly, card associations needed to make sure consumers weren't afraid to use the cards and quell merchants' and banks' growing frustration.

The card associations took action—not by fixing the fundamental problem, but with a Band-Aid. In April 2000 (shortly after the CD Universe case hit the news), Visa announced its new Cardholder Information Security Program (CISP), which would take effect in June 2001. The CISP was "intended to ensure merchants and others in the credit approval chain have appropriate security measures in place to protect cardholder information." It included 12 security requirements, known as the "Digital Dozen." Visa's senior vice president of risk management, John Shaughnessy, said the company's goal was to "create a 'duh' list—stuff that nobody could argue with."[14]

The "Digital Dozen" required merchants to adhere to strict security requirements and provide attestations of compliance to Visa. Visa said it would begin by verifying the compliance of its top 100 merchants and also conduct random tests of other merchants. Merchants were also required to immediately notify acquirers if they got hacked, and the acquirers, in turn, were required to notify Visa.

Other major card associations quickly followed suit. Mastercard released the "Site Data Protection" standards, and American Express published "Data Security Operating Policy."

Overwhelmed with multiple uncoordinated security "standards," few merchants complied with any of them. However, the card associations had succeeded in shifting the dialogue, taking

14. Paul Desmond, "Visa is Monitoring Merchants for Security Compliance," *eSecurity Planet*, June 1, 2001, http://www.esecurityplanet.com/trends/article.php/688812/Visa-is-monitoring-merchants-for-security-compliance.htm.

the focus away from themselves and placing responsibility for security on the merchants and other participants. There was little discussion of the real problem, which was the fundamental insecurity of the payment card model.

6.4 Self-Regulation

As the dark web matured, payment card breaches became an epidemic. The publicity and media attention on the problem was extensive, and it was clear that if the payment card industry did not regulate itself, it would run the risk that the government might step in to establish standards.

There were rumblings of regulation. "Some officials say it may be time for stricter government oversight of what kinds of financial information e-merchants keep, how long they can keep it and how they store it."[15]

The payment card industry pushed back, fast. "[T]he industry needs to preserve the flexibility to find solutions as it has in the past. Legislation will not help," wrote Oscar Marquis, former general counsel of the credit bureau TransUnion.[16]

Faced with the threat of government regulation, the payment card brands quickly banded together to form the PCI SSC. They implemented their own, self-managed industry security program, known as the Payment Card Industry Data Security Standard (PCI DSS). Since its founding, the PCI SSC has developed a wide array of cybersecurity-related standards, as well as requirements for data breach response processes and forensics firms. This successfully quashed calls for legislation.

Modern payment card breach response is heavily influenced by the PCI SSC and its programs. In order to understand the dynamics of a modern payment card breach (and how best to respond), you must have a strong grasp of how the PCI SSC works and the fundamentals of the PCI DSS program. In this section, we will cover important aspects of the PCI SSC and the standards it has created. Later in the chapter, we will see how these standards have directly impacted data breach response processes and liability.

6.4.1 PCI Data Security Standard

In 2004, five major card brands came together to release the first version of the PCI DSS. In order to accept payment cards, merchants all over the world were required by contract to adhere to the detailed, technical standard. The five payment brands that created the original PCI DSS were:

- Visa
- Mastercard
- American Express

15. Fran Silverman, "Cyber Pirates: Hacker's Credit Card Haul Raises Security Flag," *Hartford Courant*, January 14, 2000, http://articles.courant.com/2000-01-14/business/0001140730_1_credit-card-cd-universe-card-numbers.

16. Oscar Marquis, "ID Theft Should be Addressed by the Industry, Not Congress," *American Banker*, September 13, 2002, 9.

- Discover
- JCB

The PCI DSS is critically important for navigating payment card breaches. The standard is marketed as a tool to "help protect the safety" of payment card data. However, as we will see, it also functions as a tool to determine liability in the event of a data breach, and is part of a broader compliance toolset that the payment card brands use to recoup costs and generate revenue. At the time that PCI DSS was first deployed, the immediate effects were to:

- Quell the widespread calls for better security and regulation in the payment card industry
- Place responsibility for cardholder data security squarely on merchants, processors, and other downstream entities that handled payment card data, rather than the card brands themselves
- Give card brands a clear mechanism for leveraging fines and recouping costs of fraud from merchants and other downstream entities
- Put the payment card brands in the driver's seat when it came to cardholder data security standards

6.4.2 A For-Profit Standard

PCI DSS is a *proprietary* standard. One "tell" that it is maintained by a for-profit entity is that in order to download it, you have to enter your personal information in a form with an automatically checked box that reads, "Yes, I am interested in learning more about the PCI Security Standards Council and their training programs." (Training programs sold by the PCI SSC typically cost between $1,000 and $3,000 per seat.) The fact that it is maintained by a for-profit entity means that the administration of the PCI compliance program can, and does, generate revenue for its owners.

As per the standard: "PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data (SAD)." The PCI DSS defines "cardholder data" and "sensitive authentication data" as follows:

- **Cardholder Data**: Primary account number (PAN), cardholder name, service code, expiration date
- **Sensitive Authentication Data**: Full track data, CVV2, CID, CVC2, CAV2, PIN

PCI DSS includes 12 categories, as follows:[17]

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

17. PCI Security Standards Council, *PCI DSS*, v.3.2.1, May 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf.

3. Protect stored cardholder data.
4. Encrypt transmission of cardholder data across open, public networks.
5. Use and regularly update antivirus software or programs.
6. Develop and maintain secure systems and applications.
7. Restrict access to cardholder data by business need to know.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

6.4.3 The Man behind the Curtain

The PCI SSC oversees maintenance and implementation of the PCI DSS. Formed in 2006, the PCI SSC touts itself as a "global open body formed to develop, enhance, disseminate and assist with the understanding of security standards for payment account security."[18] Many people think it is a nonprofit or government entity. As we will see, it is neither—a fact that has far-reaching consequences for cybersecurity and breach response.

The PCI SSC's LinkedIn page states that the organization is nonprofit, as shown in Figure 6-2, but this isn't true. The PCI SSC is definitely *non*-nonprofit. As indicated in the State of Delaware's public records, the PCI SSC is actually a limited liability company "with no special attributes such as non profit or religious."[19]

Corporate filings from the Commonwealth of Massachusetts and the State of Delaware confirm that the "PCI Security Standards Council, LLC" is a *for-profit* limited liability corporation formed in Delaware on September 7, 2006, and subsequently registered in Massachusetts (Figure 6-3).

The same filing indicates that LLC is managed by five members, representing VISA Holdings, Inc., Mastercard International Incorporated, JCB Advanced Technologies, Inc, Discover Financial Services, LLC, and AETRS (American Express Travel Related Services Company, Inc.), as shown in Figure 6-4.

It's very hard to find details about the company's revenue and ownership, although details leak out here and there. For example, Discover Financial Services' (DFS) 2014 Annual Report to the Federal Reserve states that DFS holds a "total equity ownership of 20%" in the PCI SSC.[20]

---

18. PCI Security Standards Council, "About Us," https://web.archive.org/web/20160414051410/https://www.pcisecuritystandards.org/about_us/.

19. State of Delaware, "Entity Details, File Number 4215897," Department of State: Division of Corporations, https://icis.corp.delaware.gov/Ecorp/EntitySearch/EntitySearchStatus.aspx?i=4215897&d=y.

20. Discovery Financial Services, *Annual Report of Holding Companies, Board of Governors of the Federal Reserve System*, U.S. Federal Reserve, December 31, 2014, 2.

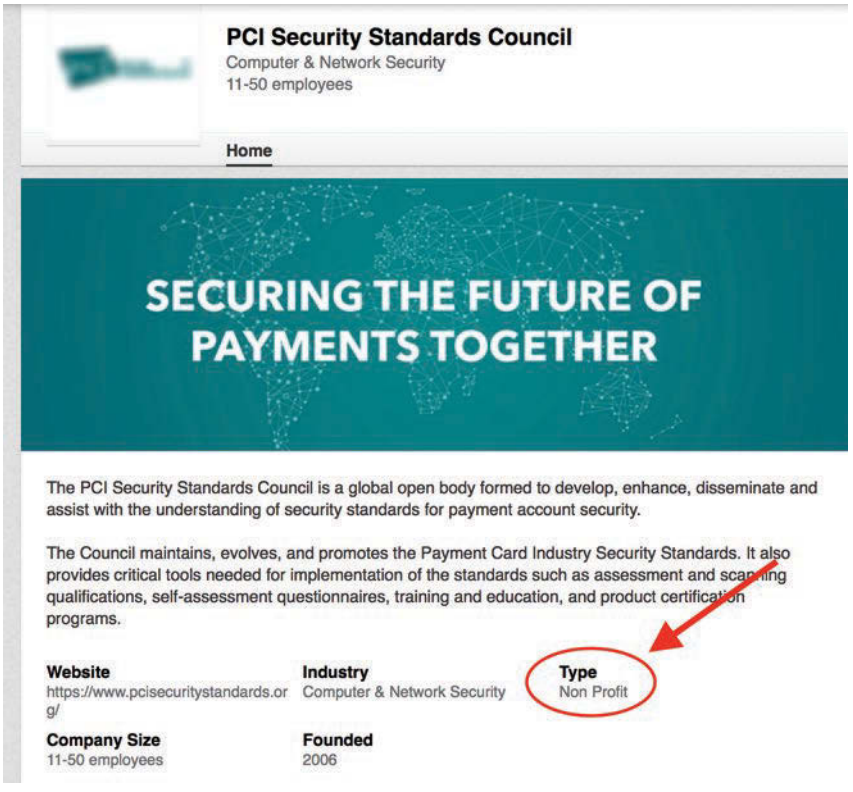


Figure 6-2. LinkedIn page for the PCI Security Standards Council, indicating (incorrectly) that the organization is a nonprofit. It is actually a for-profit LLC. Source: LinkedIn, accessed May 30, 2019, https://www.linkedin.com/company/pcissc/.

When examining the PCI SSC's standards and processes for reducing the risk of data breaches, keep in mind that this is not a government regulatory agency or an independent nonprofit. It has the ability to profit off the regulatory system that it has created, and in turn, it can pass any profits along to the card associations that own it.

Understand the Incentives

Many people think the PCI SSC is an independent third party that regulates all participants in the payment card system. It's important to understand that it is not: The PCI SSC is owned by the card associations, and the standards they create clearly reflect the interests of their owners. Do not make the mistake of thinking otherwise. In a data breach, be aware that the PCI SSC and its instruments have incentives to protect the card brands above all. Merchants and other entities that suffer a breach cannot trust them to treat all parties equally.

F

The Commonwealth of Massachusetts

William Francis Galvin
Secretary of the Commonwealth
One Ashburton Place, Room 1717, Boston, Massachusetts 02108-1512

Foreign Limited Liability Company
Application for Registration
(General Laws Chapter 156C, Section 48)

Federal Identification No.: 20-5255562

(1a) The exact name of the limited liability company:
PCI Security Standards Council, LLC

(1b) If different, the name under which it proposes to do business in the Commonwealth of Massachusetts:

(2) The jurisdiction* where the limited liability company was organized:
Delaware

(3) The date of organization in that jurisdiction: September 7, 2006

(4) The general character of the business the limited liability company proposes to do in the Commonwealth:
Development, management and oversight of data security standards and any and all acts and things as are permitted to be done by a limited liability company under the laws of the Commonwealth of Massachusetts.

(5) The business address of its principal office:
401 Edgewater Place, Suite 600, Wakefield, Massachusetts 01880

Figure 6-3. PCI SSC's registration application in Massachusetts. Source: MA SOC Filing No. 201270218250, February 15, 2012.

(7) The name and business address, if different from principal office location, of each manager:

Mike Mitchell	AETRS 200 Vesey Street UMC NY-01-30-02, New York, NY 10285
Rob Tourt	Discover Financial Services, LLC 2500 Lake Cook Road, Riverwoods, IL 600155
Lib de Veyra	JCB Advanced Technologies, Inc. 700 South Flower Street, Suite 1000, Los Angeles, CA 90017
Bruce Rutherford	Mastercard International Incorporated C/O Tax Department, 2000 Purchase Street, Purchase, NY 10577
Eduardo Perez	Visa Holdings, Inc. Attn: Taxation M1-6B, P.O. Box 8999, San Francisco, CA 94128

Figure 6-4. PCI SSC's registration application in Massachusetts shows the five managers of the company, which represent each of the five major card associations. Source: MA SOC Filing No. 201270218250, February 15, 2012.

6.4.4 PCI Confusion

For retailers and processors that make an effort to become "PCI compliant," the process can be fraught with confusion. The major card associations require all entities that process, store, or transmit cardholder data to fully comply with all aspects of the PCI DSS standard. However, only certain entities are required to have a third party *validate* their compliance, based on the number of transactions that they process each year. Visa, for example, allows most merchants that process "fewer than 20,000 Visa e-commerce transactions" and "all other merchants . . . processing up to 1M VISA transactions per year" to complete a self-assessment questionnaire, an attestation of compliance, and (in some cases) results of a vulnerability scan as evidence of compliance with PCI DSS.

Merchants and service providers that process large volumes of transactions are typically required by their card brands to have their PCI DSS compliance validated by a qualified security assessor (QSA). The QSA is an organization certified by the PCI SSC to conduct PCI DSS compliance audits. The merchant must pay for the services of the QSA.

The job of the PCI QSA is to "validate an entity's adherence to PCI DSS." In other words, if you are a merchant required to have a QSA validate your PCI DSS compliance, an employee from a company that is an approved QSA will review your company's policies, procedures, and security test results; interview your staff; and go through the PCI DSS checklist to determine whether you are in compliance with each item. Then the QSA issues a report that is shared with the PCI SSC.

The PCI QSAs often have different interpretations of the rules. "The biggest challenge with PCI is that you are at the mercy of the auditors and their skill set," said Jay White, the global information protection architect for Chevron. "With some auditors, everything becomes black and white, while others take a more nuanced view of the controls a company might have in place."[21]

6.4.5 QSA Incentives

QSAs have an unspoken incentive to satisfy their clients—the retailers and payment processors that they evaluate. QSAs are not randomly assigned. Instead, retailers can choose from a long list of PCI QSAs. If a retailer does not like the results of a PCI assessment, it has the freedom to choose a different provider next time. This creates an inherent conflict of interest for QSAs: On the one hand, they are responsible for accurately reporting the PCI compliance status of an organization; and on the other hand, they are under significant business pressure to report what the organization wants to hear. This is in contrast to government-regulated industries, such as the financial sector, where examiners work for agencies such as the Federal Deposit Insurance Corporation or the Federal Reserve.

QSAs must also stay in the good graces of the PCI SSC (which of course is owned by five payment card brands). The PCI SSC invented the concept of a QSA, and all approved firms are listed on the PCI SSC's website. (There are 390 approved QSAs listed on the PCI SSC's website as of March 2019.)

---

21. Jaikumar Vijayan, "Retailers Take Swipe at PCI Security Rules," *Computerworld*, October 15, 2007, https://www.computerworld.com/article/2552354/retailers-take-swipe-at-pci-security-rules.html.

Becoming a QSA is a substantial investment. The QSA itself must pay hefty fees to the PCI SSC for the privilege of conducting PCI DSS assessments. Each QSA pays an initial application fee, plus a "regional qualification fee" of up to $24,000 that allows the company to conduct assessments only in that specific region. If a QSA would like to conduct assessments in other regions, the company must pay additional fees for the other regions. The QSA cannot conduct assessments, however, unless individual employees of the company also complete the requisite training program, which costs approximately $3,000 per person. In addition, the QSA and all employees must pay hefty "requalification" fees every year in order to maintain their status as a PCI QSA.

A company that wants to serve as a QSA in the United States, and has a single employee trained to perform assessments, must pay at least $27,250 initially to the PCI SSC, and at least $13,650 every year thereafter. This cost is exhorbitant for smaller security firms, and any security firm engaged in PCI assessment work must price their services high enough to ensure that they recoup their annual QSA fees. The fees ultimately get passed along to the merchants and other entities that are required to hire a QSA.

In short, the QSA program is a money-making business. Over the years, the PCI SSC added additional "Assessors and Solutions" programs, such as "Approved Scanning Vendors," "Payment Application-QSA" and "PCI Forensic Investigator" programs. Merchants and other entities are required by the card brands to utilize services and/or products of these assessors. Each of these programs requires additional application and training fees, which are paid to the PCI SSC, which in turn is owned by the five major card brands.

The good standing of a QSA can be revoked at any time by the PCI SSC, which can require QSAs to "requalify" or simply stop providing QSA services. Because of this, QSAs are beholden to the PCI SSC (and therefore the card brands) in order to remain in business as QSAs.

Since the card brands make money off the PCI compliance assessment program, they have a direct financial incentive to ensure that retailers and other entities continue to hire QSAs to conduct the assessments.

6.4.6 Fines

The QSA's report can have extensive consequences for a retailer or payment processor. Gaps in PCI compliance can be expensive to correct and result in large fines levied against the noncompliant entity. In the event of a breach, the QSA's report may even be used in court to demonstrate negligence, as we will see later.

Merchants or service providers can be hit with costly fines and penalties for noncompliance—but not by the card brands directly. Instead, the card brands have created a system in which they fine intermediary banks, and then fines and liabilities trickle down to merchants at the banks' discretion.

The fines for noncompliance can be substantial—up to $200,000 per violation, according to the Visa Core Rules and Visa Product and Service Rules, which address account information security noncompliance for Visa.[22] Fines for noncompliance in this case are paid to the card brand (in this case, Visa). Banks, of course, are in a much better position to pay these fines than

22. USA Visa, *Visa Core Rules and Visa Product and Service Rules*, https://usa.visa.com/dam/VCOM/download/about-visa/15-October-2014-Visa-Rules-Public.pdf (accessed April 23, 2016).

a small mom-and-pop retailer. In the case of Cisero's, Visa fined U.S. Bank, and then let U.S. Bank decide whether to go after the McCombs to recover the money.

6.5 TJX Breach

On January 17, 2007, the TJX Companies announced, painfully, that it had "suffered an unauthorized intrusion into its computer systems that process and store information related to customer transactions. While TJX has specifically identified some customer information that has been stolen from its systems, the full extent of the theft and affected customers is not yet known."[23]

Initially, the company estimated that more than 45.6 million card numbers had been stolen over an 18-month period—the largest payment card data breach to have ever been publicly reported. That number was ultimately raised to more than 94 million breached payment card numbers. In addition, personal information such as driver's license numbers and other details for 451,000 individuals was exposed; ironically, the information had been collected for the purposes of combating fraud.

Visa reported that losses due to fraud were as high as $83 million and climbing. "You know, these [card numbers] are going to be sold off for a period of time in the future, so it's going to continue for some time out there," said Joseph Majka, vice president of investigations and fraud management for VISA USA.[24]

Banks, card brands, and TJX itself struggled to sort out the liability. The ensuing litigation established a strong precedent that demonstrated that merchants would be held accountable for losses due to payment card breaches. Even more important, it cemented the role of PCI compliance as a tool for determining who was at fault. By the time the dust had settled, the retailer's lack of PCI compliance had been broadcast throughout the news, used as evidence in court, and even triggered new state laws. In the court of public opinion and law, PCI compliance mattered.

In this section, we will walk through the important precedents that the TJX case established for determining liability in payment card breaches.

6.5.1 Operation Get Rich or Die Tryin'

As payment technology largely stalled in the United States, and PCI compliance slowly gained traction, criminals were exploring innovative new ways to steal card numbers in bulk.

Following the success of Operation Firewall and the takedown of Shadowcrew (see Chapter 5), Albert Gonzalez moved to Miami, where he continued working as a salaried informant for the Secret Service. He provided agents with information about active carders

23. TJX Companies, Inc. "The TJX Companies, Inc. Victimized by Computer Systems Intrusion; Provides Information to Help Protect Customers," press release, January 17, 2007, https://www.doj.nh.gov/consumer/security-breaches/documents/tjx-20070117.pdf.

24. Mark Jewell, "TJX Breach Could Top 94 Million Accounts," *NBC News*, October 24, 2007, http://www.nbcnews.com/id/21454847/ns/technology_and_science-security/t/tjx-breach-could-top-million-accounts.

and gave presentations about cybercrime. At one point, he even "shook the hand of the head of the Secret Service."[25]

At the same time, Albert was on a mission of his own—one that he dubbed "Operation Get Rich or Die Tryin'." By late 2004, "war driving" (enumerating wireless networks while driving, for the purposes of hacking) had become popular. Albert was intrigued. While working for the Secret Service in Miami, he enlisted the help of some of his Internet Relay Chat (IRC) buddies and convinced them to drive around the Miami area, searching for retailers with vulnerable networks. They quickly found a Marshalls with a weak wireless access point, broke in, and gave Gonzalez remote access to the network as well. From there, the group wormed their way into the servers of TJX, Marshall's parent company, and found a treasure trove of stored payment card data, which they siphoned out little by little.

6.5.2 Point-of-Sale Vulnerabilities

The initial card dumps from TJX weren't good enough for Albert. Much of the card data had been stored for extended periods, and a large percentage of the cards had expired. Albert wanted *fresh* card data. He realized that the best place to get it was from the POS systems, where customers swiped their cards. These, too, were hackable.

Albert and his friends began walking around retailers in Miami, gathering information about makes and models of POS devices. One of his colleagues managed to swipe a POS device from the checkout counter of an OfficeMax in Los Angeles, to help their research. Overseas, one of his friends in Estonia hacked into Micros Systems, a POS manufacturer; stole a list of employee usernames and passwords; and sent it over. Albert convinced his old friend, programmer Stephen Watt (who worked at Morgan Stanley), to write a sniffer program for him. The program, which Watt reportedly dashed off quickly, sniffed network traffic and logged any credit card numbers that were sent unencrypted. Armed with default credentials, Albert and his cohorts installed the sniffer program on central POS servers in multiple major retailers and captured credit card numbers in real time just as they were sent to the server for processing.

6.5.3 Green Hat Enterprises

Albert had learned his lesson about the risks of cashing out. Instead of monetizing the card data himself, he forwarded the stolen data to a team of colleagues around the country and overseas, who would cash out and mail him his share. Albert made so much money he threw himself a $75,000 birthday party in Manhattan. He regularly received packages containing hundreds of thousands of dollars in cash, at one point complaining to a friend "that he had been forced to count $340,000 by hand because his money counter was broken from overuse." (His friend responded with "several pages worth of LOLs.")[26]

Later, Albert sold the dumps to a Ukranian, Maksym Yastremskiy. Yastremskiy would sell the card numbers to buyers around the world and split the profits. "Yastremskiy arranged to

25. James Verini, "The Great Cyberheist," *New York Times Magazine*, November 10, 2010, http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

26. Sabrina Rubin Erdely, "Sex, Drugs, and the Biggest Cybercrime of All Time," *Rolling Stone*, November 11, 2010, http://www.rollingstone.com/culture/news/sex-drugs-and-the-biggest-cybercrime-of-all-time-20101111.

have the payment data encoded onto bank cards, which were then sold at nightclubs all over the world for $300 a pop, of which Albert got half."[27] He also used services such as E-Gold and WebMoney to launder funds electronically.

Before he knew it, Albert was running an international criminal carding syndicate. "No one I spoke with compared him to a gangster or a mercenary," reported James Verini of the *New York Times*, years later, "but several likened him to a brilliant executive." He dubbed his venture, "Green Hat Enterprises."

When asked to compare Albert to other cybercriminals, Seth Kosto, an assistant U.S. attorney in New Jersey, replied: "As a leader? Unparalleled. Unparalleled in his ability to coordinate contacts and continents and expertise. Unparalleled in that he didn't just get a hack done—he got a hack done, he got the exfiltration of the data done, he got the laundering of the funds done. He was a five-tool player."[28]

Green Hat Enterprises was a smashing success. At the same time, card brands began to alert the retailers to the massive card thefts and pulled in law enforcement. Federal agents were searching for the ringleaders of the massive card fraud, unaware that the criminal mastermind was right under their noses, working as a Secret Service informant.

6.5.4 The New Poster Child

When TJX revealed the breach in January 2007, the public was shocked—not just by the breathtaking scale of the theft, but by how little TJX seemed to know about what was going on in its own network and by the company's seemingly lackadaisical attitude toward security. "[T]he breach has made it something of a poster child for sloppy data security practices among retailers," reported *Computer World*.[29]

The breach was likely detected early by Citigroup, who identified TJX as a common point-of-purchase for a group of stolen card numbers. In other words, Citigroup would have found that a group of consumers whose card numbers were used fraudulently had all shopped at TJX stores.[30] TJX received notification in July 2006, although the company did not discover its ongoing network intrusion until December of that year. By then, hackers had been raiding the company's network for nearly a year and a half.

"TJX Failed to Notice Thieves Moving 80-Gbytes of Data on Its Network" screamed a headline in *Wired* magazine. Consumers were frustrated that, even after the company discovered the intrusion in December 2006, "it took the company another month to disclose the breach to consumers."[31] One forensic investigator reported that he had never seen such a "void of monitoring and capturing via logs activity" in a major retailer.

---

27. Erdely, "Sex, Drugs."

28. Verini, "Great Cyberheist."

29. Jaikumar Vijayan, "One Year Later: Five Takeaways from the TJX Breach," *Computerworld*, January 17, 2008, https://www.computerworld.com/article/2538711/cybercrime-hacking/one-year-later–five-takeaways-from-the-tjx-breach.html.

30. Jacqueline Bell, "Citigroup May Have Discovered Data Breach Early: TJX," *Law 360*, December 6, 2007, https://www.law360.com/banking/articles/41795/citigroup-may-have-discovered-data-breach-early-tjx.

31. Kim Zetter, "TJX Failed to Notice Thieves Moving 80-Gbytes of Data on Its Network," *Wired*, October 26, 2007, https://www.wired.com/2007/10/tjx-failed-to-n.

A month after the breach was announced, TJX was still unable to say just how many consumers were affected. "We don't have a number for you there. Our work is not finished," said a TJX spokesperson.[32]

6.5.5 Who's Liable?

Many banks reissued cards, an expensive process that cost up to $25 per card and irritated consumers. Hoping to recoup costs, hundreds of issuing banks represented by the Connecticut Bankers Association, Maine Association of Community Banks, and Massachusetts Bankers Association joined forces with Amerifirst and others to file a class-action lawsuit against TJX.

A key piece of the banks' case against TJX was that the retailer "had not complied with nine of the 12 security controls mandated by the Payment Card Industry (PCI) data security standards when the breach occurred."[33] The Canadian privacy commissioner conducted an eight-month investigation that cited TJX's PCI violations, which included lack of network segmentation, weak wireless security, and lack of proper logging.

TJX's PCI compliance issues were seen by many as evidence that the company had been negligent in protecting sensitive consumer data. Never mind that PCI wasn't a law and that Visa had given TJX an extension for meeting the new requirements. "Visa will suspend fines until Dec. 31, 2008, provided your merchant continues to diligently pursue remediation efforts," Visa's Joseph Majka had written in a December 2005 letter. "This suspension hinges upon Visa's receipt of an update by June 30, 2006, confirming completion of stated milestones."[34]

After the fact, the TJX case established a precedent for using PCI compliance (or lack thereof) as evidence in data breach cases. If a merchant was breached and found to be noncompliant, banks and other entities that suffered losses could use noncompliance as evidence that the merchant was negligent, strengthening their case for compensation.

6.5.6 Struggles with Security

Why wasn't TJX more secure? As with most retailers, it boiled down to cost and complexity.

In 2005, TJX's chief information officer, Paul Butka, wrote a telling email to his staff when discussing whether to upgrade from the outdated WEP wireless encryption protocol—which was widely known to be weak—to the more secure WPA technology. "WPA is clearly best practice and may ultimately become a requirement for PCI compliance sometime in the future. I think we have an opportunity to defer some spending from FY07's budget by removing the money for the WPA upgrade," he wrote.

---

32. Ellen Nakashima, "Customer Data Breach Began in 2005, TJX Says," *Washington Post*, February 22, 2007, https://www.washingtonpost.com/archive/business/2007/02/22/customer-data-breach-began-in-2005-tjx-says/dcf4720f-6385-4e4e-9b9c-9b120a0eaef8/.

33. Jaikumar Vijayan, "TJX Violated Nine of 12 PCI Controls at Time of Breach, Court Filings Say," *Computerworld*, October 26, 2007, http://www.computerworld.com/article/2539588/security0/tjx-violated-nine-of-12-pci-controls-at-time-of-breach–court-filings-say.html.

34. Ericka Chickowski, "TJX: Anatomy of a Massive Breach," *Baseline*, January 30, 2008, http://www.baselinemag.com/c/a/Security/TJX-Anatomy-of-a-Massive-Breach.

A few weeks later, another TJX staff member prophetically countered, "The absence of rotating keys in WEP means that we truly are not in compliance with the requirements of PCI. This becomes an issue if this fact becomes known and potentially exacerbates any findings should a breach be revealed."[35]

TJX was certainly not alone in its challenges. In a press release later, TJX said its security was "as good as or better than most other major U.S. retailers." This was probably true.[36]

"[L]arge companies with highly distributed, older computing environments can expect to have an especially hard time applying PCI security controls,"said Amer Deeba, an executive at Qualys. In order to become PCI compliant, retailers had to coordinate with the vendors of their POS systems, operating systems, and applications to ensure that all of the software that they relied upon was in compliance. They typically had to re-architect their networks and invest large amounts of money in software upgrades. In some cases, vendors would not or could not upgrade their software, leaving retailers with even bigger headaches. "Many of the big [retailers] are handling credit card information from all around the world and storing it in legacy systems that are no longer supported or updated by vendors."[37]

After the eight-month investigation of TJX, the Canadian privacy commissioner concluded that "TJX['s] experience illustrates how maintaining custody of large amounts of sensitive information can be a liability."

"The lesson?" The Canadian government concluded, "One of the best safeguards a company can have is not to collect and retain unnecessary personal information. This case serves as a reminder to all organizations operating in Canada to carefully consider their purposes for collecting and retaining personal information and to safeguard accordingly."[38]

There are two ways to avoid data spills:

1. Carefully secure sensitive data.
2. Reduce or eliminate sensitive data.

You can't spill hazardous data if it doesn't exist.

6.5.7 TJX Settlements

For TJX, the breach was expensive—although the company bounced back. In August 2007, the company reported data breach response costs of $256 million. Researchers estimated the final cost would be closer to $500 million to $1 billion.[39]

---

35. Chickowski, "Anatomy of a Massive Breach."

36. TJX Companies, "The TJX Companies, Inc. Announces Settlement with Attorneys General Regarding 2005/2006 Cyber Intrusion(s)," press release, June 23, 2009, http://investor.tjx.com/phoenix.zhtml?c=118215&p=irol-newsArticle&ID=1301566.

37. Vijayan, "Retailers Take Swipe."

38. Privacy Professor, "Canadian Privacy Commissioners Release TJX Investigation Report," *Privacy Guidance* (blog), September 25, 2007, http://privacyguidance.com/blog/canadian-privacy-commissioners-release-tjx-investigation-report.

39. Ross Kerber, "Cost of Data Breach at TJX Soars to $256m," *Boston.com*, August 15, 2007, http://archive.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m.

TJX settled the class-action lawsuits with issuers and consumers quickly, as follows:

- **Consumers:** The consumer class action claimed that TJX was slow to notify customers of the breach, exposing people to identity theft without the ability to seek protection. The case was settled in September 2007, just nine months after the breach notification. "TJX will offer up to $7 million in store vouchers to customers who incurred out-of-pocket or lost time costs from the intrusion, and hold a one-time, three-day customer appreciation sale in which prices at TJX stores will be reduced by 15% for all customers. The vouchers, which are transferable and stackable, would range from $30-$60 per consumer based on documented evidence."[40]
- **Issuers:** Issuers claimed that TJX was negligent in securing payment card data—and had ample evidence to back that up. They primarily sought reimbursement for the steep costs of reissuing cards. During 2006, Visa had rolled out its new "Account Data Compromise Recovery" (ADCR) program that "provides automatic reimbursement to U.S. issuers for incremental counterfeit fraud losses from the theft of improperly stored card information." However, Visa's ADCR did not cover costs such as card reissuing. In late 2007, the issuers settled with TJX for $40.9 million. "It is expected that financial institutions will receive greater reimbursement by opting into the TJX settlement than they would have received under the traditional or ADCR programs," commented *Business Wire*.[41]

Forty-one state attorneys general also filed suit against TJX in the wake of the breach. Two years later, the case finally settled in a landmark agreement. According to the company's press release, TJX agreed to:[42]

- Provide $2.5 million to establish a new Data Security Fund for use by the states to advance effective data security and technology
- Provide a settlement amount of $5.5 million together with $1.75 million to cover expenses related to the states' investigations
- Certify that TJX's computer system meets detailed data security requirements specified by the states
- Encourage the development of new technologies to address systemic vulnerabilities in the U.S. payment card system

Notably, the settlement required TJX to implement specific security technologies, including upgrading its WEP-encrypted access points to WPA, using virtual private networks (VPNs) and installing antivirus software. Gartner analyst Avivah Litan criticized the technical stipulations,

40. Ron Zapata, "TJX Settles Consumer Class Actions over Data Breach," *Law 360*, September 24, 2007, https://www.law360.com/articles/35681/tjx-settles-consumer-class-actions-over-data-breach.

41. "Visa and TJX Agree to Provide U.S. Issuers up to $40.9 Million for Data Breach Claims," *Business Wire*, November 30, 2007, https://www.businesswire.com/news/home/20071130005355/en/Visa-TJX-Agree-Provide-U.S.-Issuers-40.9.

42. TJX Companies, "TJX Companies, Inc. Announces Settlement."

stating, "I think the AGs are better off focusing on disclosure rules and consumer protection than on security technology. . . . As soon as the government starts mandating or recommending technologies like end-to-end encryption, their mandates or recommendations will become out of date."[43]

For retailers, the 2009 TJX attorneys general settlement was a wake-up call. One law firm issued a client news release, stating: "The TJX Settlement is a warning. All companies maintaining personal information . . . must implement a secure information protection program with regular auditing procedures."[44]

Despite the legal turmoil and direct breach costs, for TJX, the damage wasn't sustained. One commentator complained, "You'd think with such a heavily-publicized breach of personal information that people would be going out of their way to avoid shopping at TJX properties like TJ Maxx and Marshall's. Nope. TJX is actually enjoying a healthy 8% increase in revenue over 2006 according to industry reports. . . . It's no wonder so many companies are slow to take compliance initiatives around information security seriously."[45]

6.5.8 Data Breach Legislation 2.0

The TJX breach generated a new wave of legislative activity, primarily designed to authorize third-party claims against breached vendors and establish security standards for payment card data. "In response to the public and industry concern data breaches have generated, legislators at the state level are rolling out 'Data Breach Legislation 2.0,'" reported the International Association of Privacy Professionals, a year after the TJX breach was announced. "Further, legislators often are turning to the Payment Card Industry Data Security Standards (the PCI DSS) as the benchmark cybersecurity standard for these new statutes. . . . PCI allows legislators to side-step the need to become data security experts and, at the same time, adopt a standard that accounts for data security's constantly changing nature."[46]

Following the TJX breach, lawmakers in states including Minnesota, Massachusetts, Connecticut, New Jersey, California, and Texas proposed new laws regarding payment card data security. Minnesota passed the Plastic Card Security Act shortly thereafter, based on a core PCI provision that disallowed storage of certain card data. Under the law, "any company that suffers a data breach and is found to have been storing prohibited card data on its systems will have to reimburse banks and credit unions the costs associated with blocking and reissuing cards. Such companies could also be subject to private action brought by individuals who might

---

43. Jaikumar Vijayan, "TJX Reaches $9.75 Million Breach Settlement with 41 States," *Computerworld*, June 24, 2009, https://www.computerworld.com/article/2525965/cybercrime-hacking/tjx-reaches–9-75-million-breach-settlement-with-41-states.html.

44. Tara M. Desautels and John L. Nicholson, "TJ Maxx Settlement Requires Creation of Information Security Program and Funding of State Data Protection and Prosecution Efforts," Pillsbury Law, July 1, 2009, https://www.pillsburylaw.com/images/content/2/6/v2/2626/7F4F43B367B5276B0CFA6D13CFF4044C.pdf.

45. Mark Tordoff, "TJX Settlement Shows Why Compliance Isn't Taken Seriously," *Toolbox* (blog), September 26, 2007, https://it.toolbox.com/blogs/mark-tordoff/tjx-settlement-shows-why-compliance-isnt-taken-seriously-092607.

46. Luis Salazar, "Data Breach Legislation 2.0," *IAPP*, January 1, 2008, https://iapp.org/news/a/2008-01-data-breach-legislation-2.0.

have been affected by a violation of the state law."[47] This law set the stage for additional lawsuits in subsequent data breaches, including the 2014 Target breach.

In the months that followed the TJX breach, card brands used the TJX case to push PCI compliance programs—and it worked. By October 2007, "Visa announced that 65 percent of level-one merchants and 43 percent of level-two merchants are compliant, up from 36 percent and 15 percent at the start of the year, respectively."[48] Merchants that did not comply were hit with fines.

Banks rallied behind "legislation that incorporates PCI DSS as a means of establishing retailer liability for data breaches, with the expectation that it will open the doorway to damage recoveries for them."[49] Texas very nearly became the first state to mandate that retailers comply with PCI DSS when the state House passed H.B. No. 3222 in 2007—but the bill died in Senate committee.

6.6 The Heartland Breach

In 2008, the Heartland breach became the largest payment card breach the world had ever seen, with 130 million card numbers stolen. Heartland, a payment processor based in Princeton, New Jersey, processed far more credit card numbers than any one merchant. The company acted as a middleman, receiving swiped card numbers from approximately 200,000 merchants and connecting them with the card networks. Heartland processed $66.9 billion dollars' worth of transactions in 2008.

Unlike TJX, Heartland had been certified PCI compliant at the time of the breach. As a result, the Heartland breach raised important questions regarding the value of PCI compliance for proactively protecting payment card data.

In this section, we will discuss the Heartland case and the issues that it raised regarding PCI compliance. We will also study Heartland's impressive response and show how the technologies it implemented following the breach moved the entire industry forward.

6.6.1 Heartland Gets Hacked

Albert Gonzalez was on top of the cybercriminal world. He was a millionaire who controlled an international cybercrime ring. But by day, he still worked for the Secret Service, and he hated the daily grind. He was constantly looking for new challenges—whether it was checking for vulnerabilities in POS systems at local retailers such as Toys R' Us or surveying the area for weak wireless networks that he could hack. In late 2007, he teamed up with two Eastern

47. Jaikumar Vijayan, "Minnesota Becomes First State to Make Core PCI Requirement a Law," *Computerworld*, May 23, 2007, http://www.computerworld.com/article/2541431/security0/minnesota-becomes-first-state-to-make-core-pci-requirement-a-law.html.

48. Dan Kaplan, "TJX Settles with Banks over Data Breach," *SC Media*, December 19, 2007, https://www.scmagazine.com/tjx-settles-with-banks-over-data-breach/article/554018.

49. Salazar, "Data Breach Legislation 2.0."

European criminals to hack into payment processor Heartland Payment Systems, as well as 7-11, Hannaford Brothers, and other major retailers.[50]

The hackers gained their foothold in the Heartland network during late December 2007. Leveraging a SQL injection vulnerability in an Internet-facing website, the criminals wormed their way into the network and installed a sniffer tool, capturing fresh payment card data as it was in transit across the network.

Visa alerted Heartland to "suspicious activity" in October 2008. Heartland reacted quickly, working closely with the card brands and pulling in multiple forensic investigators. When a breach was confirmed on January 12, 2009, they quickly reported it to the authorities. A week later, Heartland issued a press release along with customer support programs, such as a website for consumers.[51]

6.6.2 Retroactively Noncompliant

Heartland Payment Systems was PCI compliant—or so it thought. In April 2008, the company underwent its routine examination by a PCI QSA and was certified compliant. Nine months later, the company discovered that it had been hacked.

Then the lawsuits began. Visa, Mastercard, American Express, and Discover all filed claims, in addition to issuing banks. Suddenly, in March 2009, Visa announced that Heartland was no longer considered a PCI compliant service provider. In fact, Visa's chief enterprise risk officer, Ellen Richey, said that despite its QSA certification, the fact that Heartland was breached meant that it wasn't PCI compliant in the first place. "As we've said before," she continued, "no compromised entity has yet been found to be in compliance with PCI DSS at the time of a breach."[52]

Security professionals were floored. "What we see is that although no PCI-compliant company seems to ever get breached, many are certified and then found non-compliant after the breach," said Rich Mogull, founder of Securiosis. "Thus, it's clear the certification process is flawed. While I don't expect certification to impart immunity from attack, decertifying all these companies seems disingenuous."[53]

Many questioned the value of the PCI standards, an opinion that Visa executives dismissed as "premature." Others pointed out that Visa's claim that Heartland was retroactively noncompliant could be "an attempt by the credit card company to protect itself legally and prevent the payment processors from using PCI as a shield against breach-related lawsuits filed by banks and credit unions."[54]

Heartland executives emphasized that their network had been examined in detail by PCI QSAs, none of whom identified the vulnerability that was exploited by the hackers.

---

50. United States v. Albert Gonzalez, 2009R00080 (D.N.J. 2009), https://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf.

51. Heartland Payment Systems, "Heartland Payment Systems Uncovers Malicious Software In Its Processing System," press release, January 20, 2009, http://web.archive.org/web/20090127041550/http://2008breach.com/Information20090120.asp.

52. Jaikumar Vijayan, "Visa: Post-Breach Criticism of PCI Standard Misplaced," *CSO*, March 20, 2009, https://www.cso.com.au/article/296278/visa.

53. Dan Kaplan, "Visa: Heartland, RBS WorldPay No Longer PCI Compliant," *SC Media*, March 13, 2009, https://www.scmagazine.com/visa-heartland-rbs-worldpay-no-longer-pci-compliant/article/555578.

54. Vijayan, "Visa: Post-Breach Criticism."

Furthermore, after the breach Heartland was required to hire a PCI Qualified Incident Response Assessor (at its own expense), to identify the source of the compromise—an investigation that took six weeks.

6.6.3 Settlements

Ultimately, Heartland settled with Visa for $60 million, Mastercard for $41.1 million, American Express for $3.6 million, and Discover for $5 million. The company also settled a consumer class-action lawsuit by establishing a $2.4 million fund for consumer claims.[55]

Industry expert Avivah Litan called the settlements fair and reasonable, noting that the card brands' response to breaches had matured. "Visa and its member banks have much more experience with breaches now than they did when the TJX breach hit," she said. "They know how to settle these matters more amicably." Indeed, despite the fact that the Heartland breach affected far more cardholders, their overall costs were estimated to be far less than the $250 million that TJX had set aside. According to Litan, this was due in part to Heartland CEO Bob Carr's "collegial spirit" and productive working relationship with the card brands, which helped the company avoid "endless litigation."[56]

Takedown of Albert Gonzalez

In the summer of 2007, law enforcement agents arrested Maksym Yastremskiy, Albert Gonzalez's cohort, in a Turkish nightclub. Yastremskiy was responsible for converting Green Hat Enterprises' stolen credit card numbers to cash. An investigation of Yastremskiy's laptop revealed that his top source for payment card data was linked to the email address "soupnazi@efnet.ru." Shocked Secret Service agents recognized Gonzalez's nickname.

Albert Gonzalez was arrested on the morning of May 7, 2008. "[A]gents rushed into his suite at the National Hotel in Miami Beach. With him were a Croatian woman, two laptops and $22,000," reported the *New York Times*. "Over time, he started talking. Months later, he led Secret Service agents to a barrel containing $1.2 million buried in his parents' backyard."[57]

Ultimately, Gonzalez was sentenced to serve two concurrent 20-year sentences in prison, which at the time was the longest sentence ever received in the United States by a hacker. In addition, he forfeited millions of dollars' worth of stolen cash and property, and was forced to pay $25,000 plus restitution.[58]

---

55. Penny Crosman, "Heartland and Discover Agree to $5 Million Data Breach Settlement," *Bank Systems & Technology*, September 3, 2010, http://www.banktech.com/payments/heartland-and-discover-agree-to-$5-million-data-breach-settlement/d/d-id/1294095?.

56. Linda McGlasson, "Heartland, Visa Announce $60 Million Settlement," *Bank Info Security*, January 8, 2010, http://www.bankinfosecurity.com/heartland-visa-announce-60-million-settlement-a-2054.

58. Verini, "Great Cyberheist."

58. Grant Gross, "Hacker Gonzalez Pleads Guilty to 20 Charges," *CSO*, September 11, 2009, https://www.csoonline.com/article/2124329/identity-theft-prevention/hacker-gonzalez-pleads-guilty-to-20-charges.html; Angela Moscaritolo, "Hacker Albert Gonzalez Receives 20 Years in Prison," *SC Media*, March 25, 2010, https://www.scmagazine.com/hacker-albert-gonzalez-receives-20-years-in-prison/article/557561.

6.6.4 Making Lemonade: Heartland Secure

Unlike most merchants, Heartland was in a unique position to change the industry after experiencing its breach. As the fifth-largest merchant acquirer in the United States, it held significant market share. After the breach, Heartland's team conducted an analysis and identified a key area of weakness: the interception of sensitive data in transit across networks within the payment system. Theft of payment card data had been rampant for years, but the theft of data *in transit* across the network was a relatively new method used by criminals, notably emerging in the spotlight during the Hannaford breach of 2008 (also perpetrated by Albert Gonzalez).

According to CEO Bob Carr, Heartland considered three possible solutions for securing payment card data throughout the network:[59]

- **End-to-end encryption**, in which the payment card data is encrypted from the point where it is swiped all the way throughout the network, including both while it is in transit and in storage.
- **Tokenization**, where the credit card numbers are replaced with randomly generated strings ("tokens") after they are swiped, so that merchants and other entities do not have to store actual card data to reference in the event of disputes.
- **Chip (EMV) technology**, where each card contains a "smart" microchip that can be used to facilitate encrypted data exchange, rather than relying on a simple magnetic stripe.

Of these three, Heartland prioritized the deployment of end-to-end encryption as a means of securing data in transit. Carr "emphasized that Heartland's end-to-end encryption model positioned Heartland to secure much of this process . . . using its own resources; only [a fraction] required cooperation from the card brand networks."[60]

To implement the end-to-end encryption model, Heartland worked with a POS development partner to design the Heartland E3 Encrypting Payment Device. This POS terminal encrypted PINs using hardware (TPM) chips within the device and transmitted the data to the payment processor, which held the corresponding keys. The devices were more expensive than a typical POS system (selling for $300 to $500 at the time), but Carr pointed out that merchants had to weigh these costs against PCI compliance requirements and associated risks.[61]

Eventually, Heartland rolled out the Heartland Secure program, which combined the E3 end-to-end encryption solution, EMV ("chip") card support, and tokenization technology. By 2015, Heartland was so confident in the security of its new system that it offered the world's first Merchant Breach Warranty for Heartland Secure merchants: "If the encryption

59. Julia S. Cheney, *Heartland Payment Systems: Lessons Learned from a Data Breach*, (discussion paper, Federal Reserve Bank of Philadelphia, January 2010), https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2010/d-2010-january-heartland-payment-systems.pdf.

60. Cheney, *Heartland Payment Systems.*

61. Cheney, *Heartland Payment Systems.*

fails on a Heartland Secure machine, Heartland will reimburse the merchant for the amount of compliance fines, fees and/or assessments the merchant must pay to the card brands, issuing banks and acquiring bank(s)."[62]

Michael English, Heartland's executive director of product development, cut to the chase: "Through encryption and tokenization, a merchant eliminates clear text card data so if their network is breached, there is no card data to steal and monetize."[63] Although Heartland's breach was devastating in the short term, the company's reaction spurred the deployment of new technologies and increased security throughout the payment ecosystem.

6.7 PCI and Data Breach Investigations

Over time, more and more retailers became PCI compliant—and continued to get hacked. In court, merchants sought to use documentation of PCI compliance as a defense against card brands' fines and litigation. The card brands, in turn, had every incentive to prove that merchants were not actually PCI compliant, even after the fact—and they had the upper hand. In this section, we will show how the card brands stacked the deck against merchants with respect to data breach investigations and discuss how attorney-client privilege can provide protection for parties involved in postbreach litigation.

6.7.1 PCI Forensic Investigators

The PCI SSC established the role of the PCI Forensic Investigator (PFI), which investigates a merchant, collects evidence, and provides a full report to the card brands. Based on their contracts, card brands can require merchants to have a forensic investigation conducted, at the merchant's expense.[64] The merchant must select a PFI from a short list of approved vendors.

At the time of this writing, there are 20 approved PFIs that serve the U.S. region. In order to become a PFI serving the United States, a firm must pay the PCI SSC a fee of $27,500 to "qualify," in addition to fees for training specific employees.

Hiring a PFI, however, is not like hiring a truly independent forensic investigator (despite the fact that the PCI SSC says "PFIs are required to uphold strict independence requirements"). PFIs must be QSAs, first and foremost. They have specific contractual obligations to the PCI SSC. However, they cannot be the same QSA that operates as the merchant's QSA because, according to the PCI SSC, "they would be potentially investigating their own work."

62. "Heartland First to Offer Comprehensive Merchant Breach Warranty," *Business Wire*, January 12, 2015, https://www.businesswire.com/news/home/20150112005260/en/Heartland-Offer-Comprehensive-Merchant-Breach-Warranty.

63. "Heartland First to Offer."

64. PCI Security Standards Council, *Forensic Investigator FAQ*, https://www.pcisecuritystandards.org/documents/PCI_Forensic_Investigator_FAQ.pdf (accessed January 12, 2018).

The "independence" largely ends there. Importantly, PFIs are contractually obligated to:

- Ensure that potential evidence is acquired in a forensically sound manner and "could be used in [a] court of law."[65]
- Investigate and report any deficiencies in PCI compliance "observed during their investigation."[66]
- Deliver preliminary and final incident reports to affected payment brands, the merchant's acquiring bank, and the merchant.

Yes, that's right: If a card brand such as Visa or Mastercard suspects you may have suffered a breach, it can require you to pay to hire an investigator from its list who will collect evidence from your network, determine whether there might be any gaps in compliance, and then submit that report to the card brands and banks, which can then use that against you in court, if needed.

Just because you're footing the bill for an investigator doesn't mean he or she is working for you!

Hire Your Own Investigator

If your organization is hit with a potential payment card breach, you may be required to hire a PFI to investigate. Keep in mind that any findings will be included in a report that is submitted to the card brands and could be used against you in court.

Often, it's a good idea to hire your own investigator that is *not* a PFI and therefore is truly independent of the card associations. Your investigator may have different findings, which can help your case.

6.7.2 Attorney-Client Privilege

Payment card breaches often result in litigation because of the clear financial losses that they can generate. When they do, any and all information can be used against you: reports generated by forensics firms and IT companies, emails and meeting notes generated by your response team, correspondence between executives, and more. Whenever possible, it's a good idea to protect your data from discovery using attorney-client privilege.

The case of Genesco, Inc., versus Visa set an important precedent for the use of attorney-client privilege in data breach cases. On December 10, 2010, a U.S. apparel company, Genesco,

65. Rodney McKemmish, "When is Digital Evidence Forensically Sound?" in *Advances in Digital Forensics IV*, IFIP Advances in Information and Communication Technology 285 (Boston: Springer, 2008), https://link.springer.com/content/pdf/10.1007/978-0-387-84927-0_1.pdf.

66. PCI Security Standards Council, *Responding to a Data Breach*, https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf (accessed January 12, 2018).

publicly announced that it had suffered a large credit card data breach that spanned over a year—but the company was not yet sending out individual notifications since it did not retain customer names in combination with card data, and "the investigation [was] still underway." Most of the Genesco's customers didn't recognize its name, anyway. The company operated a variety of brands: Journeys shoes, Dockers, Footwear, Lids, Johnston & Murphy, and more.

Genesco was required to hire a PFI. Trustwave, its PFI, submitted a report to Visa claiming that Genesco was deficient in its PCI compliance. Genesco contested the claims, submitting its own appeal to Visa in March 2011. Visa fined Genesco's banks (Wells Fargo and Fifth Third) $5,000 each for violations of PCI compliance, and then later charged them $13 million together for the costs of the breach investigation and associated losses.[67] Mastercard also assessed a total fine of more than $2 million. The banks, in turn, charged Genesco.

Unlike most merchants, however, Genesco sued, claiming that "at the time of the Intrusion and at all relevant times Genesco was in compliance with the PCI DSS requirements."[68] Genesco's general counsel hired the firm Stroz Friedberg "to provide consulting and technical services to assist . . . in rendering legal advice to Genesco about the Intrusion and Trustwave's report."[69] Later, Genesco's general counsel hired IBM to assist with remediation.

Visa subpoenaed the Stroz firm, seeking evidence that could be used to support its claims in the case. Critically, the judge ruled that the Stroz firm's work was protected by attorney-client privilege because it had been conducted "in anticipation of potential litigation and/or legal or regulatory proceedings."[70] Later, Visa also subpoenaed IBM, and the judge again ruled that the work was protected by attorney-client privilege.

Effectively, the courts ruled that attorney-client privilege protection extended "to counsel's communications with agents and experts who are retained by counsel for the purpose of providing legal advice." This was a major boon for crisis management and data breach response teams, who suddenly had court precedent that communications in a suspected breach investigation could potentially be protected from discovery by attorney-client privilege.

The protection did not extend to documentation produced in the ordinary course of business. The court ruled that "remedial measures that Genesco took in response to Trustwave's report must be produced because the Trustwave report reflects that those measures were undertaken in the ordinary course of business, not for Genesco's counsel."

---

67. Kim Zetter, "Retailer Sues Visa over $13 MILLION 'Fine' for Being Hacked," *Wired*, March 12, 2013, https://www.wired.com/2013/03/genesco-sues-visa/.

68. Davis Wright Tremaine, "Genesco Wins One, Loses One in Its Case Challenging PCI DSS Fines and Assessments," *Privacy & Security Law Blog*, December 12, 2013, http://www.privsecblog.com/2013/12/articles/financial-services/genesco-wins-one-loses-one-in-its-case-challenging-pci-dss-fines-and-assessments-2.

69. Genesco, Inc. v. Visa, Inc., Case No. 3: 13-0202, at 22 (M.D. Tenn. 2014), http://cases.justia.com/federal/district-courts/tennessee/tnmdce/3:2013cv00202/55283/297/1.pdf.

70. Genesco v. Visa.

Preserving Privilege

Since the Genesco case, many data breach professionals recommend the following practices in a potential data breach:

- Engage legal counsel as soon as possible.
- Ensure it is clear that you are engaging legal counsel in anticipation of litigation and not as part of the ordinary course of business.
- Direct legal counsel to hire forensic investigators and other third parties involved in the investigation.
- Make sure to include wording in third-party contracts that makes it clear their work is conducted on behalf of counsel for the purposes of rendering a legal opinion.
- Include legal counsel on all communications and label materials as privileged to avoid uncertainty.

These actions can help to preserve attorney-client privilege, which can protect your organization in the event that a data breach results in litigation.

6.8 Conclusion

Payment card breaches have long been epidemic. The effects ripple throughout our communities: Merchants and payment processors are hit with fines; banks suffer enormous losses and pass these on to consumers in the form of price hikes or additional fees. Consumers also have to deal with rampant fraud and the annoyances of fraud monitoring.

In a potential payment card breach, you may interact with any of the following players (among others):

- *The Bank* - If you are a merchant experiencing a potential data breach, your acquiring bank may be the one to notify you of the suspected compromise. As friendly as you may be with your banker, if the bank is hit with fines, penalties, or other losses, it may decide to go after you.
- *Card Brands* - The card brands support payment processing but can also levy fines against acquiring banks or require merchants to pay for expensive forensics investigations conducted by a PFI.
- *Forensic Investigators* - A PFI is paid by the suspected compromised entity yet obligated to report findings to the card brands and acquiring banks.
- *Attorneys* - If you have engaged your attorney for the purposes of providing legal advice in anticipation of potential litigation, then his or her work may be protected under

attorney-client privilege. Your attorney may be the one advisor whom you actually *can* trust—and if done correctly, the attorney can sometimes extend the attorney-client privilege to other parties who assist you in the investigation.

Organizations that suffer a payment card breach should be aware of the complex relationship between each of these participants and understand the various incentives that influence their actions. In this chapter, we discussed the impacts of payment card breaches and showed how merchants are disproportionately affected. We then dug into PCI compliance in depth, revealing how the PCI DSS is used as a tool to sort out liability following a breach.

Finally, we discussed tips for organizations involved in a breach. Today, it is considered best practice to hire outside counsel very early on, in order to preserve privilege. In addition, if you are required to hire a PFI, consider getting a second opinion from a forensics investigator who is truly independent.

In the next chapter, we will step through a landmark payment card breach case, discuss how retail breaches evolved, and identify key turning points that changed cybersecurity and breach response practices globally.

This page intentionally left blank

Chapter 7

Retailgeddon

Far out in western Pennsylvania, cars sat parked in the lot of a white, nondescript building. Four flags flew proudly above the main entrance. The exterior of Fazio Mechanical Services was plain—but despite its humble facade, the tiny HVAC company boasted an impressive clientele: Sam's Club, Super Valu, Trader Joe's, and Target, among many others.

Inside the white walls of the building, an email quietly landed in someone's inbox. The reader clicked, triggering installation of malicious software and opening the door for cybercriminals. Little did anyone know that this one tiny act would trigger an avalanche that would lead to the theft of 40 million credit card numbers and eventually bury an international retailer in a multiyear data breach crisis that included lawsuits, congressional investigations, and nearly $300 million in cumulative expenses.[1] With a click, the infamous Target breach began.

Target's HVAC vendor, Fazio Mechanical, didn't stand a chance. The small, family-owned company had no real-time malware protection (instead, it had a free version of Malwarebytes Anti-Malware Scanner, which was not licensed for corporate use and ran only on demand).[2] Criminals lurked in Fazio Mechanical's systems and eventually captured a password to a Target web portal.[3]

On November 12, 2013, the criminals used Fazio Mechanical's credentials to access Target's network.[4] From there, criminals wormed their way deep inside Target's network, eventually installing malware on the retailer's point-of-sale (POS) systems that would capture and steal credit card numbers as customers swiped them. The criminals initially installed the malware on a small group of POS terminals between November 15 and November 28, testing and honing their tools.[5]

---

1. Target, *2016 Annual Report*, accessed January 12, 2018, https://corporate.target.com/_media/TargetCorp/annualreports/2016/pdfs/Target-2016-Annual-Report.pdf.

2. Brian Krebs, "Email Attack on Vendor Set Up Breach at Target," *Krebs on Security* (blog), February 12, 2014, https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target.

3. Fazio Mechanical Services, "Statement on Target Data Breach," accessed January 12, 2018, https://web.archive.org/web/20140327052645/http://faziomechanical.com/Target-Breach-Statement.pdf.

4. *Hearing on "Protecting Personal Consumer Information from Cyber Attacks and Data Breaches" Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong. (March 26, 2014), https://corporate.target.com/_media/TargetCorp/global/PDF/Target-SJC-032614.pdf (written testimony of John Mulligan, Chief Financial Officer, Target).

5. Brian Krebs, "Target Hackers Broke in Via HVAC Company," *Krebs on Security* (blog), February 5, 2014, https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company.

By the end of November, the criminals had pushed their malware out to the majority of Target's POS systems, ultimately compromising POS devices at more than 1,800 stores across the United States.[6] The malware was programmed to copy customer credit card numbers to an internal file share, where it was collected and transferred to an outside server. Throughout December 2013, the criminals transferred millions of stolen credit card numbers out of Target's network and then uploaded them to a carding forum, where they were sold.

The timing was impeccable. "At the critical moment—when the Christmas gifts had been scanned and bagged and the cashier asked for a swipe—the malware would step in, capture the shopper's credit card number, and store it on a Target server commandeered by the hackers."[7] Because the hack coincided with Target's peak shopping period, criminals managed to collect a whopping 40 million credit card numbers in two weeks.

Target knew nothing of the theft until mid-December, when it was alerted by the U.S. Department of Justice and the Secret Service. By then, the damage was done. By December 11, Easy Solutions, a fraud tracking company, had noted a "10 to twentyfold increase in the number of high-value stolen cards on black market websites, from nearly every bank and credit union."[8]

Card issuers and banks were well aware of the breach and had identified Target as a common point-of-purchase—a place where all the affected cards had been used and therefore a likely source of compromise. They kept quiet, waiting for law enforcement and card brands to investigate—until someone tipped off investigative journalist Brian Krebs.

On December 18, 2013, Krebs outed the retailer, after sources from two large banks leaked information to him about the breach. "Nationwide retail giant Target is investigating a data breach potentially involving millions of customer credit and debit card records," reported Krebs on his popular blog, *Krebs on Security*. "According to sources at two different top 10 credit card issuers, the breach extends to nearly all Target locations nationwide, and involves the theft of data stored on the magnetic stripe of cards used at the stores."[9]

A media uproar ensued. Taken by surprise, Target's management team fumbled the response. The company remained silent during the first day. The next day, it issued a terse statement confirming the breach and disclosed that up to 40 million cards may have been stolen, affecting customers who shopped at Target between November 27 and December 15 (later extended to December 18).[10]

As banks and customers struggled to rein in card fraud and issue replacements in the busy days before Christmas, news of the breach quickly ignited a massive public relations nightmare. "Target's once-envied reputation may never fully recover from the massive data

6. Krebs, "Target Hackers Broke In."

7. M. Riley, B. Elgin, D. Lawrence, and C. Matlock, "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," *Bloomberg*, March 17, 2014, https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data.

8. Elizabeth A. Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow," *New York Times*, January 10, 2014, https://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

9. Brian Krebs, "Sources: Target Investigating Data Breach," *Krebs on Security* (blog), December 18, 2013, https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach.

10. Melanie Eversley and Kim Hjelmgaard, "Target Confirms Massive Credit-Card Data Breach," *USA Today*, December 18, 2013, https://www.usatoday.com/story/news/nation/2013/12/18/secret-service-target-data-breach/4119337.

breach," reported Kim Bhasin of the *Huffington Post*. "Public perception of Target fell off a cliff after the breach and remains at historic lows."[11]

Bad news continued to leak out over the coming weeks, like a car wreck in slow motion. Fourth-quarter profits were down a whopping 46%. In January, Target announced that the personal information of up to 70 million people might have been exposed (including name, address, phone number, and email address), bringing the total number of potentially affected people to 110 million. Investigative reporters from *Bloomberg* revealed shocking details of the hack, which showed that Target had repeatedly missed internal alerts from its expensive intrusion detection system (IDS). Former employees shared unflattering details of Target's internal IT management, scarring the company's reputation.

As the retailer continued to struggle with the breach response over the coming months, even loyal customers lost patience. "Wow do I regret shopping at Target," vented one frustrated customer on Facebook. "Because they can't secure info I had to have a card canceled and it dropped my credit score 12 points," Another customer added, "I was understanding in December . . . but now I am just pissed off."[12]

The chief information officer (CIO) stepped down. The chief executive officer (CEO) stepped down. Target hit bottom.

The Target breach was the first of what would become a series of major, public POS breaches affecting retailers during 2013-14, which we will refer to as Retailgeddon.

Retailgeddon was a turning point. It happened because of advancements in cybercriminal technology combined with a dramatic leap forward in investigative reporting tactics. Payment card breaches were already happening; but the epidemic got worse, and at the same time, the media suddenly had a way to detect and report on these breaches. As a result, retailers across the country suddenly found themselves in the headlines for being hacked.

In this chapter, we will outline the changes that caused the Target breach to blow up, and analyze the retailer's response. Then, we will discuss the impacts on Retailgeddon on the wider communities and show how the resulting rollout of EMV ("the chip") diverted funds from retailers that might otherwise have been invested in more modern and secure payment technologies.

7.1 Accident Analysis

Imagine that you are driving down a straight road in the desert, pushing 80 mph in a little red sports car. Suddenly, the road before you changes. You find yourself careening around the corner of a snowy mountain pass, with a steep drop off and no guard rail—but still in your little red sports car. Eek!

This is essentially what happened to Target. Between 2008-13, enormous new cyber risks emerged for retailers, but many executives didn't see them coming. Target's leadership continued to drive the company using their familiar techniques, not realizing that the road had become very dangerous and their car was not well equipped to handle curves.

11. Kim Bhasin, "Target's Reputation May Never Be the Same Again," *Huff Post UK*, January 27, 2014, http://www.huffingtonpost.co.uk/entry/target-reputation_n_4673894.

12. Bhasin, "Target's Reputation."

Target was hardly the only retailer in this position. The company's spotty cybersecurity posture was very much the norm for the retail industry, as evidenced by the pileup of retail breaches that occurred in the same time frame as the Target breach. The threat landscape had changed quickly, and retailers did not adapt.

Why did Target, in particular, become the "poster child of mega retail breaches"?[13]

Much like a car accident, the Target data breach crisis was the result of multiple factors. Timing was undeniably a huge factor: The company was in the wrong place at the wrong time. A year earlier, and Krebs might not have broken the story before the company was ready. A year later, and no one would have been shocked—the public had become desensitized to payment card breaches. Any other month, and the pressure of the holiday shopping season wouldn't have complicated the breach response.

At that particular moment in cybercrime history:

- Commercial exploit kits had recently become widely available, enabling criminals to compromise and control large numbers of endpoint systems with relatively little effort.
- Attackers had developed sophisticated tools and techniques for pivoting through the supply chain and moving laterally within the networks of hacked organizations.
- Carder forums and the darknet markets had developed into full-fledged e-commerce systems, capable of moving very large quantities of stolen card numbers.
- Retailers still had huge gaps in their cybersecurity, incident response, and breach preparedness programs.
- Financial institutions had reached a breaking point with respect to payment card breaches and were searching for ways reduce their losses.
- Investigative reporter Brian Krebs had developed strong ties with financial institutions and gained access to darknet markets, enabling him to uncover data breach scandals far more quickly than ever before.

All of these factors combined to create a very slippery road—and drivers weren't paying attention.

7.1.1 Pileup

Immediately on the heels of the Target breach, Neiman Marcus and Michaels announced their own credit card data breaches.[14] Throughout 2014, wave after wave of POS breaches hit the news. Sally Beauty, a beauty products retail chain, was outed in March 2014, after 260,000 credit cards stolen from their stores reportedly went up for sale on the dark web. An analysis by Krebs indicated that the company was breached due to credential theft from an employee remote access portal, and malware was installed on approximately 6,000 POS systems.[15]

---

13. Jennifer LeClaire, "Cost of Target Data Breach: $148 Million Plus Loss of Trust," *Newsfactor*, August 20, 2014, https://www.newsfactor.com/story.xhtml?story_id=00100016BSDE.

14. Bill Hardekopf, "The Big Data Breaches of 2014," *Forbes*, January 13, 2015, https://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/.

15. Brian Krebs, "Deconstructing the 2014 Sally Beauty Breach," *Krebs on Security* (blog), May 7, 2015, https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach.

In May, casino operating company Affinity Gambling announced a data breach of POS systems at casino resorts. By June, PF Chang's China Bistro announced a data breach affecting 33 restaurants in 16 states, which dated back to September 2013.[16]

On July 31, 2014, the Department of Homeland Security (DHS), Secret Service, the National Cybersecurity and Communications Integration Center (NCCIC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) issued a joint alert warning of a new, potent POS malware strain known as Backoff.[17] Within weeks of the federal alert about Backoff, UPS announced that it had been hit—and it discovered the breach only because of the government's alert.[18]

The same month, supermarket chain Supervalu announced a "potential data breach that might have affected more than 1,000 stores" in which "hackers [installed] malicious software onto the company's point-of-sale network." Dairy Queen, too, confirmed that the company was investigating a breach, after being alerted by the Secret Service. The organization's franchise system—where stores were operated independently—made it tricker to coordinate the DQ investigation and incident response.[19]

Despite the unending reports of retail breaches, there were indications that the public announcements represented just the tip of the iceberg. In August 2014, the *New York Times* reported that "seven companies that sell and manage in-store cash register systems have confirmed to government officials that they each had multiple clients affected, the government said Friday. Some of those clients, like UPS and Supervalu, have stepped forward, but most have not."[20]

The onslaught continued in early September 2014, when Krebs broke the story that Home Depot had been hacked. Fifty-six million debit and credit card numbers were compromised. According to Krebs, Home Depot's POS systems had been infected with "the same malware as Target"—a new variant of BlackPOS. By late September, sandwich chain Jimmy John's had likewise confirmed a credit card breach at 216 stores (although the story was largely dwarfed by Home Depot's far more massive breach).[21]

Kmart announced a cardholder data breach in October 2014, disclosing that "the payment data systems at Kmart stores were purposely infected with a new form of malware (similar to a computer virus). This resulted in debit and credit card numbers being compromised."[22] As

16. Brian Krebs, "P.F. Chang's Breach Likely Began in Sept. 2013," *Krebs on Security* (blog), June 18, 2014, https://krebsonsecurity.com/2014/06/p-f-changs-breach-likely-began-in-sept-2013; John H. Oldshue, "P.F. Chang's Data Breach Spans 33 Restaurants in 16 States," LowCards.com, August 4, 2014, https://www.lowcards.com/p-f-changs-data-breach-spans-33-restaurants-16-states-25949.

17. U.S. Department of Homeland Security, *Backoff: New Point of Sale Malware* (Washington, DC: US-CERT, July 31, 2014), 3, https://www.us-cert.gov/sites/default/files/publications/BackoffPointOfSaleMalware_0.pdf.

18. UPS Store, *Data Security Incident Information*, 2014, https://web.archive.org/web/20140830000548/http://www.theupsstore.com/security/Pages/default.aspx.

19. Brian Krebs, "DQ Breach? HQ Says No, But Would it Know?" *Krebs on Security* (blog), August 26, 2014, https://krebsonsecurity.com/2014/08/dq-breach-hq-says-no-but-would-it-know.

20. Nicole Perlroth, "U.S. Finds 'Backoff' Hacker Tool Is Widespread," *New York Times*, August 22, 2014, https://bits.blogs.nytimes.com/2014/08/22/secret-service-warns-1000-businesses-on-hack-that-affected-target/.

21. Brian Krebs, "Jimmy John's Confirms Breach at 216 Stores," *Krebs on Security* (blog), September 24, 2014, https://krebsonsecurity.com/2014/09/jimmy-johns-confirms-breach-at-216-stores/.

22. Alasdair James, "Kmart Investigating Payment System Breach," Kmart, October 10, 2014, http://www.kmart.com/en_us/dap/statement1010140.html.

the year came to an end, Staples rounded off the list by announcing that a breach "may have affected 1.16 million customers' cards."[23]

Data Breach Fatigue

It's no wonder that the term "breach fatigue" entered mainstream use in 2014. By April, according to the Ponemon Institute, 30% of people surveyed had received two breach notification letters in the previous two years, 15% received three letters, and 10% received more than five letters.[24] By May, 110 million Americans—nearly a third of the nation's population—had had their personal data exposed in a breach during the prior year. And the breach announcements just kept coming![25]

"Breach fatigue" is a term to describe the apathy experienced by consumers who have been desensitized to news of data breaches. "I feel nothing," wrote one consumer, Elise Hu, after the Home Depot breach was announced. "How many megahacks have we consumers faced in recent memory? . . . But because banks are responsible for making us whole if our credit cards are misused, and we are simply issued new cards (an annoying hassle, but not life-altering), I join you in reacting to news of these hacks with a shrug."[26]

Neal O'Farrell, the founder of the Identity Theft Council, expressed concern about the impact of breach fatigue on security efforts. "The more breaches consumers go through without experiencing any direct and tangible financial consequences, the less likely they are to care or worry about the next breach, or the next one, or the one after that," he writes. "[Consumers are] less likely to respond, to beef up their vigilance, and equally less likely to alter their behavior or change their habits. Consumers are also more likely to ignore any alarms, alerts or notifications, and less likely to demand or accept offers of free credit monitoring or identity protection."[27]

The consequences of breach fatigue go far beyond the individual consumer. As O'Farrell points out, apathetic consumers are less likely to hold breached organizations accountable, leading to less oversight and fewer proactive security measures. "[T]hey'll be too tired and cynical to be outraged anymore. . . . And without that rage, nothing has even a remote chance of changing."

(*Continues*)

23. Tom Huddleston Jr., "Staples: Breach May Have Affected 1.16 Million Customers' Cards," *Fortune*, December 19, 2014, http://fortune.com/2014/12/19/staples-cards-afiected-breach.

24. Experian, "Top Findings from Ponemon Institute Study Show Data Breach 'Fatigue' Possibly Increasing Consumers' Fraud Risk but Many Want Protection Provided by Breached Organizations," *Experian News*, May 14, 2014, https://www.experianplc.com/media/news/2014/top-findings-from-ponemon-institute-study-show-data-breach-fatigue-possibly-increasing.

25. Jose Pagliery, "Half of American Adults Hacked this Year," *CNN Tech*, May 28, 2014, http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/index.html.

26. Elise Hu, "I Feel Nothing: The Home Depot Hack and Data Breach Fatigue," *All Things Considered*, NPR, September 3, 2014, https://www.npr.org/sections/alltechconsidered/2014/09/03/345539074/i-feel-nothing-the-home-depot-hack-and-data-breach-fatigue.

27. Neal O'Farrell, "Data-Breach Fatigue: Consumers Pay the Highest Price," *Huff Post*, December 16, 2014, https://www.huffingtonpost.com/creditsesamecom/data-breach-fatigue-consu_b_5990040.html.

(*Continued*)

Even judges seemed to succumb to "breach fatigue." After years of litigation, in 2017 a federal district court judge dismissed a lawsuit filed by financial institutions against Schnuck Markets, Inc. "The breach at Defendant's stores took place during what seemed to be the boom of data breach activity, at a time when many retailers were caught either unaware or unluckily in the cross-hairs of cybercrime," wrote judge Michael J. Reagan in his ruling. "Unfortunately, losses were sustained, losses that in retrospect should have or could have been prevented, but not every loss can be compensated via legal action."[28]

In short: a judicial "meh."

7.1.2 Small Businesses Under Attack

At the time that Fazio Mechanical was hacked, small businesses across the United States were in the midst of an epidemic. Their bank accounts were being drained by cybercriminals who sent phishing emails to employees, stole their online banking credentials, and then transferred tens of thousands of dollars to money mules through wire transfers or fake payroll entries. Criminals found that small businesses were easy prey—few had the resources or knowledge to invest in security, and most small business owners thought that no one would want to break into their companies.

"[W]hile small businesses may assume that they have nothing a targeted attacker would want to steal, they forget that they retain customer information, create intellectual property, and keep money in the bank," observed Symantec's research team in their 2012 *Internet Security Threat* report. "[M]oney stolen from a small business is as easy to spend as money stolen from a large business."[29]

Direct theft of funds from online business bank accounts was a huge problem. "Each week, I reach out to or am contacted by organizations that are losing hundreds of thousands of dollars via cyber heists," wrote Krebs in late 2012.

> In nearly every case, the sequence of events is virtually the same: The organization's controller opens a malware-laced email attachment, and infects his or her PC with a Trojan that lets the attackers control the system from afar. The attackers then log in to the victim's bank accounts, check the account balances—and assuming there are funds to be plundered—add dozens of money mules to the victim organization's payroll. The money mules are then instructed to visit their banks and withdraw the fraudulent transfers in cash, and wire the money in smaller chunks via a combination of nearby MoneyGram and Western Union locations.[30]

Table 7-1 shows just a sample of the small businesses that fell victim to these cyberheists, which Krebs wrote about between 2009–13. As you can see, attackers weren't just targeting

28. Community Bank of Trenton v. Schnuck Markets, Inc., No. 15-cv-01125-MJR (S.D. Ill. 2017), https://cases.justia.com/federal/district-courts/illinois/ilsdce/3:2015cv01125/71778/68/0.pdf.

29. Symantec, "Internet Security Threat Report 2014," *ISTR 19* (April 2014), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf (accessed January 14, 2018).

30. Brian Krebs, "MoneyGram Fined $100 Million for Wire Fraud," *Krebs on Security* (blog), November 19, 2012, https://krebsonsecurity.com/2012/11/moneygram-fined-100-million-for-wire-fraud.

financial institutions or large organizations. Many of the businesses compromised were in manufacturing, services and other industries that might not immediately seem high risk for cybercrime. Fazio Mechanical, a refrigeration and HVAC company, fit right in.

Table 7-1 Example: Small Businesses That Fell Victim to Cyberheists

Amount Stolen	Business Name	Type	Location
$63,000[31]	Green Ford Sales, Inc.	car dealership	Abilene, KS
$75,000[32]	Slack Auto Parts	automotive	Gainesville, GA
$100,000[33]	JM Test Systems	electronics	Baton Rouge, LA
$180,000[34]	Primary Systems Inc.	building security and maintenance	St. Louis, MO
$200,000+[35]	Downeast Energy & Building Supply	heating and hardware	Brunswick, ME
$223,500[36]	Oregon Hay Products Inc.	hay compressing	Boardman, OR
$560,000[37]	Experi-Metal Inc.	custom metals	Sterling Heights, MI
$588,000[38]	Patco Construction	construction	Sanford, ME
$800,000[39]	J.T. Alexander & Son Inc.	fuel distribution	Mooresville, NC
$801,495[40]	Hillary Machinery, Inc.	machine tool dealer	Plano, TX
$3.5 million[41]	TRC Operating Co.	oil production	Taft, CA

31. Brian Krebs, "Sold a Lemon in Internet Banking," *Krebs on Security* (blog), February 23, 2011, https://krebsonsecurity.com/2011/02/sold-a-lemon-in-internet-banking.

32. Brian Krebs, "Businesses Reluctant to Report Online Banking Fraud," *Washington Post*, August 25, 2009, http://voices.washingtonpost.com/securityfix/2009/08/businesses_reluctant_to_report.html.

33. Krebs, "Businesses Reluctant."

34. Brian Krebs, "Cyberheists 'a Helluva Wake-up Call' to Small Biz," *Krebs on Security* (blog), November 6, 2012, http://krebsonsecurity.com/2012/11/cyberheists-a-helluva-wake-up-call-to-small-biz.

35. Brian Krebs, "Data Breach Highlights Role of 'Money Mules,'" *Washington Post*, September 16, 2009, http://voices.washingtonpost.com/securityfix/2009/09/money_mules_carry_loot_for_org.html.

36. Brian Krebs, "Hay Maker Seeks Cyberheist Bale Out," *Krebs on Security* (blog), April 11, 2013, https://krebsonsecurity.com/2013/04/hay-maker-seeks-cyberheist-bale-out.

37. Brian Krebs, "Court Favors Small Business in eBanking Fraud Case," *Krebs on Security* (blog), June 17, 2011, https://krebsonsecurity.com/2011/06/court-favors-small-business-in-ebanking-fraud-case (accessed January 14, 2018).

38. Brian Krebs, "Maine Firm Sues Bank After $588,000 Cyber Heist," *Washington Post*, September 23, 2009, http://voices.washingtonpost.com/securityfix/2009/09/construction_firm_sues_bank_af.html.

39. Brian Krebs, "NC Fuel Distributor Hit by $800,000 Cyberheist," *Krebs on Security* (blog), May 23, 2013, https://krebsonsecurity.com/2013/05/nc-fuel-distributor-hit-by-800000-cyberheist.

40. Brian Krebs, "Texas Bank Sues Customer Hit by $800,000 Cyber Heist," *Krebs on Security* (blog), January 26, 2010, https://krebsonsecurity.com/2010/01/texas-bank-sues-customer-hit-by-800000-cyber-heist.

41. Brian Krebs, "Cyberheist Victim Trades Smokes for Cash," *Krebs on Security* (blog), August 14, 2015, https://krebsonsecurity.com/category/smallbizvictims.

Small businesses were also increasingly used "as pawns in more sophisticated attacks."[42] For example, in 2012 "watering hole" attacks became prevalent. Cybercriminals would hijack a vulnerable website and use it to host malware that would infect visitors. By compromising the "watering hole," criminals could spread malware through a group of users that visited the site, even if they were wise enough to avoid clicking on links in phishing emails. Small businesses often had vulnerable websites since they typically had very limited resources to devote to IT.

"[T]he lack of adequate security practices by small businesses threatens all of us," declared Symantec in the 2013 *Internet Security Threat Report*.[43]

Was Target Targeted?

Many people assume that the Target breach was the result of an intentional attack to break into the retailer and steal credit card numbers. After all, stealing 40 million card numbers seems like a pretty huge accomplishment for a criminal! Clearly it must have been the result of a carefully planned and executed attack—like the team in *Ocean's 11*, but in cyberspace!

In reality, no evidence has been published that indicates that attackers broke into Fazio Mechanical with the intent of accessing Target's systems. It is possible, of course, but based on common attack patterns of the time, it's more likely that the attackers sent out a mass phishing email that happened to snare a user at Fazio Mechanical. Once inside, the criminals installed software that automatically stole passwords. Upon finding a password for Target in their loot, they naturally would have set their sights on a bigger prize.

"Many readers have questioned why the attackers would have picked on an HVAC firm as a conduit for hacking Target," said Krebs, in a follow-up to his initial exposé. "The answer is that they probably didn't, at least at first. Many of these email malware attacks start with shotgun attacks that blast out email far and wide; only after the attackers have had time to comb through the victim list for interesting targets do they begin to separate the wheat from the chaff."[44]

7.1.3 Attacker Tools and Techniques

The Target breach illustrates key developments in attacker tools and techniques that had emerged over the years and converged. These included maturation of:

- **Commercial exploit kits** used to compromise endpoints and install arbitrary malware
- **Credential theft and commercial credential-stealing tools** such as ZeuS and Citadel
- **RAM-scraping malware designed to steal payment card numbers** from the memory of POS systems
- **Carder shops** with e-commerce features, as previously discussed in §5.3.6, "Modern Dark Data Brokers."

42. Symantec, "Internet Security Threat Report 2014," *ISTR 19* (April 2014), http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

43. Symantec, "Internet Security Threat Report 2014."

44. Krebs, "Email Attack on Vendor."

In this section, we will dissect the attack on Fazio Mechanical and subsequent compromise of Target. As we will see, each of these key technical developments contributed to the sequence of events, which enabled a click on a phishing email to lead to the compromise of 40 million payment card numbers and 110 million peoples' personal information.

7.1.3.1 Commercial Exploit Kits

The epidemic of small business breaches was possible only because of the development of exploit kits. An *exploit kit* is software designed to help criminals efficiently and effectively distribute malware and manage botnets of infected computers. Modern exploit kits are user friendly, with point-and-click interfaces and dashboards that display statistics. MPack, an early commercial exploit kit, was developed by Russian programmers in 2006 and sold on the underground for $700 to $1000. The developers offered one year of support, as well as extra modules with new exploits that ranged in price from $50 to $150.[45]

MPack consisted of a collection of PHP scripts with a database backend. Customers (i.e., cybercriminals) installed the MPack exploit kit onto a server and then found ways to drive traffic to their malicious site. Often, this was accomplished by sending spam to a large number of email addresses. Another method was to hack legitimate websites and inject code that would load malware from the criminal's server. When users visited the legitimate site, their web browsers would also run the malicious code.[46] By May 2007, researchers at PandaLabs reported that they had detected more than 10,000 compromised websites that inclued links to an MPack server.[47]

In 2010, the Blackhole exploit kit emerged, introducing groundbreaking new features. Most important, it offered a software-as-a-service (SaaS) rental model. Instead of setting up their own servers, customers could license Blackhole in the cloud. This made it far more accessible to less technical users. The exploit kit also featured a handy management console for users, which provided a statistical breakdown of infections by victim operating system, browser software, country, exploit type, and more. Customers could rent the kit for $50/day, $500/month, or $1,500/year.[48]

"Blackhole is now the world's most popular and notorious malware exploit kit," reported Sophos in its 2013 *Annual Threat Report*. "It combines remarkable technical dexterity with a business model that could have come straight from a Harvard Business School MBA case study."[49] At its peak in 2012, the Blackhole exploit kit was responsible for a whopping 27% of all exploit sites and infected redirects.[50]

---

45. Robert Lemos, "MPack Developer on Automated Infection Kit," *Register*, July 23, 2007, https://www.theregister.co.uk/2007/07/23/mpack_developer_interview; Robert Lemos, "Newsmaker: DCT, MPack Developer," *Security Focus*, July 20, 2007, http://www.securityfocus.com/news/11476/2.

46. Hon Lau, "MPack, Packed Full of Badness," *Symantec Connect*, May 26, 2007, https://www.symantec.com/connect/blogs/mpack-packed-full-badness.

47. Websense Security Labs, "Large Scale European Web Attack," *Websense Alerts*, June 18, 2007, https://web.archive.org/web/20080618075317/http://securitylabs.websense.com/content/Alerts/1398.aspx.

48. Fraser Howard, "Exploring the Blackhole Exploit Kit," *Naked Security by Sophos*, March 2012, https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-3/.

49. Sophos, *Security Threat Report 2013*, https://www.sophos.com/en-us/medialibrary/pdfs/other/sophossecuritythreatreport2013.pdf.

50. Sophos, *Security Threat Report 2013*, 7.

Waves of spam campaigns flooded inboxes around the world. In response to the sharp rise in spam volumes during 2012, Trend Micro conducted an investigation of more than 245 spam campaigns to determine the cause. It found that the vast majority of the spam emails linked to websites infected with the Blackhole exploit kit. While the authors pointed out that the techniques used were nothing new, "the Blackhole Exploit Kit spam campaign poses a considerable challenge to conventional techniques because of the skill with which the attacks are conducted as well as the mechanics used that overwhelm conventional methods of detection and blocking by sheer number."[51]

Seeing the massive success of Blackhole, in late 2012 the kit's authors (led by a Russian developer named "Paunch") announced a new exploit framework. The Cool Exploit Kit rented for $10,000/month. Why so pricey? The authors announced that they had "[set] aside a $100K budget to purchase browser and browser plug-in vulnerabilities, which are going to be used exclusively by us, without being released to public." In other words, Cool Exploit Kit was packed full of zero-day vulnerabilities, which were virtually guaranteed to be unpatched.[52]

The Cool Exploit Kit quickly became popular. At the same time, the Blackhole exploit kit rapidly declined.[53] By the fall of 2013, new kits such as Neutrino, Sweet Orange, and Redkit had taken over, with Blackhole accounting for just a tiny percentage of attacks. Its fate was sealed when Paunch, the Russian developer behind the Blackhole exploit kit, was arrested in late 2013 (and ultimately sentenced by a Russian court to seven years of imprisonment in a Russian penal colony).[54]

The attacks on Fazio Mechanical (and subsequently Target) represent that time period perfectly. According to news reports, the breach at Fazio Mechanical began with a "malware-laden phishing email" sent "at least two months before thieves started stealing card data from thousands of Target cash registers."[55] This means the initial compromise at Fazio started in September 2013, or earlier. A Fazio Mechanical employee could easily have been hit with one of the many spam campaigns that flooded the globe during 2012, clicked on a link, and been infected by a website infected with the Blackhole exploit kit or a similar tool. From there, criminals would have had free rein to install the payload of their choice.

7.1.3.2 Credential Theft

How did criminals leap from Fazio Mechanical's network all the way to Target's POS systems? This was the big topic of discussion in the months following the Target breach. In late January 2014, a Target spokesperson confirmed that the breach had been traced back to stolen vendor

51. Jon Oliver et al., "Blackhole Exploit Kit: A Spam Campaign, Not a Series of Individual Spam Runs" (research paper, Trend Micro Inc., July 2012), 5, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_blackhole-exploit-kit.pdf.

52. Brian Krebs, "Crimeware Author Funds Exploit Buying Spree," *Krebs on Security* (blog), January 7, 2013, https://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree.

53. MSS Global Threat Response, "Six Months after Blackhole: Passing the Exploit Kit Torch," *Symantec Connect*, April 7, 2014, https://www.symantec.com/connect/blogs/six-months-after-blackhole-passing-exploit-kit-torch.

54. Brian Krebs, "'Blackhole' Exploit Kit Author Gets 7 Years," *Krebs on Security* (blog), April 14, 2016, https://krebsonsecurity.com/2016/04/blackhole-exploit-kit-author-gets-8-years.

55. Krebs, "Email Attack on Vendor."

credentials. The following week, Krebs revealed that the credentials were stolen specifically from Fazio Mechanical Services.[56]

Many security professionals speculated that Fazio Mechanical had a dedicated connection to Target's internal network for the purposes of maintaining refrigeration or HVAC systems that they deployed. However, the company's owner, Ross E. Fazio, put such speculation to rest in a February 2014 press release. "Fazio Mechanical does not perform remote monitoring or control of heating, cooling or refrigeration systems for Target," he wrote. "Our data connection with Target was exclusively for electronic billing, contract submission and project management."[57]

Former Target employees squealed to the media. One unnamed source told Krebs that "nearly all Target contractors access an external billing system called Ariba, as well as a Target project management and contract submissions portal called Partners Online."[58]

The Ariba system, which facilitates online invoicing and payment between suppliers and their customers, seemed to be a likely target for criminals. Krebs's article drilled into it. He interviewed a former member of Target's security team, who explained that "internal applications at Target used Active Directory (AD) credentials and I'm sure the Ariba system was no exception. . . . This would mean the server had access to the rest of the corporate network in some form or another." In other words, criminals could have logged into the Ariba system using stolen vendor credentials, exploited a vulnerability in the underlying server, and then leveraged that access to leap into Target's internal network. It was a solid theory.

7.1.3.3 Password-Stealing Trojans

By late 2013, criminals had long since recognized that passwords were the keys to the kingdom. Banking credentials, of course, were highly prized by criminals, but other credentials were valuable as well. "Logins for everything from Amazon.com to Walmart.com often are resold—either in bulk, or separately by retailer name—on underground crime forums," reported Krebs in late 2012. "A miscreant who operates a . . . botnet of respectable size (a few thousand bots, e.g.) can expect to quickly accumulate huge volumes of 'logs,' records of user credentials and browsing history from victim PCs."[59]

Krebs reported that Fazio Mechanical had been infected with Citadel banking Trojan (this was based on statements from two sources, but he was not able to confirm this detail).[60] Citadel is a variant of the ZeuS banking Trojan, which was designed to steal users' web and banking credentials.

---

56. D. Yadron, P. Ziobro, and C. Levinson, "Target Hackers Used Stolen Vendor Credentials," *Wall Street Journal*, January 29, 2014, https://www.wsj.com/articles/holder-confirms-doj-is-investigating-target-data-breach-1391012641; Krebs, "Target Hackers Broke In."

57. Fazio Mechanical Services, "Statement."

58. Krebs, "Email Attack on Vendor."

59. Brian Krebs, "Exploring the Market for Stolen Passwords," *Krebs on Security* (blog), December 26, 2012, https://web.archive.org/web/20140628170043/http://krebsonsecurity.com/2012/12/exploring-the-market-for-stolen-passwords.

60. Krebs, "Email Attack on Vendor."

ZeuS—also known as Zbot—was "the mother of banking Trojans," according to Trend Micro. It first was observed in late 2006 and quickly grew to become the world's largest botnet.[61] By 2009, one security company estimated that 3.6 million computers in the United States were infected with ZeuS.[62]

ZeuS offered criminals an effective way to capture not only banking passwords, but also answers to secret questions, callback numbers, and any arbitrary information that the criminal wanted to steal. According to SecureWorks, "The transition to information-stealing malware was pragmatic because stolen credentials resulted in fewer successful fraudulent transactions as banks increased their fraud controls. New solutions were needed for criminals to bypass challenge questions and fraud detection based on IP addresses in specific geographic locations."[63]

To combat the epidemic of password theft, bank regulators urged financial institutions to use "out-of-band" authentication methods, such as mobile transaction authentication numbers (mTANs) sent to users' mobile phones.[64] By then, ZeuS authors had already released the "ZeuS-in-the-mobile" (ZitMo) function, which presents victims with a web form requesting their cell-phone number, and then sends the user a link to install the ZitMo malware (typically disguised as a security update or utility). Once infected, the user's phone would send a copy of any text messages with mTANs to the criminals, who combined these with the user's stolen banking credentials to remotely log into their account.[65]

According to a 2012 Trend Micro report, 66% of the malware distributed by the Blackhole exploit kit was a ZeuS variant, and another 29% was the Cridex malware, another bot often used to steal banking credentials. That meant that 95% of the malware distributed by the Blackhole exploit kit in early 2012 was designed to steal credentials.[66]

In a game-changing development, the full source code of ZeuS was leaked to the world in the spring of 2011. "Now What?" wrote Trend Micro. "With the ZeuS source code in our hands, we will know how [it] . . . was engineered, thus helping us improve our existing solutions."[67]

Cybercriminals, however, also leveraged the newly available code base. "With the release and leakage of the source code the ZeuS/Zbot could easily become even more widespread and an even bigger threat than it already is today," wrote security analyst Peter Kruse, who first announced the leak.[68]

Citadel, which was implicated in the Fazio/Target attack, was one such variant that became popular in early 2012. Like the Blackhole exploit kit, Citadel used a SaaS model. Customers

---

61. SecureWorks Counter Threat Unit, "Evolution of the GOLD EVERGREEN Threat Group," *SecureWorks*, May 15, 2017, https://www.secureworks.com/research/evolution-of-the-gold-evergreen-threat-group.

62. Dune Lawrence, "The Hunt for the Financial Industry's Most-Wanted Hacker," *Bloomberg*, June 18, 2015, https://www.bloomberg.com/news/features/2015-06-18/the-hunt-for-the-financial-industry-s-most-wanted-hacker.

63. SecureWorks, "Evolution."

64. Federal Financial Institutions Examination Council, *Supplement to Authentication in an Internet Banking Environment*, 2011, https://www.ffiec.gov/pdf/authentication_guidance.pdf.

65. Denis Maslennikov, "ZeuS-in-the-Mobile: Facts and Theories," SecureList.com, October 6, 2011, https://securelist.com/zeus-in-the-mobile-facts-and-theories/36424.

66. Oliver et al., "Blackhole Exploit Kit."

67. Roland Dela Paz, "ZeuS Source Code Leaked, Now What?" *Trend Micro* (blog), May 16, 2011, https://blog.trendmicro.com/trendlabs-security-intelligence/the-zeus-source-code-leaked-now-what/.

68. Peter Kruse, "Complete ZeuS Sourcecode has Been Leaked to the Masses," *CSIS*, May 9, 2011, https://web.archive.org/web/20110720042610/https://www.csis.dk/en/csis/blog/3229.

rented it for a $2,399 base fee plus $125/month. Users could purchase additional software modules such as antivirus evasion tools and more. But what really set Citadel apart was its customer support systems, which included a web-based trouble ticket service, chat rooms, and social forums where users could exchange ideas and even fund new developments.[69] In 2017, Mark Vartanyan, a Russian crimeware developer linked to Citadel, was sentenced to five years in prison by a U.S. district court. According to prosecutors, Citadel malware was responsible for more than $500 million in financial losses.

Once criminals installed Citadel on Fazio Mechanical's systems, they would have had the ability to capture the user's web application passwords, as well as stored passwords and any other data submitted in web forms. The criminals might have used these passwords themselves—or they might have packaged them up and sold them in an online credential shop.[70] Many people assume that the same criminals who hacked Fazio Mechanical also stole Target's credit card numbers—but there is no evidence that this was the case. More than two months elapsed between the time that Fazio Mechanical was first hacked and the time that Target's credit card numbers were stolen. This is more than enough time for an initial hacker to capture credentials and sell them on the dark web to another criminal group that deliberately targeted retailers.

7.1.3.4 POS Malware

Target rocked the industry in December 2013 with the theft of 40 million payment card numbers. This was made possible by the BlackPOS malware (also known as Kaptoxa), a memory-scraping tool that criminals installed on Target's POS systems. The BlackPOS malware is not, by anyone's estimation, a "sophisticated" tool. Rather, it is a straightforward utility that criminals installed on a retailer's POS system. It snatches payment card numbers from the memory (RAM) of the POS system. As the customer swipes a card, the POS device reads the card data into RAM. BlackPOS then copies the data to a file, where it is stored in plain text files and ultimately exported to an FTP server.[71]

Researchers at IntelCrawler, a cybersecurity intelligence company, identified a 17-year-old Russian teenager with the nickname "ree[4]" as the author of the BlackPOS malware. The researchers were quick to point out that ree[4] did not himself hack Target. Instead, he sold "more then 40 builds of BlackPOS to cybercriminals from Eastern Europe and other countries, including the owners of underground credit cards shops such as '.rescator', 'Track2.name', 'Privateservices.biz' and many others."[72] The going price for the malware was $2,000 or 50% of any sales from captured payment card data.

For criminals, memory-scraping POS malware was a smashing success. Many variants emerged and were peddled on the dark web. The Backoff malware, which reportedly was seen in multiple forensic investigations, was capable of scraping memory for card data and

69. Brian Krebs, "'Citadel' Trojan Touts Trouble-Ticket System," *Krebs on Security* (blog), January 23, 2012, https://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system.

70. Brian Krebs, "Exploring the Market for Stolen Passwords," *Krebs on Security* (blog), December 26, 2012, https://web.archive.org/web/20140628170043/http://krebsonsecurity.com/2012/12/exploring-the-market-for-stolen-passwords.

71. IntelCrawler, "The Teenager Is the Author of BlackPOS/Kaptoxa Malware (Target), Several Other Breaches May Be Revealed Soon," January 17, 2014, https://web.archive.org/web/20140809015838/http://intelcrawler.com/about/press08.

72. IntelCrawler, "Teenager."

logging keystrokes. It had advanced persistence capabilities and a built-in command-and-control channel used for issuing commands and updates. Reportedly, Backoff variants had "low to zero percent anti-virus detection rates," meaning that even organizations with mature, updated antivirus and patch management processes could unwittingly fall victim.

Essentially, malware authors had picked up where Albert Gonzalez left off (see Chapter 6). Toward the end of his cybercriminal career, Gonzalez had pushed to find new and better ways to tap into sources of "fresh" cardholder data, ultimately leading his team to steal and analyze POS systems. From there, Albert and his cohorts hacked into POS servers and scraped card data from network traffic as it was sent in real time. In the years since the TJX breach, retailers had increased their use of network encryption, and so sniffing cardholder data from network traffic was clearly a losing battle. Better to capture cardholder data from the source: the POS devices themselves.

Throughout 2013, retailers quietly uncovered data breaches, typically after being alerted by law enforcement and banks that had identified them as the common points of purchase. These were rarely reported in the media, but the problem became a major priority for card brands, retail security professionals, and investigators. Memory-scraping POS malware became so pervasive that in the spring of 2013, Visa released a "data security alert," as follows:[73]

> Visa has seen an increase in network intrusions involving grocery merchants. Once inside a merchant's network, hackers install memory-parsing malware on Windows-based cash register systems or back-of-house (BOH) servers to extract full magnetic-stripe data.

The Visa alert came shortly after Schnuck Markets announced a breach of 2.4 million card numbers.[74] Visa included "recommended mitigation strategies," which included network security measures, cash register/POS security, administrative access controls (including a reminder to "[u]se two-factor authentication when accessing payment processing networks"), and incident response tips.

Over the next year, it became painfully clear that retailers did not heed its advice.

7.2 An Ounce of Prevention

There were many ways that Target could have prevented its data breach from occurring. Afterwards, U.S. Senator John Rockefeller, chair of the Senate Committee on Commerce, Science, and Transportation, commissioned a report entitled *A "Kill Chain" Analysis of the 2013 Target Data Breach*. The authors of the report used a "kill chain framework" (first developed at Lockheed Martin) to analyze the Target breach and determine how the disaster

73. Visa Data Security Alert, "Preventing Memory-Parsing Malware Attacks on Grocery Merchants," Visa, April 11, 2013, https://web.archive.org/web/20130512105230/https://usa.visa.com/download/merchants/alert-prevent-grocer-malware-attacks-04112013.pdf.

74. Judy Greenwald, "Data Breach Case against Schnuck Markets Dismissed," *Business Insurance*, May 3, 2017, http://www.businessinsurance.com/article/20170503/NEWS06/912313250/Schnuck-Markets-data-breach-lawsuit.

could have been prevented. Lockheed's cyber "kill chain" describes the different phases of an attack:

- **Reconnaisance** - Gather information about the target, such as IP addresses, email addresses, etc.
- **Weaponization** - Prepare for exploitation, for example, by crafting a phishing email payload or malware-laden USB drive.
- **Delivery** - Deliver the "weaponized" content to the target (ie. send the email, drop the USB nearby, etc.
- **Exploitation** - Take advantage of a vulnerability, enabling malicious code to run on the target's system.
- **Installation** - Load malicious software onto the target system.
- **Command and Control** - Remotely control the target system through a channel that facilitates software updates, data exfiltration, and attacker commands.
- **Actions on Objectives** - Accomplish ultimate goals.

The Senate concluded that "Target missed a number of opportunities along the kill chain to stop the attackers and prevent the massive data breach."[75]

7.2.1 Two-Factor Authentication

If, as the evidence suggests, criminals stole a vendor password and used it to log in to a Target application, then in theory the attack could have been nipped in the bud through the use of strong two-factor authentication.[76] For example, had Target distributed a hardware token that generates one-time PINs for vendors to use when logging in, then the attackers would have been unable to log in remotely at their leisure.

According to a "source who managed Target vendors," Target rarely required vendors to use two-factor authentication. It was reserved for vendors in "the highest security group—those required to directly access confidential information."[77] Fazio Mechanical's access was intended to be very, very limited.

Two-factor authentication is required by the Payment Card Industry Data Security Standards (PCI DSS) for all remote access to systems within the scope of the PCI DSS requirements. However, Target did not expect that its vendor-facing application was within the scope of PCI DSS (see §7.2.3 on segmentation). "In fairness to Target, if they thought their network was properly segmented, they wouldn't have needed to have two-factor access for everyone," commented Gartner analyst Avivah Litan.[78]

---

75. S. Comm. on Commerce, Science, and Transportation, *A "Kill Chain" Analysis of the 2013 Target Data Breach* (Washington DC: U.S. Senate, March 26, 2014), https://www.commerce.senate.gov/public/_cache/files/24d3c229-4f2f-405d-b8db-a3a67f183883/23E30AA955B5C00FE57CFD709621592C.2014-0325-target-kill-chain-analysis.pdf.

76. S. Comm. on Commerce, Science, and Transportation, *"Kill Chain" Analysis*.

77. Krebs, "Email Attack on Vendor."

78. Krebs, "Email Attack on Vendor."

Tip: Deploy Two-Factor Authentication

Two-factor authentication is the solution for a myriad of cybersecurity problems. Many organizations are loathe to deploy it because of the cost and setup time involved. Even when it is deployed, many organizations use it only for "high-risk" accounts, forgetting that *any* account can be an access point into the network.

Fortunately, two-factor authentication (2FA) is becoming increasingly accessible as the technology matures. In 2013, when Target was hacked, strong 2FA was expensive and annoying for both IT staff and vendors. Today, tools make 2FA easy to deploy and simple to use. Mobile apps designed to implement 2FA have proliferated, raising the bar for attackers and giving vendors an easy, hardware-free solution.

No security measure is a silver bullet, but in many cases, 2FA is the ounce of prevention that obviates the need for a pound of cure.

7.2.2 Vulnerability Management

According to former employees, Target's security team expressed concerns about vulnerabilities in the retailer's POS infrastructure months before the massive breach began. "At least one analyst at the Minneapolis-based retailer wanted to do a more thorough security review of its payment system, a request that at least initially was brushed off." reported the *Wall Street Journal*.[79]

Law enforcement, the federal government, and card brands such as Visa had issued several memos during the spring and summer of 2013, warning retailers about new attacks on POS systems. However, Target's security team apparently did not have enough staff to handle the number of issues reported. According to the *Wall Street Journal*, which interviewed a former employee, Target's security team received "numerous threats each week and could prioritize only so many issues at its monthly steering committee meetings."[80]

Shortly after the breach, Target hired Verizon to conduct an internal penetration test. According to the report, which was later leaked and published by Brian Krebs, "the Verizon consultants found systems missing critical Microsoft patches, or running outdated [web server] software such as Apache, IBM WebSphere, and PHP. These services were hosted on web servers, databases, and other critical infrastructure. . . . In several of these instances where Verizon discovered these outdated services or unpatched systems, they were able to gain access to the affected systems without needing to know any authentication credentials."[81]

Importantly, the issue wasn't that Target security staff didn't know about the vulnerabilities. The Verizon consultants actually found that Target had a "comprehensive" vulnerability scanning program—they simply weren't *remediating* the vulnerabilties that were reported.

This common problem typically results from issues with staffing, internal audit, and security management functions. Lack of human resources is perhaps the most common challenge

79. D. Yadron, P. Ziobro, and D. Barrett, "Target Warned of Vulnerabilities Before Data Breach," *Wall Street Journal*, February 14, 2014, https://www.wsj.com/articles/target-warned-of-vulnerabilities-before-data-breach-1392402039.

80. Yadron, Ziobro, and Barrett, "Target Warned of Vulnerabilities."

81. Krebs, "Inside Target Corp."

underlying security problems. Like many institutions, Target had clearly invested in expensive, enterprise-quality security tools, but (based on public reports) probably did not have enough staff to monitor the output of those tools or resolve the issues that were reported. This imbalance is all too common.

Ideally, Target would have had enough staff and resources to fix all of the vulnerabilities that were reported on their scans in a timely manner. A healthy audit program should ensure that chronic vulnerability remediation issues are detected and escalated. For example, many organizations hire third-party auditors to conduct an annual vulnerability scan and report to upper management or have an internal audit function that periodically reviews scan output and escalates systemic concerns. Cybersecurity teams can also provide regular monthly or quarterly summary reports to management for review. If vulnerabilities are not quickly remediated, this should trigger the organization's leadership to review the team's processes and evaluate whether additional resources should be allocated.

Unfortunately, many organizations do not devote sufficient resources to properly manage their cybersecurity programs, or they make the mistake of spending money on tools rather than people. This can happen for many reasons. Quite often, executive management teams or financial officers do not understand the importance of cybersecurity and choose not to invest in it. In some cases, there is budget for tools but not labor to support them because executive teams are more comfortable making a one-time software purchase than creating a position. Other times, the organization as a whole may be budget-constrained, and as a cost center, cybersecurity is among the first programs to be cut.

For most retailers in 2013, cybersecurity was not a priority, and security budgets were tight throughout the industry. This led to systemic issues such as lack of timely vulnerability remediation.

Tip: Staffing and Auditing

Based on public reports, Target's internal network was riddled with vulnerabilities—and the security team knew about it. However, the team was apparently stretched too thin to address the issues.

Organizations can reduce the risk of a data breach by ensuring that the cybersecurity team has enough resources to detect *and remediate* vulnerabilities. All too often, organizations spend money purchasing expensive cybersecurity tools such as vulnerability scanners, but fail to budget for the human resources needed to review and remediate the output.

Any request for an equipment or a software purchase should be accompanied by an estimate of the labor needed to effectively use the tool. Budget needs to be allocated not just for the tool itself, but also the manpower to leverage it.

Effective auditing is also critical. Whether you choose to use an internal or external auditor (or both), the cybersecurity team's activities should be documented, reviewed, and reported to upper management. Upper management, in turn, needs to be committed to appropriately funding cybersecurity. In tough times, budgets can be thin, and cybersecurity resources may be constrained. At all times, funding for tools and human resources should be appropriately balanced. Decisions should be made on the basis of an informed risk assessment rather than ignorance.

7.2.3 Segmentation

Network segmentation refers to the process of dividing a network into separate sections, typically based on risk or function. Effective network segmentation blocks the flow of traffic between segments, thereby reducing the risk of data breaches and containing incidents to specific segments. In 2013, network segmentation was not required by PCI DSS, but it was explicitly recommended as a way of reducing risk. "[A]dequate network segmentation isolates systems that store, process, or transmit cardholder data from those that do not."[82]

In the Target breach, attackers were able to leap from a vendor-accessible server all the way into the bowels of Target's cardholder data environment. Evidence suggests that Target attempted to segment the network, but the attackers may have leveraged server management accounts and interfaces to hop from one segment to another.

Tip: Effective Network Segmentation

The Target breach was only possible because criminals were successfully able to move from a vendor-accessible system to the network segment which contained highly sensitive POS systems. Effective network segmentation could have contained the breach and prevented the criminals from ever accessing the POS systems.

Network segmentation isn't flashy, and it requires an organized, methodical approach. When done properly, organizations start off by classifying data and categorizing systems based on risk and function. The network is then divided into segments, and network engineers configure firewalls and virtual LANs (VLANs) to restrict the flow of traffic between segments. Any exceptions should be carefully tracked and monitored.

It's important to test the effectiveness of your network segmentation because networks continually evolve. A first step is to conduct routine port scans to verify that network segmentation processes are effective. Ideally, organizations should conduct periodic penetration tests, in which a skilled human poses as an attacker and attempts to bypass segmentation. This will uncover more subtle flaws in segmentation implementations.

Segmentation has parallels in other industries. In the beef industry, for example, producers use a variation of segmentation to reduce the risk of E. coli outbreaks. Heidi DeArment, a financial executive who formerly worked for two organic beef producers, described how producers divide ground meat into lots for testing. "If you kill an animal, and then grind its meat, and then test its blood, you are 100% sure that the animal does or does not have E. coli," she explained. "If you kill 10,000 of them, you may or may not get enough sample that's representative of the whole lot."[83] The larger the lot size, the greater the risk that E. coli will remain undetected and spread throughout the lot. By breaking the lot into smaller sections, producers can more effectively detect problems and control risk.

(*Continues*)

82. Payment Card Industry Data Security Standard, v.3.0, November 2013, p. 11, https://www.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf.

83. Personal conversation with the author, March 2018.

(*Continued*)

Consumer-facing brands such as Target must take special precautions to protect their image. A data breach can hit their bottom line harder and faster than with companies that rely less on consumer brand recognition. Again, there are parallels in other industries. DeArment points out that the risk a producer takes is often aligned with the importance of their brand. "If [an organic beef supplier] had an E. coli outbreak, everyone would remember that," she said. "The further away you get from a commodity product, the more you expect a higher level of security—whether it's a data breach or a bacterial outbreak."

7.2.4 Account and Password Management

Target's network was riddled with weak, default, and improperly stored passwords, according to the Verizon penetration testers that examined it shortly after the breach. "[W]hile Target has a password policy, the Verizon security consultants discovered that it was not being followed," stated the report. "The Verizon consultants discovered a file containing valid network credentials being stored on several servers. The Verizon consultants also discovered systems and services utilizing either weak or default passwords. Utilizing these weak passwords the consultants were able to instantly gain access to the affected systems."[84]

An attacker could certainly have leveraged default or weak credentials to move laterally throughout Target's network or to gain access to servers and POS systems. In February 2014, shortly after Retailgeddon was in full swing, the FBI issued a memo to retailers, warning that "it may be a 'vulnerability' to connect credit and debit card readers to remote management software, which makes it easier to manage and monitor internal networks from afar, when combined with weak password selection."[85] The FBI's warning implies that weak passwords may have been a factor in one or all of the retail breaches that occurred in that time frame.

All told, the Verizon penetration testers reportedly cracked 86% of Target's passwords. Their report indicated that 17.3% of the passwords were only 7 characters. The top 10 passwords included "t@rget7," "summer#1" and "sto$res1"—passwords that superficially might seem complex, but in reality are easy to crack for an attacker using automated tools. Moreover, the presence of files containing stored passwords would have been very helpful for criminals seeking to expand their access to Target's most sensitive resources.

Researchers from Dell Secureworks who analyzed reports of the malware used in the Target attacks determined that the hackers used "an improperly secured service account" to exfiltrate the data. "Organizations should ensure that service accounts, including default credentials provided with third-party software, are properly secured and provided only to those who need them to perform their job function," they advised.[86]

---

84. Krebs, "Inside Target Corp."

85. Yadron, Ziobro, and Barrett, "Target Warned of Vulnerabilities."

86. Keith Jarvis and Jason Milletary, "Inside a Targeted Point-of-Sale Data Breach," Dell Secureworks, January 24, 2014, https://krebsonsecurity.com/wp-content/uploads/2014/01/Inside-a-Targeted-Point-of-Sale-Data-Breach.pdf.

Tip: Account and Password Management

Passwords and accounts are surprisingly difficult to manage, particularly in large, complex environments. An important first step is to centralize accounts to the greatest extent possible, using Active Directory or a similar tool. Then, you can implement password length or complexity rules centrally.

Things start to get tricky when you consider the myriad of application accounts that exist, often hosted in the cloud or on third-party systems. Technical staff often need access to shared administrator accounts or service accounts. This leads to weak passwords and files with passwords that are stored in shared folders—a treasure trove for hackers.

Vendor equipment and software poses a special challenge for account management. Often, vendor equipment comes preconfigured with accounts that cannot be changed by local IT staff or that local IT aren't aware exist. POS systems frequently fall into this category. The result is that attackers can simply look up default equipment passwords, or reuse credentials that they discovered on a previous victim's network.

"Audit early, audit often" is a smart rule of thumb. When systems are installed and configured, they should be checked for default or weak credentials. IT staff or third-party auditors can audit files of encrypted passwords to determine how "crackable" they are, as the Verizon team did at Target.

What makes a strong password? Today, experts agree that password length is the most important fact. At the time of this writing, 14 characters is considered an effective minimum length for a strong password. This number will only increase in the future.

Humans are not naturally good at remembering passwords (or pass phrases), particularly long or complex ones. In order to prevent passwords from being stored in files throughout the network, you need to deploy a password management solution. This is especially important for IT administrators, who typically have many passwords and accounts to manage, and who may need to share account credentials (shared accounts are not ideal, but there are times when they are necessary). It's wise to routinely search the network for files containing passwords, so that they are uncovered quickly and do not fall into the wrong hands.

7.2.5 Encryption/Tokenization

In the Target breach, criminals stole credit card numbers from the memory of POS systems that they had hacked. As we learned in Chapter 2, "Hazardous Material," data is akin to hazardous material. An effective way to reduce risk would have been to prevent Target's POS systems from ever processing cleartext payment card numbers in the first place. Far from being a pipe dream, the technology to support this was readily available.

After the 2009 Heartland breach (see § 6.6), CEO Robert Carr set out to build a secure payment processing system. Heartland announced the launch of its E3 terminals in 2010. The E3 POS systems use hardware to encrypt the card data as it is swiped or entered. That means payment card numbers are never stored unencrypted, even in the device memory. "If the bad guys are intercepting transactions on the way to CPU, if you don't encrypt those and

get that data out of the clear, you don't have a solution," said Carr. Heartland also supports tokenization (the replacement of card numbers with nonsensitive data) for card-on-file and other purposes.[87,88]

When asked why retailers continued to suffer from data breaches, Carr said that companies simply weren't investing in effective solutions such as end-to-end encryption and tokenization. "[E]ven though solutions are being introduced, encryption being one we [adopted] . . . a lot of companies haven't implemented the basics, and they are paying the price for it."[89]

It didn't help that the most effective solutions, end-to-end encryption and tokenization, were not advertised or required by the card brands. It was up to individual retailers to go "above and beyond" and purchase POS systems that included these effective technologies.

Tip: End-to-End Encryption

Encryption is a powerful tool for preventing data breaches, especially when deployed "end to end." "End-to-end" encryption is different from "encryption in transit." With encryption in transit, data is wrapped up in an encrypted "envelope" as it is sent across a network. When it arrives at the other end, the receiving device unwraps the data and it is unencrypted again.

With end-to-end encryption, the data is encrypted even before it is transmitted across the network. In the context of payment card breaches, this means the card data can be encrypted using hardware built into the magnetic stripe reader, keypad, or other form of entry. The data is stored encrypted in memory and on any device hard drive.

End-to-end encryption reduces the opportunities that an attacker has to access sensitive data. In the modern world, endpoint devices and user accounts are compromised all the time. End-to-end encryption adds an extra layer of protection, so that when a device or account is compromised, the attacker does not have instantaneous access to the data in memory or on the hard drive.

Deploy end-to-end encryption wherever you can: on POS systems, in email accounts, and in the cloud. By doing so, you can make sure that a hacked device is not equivalent to a breach.

87. "Tokenization," Heartland, accessed January 14, 2018, https://developer.heartlandpaymentsystems.com/DataSecurity/Tokenization.

88. "Heartland Payment Systems® Installs E3™ Terminals at 1,020 Merchants since May 24 Launch of Its End-to-End Encryption Solution," *Business Wire*, June 24, 2010, http://www.businesswire.com/news/home/20100624005625/en/Heartland-Payment-Systems-Installs-E3-Terminals-1020.

89. Kelly Jackson Higgins, "Heartland CEO On Why Retailers Keep Getting Breached," *Dark Reading*, October 6, 2014, https://www.darkreading.com/attacks-breaches/heartland-ceo-on-why-retailers-keep-getting-breached/d/d-id/1316388.

7.3 Target's Response

"I am convinced that life is 10% what happens to me and 90% how I react to it," said radio pastor Charles Swindoll. In the same vein, data breach crises are typically only 10% about what happens and 90% how the organization reacts. This was very clear in the case of Target.

The Target breach marked a paradigm shift in breach response best practices. This was largely due to the rise of investigative journalist Brian Krebs, as we will see. Before the Target breach, retailers worked quietly with law enforcement for weeks or months until they were ready to disclose. TJX, Heartland, and similar companies responded to their breaches in this manner. This is not to say that breached retailers could take all the time in the world, but typically they had time to prepare their response, arrange for public notification, craft public statements, and so on. Quite often, the breached retailer was never publicly named, and consumers simply received a generic letter notifying them that their debit card numbers would be replaced.

The Target breach didn't happen that way. Target was outed—suddenly and deliberately—by Krebs.

Krebs, himself, represented a new development in high-tech investigative journalism. He knew how to access the dark web and could see when payment card numbers suddenly flooded the market, indicating a large breach. He also had strong ties in the banking industry and happily traded information with bankers, who were desperate to find ways to cut their losses due to fraud. As a result, Krebs had the ability to detect payment card breaches and find out the source—and his goal was to publish this information.

Not only did Krebs unexpectedly break the story of the Target breach, he kept digging. He found out what happened in the early days of the breach and revealed that Target hadn't detected it. He inspired others to dig for details, too, from researchers at Dell Secureworks to colleagues at Bloomberg News.

Taken by surprise, Target spun its wheels. The company failed to react effectively to the ensuing media uproar. Even worse, the onslaught of investigative news reports exposed all the mistakes they had made earlier in their breach response. Target's crisis communications (or lack thereof) only served to inflame the situation. While the loss of 40 million card numbers was undoubtedly huge, it was the company's *response* that turned its breach into a full-scale corporate disaster.

In this section, we'll dissect Target's initial response to the breach and then step through its crisis communications tactics, identifying lessons that other organizations can employ to minimize the negative impacts of a breach. We will analyze the impacts of the Target breach on the wider community, including banks, credit unions, and consumers. Finally, we will show how the Target breach, and others like it, spurred the rollout of "chip" cards—a development that did not actually reduce the risk of large-scale cardholder data breaches.

7.3.1 Realize

By all accounts, Target had invested significant funds into its security infrastructure—more than most retailers. A Bloomberg *Businessweek* investigative report revealed that "[s]ix months earlier the company began installing a $1.6 million malware detection tool made by the

computer security firm FireEye. . . . Target had a team of security specialists in Bangalore to monitor its computers around the clock. If Bangalore noticed anything suspicious, Target's security operations center in Minneapolis would be notified."[90]

Yes, despite its fancy equipment and army of analysts, Target didn't notice when hackers broke into its network. Target didn't notice when the criminals hunted through its systems and ultimately gained access to the POS devices and customer databases. Target didn't notice when the criminals installed malware on its POS systems or when they returned again and again to install updates and hack into other servers. Target didn't notice when the criminals exported the card numbers to servers outside the network, where they were eventually sold on the black market.

Recall the DRAMA model of data breach response (Develop, Realize, Act, Maintain, Adapt) from Chapter 4. As discussed in § 4.3, during the prodromal phase of a breach, organizations must "realize" than a potential breach has occurred. This typically includes the following actions:

- **Recognize** the prodromes of a data breach.
- **Escalate** to the data breach response team.
- **Investigate** by preserving and analyzing available evidence.
- **Scope** the breach.

It wasn't that Target's staff didn't care that criminals were siphoning off millions of card numbers. It was that the organization didn't *realize* that this was happening. As reporters later discovered, there were plenty of signs—such as repeated IDS alerts—which were never escalated to appropriate staff members and therefore not properly investigated in a timely manner.

How could Target have missed such seemingly obvious signals? In this section, we will dive into the issues that occurred during Target's "realize" phase and provide cost-effective tips for better protecting your organization.

7.3.1.1 Missed Alerts

One of the most damning revelations about the Target breach was that staff had received alerts—many alerts—about the criminals' activities as they installed and fine-tuned their malware. The FireEye system alerted Target's Bangalore team to suspicious activity on November 30, as the attackers installed exfiltration malware designed to export the stolen credit card numbers. Target's antivirus software, Symantec Endpoint Protection, had also alerted days earlier when suspicious activity was detected on the same server. "Bangalore got an alert and flagged the security team in Minneapolis," Bloomberg revealed. "And then . . . Nothing happened. For some reason, Minneapolis didn't react to the sirens."[91]

Target's FireEye system was capable of automatically blocking malware, reducing the load on human staff, but according to people who reviewed FireEye's configuration after the breach, Target had disabled that functionality.

---

90. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

91. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

In the days that followed, the criminals continued to collect the credit card numbers and stage them on an internal system. On December 2, the criminals began exporting the card numbers. The criminals continued to siphon off payment card data until December 18—nearly a week after Target was first notified by law enforcement.[92]

In the meantime, the FireEye system continued to send alerts. Had Target's team reacted to the alerts between November 30 and December 2, it could have stopped the card numbers from ever leaving Target's network, thereby preventing one of the world's biggest data breaches.

Target reportedly did not learn of the breach until the company was informed by the U.S. Department of Justice and the Secret Service on December 12. However, there is evidence that someone within Target had stumbled across the malware earlier. On December 11, a malware sample was uploaded to the public service, "VirusTotal," where it was scanned for traces of malware. According to researchers from Dell Secureworks. "The submission was attributable to someone within Target because the malware was widely thought to be custom-made specifically for the Target intrusion."[93]

There is no indication that anyone within Target understood the significance of the malware until long afterwards—or if they did, they didn't sound the alarm.

7.3.1.2 Reasons for Inaction

Why was Target "asleep at the wheel" (as one newscaster put it)?[94] No one knows for sure. There are many reasons that security teams don't respond to alerts. All too often, security teams are bombarded with far more IDS alerts than they can possibly handle. This frequently happens when new intrusion detection equipment is installed but not carefully "tuned." A poorly tuned IDS can result in a flood of meaningless alerts that are triggered by perfectly normal activity—overwhelming analysts, who learn to ignore them.

Security tools such as FireEye are often configured with prevention capabilities disabled, at least at first. IT teams are concerned about false positives—legitimate traffic that should be allowed, but gets flagged as suspicious. This risk is especially high when human resources have not been allocated to carefully tune the system and minimize false positives.

Target may also have simply not had sufficient staff to handle its case load or perhaps been understaffed due to the Thanksgiving holiday. Many security teams respond quickly during normal business hours, but don't have an effective monitoring or response process after normal business hours or on the weekends.

All of these issues stem from lack of effective management, training, and budgeting—not surprising, given that Target did not have a chief information security officer (CISO) prior to the breach, and therefore there was no executive whose primary responsibility was overseeing information security.[95]

---

92. *Hearing on "Protecting Personal Consumer Information*" (written testimony of John Mulligan).

93. Jarvis and Milletary, "Inside a Targeted."

94. Bloomberg, "How Target Could Have Prevented Customer Data Hack," *YouTube*, 6:19 min, posted March 13, 2014, https://www.youtube.com/watch?v=G68hY3TsGYk.

95. Kristin Burnham, "Target Hires GM Exec As First CISO," *InformationWeek*, June 11, 2014, https://www.informationweek.com/strategic-cio/team-building-and-stafing/target-hires-gm-exec-as-first-ciso/d/d-id/1269600.

Target: A Timeline of Missed Alerts

Target missed many opportunities to stop the intrusion before it became a disaster, a fact that impacted not only the breach itself, but also the public's perception afterwards. Here is a summary of how the events and corresponding alerts unfolded.

- 11/27/13 First day that customer credit card numbers may have been stolen, according to Chief Financial Officer (CFO) John Mulligan. "The theft of the payment card data affected guests who shopped at our U.S. stores from November 27 through December 18."[96]
- 11/28/13 - Symantec antivirus software alerts on exfiltration server (approximate date).[97]
- 11/30/13 - By this date, attackers had deployed malware on most Target POS systems.[98]
- 11/30/13 - Attackers install exfiltration malware on internal dump server; FireEye alerts; Target's Bangalore monitoring team sends the alert to Minneapolis responders.[99]
- 12/2/13 - Credit card data is first transferred out of the Target network to an external server.[100]
- 12/2/13 - Attackers update exfiltration malware; FireEye alerts.[101]
- 12/2/13-12/18/13 - Attackers continue to exfiltrate credit card data. According to Dell Secureworks, data is sent from compromised POS systems to an internal file share. A compromised internal server then transfers the credit card data files out of the Target network via FTP between the hours of 10 a.m. and 6 p.m. local time.[102]

The Target case perfectly illustrates why "detect" and "realize" are not the same thing. It is not enough for an automated tool to "detect" malware and generate an alert, or even for a security staff member to notice it. The organization must become aware of the incident and understand its scope. In the case of Target, individual staff members saw the alerts, but the response was stillborn: The team failed to escalate, investigate, and scope the breach.

96. *Hearing on "Protecting Personal Consumer Information"* (written testimony of John Mulligan).

97. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

98. Krebs, "Target Hackers Broke In."

99. Jarvis and Milletary, "Inside a Targeted"; Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

100. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

101. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms"; Jarvis and Milletary, "Inside a Targeted Point-of-Sale."

102. Jarvis and Milletary, "Inside a Targeted."

Tip: Invest in Human Resources

Many companies invest in expensive security equipment, only to find that they still miss important indicators of a breach. When you budget for security tools, make sure that you include a proportional investment for the human resources needed to monitor, tune, and react to alerts. This is not a one-time investment; people need ongoing training in order to recognize the latest threats, determine what to escalate, and how to respond.

7.3.1.3 Industry Standard

Target's missed breach detection was in no way unusual. According to Verizon, 99% of payment card breaches in 2013 were detected by someone other than the victim. "[W]e continue to see notification by law enforcement and fraud detection as the most common discovery methods," reported Verizon researchers in their 2014 *Verizon Data Breach Investigations Report*. "In many cases, investigations into breaches will uncover other victims, which explains why law enforcement is the top method of discovery and the top contributor of POS intrusions in our dataset." Only 1% of POS intrusions were discovered within days; 85% took weeks (as in the case of Target), and the remainder took months or years. In short, Target's detection and reaction times were utterly normal.[103]

The early stages of a POS data breach response can last for weeks or even months, as the merchant conducts an internal review and decides whether to notify the public at all. Law enforcement is rarely interested in "outing" the merchant or forcing the merchant to disclose. They want merchants to feel comfortable notifying them and sharing evidence. Normally, in large breaches, law enforcement works quietly with the merchant and/or card brands to gather evidence and provide assistance when possible. Law enforcement tends to focus on tracking down the culprits responsible and ultimately bringing them to justice. Their investigation may involve piecing together information from many different breaches in order to take down a crime ring.

Alternatively, card brands or banks may discover the breach, by identifying that a merchant is a common point of purchase. Card brands are under no obligation to disclose which merchant was responsible, and they typically don't. Instead, when fraud is detected, the card brands send banks a list of impacted cards, which the banks may choose to reissue. Banks can sometimes also identify common points of purchase, although their data set is typically much smaller, and so they often do not have enough information to identify the source of the compromise. Even in cases where it appears that a merchant is the source, banks have to be very careful because it is possible that the breach actually occurred further up in the chain (such as with the merchant's payment processor).

Often, the public never learns that a particular merchant was breached. Affected consumers frequently receive generic letters from the card brands informing them that their card numbers

103. *2014 Data Breach Investigations Report*, Verizon Enterprise, 2014, 18, http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf.

were stolen. By state law, merchants may be required to report a breach—but many simply don't.

In the case of Target, U.S. federal agents investigated and notified the company on December 12, 2013. According to Bloomberg, "[T]he authorities had more than just reports of fraudulent charges to go on, however: They had obtained the actual stolen data, which the hackers had carelessly left on their dump servers."[104]

Based on past retail payment card breaches, it was reasonable for Target to expect that it could conduct an investigation spanning weeks or even months, with input and guidance from law enforcement. Once it understood the scope and had evalutated its options, it could determine next steps, prepare notifications if appropriate, and so on.

But the Target data breach was unprecedented. It wasn't the way it was breached, or the missed alerts, or the vulnerable POS systems (although none of that helped). Contrary to popular opinion, Target's detection capabilities and reaction times were completely normal (by many accounts, better than average) for its industry at that time.

Target's data breach was different because its time was unexpectedly cut short—by reporter Brian Krebs.

7.3.2 The Krebs Factor

Krebs, by himself, represented a significant development in data breach response. A former *Washington Post* reporter, Krebs had left the newspaper in 2009 to strike out on his own. He had been obsessed with computer crime since 2001, when a computer worm infected his computer. "It felt like someone had broken into my home," Krebs told the *New York Times* years later.[105] In 2009, Krebs started his own blog, *Krebs on Security*. In 2010, he received the "Best Non-Technical Security Blog" award by Security Blogger Meeting, and had been named one of the top 10 cybersecurity journalists by the SANS Institute.

Krebs broke stories—and hearts. Executive hearts, that is. He broke the Target story on December 18, 2013. "Nationwide retail giant Target is investigating a data breach potentially involving millions of customer credit and debit card records, multiple reliable sources tell KrebsOnSecurity," he wrote. "The sources said the breach appears to have begun on or around Black Friday 2013—by far the busiest shopping day of the year."[106]

How did Krebs find out about the Target breach? According to the *New York Times*, in December 2013, Krebs had already been "poking around private, underground forums where criminals were bragging about a fresh haul of credit and debit cards." Soon afterwards, a "source" in the banking industry called him to report that the bank was seeing high levels of payment card fraud. The bank had visited a carder shop, bought back a batch of its own cards, and found what appeared to be a common point of purchase: Target.[107] Krebs confirmed with other sources and quickly published his scoop.

---

104. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

105. Nicole Perlroth, "Reporting from the Web's Underbelly," *New York Times*, February 16, 2014, https://www.nytimes.com/2014/02/17/technology/reporting-from-the-webs-underbelly.html.

106. Krebs, "Sources: Target Investigating."

107. Perlroth, "Reporting from the Web's Underbelly."

The following day, after Target confirmed the theft, Krebs reached out to a colleague at a small New England bank to see whether the bank had received any notification from Visa or Mastercard. His contact there said that the bank hadn't officially been told anything but was "anxious to determine how many of the bank's cards were most at risk of being used for fraud, and how many should be proactively canceled and re-issued to customers." Krebs struck a deal: He would show the bank's staff how to purchase a batch of its own cards from a carder shop, in exchange for permission to write about the bank's story. The bank agreed.[108]

Krebs was successful for two reasons: First, he had infiltrated the dark web and gained a reputation for knowing his way around carder shops and darknet markets. "Over the past year, I've spent a great deal of time trolling a variety of underground stores that sell 'dumps'—street slang for stolen credit card data that buyers can use to counterfeit new cards and go shopping in big-box stores for high-dollar merchandise that can be resold quickly for cash," Krebs wrote in the summer of 2014.[109] This familiarity meant that he knew when a major breach had taken place because cards would start to flood the markets.

"When you see a single [black market] carding store start selling millions of cards out onto the market, something big just happened and so it's time to get to work," he explained.[110]

Second, Krebs had built a relationship with bankers over the years and had become a one-man information clearinghouse. He had been reporting on developments in the darknet markets, fraudulent wire transfers, and payment card breaches for years, gaining contacts within the financial industry along the way. By 2013, smaller banks in particular were desperate for information that would help them respond quickly to suspected payment card breaches. Larger banks had teams of fraud analysts and, by virtue of their size, could identify breaches and common points of purchase relatively quickly.

"The smaller banks usually need to compare notes with other banks, and that's sort of where I come in," said Krebs. "I reach out to banks that I have a relationship with and say, "Hey, it looks like a whole bunch of your cards are for sale in this huge batch that just went online. Here's how you can go get them. Just FYI, I've been really interested in whether you see any patterns."[111]

After breaking the Target story and publishing his follow-up piece on the smaller bank, Krebs found himself awash in requests from bankers. "Over the last year in particular since the Target breach, I've just become sort of the ISAC [information sharing and analysis center] of the small banking industry," Krebs said—clearly filling a much-needed gap. "I just say I'm happy to share information with you about what I'm seeing as long as you're able to do the same."[112]

---

108. Brian Krebs, "Cards Stolen in Target Breach Flood Underground Markets," *Krebs on Security* (blog), December 20, 2013, https://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets.

109. Brian Krebs, "Peek Inside a Professional Carding Shop," *Krebs on Security* (blog), June 4, 2014, https://krebsonsecurity.com/2014/06/peek-inside-a-professional-carding-shop.

110. Jay MacDonald, "'Spam Nation' Author Brian Krebs Sheds Light on Card Data Black Market," CreditCards.com, November 18, 2014, https://www.creditcards.com/credit-card-news/spam-nation-brian-krebs-data-black-market-1278.php.

111. MacDonald, "'Spam Nation' Author."

112. MacDonald, "'Spam Nation' Author."

Armed with access to the darknet markets and a loyal following of small banks that were happy to share details, Krebs broke story after story of retail payment card breaches. The Neiman Marcus and Michaels breaches were publicized within weeks of Target. Sally Beauty, P.F. Chang's China Bistro, and many others were quickly outed due to Krebs's reporting.[113]

Thanks to Krebs, as soon as stolen cards went up for sale on the dark web, news could quickly burst into the mainstream media. That meant that retailers could no longer expect to quietly handle the investigation behind the scenes and take weeks to craft press releases. Nor could they rely on the card brands to release a vague, anonymous letter on their behalf. Retailers had to be prepared for an immediate public response as soon as a payment card theft was detected. This pressure spurred the development of specialized third-party incident response teams run by cybersecurity firms, as well as prepackaged call center and credit monitoring services that could be activated quickly. It also fueled growth for insurers' breach response services (as discussed in Chapter 12, "Cyber Insurance").

Tip: Prepare to Make an Immediate Public Statement

Payment card breaches are easily detected by third parties, including banks and card associations that identify a common point of purchase—as well as anyone who monitors the dark web. Your first heads-up that your organization has been breached might come as a phone call from a reporter. Your first response matters. As soon as the media finds out about a payment card breach, the clock starts ticking—fast.

Prepare a statement and a plan in advance, so that you can respond immediately to a third party who discovers that you've been breached.

7.3.3 Communications Crisis

Getting "outed" by Krebs was bad. Target's reaction, however, was far worse. Throughout the weeks that followed, Target's team made critical errors that inflamed public response: at times stonewalling the press, and at other times launching heavy-handed attempts to win back the public's trust. As we will see, Target:

- Clammed up, which fueled suspicion and speculation
- Released "cold" and uncaring statements
- Failed to take responsibility
- Avoided apologizing
- Did not provide sufficient call center resources, frustrating consumers
- Offered compensation that was then not available

113. Brian Krebs, "Hackers Steal Card Data from Neiman Marcus," *Krebs on Security* (blog), January 10, 2014, https://krebsonsecurity.com/2014/01/hackers-steal-card-data-from-neiman-marcus; Brian Krebs, "Banks: Credit Card Breach at P.F. Chang's," *Krebs on Security* (blog), June 10, 2014, http://krebsonsecurity.com/2014/06/banks-credit-card-breach-at-p-f-changs.

- Released a series of news stories with new information, generating intense media interest
- Failed to control media communications, leading to multiple damning leaks

Ultimately, this communications catastrophe became an avalanche that took down the company's leadership and badly damaged their bottom line.

7.3.3.1 Talk to the Hand

Target's first PR mistake was stonewalling Krebs. Upon hearing of the potential Target breach, Krebs called the retailer for a statement—but Target clearly wasn't ready to answer questions. Although the company's spokesperson reportedly returned his call hours later,[114] Target declined to comment. As a result, Target missed its first opportunity to tell its side of the story. Even worse, when the story ran that evening, it portrayed the company as uncooperative, stating that "Minneapolis, Minn. based Target Brands Inc. has not responded to multiple requests for comment."[115]

The company stuck to its "minimal disclosure" strategy throughout the ensuing weeks. Its initial public notification shared few details and no offer of compensation or credit monitoring. "We regret any inconvenience that this may cause," said CEO Gregg Steinhafel, in a terse statement that came across as cold and uncaring.

Consumers were furious. In the days that followed, many were hit with fraudulent charges or were notified that they had to wait for reissued cards—far more than an "inconvenience" in the days leading up to Christmas. One shopper, whose bank account was drained of $850, said, "I had to borrow money for the Christmas dinner and from my brother and I also had to borrow money for my rent."[116]

"Why did Target take so long to report data security breach?" asked one *NBC News* reporter.[117] There were no good answers.

"I won't shop at Target again," exclaimed one angry "guest," who suffered fraud just days before Christmas.[118]

Customers called the company's hotline with questions, only to experience long waiting times. As Target struggled to handle the onslaught of angry calls, customers got angrier. "Customers seeing red over Target's hacking response," screamed one headline.[119]

---

114. Perlroth, "Reporting from the Web's Underbelly."

115. Krebs, "Sources: Target Investigating."

116. Michael Finney, "Woman's Debit Card Suspended Due to Target Breach," *abc7 News*, January 14, 2014, http://abc7news.com/archive/9393709.

117. Kelli Grant, "Why Did Target Take So Long to Report Data Security Breach?" *NBC News*, December 20, 2013, https://www.nbcnews.com/business/why-did-target-take-so-long-report-data-security-breach-2D11783300.

118. Alexandra Klausner, "'I Won't Shop at Target Again': Angry Fraud Victims Condemn Store after Details of up to 40 MILLION Credit Cards are Stolen by Hackers," *Mail Online*, December 19, 2013, http://www.dailymail.co.uk/news/article-2526235/Over-1-MILLION-Target-customers-account-information-stolen-Black-Friday-weekend-in.html.

119. Aimee Picchi, "Customers Seeing Red Over Target's Hacking Response," *CBS News*, December 20, 2013, https://www.cbsnews.com/news/customers-seeing-red-over-targets-hacking-response.

In response, Target sent out an email that discouraged consumers from calling. "We continue to experience a high volume of calls to our call center and have more than doubled the number of team members taking calls around the clock to help them resolve any issues they may have. We have communicated to 17 million guests via email and reminded them that unless they have seen fraudulent activity on their account, there is no urgent need to call."[120]

The media, like consumers themselves, were rebuffed. "Target has yet to honor a single request for comment from this publication, and the company has said nothing publicly about how this breach occurred," reported Krebs, nearly a month after the breach was first announced. Lacking responses from Target, consumers speculated, and journalists turned to investigative reporting.

Tip: Two-Way Communication

When a breach happens, it's natural for an organization to freeze up. Executives and PR teams are afraid to say the wrong thing, and as a result, they often say nothing at all. To make matters worse, lawyers often advise executives to stay mum. Unfortunately, silence can very quickly erode trust, and the void of communication will be filled by angry stakeholders.

As the "Act" imperative in our "DRAMA" model implies, it's important to say *something*, and quickly. Remember the following crisis communications tips, which were introduced in § 3.3.5:

- **Tell It Early, Tell It Yourself.** Maintain a congenial relationship with the media. By providing a quote when contacted by the press, you send the message that you are not trying to hide.
- **Apologize Clearly and Quickly.** A sincere apology diffuses anger and shows respect for your stakeholders.
- **Listen!** Prepare your staff to listen to stakeholders. For example, you might consider opening a call center in response to the breach, so that members of the public can quickly speak with a real human. Likewise, shareholders, regulators, and other stakeholders need a point of contact who can listen to their concerns and diffuse strong emotions.

Target learned the hard way that communication—from the beginning—is the foundation of an effective breach response.

7.3.3.2 Victimization

"Evasion of responsibility" appeared to be Target's primary image repair strategy from the beginning—and it backfired. "We take this matter very seriously and are working with law

120. Target, "Target Data Security Media Update #2," press release, December 23, 2013, https://corporate.target.com/press/releases/2013/12/target-data-security-media-update-2.

enforcement to bring those responsible to justice," said the company in its initial notification letter.[121]

Clearly, Target was a victim, like consumers themselves. "It was a crime against Target, our team members, and most importantly, our guests," said CEO Gregg Steinhafel.[122]

The public didn't buy it. "Consumers are frustrated when a company doesn't do a good job either protecting their info or informing them of any problems," said Ed Mierzwinski, consumer program director U.S. PIRG.[123]

"Don't play the victim," urged Visa, in a guide for merchants released in 2008. "[Y]ears ago, when announcing a data breach, it may have been possible for companies to successfully portray themselves simply as fellow victims. Today, this is a flawed and dangerous strategy. Although you may have had a crime committed against you, the public and business press will still hold you accountable and will not consider you a co-victim."[124]

If only Target had heeded Visa's advice. The problem with the "victim" strategy is that it did not give Target room to take responsibility, which ultimately led to questions of competence and character, and led to the downfall of the company's senior management team.

Tip: Take Responsibility

Target's claim that the company was a "victim" rang hollow. Consumers felt that Target had a duty to protect their data but fell down on the job. While "victimization" can be a successful image repair tactic in other contexts, it doesn't usually work well for data breach response. This is particularly true when the organization had obvious gaps in its cybersecurity program, as was the case with Target.

The "victimization" strategy can also backfire by eroding confidence in an organization's leadership team. Recall the 3 C's of Trust from § 3.2.3: Competence, Character, and Caring. If the organization's leadership doesn't take responsibility for the breach and provide an adequate explanation for what went wrong, stakeholders will typically blame lack of competence, character, or caring. In the case of Target, this contributed to the downfall of its CEO.

Only by taking responsibility can leadership have a chance of maintaining confidence and righting the ship.

---

121. Target, "Target Confirms Unauthorized Access to Payment Card Data in U.S. Stores," press release, December 19, 2013, https://corporate.target.com/press/releases/2013/12/target-confirms-unauthorized-access-to-payment-car.

122. Target, "A Message from CEO Gregg Steinhafel about Target's Payment Card Issues," *Bullseye View*, December 20, 2013, https://corporate.target.com/article/2013/12/target-ceo-gregg-steinhafel-message.

123. Beth Pinsker, "Consumers Vent Frustration and Anger at Target Data Breach," *Reuters*, January 14, 2014, http://www.reuters.com/article/us-target-consumers/consumers-vent-frustration-and-anger-at-target-data-breach-idUSBREA0D01Z20140114.

124. Visa, *Responding to a Data Breach: Communications Guidelines for Merchants*, 2008, 8, https://usa.visa.com/dam/VCOM/global/support-legal/documents/responding-to-a-data-breach.pdf.

7.3.3.3 Trust Us—Before Christmas, Please

As the countdown to Christmas wound down, Target's executive team was clearly panicked. For retailers, a tarnished image can quickly impact sales. They released a web-based "Message from CEO Gregg Steinhafel about Target's Payment Card Issues" with a series of YouTube embedded videos (since deleted). The message incorporated several image repair strategies:[125]

- The title of the first video, *Target CEO Expresses Gratitude*, was clearly an attempt to humanize the company and capitalize on the general tendency toward goodwill during the holiday season (*bolstering*).
- Target attempted to *minimize* the injury with statements such as: "We want our guests to understand that just because they shopped at Target during the impacted time frame, it doesn't mean they are victims of fraud. In fact, in other similar situations, there are typically low levels of actual fraud. Most importantly, we want to reassure guests that they will not be held financially responsible for any credit and debit card fraud."
- *Evasion of responsibility* continued, with the assertion that "[i]t was a crime against Target, our team members, and most importantly, our guests."
- Target made a weak attempt at demonstrating *corrective action* ("The issue has been identified and eliminated"), but the lack of details and questions regarding the management team's competence rendered the statement unconvincing.
- A promise of credit monitoring (*compensation*/*corrective action*) was buried midway through the page: "[T]o provide guests with extra assurance, we will be offering free credit monitoring services," said Target. However, there was no way for consumers to actually sign up for credit monitoring, fueling frustration and the growing perception of incompetence. Indeed, it wasn't until mid-January that affected Target customers could actually sign up for the service. Also, credit monitoring is of limited use in payment card breaches since it doesn't stop anyone from fraudulently using a stolen card number.
- Target offered consumers a special deal: "We're in this together, and in that spirit, we are extending a 10% discount—the same amount our team members receive—to guests who shop in U.S. stores on Dec. 21 and 22." It concluded with a hearty, "Valid in store only. Limit one offer per guest to be used in a single transaction. Void if prohibited by law. Not valid in Canada. No cash value." The discount, which may have been intended as a form of *compensation*, instead reinforced the impersonal and transactional nature of Target's relationship with its "guests."

It didn't work. Target's fourth-quarter profits dropped 46% in 2013, a precipitous decline largely attributed to the data breach.[126] Shares fell 11% in the two months following the breach,

125. Target, "Message from CEO Gregg Steinhafel."

126. Maggie McGrath, "Target Profit Falls 46% on Credit Card Breach and the Hits Could Keep Coming," *Forbes*, February 26, 2014, https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming.

and only made strong gains after a conference call in which CFO John Mulligan "reassured investors that customers were beginning to return to its U.S. stores."[127]

Tip: Offer Real Value

When developing compensation or corrective action strategies, think about what will *genuinely* be valuable for your stakeholders or help to correct the issue. Offers that simultaneously benefit the breached organization (such as Target's 10% discount) can seem like a cheap bribe to consumers when the trust relationship has been damaged. Instead, choose offers that clearly and unequivocally benefit the wronged party, with no possibility of an ulterior motive. This may be more expensive in the short term, but it will undoubtedly be the most effective way to repair relationships.

7.3.3.4 Nonapologizing Profusely

Missing from Target's crisis communications messages was a clear apology. The absence was striking. For example, in Steinhafel's written "message" published on December 20, he apologized only for the difficulty that "guests" experienced when attempting to reach Target's customer service representatives. "We apologize and want you to understand that we are experiencing unprecedented call volume." The CEO's message did not include an apology for the breach itself or for Target's delayed notification, which had the public up in arms.

Apologies are a critical element of relationships, both for individuals and organizations. "It is an important social ritual, a way of showing respect and empathy for the wronged person," writes psychotherapist Beverly Engel. "It is also a way of acknowledging an act that, if otherwise left unnoticed, might compromise the relationship. Apology has the ability to disarm others of their anger and to prevent further misunderstandings. While an apology cannot undo harmful past actions, if done sincerely and effectively, it can undo the negative effects of those actions."[128]

In many data breach cases, organizations refrain from apologizing because they fear this will increase their liability. However, as we will see in Chapter 9, a clear apology can quickly diffuse anger and actually help to reduce lawsuits. (See § 9.6.4 for details.)

According to researchers from Ohio State University's Fisher College of Business, there are six key elements of an apology:[129]

1. Expression of regret
2. Explanation of what went wrong

---

127. Dhanya Skariachan and Jim Finkle, "Target Shares Recover after Reassurance on Data Breach Impact," *Reuters*, February 26, 2014, https://www.reuters.com/article/us-target-results/target-shares-recover-after-reassurance-on-data-breach-impact-idUSBREA1P0WC20140226; Yahoo! Finance, *Target Corporation (TGT)*, 2014, https://finance.yahoo.com/quote/TGT/history?period1=1357023600&period2=1420009200&interval=1d&filter=history&frequency=1d.

128. Beverly Engel, *The Power of Apology: Healing Steps to Transform All Your Relationships* (Hoboken, NJ: Wiley & Sons, 2002), 12.

129. Jeff Grabmeier, "The 6 Elements of an Effective Apology, According to Science," *Ohio State University News*, April 12, 2016, https://news.osu.edu/news/2016/04/12/effective-apology.

3. Acknowledgment of responsibility
4. Declaration of repentance
5. Offer of repair
6. Request for forgiveness

"Our findings showed that the most important component is an acknowledgement of responsibility," said Roy Lewicki, professor emeritus of management and human resources at the college. "Say it is your fault, that you made a mistake."[130]

The longer Target waited, the more the public's resentment and anger boiled. The company said things that *implied* it felt badly: "we recognize this issue has been confusing and disruptive,"[131] "[t]he privacy and protection of our guests' information is a matter we take very seriously."[132] But the key elements of an apology were missing. Target did not accept responsibility, and as a result, it couldn't effectively explain what went wrong, declare repentence, or request forgiveness.

Tip: Apologize

When a data breach happens, an apology is often the first step on the path to image repair. The longer you wait, the more anger builds.

Apologize clearly, quickly, and earnestly to affected stakeholders. Remember the key elements of an apology, as describe by Ohio State University researchers:[133]

1. *Expression of regret*
2. *Explanation of what went wrong*
3. *Acknowledgment of responsibility*
4. *Declaration of repentance*
5. *Offer of repair*
6. *Request for forgiveness*

Apologizing enables you and your stakeholders to begin the repair process and move forward.

7.3.3.5 Getting Personal

Starting on December 20, Target's breach communications became noticeably, and strangely, personal. Clearly someone had informed company executives that their initial communications

130. Grabmeier, "6 Elements."

131. Target, "Message from CEO Gregg Steinhafel."

132. Target, "Message from CEO Gregg Steinhafel."

133. Grabmeier, "6 Elements."

were terse and impersonal. Suddenly, Target sent new emails to "guests" that were "signed" by the CEO (never mind the oddities of including a scribbled signature on an email).

Subsequently, the company released an article called "Behind the Scenes of the Recent Target Data Breach," which featured photographs and videos of uncomfortable and sad-looking executives. One could almost see the PR consultants coaching Target's executives, telling them to "humanize" their response. And they did—but the results were not confidence-inspiring.

By January, Target was desperate to repair its image. Steinhafel gave a much-touted, exclusive interview to CNBC. Unfortunately, the results were unflattering. The CEO appeared nervous, frequently spoke too quickly, and fell back on "canned" generic phrases such as "safe and secure," which he repeated no less than nine times:[134]

> [I]t was about making our environment safe and secure.
>
> [B]y 6:00 at night, our environment was safe and secure.
>
> I can tell you that we are highly confident that Target's environment is safe and secure.
>
> [W]e really want to assure them that Target's environment is safe and secure.
>
> We removed that malware so that we could provide a safe and secure shopping environment.
>
> We're very confident that our . . . environment is safe and secure.
>
> We know in our heart of hearts, our environment is safe and secure.
>
> We think it's really important that we have safe and secure environment.
>
> I can tell you that we are highly confident that Target's environment is safe and secure.

"[T]here was this singular focus on the 'guest' and this constant repetition of the 'guest,'" pointed out Paul Argenti, professor of corporate communication at Dartmouth. "[H]e bridged to a canned response."[135]

Throughout the CNBC interview, Steinhafel gave the strong impression that he had something to hide. He dodged requests for details, changed the topic, and at one point said outright, "we're in the middle of a criminal investigation, as you can appreciate. And we can only share so much." (Host Becky Quick did not appear to appreciate.)[136] *Reuters* reported, "the No. 3 U.S. retailer was vague in providing details about what it knew and when."[137]

No wonder Steinhafel was nervous: he was actively misleading the public. "Sunday [December 15] was really day one," he said. "[T]hat was the day that we confirmed that we had an issue. . . . Monday . . . day two was really about—initiating the investigation work and the forensic work. . . . Day three was about preparation. We wanted to make sure our stores and

---

134. "CNBC Exclusive: CNBC Transcript: Target Chairman & CEO Gregg Steinhafel Speaks with Becky Quick Today on CNBC," press release, January 13, 2014, https://www.cnbc.com/2014/01/13/cnbc-exclusive-cnbc-transcript-target-chairman-ceo-gregg-steinhafel-speaks-with-becky-quick-today-on-cnbc.html.

135. Jena McGregor, "Target CEO Opens Up about Data Breach," *Washington Post*, January 13, 2014, https://www.washingtonpost.com/news/on-leadership/wp/2014/01/13/target-ceo-opens-up-about-data-breach.

136. Becky Quick, "Target CEO Defends 4-Day Wait to Disclose Massive Data Hack," *CNBC*, January 12, 2014, https://www.cnbc.com/2014/01/12/target-ceo-defends-4-day-wait-to-disclose-massive-data-hack.html.

137. R. Kerber, P. Wahba, and J. Finkle, "Target Apologizes for Data Breach, Retailers Embrace Security Upgrade," *Reuters*, January 13, 2014, https://www.reuters.com/article/us-target-databreach-retailers/target-apologizes-for-data-breach-retailers-embrace-security-upgrade-idUSBREA0B01720140113.

our call centers could be as prepared as possible. And day four was notification. So, throughout that four-day process, to some people it probably felt longer than that, we worked around the clock to try and do the right thing, to be transparent, truthful, and then share what we knew as quickly as we could."

But Sunday, December 15, wasn't "day one," and the investigation had been initiated well before Monday. Journalists later discovered that the Department of Justice and the Secret Service had informed Target on December 12, three days earlier. Steinhafel was quick to emphasize that "day one" was the day the breach was "confirmed"—but the reality was that Target had been informed days earlier, and the "four-day process" was really a week. Fearful of even more public backlash, Target chose to mislead people rather than disclose the truth.

Steinhafel did finally clearly apologize and take responsibility—a refreshing step forward that earned him kudos in the media. Unfortunately, these statements did not make it into many of the clips, such as the NBC Business Report evening segment—a powerful reminder that news outlets will choose the juiciest snippets to run, and not necessarily those that the breached organization would like to see featured.

Steinhafel also successfully humanized the story, sharing that he found out about the breach while having coffee with his wife Sunday morning—an "everyday Joe" experience that many could relate to. Shareholders, however, did not want to hear that the CEO was as surprised as consumers. Throughout the interview, Steinhafel worked hard to seem caring, but provided little reassurance that the company was competently managing cybersecurity—a mistake that would ultimately cost him his job.

Tip: Be Genuine and Confident

Strong leaders are invaluable in a crisis, in part because personal statements work best when they are *genuine*. This is particularly true with video and audio messages. You can have teams of PR staff write carefully crafted statements for the CEO to read on a teleprompter, and they will often come across looking just like that: overproduced.

The most effective statements are true and come from the heart. Consider involving your spokesperson (such as the CEO) intimately when crafting personal statements, and make sure that the content truly resonates for him or her.

7.3.3.6 Phishing the Victims

Adding insult to injury, cybercriminals copied Target's notification emails and website design and sent mass phishing emails that looked like they came from Target—but in fact, they contained links to scam websites that stole victims' personal information.[138] Unfortunately, Target had used a scammy, non-Target email address to send its official notifications, which contributed to the perception that they either did not understand good cybersecurity practices or did not care. After Target released its early notifications, a *Forbes* contributor pointed out the "beautifully horrible" address, which consisted of a 50-character alphanumeric string at

138. Catey Hill, "Email 'from Target' to Customers is a Phishing Scam," *MarketWatch*, December 20, 2013, https://www.marketwatch.com/story/scammers-pounce-on-target-fiasco-2013-12-20.

the domain target.bfi0.com. "Many users would decide this is a scam e-mail (or wouldn't even notice any of this which is more concerning given how often true scammers behave nearly identically)."[139]

To alleviate the damage, Target released a series of updates and warnings. On the day before Christmas, Target issued an update, which said that "[w]e are aware of limited incidents of phishing or scam communications. To help our guests feel confident that what they are hearing from Target is really from us, we are in the process of setting up a dedicated resource on our corporate website where we will post pdfs of all official communications that Target sends to our guests."[140]

Tip: Plan for Phishing Attacks

Cybercriminals will take any opportunity to get people to click on a link or visit a malicious website. After a major data breach, it's common to see a flood of scam messages and websites targeting victims, which often mimic real notifications or offers of compensation. In addition to Target, this was the case in the Equifax and Anthem breaches, and countless others.

Protect your stakeholders by taking precautions from the very beginning. Post web pages and send emails using a well-known, widely trusted domain whenever possible. Educate recipients so they know how to tell the difference between real and fake communications from your team. To the greatest extent that you can, design your communications plan with cybersecurity in mind, so that victims don't have to suffer twice.

7.3.3.7 A Bad News Campaign

Target didn't just ignite a media frenzy—it stoked the flames over a period of several months, by fueling ongoing news stories and releasing new updates regularly. The Target breach essentially grew into a bad multimedia marketing campaign, complete with regular email, social media, and television and magazine spotlights. This was the exact opposite of Visa's sage advice for handling a breach, which it had distributed to merchants for years: "Make it a one-day story. By communicating early and delivering on promised updates, the company reduces the chances the media may make more of the story than it might deserve."[141]

As the crisis wore on, Target unintentionally gave reporters incentives to investigate, by obviously hiding information and repeatedly making misleading or even false statements. For example, on December 24, *Reuters* reported that the "hackers who attacked Target Corp. . . . also managed to steal encrypted personal identification numbers (PINs), according to a senior

139. James Lyne, "Target's Latest Failure and How to Spot a Scam," *Forbes*, January 7, 2014, https://www.forbes.com/sites/jameslyne/2014/01/07/targets-latest-failure-and-how-to-spot-a-scam.

140. Lyne, "Target's Latest Failure."

141. Visa, *Responding to a Data Breach*.

payments executive familiar with the situation." This contradicted Target's earlier statement that there was "no indication that debit card PINs were impacted."[142]

Upon hearing *Reuters*' claim, Target dug its heels in, insisting that "no unencrypted PIN data was accessed" and that PIN data had not been "compromised."[143] Then, three days later, the company issued another press release, admitting that "strongly encrypted PIN data was removed" from its network, in addition to the card numbers themselves.[144] The reversal set off another media frenzy and added to widespread mistrust and the perception that Target was either incompetent or dishonest.

"The harder a journalist has to work to dig up the information about your breach, the more value the reporter and his/her editors will place on the story—and this will be reflected in where it is played and how long it is considered newsworthy," explained the Visa guide for merchants.[145] The stolen PIN announcement was newsworthy because of the new information, but it became scandalous because Target apparently tried to cover it up.

Let's take a look at how Target's breach developed into multiple storylines during the first few weeks following the breach:

- Target's initial lack of response to Brian Krebs ensured that he would publish his article without their input. Target then fumbled its original announcement the next day and followed up with multiple multimedia communications in the subsequent days, unnecessarily giving reporters more fodder, spread out over time.
- By late December, several states—including New York, Connecticut, South Dakota, and Massachusetts—had all issued public statements regarding the data breach and opened investigations. In response, Target's general counsel, Tim Baer, held a conference call with attorneys general from several states. The state investigations themselves were considered newsworthy. The *Wall Street Journal* reported on the call, including that a follow-up call was scheduled for the beginning of January, after the holidays.[146] Legislators (such as U.S. Senator Chuck Schumer) held press conferences in response to massive public outcry regarding the breach.
- Days before the new year, Target revealed that encrypted PINs had also been stolen, reversing earlier statements. This fueled a general lack of trust and incentivized reporters to dig even more.

---

142. Jayne O'Donnell, "Target: PINs not Part of Stolen Credit Card Info," *USA Today*, December 19, 2013, https://www.usatoday.com/story/money/personalfinance/2013/12/19/target-credit-debit-card-data-breach/4125231.

143. Jim Finkle and David Henry, "Exclusive: Target Hackers Stole Encrypted Bank PINs - Source," *Reuters*, December 25, 2013, https://www.reuters.com/article/us-target-databreach/exclusive-target-hackers-stole-encrypted-bank-pins-source-idUSBRE9BN0L220131225.

144. David Goldman, "Target Confirms PIN Data was Stolen in Breach," *CNN Tech*, December 27, 2013, http://money.cnn.com/2013/12/27/technology/target-pin/index.html.

145. Visa, *Responding to a Data Breach*.

146. Sara Germano and Robin Sidel, "Target Discusses Breach with State Attorneys," *Wall Street Journal*, December 23, 2013, https://www.wsj.com/articles/target-discusses-breach-with-state-attorneys-1387842976?mg=prod/accounts-wsj.

- On January 10, 2014, Target revealed that in addition to the 40 million payment card numbers, personal information (name, address, phone, email address) for up to 70 million customers had also been exposed.[147] According to Target, a range of 70 million to 110 million people were affected, in total.[148] The news sent another round of shock waves across the nation. Stock prices, which had been fairly steady since the new year, dropped—leading to even more news stories.
- In an effort to repair Target's image, CEO Gregg Steinhafel gave a much-touted, exclusive interview to CNBC. Excerpts from the 30-minute interview ran throughout the day on Monday, January 13, 2014, from the 6 a.m. "Squawk Box" all the way through the Nightly Business Report.[149]
- In response to widespread anger and distrust, Congress held multiple hearings on the Target breach, including testimony from CFO John Mulligan. The FTC likewise opened an investigation.

Bad news continued to leak out, drop by drop, into a torrent of media activity.

Tip: Be Boring

Major data breaches can turn into major news campaigns if you're not careful. By hiding information, and even reversing statements, Target gave journalists the impression that there was dirt to dig up if they put in the effort. Then, conversely, Target flooded the press with statements, updates, and videos that all came out at different times, feeding the media frenzy.

Reduce media interest in your data breach story by publishing information all at once (at least, to the greatest extent possible). Consider disclosing information that might otherwise be found by investigative journalists, so as to not leave any incentive for reporters to dig for a scoop. In this way, you can minimize the risk that your data breach will turn into a bad news campaign.

7.3.3.8 Media Leaks

Smelling a juicy story, major news outlets responded by putting together investigative teams. Target's employees (past and present), vendors, law enforcement, and contractors seemed all too happy to squeal.

Investigative journalists from Bloomberg's *Businessweek* reportedly "spoke to more than 10 former Target employees familiar with the company's data security operation, as well as eight people with specific knowledge of the hack and its aftermath, including former employees, security researchers, and law enforcement officials." These sources revealed a series of unflattering

147. Target, "Target Provides Update on Data Breach and Financial Performance," press release, January 10, 2014, https://corporate.target.com/press/releases/2014/01/target-provides-update-on-data-breach-and-financia.

148. Elizabeth A. Harris and Nicole Perlroth, "For Target, the Breach Numbers Grow," *New York Times*, January 10, 2014, https://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html

149. CNBC, "CNBC Exclusive."

details, which Bloomberg's staff leveraged to put together their "Missed Alarms" exposé. "The story they tell is of an alert system, installed to protect the bond between retailer and customer, that worked beautifully. But then, Target stood by as 40 million credit card numbers—and 70 million addresses, phone numbers, and other pieces of personal information—gushed out of its mainframes."[150]

Similarly, the *Wall Street Journal* seemed to have no problem lining up sources to get the inside scoop on the Target breach. "The new details, culled from interviews with former Target employees, people with knowledge of the post-breach investigation and others who work with large corporate networks, show that the breach wasn't entirely a bolt from the blue, but instead a sophisticated attack on a known point of vulnerability," the newspaper wrote in its February 2014 report.[151]

Even worse, Krebs was able to get a copy of Target's highly confidential internal penetration testing report, produced by Verizon in the weeks following the breach, and used it to produce a damning takedown. "The results of that confidential investigation—until now never publicly revealed—confirm what pundits have long suspected: Once inside Target's network, there was nothing to stop attackers from gaining direct and complete access to every single cash register in every Target store," Krebs revealed. "Target commissioned the study 'in anticipation of litigation' from banks that might join together to sue the retailer in a bid to recoup the costs of reissuing cards to their customers."[152]

Target, it was clear, did not have control over its media communications. It is normal for the media to come knocking when a major PR incident occurs. While leaks do happen, it's rare for so many individuals to willingly share ugly details with reporters. This behavior indicates a lack of loyalty to the company and can also stem from a lack of training and weak "security culture"—issues that also may have contributed to the breach itself. Human resources are an essential part of every organization's information security program. The evidence suggests that at Target, this fact was overlooked.

Tip: Control Your Media Communications

It is absolutely critical to control your organization's communications in the aftermath of a breach. When there's a story of interest, journalists may target any person in the organization for details, from the low-level IT staff to your highest-paid executives.

Before a crisis hits, make sure to train your staff. Have a designated point of contact for the media, and make sure everyone knows who it is. Consider printing small cards or posters to hang throughout the building with key contact information in the event of a crisis. Make sure everyone knows not to speak to the media and to refer callers to the designated contact. Include key information in regular employee training.

The time to have these conversations is *before* the crisis hits. Afterwards, all bets are off.

150. Riley, Elgin, Lawrence, and Matlock, "Missed Alarms."

151. Yadron, Ziobro, and Barrett, "Target Warned of Vulnerabilities."

152. Krebs, "Inside Target Corp."

7.3.3.9 Malware Leaks

Target didn't know it, but its technical staff accidentally leaked highly sensitive information to the public, even before the breach was publicly announced. This would later come back to haunt the company.

On December 11, someone uploaded a sample of malware from a Target server to the VirusTotal analysis service. Users around the world upload malware to VirusTotal, which runs automated threat analysis tools and then provides reports of the results. In all likelihood, one of Target's technical staff (or a third-party analyst) discovered the infected "exfiltration" server and uploaded the malware to see what it was. VirusTotal maintains vast libraries of malware and reports, which security professionals can leverage to diagnose issues on their own networks.

The problem is that VirusTotal does not keep uploaded malware samples confidential. Instead, the organization shares its databases of malware with many organizations—and malware can contain very revealing information. Dell Secureworks researchers obtained a copy of the malware uploaded from Target and found that it was used to transfer batches of stolen payment card numbers from the criminals' internal staging server to a system outside Target's network. The malware contained the internal Target server IP address, a key process name, and various other details that enabled the researchers to pinpoint installation dates and likely times of exfiltration.

Similarly, responders within Target apparently uploaded the POS malware to ThreatExpert on December 18, 2013. ThreatExpert, like VirusTotal, is a third-party service that analyzes malware samples and provides information to responders. ThreatExpert, too, shares its database with others. Researchers from Dell Secureworks obtained a copy of the Target POS malware, which was designed to scrape card numbers from memory and then periodically move them to an internal Target server. The researchers found that the malware contained the hard-coded IP address of Target's internal server, as well as the Windows domain name, user account credentials, and even a file containing a stolen credit card number. It is not clear precisely where the researchers obtained their sample of the malware, but the internal IP address and user account credentials were published in ThreatExpert's report on the malware.[153]

On January 14, 2014, Krebs blogged about the malware, having been tipped off by "a source close to the investigation."[154] Ten days later, Dell Secureworks published an in-depth analysis, revealing further technical details of the breach and further fanning the flames of media attention. Later, its whitepaper was cited by the Congress during that body's investigations into the Target breach.[155]

The moral of the story is that malware can be very revealing. Malware samples can contain sensitive information regarding a hacked organization's internal network configuration, accounts, and even snippets of stolen data. By analyzing timestamps from compiled malware samples, researchers can make educated guesses about precisely when and how an organization

153. Threat Expert, *Submission Summary*, January 8, 2014, https://krebsonsecurity.com/wp-content/uploads/2014/01/POSWDS-ThreatExpert-Report.pdf.

154. Brian Krebs, "A First Look at the Target Intrusion, Malware," *Krebs on Security* (blog), January 15, 2014, https://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware (accessed January 16, 2018).

155. U.S. Comm. on Commerce, Science, and Transportation, *"Kill Chain" Analysis*; Jarvis and Milletary, "Inside a Targeted."

was compromised. By viewing the upload time, they can tell when defenders might have discovered the malware and calcuate the length of time between detection and disclosure.

Tip: Carefully Evaluate Malware Analysis Services

Services such as VirusTotal and ThreatExpert can be very useful, but the information they provide comes at a price. Often, they share malware samples that users upload with third parties. In some cases, this can reveal sensitive information about when and how an organization was compromised.

All staff members who detect and analyze malware—including system administrators, security team members, and forensic investigators—should be trained to understand the tradeoffs of using third-party malware analysis services. It's important to consider what information you may be revealing when you share a malware sample with any third party. You may uncover details about the criminals who installed it, but you may also be sharing confidential or even damaging information about the organization you serve.

Carefully examine the terms of service for any malware analysis tools you use, and make sure you understand the potential for disclosure. Establish a clear written policy for malware analysis at your organization. Educate your investigators. By taking these precautions, you can reduce your risk of an unexpected media scandal.

7.3.3.10 Image of Incompetence

Throughout the Target breach, many stakeholders were left with the following negative perceptions:

- **Incompetence** - Target did not competently manage or oversee the company's cybersecurity program.
- **Lack of Character** - Target lacked courage and integrity.
- **Uncaring** - Target did not genuinely care about the welfare of the consumer more than its own profit margins and pocketbooks.

These things were not necessarily true, but throughout Target's response, its actions (or lack thereof) contributed to negative perceptions in all three of these categories. These perceptions undermined trust that stakeholders had in the organization. With the release of Steinhafel's videos and a concerted effort by the company's public relations team, some of these negative perceptions were corrected, but not all.

In March 2014, when Bloomberg released its exposé, consumers were still struggling to make sense of Target's reaction. Bloomberg's *Businessweek* editor John Tyrangiel went on television to analyze Target's breach response, in a segment that perfectly captured consumer sentiment.[156]

156. Bloomberg, "How Target."

"Incredible, the amount of time it took between the time that hack actually happened and when Target actually made a statement," opened the host. "Do we know why they were asleep at the wheel here?"

"Well, that's really the big mystery," responded Tyrangiel. The commentators reviewed the facts: Target had clearly invested a lot of money in cutting-edge security tools, far more than most retailers at the time. The company appeared to care about cybersecurity, and there were signs that it had the best intentions. "We found no one who said there was any kind of cover-up," emphasized Tyrangial.

The attack itself was nothing special; the host described it as "a very run-of-the-mill operation." The tools effectively alerted, and Target's team had multiple opportunities to stop the breach. After analyzing the facts, Tyrangial concluded:

"It's just gross incompetence." That was that. It was a verdict that was widely accepted. Yes, stakeholders expressed concerns about all three C's, including caring and character, but by March the overwhelming sentiment was that Target's team was simply not competent with respect to cybersecurity.

Unwittingly, Target had helped to create this image of incompetence through its bumbled public response. It wasn't the worst mistake for a retailer to make, but it did mean that to repair its image, a change of management would ultimately be required.

On May 5, 2014, Steinhafel "resigned" after 35 years with Target, in what was perhaps the earliest case in which the CEO of a major company was ousted in large part due to a data breach.[157] After fumbling the breach response out of the gate, Target's subsequent communications only inflamed the public and ignited negative media attention for months. By "humanizing" Target's breach communications with Steinhafel's image, he became a symbol of Target's cybersecurity failures. As a result, Steinhafel's resignation became the company's only path to recovery.

7.3.4 Home Depot Did a Better Job

In September 2014, just nine months after the Target breach, Krebs announced that Home Depot was investigating a breach—one that might have started in April or May and might be far larger than the Target breach. This time, Krebs' announcement included screenshots of a carding forum, rescator[dot]cc, where the Home Depot credit card numbers were being sold. Two weeks later, Home Depot revealed that 56 million payment cards had been compromised.[158]

Yet despite the massive scale of the breach, Home Depot largely preserved its reputation. The company's sales actually grew that quarter, exceeding analysts' expectations. Not only did CEO Frank Blake's reputation sustain the megabreach, he retired shortly thereafter and was lauded for his handling of the tough situation.[159]

---

157. The Street, "Target CEO Gregg Steinhafel Resigns Post-Customer Data Breach," *YouTube*, 1:45 min, posted May 5, 2014, https://www.youtube.com/watch?v=bKxyETHsdvc.

158. Kate Vinton, "With 56 Million Cards Compromised, Home Depot's Breach Is Bigger Than Target's," *Forbes*, September 18, 2014, https://www.forbes.com/sites/katevinton/2014/09/18/with-56-million-cards-compromised-home-depots-breach-is-bigger-than-targets.

159. John Kell, "Home Depot Shrugs Off Data Breach with Sales Growth," *Fortune*, November 18, 2014, http://fortune.com/2014/11/18/home-depot-earnings-breach.

"Home Depot's data breach is worse than Target's, so where's the outrage?" queried *MarketWatch*.[160]

The Target and Home Depot breaches were similar in many ways: Both were large retailers unexpectedly outed by Krebs. In both cases, tens of millions of payment card numbers were exposed (40 million and 56 million, respectively). But while Target's reputation—and sales—plummeted, Home Depot's did not.

To be sure, Home Depot had a leg up in a couple ways. First, the company's breach was announced in September—not December like Target, when holiday sales added an enormous urgency to the breach response. Second, by the time the Home Depot breach occurred, retail breaches were a dime a dozen. Many people had "breach fatigue."

Even so, there were other factors that likely had an even greater impact.

Home Depot launched a proactive consumer response. When Krebs contacted Home Depot about the breach, the company provided a straightforward statement. "I can confirm we are looking into some unusual activity and we are working with our banking partners and law enforcement to investigate," said spokesperson Paula Drake, who read from a statement (already prepared!) "Protecting our customers' information is something we take extremely seriously, and we are aggressively gathering facts at this point while working to protect customers. If we confirm that a breach has occurred, we will make sure customers are notified immediately. Right now, for security reasons, it would be inappropriate for us to speculate further—but we will provide further information as soon as possible."[161]

Hours later, Home Depot released a public message on its website, which was "mercifully free of mealy-mouthed corporate jargon," as *Fortune* magazine put it. Where Target referred obliquely to its "payment card issues" in its early messages, Home Depot shot straight from the beginning by disclosing a "possible payment data breach."[162] No doubt Target's lawyers believed they were protecting the company from harm by withholding details and carefully crafting each word, but as a result Target lost badly in the court of public opinion—a mistake that Home Depot did not repeat.

Home Depot also included an apology and immediate reassurance of credit monitoring in its very first press release, even before the breach was confirmed. "We know that this news may be concerning and we apologize for the worry this can create. . . . If we confirm a breach, we will offer free identity protection services, including credit monitoring, to any potentially impacted customers."[163]

Even more important, Home Depot immediately engaged a call center that was capable of handling 50,000 calls a day. According to news reports, the call volume never rose above

160. Catey Hill, "Home Depot's Data Breach is Worse than Target's, so Where's the Outrage?" *MarketWatch*, September 25, 2014, https://www.marketwatch.com/story/yawn-who-cares-about-home-depots-data-breach-2014-09-24.

161. Brian Krebs, "Banks: Credit Card Breach at Home Depot," *Krebs on Security* (blog), September 2, 2014, https://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/.

162. Target, "Message from CEO Gregg Steinhafel"; Home Depot, "Message to our Customers about News Reports of a Possible Payment Data Breach," *Home Depot Media Center*, September 3, 2014, https://web.archive.org/web/20140903143546/https://corporate.homedepot.com/MediaCenter/Pages/Statement1.aspx.

163. Home Depot, "Message to our Customers."

25% of the center's capacity, but CEO Frank Blake "preferred to be safe."[164] That meant that concerned customers could pick up the phone and talk to a human being, without the added frustration of long wait times experienced by Target customers.

"[Blake] took full responsibility, empowered his team to fix the problem, and kept the focus where it needed to be, squarely on the customer," reported *Fortune* magazine in an article entitled "How Home Depot CEO Frank Blake Kept His Legacy from Being Hacked."[165] By taking reponsibility, Home Depot was also able to issue a genuine apology, and take corrective action. Within weeks, Home Depot announced that it had "rolled out enhanced encryption of payment data" and was planning on completing its deployment of EMV card readers by the end of 2014.[166]

The Home Depot breach caused significant ripple effects that impacted banks and credit unions. For example, a study conducted by the Independent Community Bankers of America indicated that "the nation's community banks reissued nearly 7.5 million credit and debit cards at a total reissuance cost of more than $90 million as a result of the Home Depot data breach."[167]

Despite the impact, there was noticeably less consumer outrage during the Home Depot breach response compared with the Target breach. Why? Home Depot effectively preserved the 3 C's (Competence, Character, and Caring), told its story early and proactively, took responsibility, apologized, effectively listened, responded to customers seamlessly, and made amends. The result? Increased sales, and an even-more-respected CEO.

7.4 Ripple Effects

The Target data breach had ripple effects throughout the financial and retail sectors (indeed, throughout the world) that still reverbrate today.

7.4.1 Banks and Credit Unions

Financial institutions suffered immediate losses. In closed-door meetings throughout the United States, bankers grumbled about costs and exchanged notes on fraud.

Two months after the breach, the Consumer Bankers Association (CBA) and the Credit Union National Association (CUNA) jointly reported that their members' combined costs for card replacement exceeded $200 million.[168] This included replacement of 21.8 million cards, which represented only 54.5% of the 40 million card numbers stolen in the Target breach.

---

164. Jennifer Reingold, "How Home Depot CEO Frank Blake Kept His Legacy from Being Hacked," *Fortune*, October 29, 2014, http://fortune.com/2014/10/29/home-depot-cybersecurity-reputation-frank-blake.

165. Home Depot, "Message to our Customers."

166. Vinton, "56 Million Cards Compromised."

167. CBInsight, "Community Banks Reissue Nearly 7.5 Million Payment Cards Following Home Depot Data Breach," press release, December 18, 2014, http://do1.cbinsight.com/press-release/community-banks-reissue-nearly-7-5-million-payment-cards-following-home-depot-data-breach.

168. Consumer Bankers Association (CBA), "Cost of Target Data Breach Exceeds $200 Million," *National Journal*, February 18, 2014, https://web.archive.org/web/20140306224523/http://www.nationaljournal.com/library/113696.

These numbers do not include the cost of fraud or even the full cost of issuing cards through the end of the breach response. "Credit unions have replaced or will replace 85% of their cards affected by the Target breach at no cost to their members," said Bill Cheney, CEO of CUNA.

While some costs are easy to track and quantify (such as those for card replacement and fraud), others are more nebulous. For example, costs for increased customer support following a megabreach rarely get reported. A perfect example is J.P. Morgan Chase, which announced days after the Target breach that it would open some branches an extra day, a Sunday, to "assist customers through the last few days of holiday shopping." Undoubtedly, the bank had to pay additional labor costs and overtime fees to keep bank branches open an extra day (not to mention the loss of employee goodwill involved with suddenly requiring staff to work on the Sunday before Christmas).[169]

Here are some of the costs that financial institutions bore due to the Target breach:[170]

- Card replacement costs
- Member notification
- Losses due to fraudulent transactions
- Increased customer service costs
- Fraud monitoring
- Loss of customers / decline of new customers
- Promotional campaigns to rebuild trust

Where did the money come from? Target's settlements with issuing banks eventually totaled $67 million (Visa) and $39.3 million (Mastercard)—not even enough to cover the cost of reissuing the cards, let alone fraudulent transactions and other fees. A significant chunk of the settlement funds went to the card brands themselves. Also, financial institutions did not receive their share of the settlement funds for years after the breach occurred.

While card brands touted the "zero-liability" policy, the banks paid the price. As one banker wrote: "Most people do not realize that it is NOT Target or any other businesses that has endured the losses of this compromise or any compromise or fraud losses, but rather their bank that issued them the card that suffers the loss and stands behind our customers!"[171] Ultimately, banks and credit unions recouped those costs in the only way they could: by raising fees for consumers.

---

169. Sara Germano, "Target's Data-Breach Timeline," *Corporate Intelligence* (blog), *Wall Street Journal*, September 25, 2014, https://blogs.wsj.com/corporate-intelligence/2013/12/27/targets-data-breach-timeline.

170. Smart Card Alliance Payments Council, *The True Cost of Data Breaches in the Payments Industry* (White Paper PC-15001, Smart Cards Alliance, March 2015), http://www.emv-connection.com/downloads/2015/03/The-Cost-of-Data-Breaches.pdf.

171. Benchmarking & Survey Research/ABA, *Target Breach Impact Survey* (American Banker's Association, July 2014), 14, https://www.aba.com/Tools/Function/Payments/Documents/TargetBreachBankImpact.pdf.

7.4.2 Widespread Card Fraud

Once card numbers were stolen from Target, they quickly appeared on a carder shop, rescator[dot]la, run by Russian cybercriminal "Rescator," who has been traced to Ukranian resident Andrey Hodirevski.[172] In 2010, Hodirevski's personal web page listed his future goals, which included "World Domination ($ will probably have to rob all the banks in the world)."[173]

Financial institutions scrambled to stop the bleeding. Days after the Target breach was announced, Krebs teamed up with a local bank to explore the black market store, with the goal of finding and purchasing the bank's own cards. According to Krebs, Rescator's forum was "remarkably efficient and customer-friendly." The duo created an account on the site and funded it with $450 via wire transfer (other options included Bitcoin, Litecoin, WebMoney, and PerfectMoney, in addition to the more mainstream Western Union and MoneyGram).[174]

Card shops typically assigned "base names" to groups of card numbers stolen from the same merchant and often advertised the "valid rate" (i.e., the percentage of cards that had not been canceled by the banks). In December 2014, the Target cards had been uploaded under the base name "Tortuga" (tortoise), with a 100% valid rate. These "fresh" cards fetched a premium. Krebs and his colleague found that the prices for bank cards ranged from $26.60 to $44.80. Many of the Tortuga cards included a money-back guarantee, meaning that if the card was not valid at the time of purchase, it would be replaced or refunded.[175]

Importantly, the Target dumps were sold along with the city, state, ZIP code, and country of the store where the card number was stolen. This information was very helpful for fraudsters since banks often placed fraud alerts on cards limiting their use outside the cardholder's typical geographic region. With geographic information, criminals could monetize the data by creating cloned cards and using them in the cardholder's area, dramatically reducing the likelihood that the cards would be blocked.[176]

One thing the Target dumps did *not* include were CVV numbers, meaning the data was unlikely to be used for fraudulent purchases online.

Over time, the valid rate of the Target cards declined. The cards were sold under new base names, advertised with different valid rates. By mid-February 2014, Target cards (sold under the base name "Beaver Cage") advertised a mere 60% valid rate and sold for only $8 to $28. Figure 7-1 illustrates the falling validity rate for the Target cards over time. Note that this chart produced by Krebs is based on numbers advertised by the Rescator criminals. As Krebs himself pointed out, "[C]ertainly Rescator has a vested interest in fudging the numbers."[177]

---

172. Brian Krebs, "Who's Selling Credit Cards from Target?" *Krebs on Security* (blog), December 24, 2013, https://krebsonsecurity.com/2013/12/whos-selling-credit-cards-from-target.

173. Krebs, "Who's Selling Credit Cards."

174. Krebs, "Cards Stolen in Target Breach."

175. Krebs, "Cards Stolen in Target Breach."

176. Krebs, "Cards Stolen in Target Breach."

177. Brian Krebs, "Fire Sale on Cards Stolen in Target Breach," *Krebs on Security* (blog), February 19, 2014, https://krebsonsecurity.com/2014/02/fire-sale-on-cards-stolen-in-target-breach.

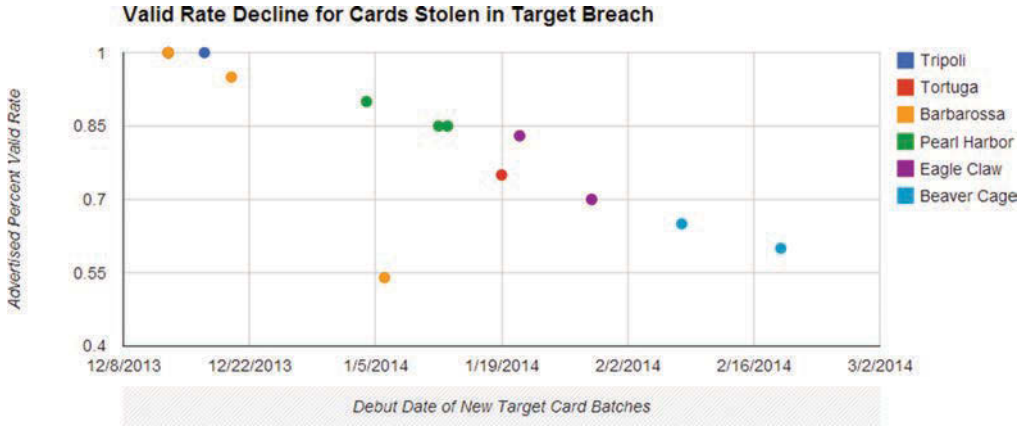


Figure 7-1. The valid rate of Target card dumps over time, advertised under different "base names" on the Rescator card forum. Source: Krebs, "Fire Sale on Cards."

7.4.3 To Reissue or Not to Reissue?

Many people are surprised to learn that banks and credit unions don't immediately reissue cards as soon as they're suspected stolen. The reason, of course, is that banks weigh the risk of fraud with the cost and hassle of reissuing.

According to an American Bankers Association survey, the average cost to reissue a debit card in the Target breach was $9.72, and the average cost to reissue a credit card was $8.11. This includes the cost of the card stock, postage, customer support, among other expenses. Small banks and credit unions paid the most ($11 to $13 per card); larger banks were able to leverage economies of scale and paid approximately $2 to $3 per card.[178]

Merchants, too, take a hit when cards are reissued—particularly those that rely on recurring autopays. One business owner complained, "At my gym, the most popular and profitable payment plan relies on customers signing up and paying monthly through automatic credit card payments. With each credit card breach, I'm losing customers and money."[179]

Consumers, too, are frustrated when their cards are canceled and have to be reissued. Larger banks are able to invest in on-site card printers, but many smaller ones can't afford that, and their customers have to wait for new cards to arrive in the mail. This gives larger banks a leg up on customer service in the event of a breach. After the Target breach, so many cards were reissued that there was a global shortage of card stock, further adding to the delays.

All of these factors create strong pressures for banks and credit unions *not* to reissue cards. Added to this is the fact that many cards stolen in a breach will never be used, particularly in a breach as large as Target where criminals have a massive number of cards to pick from.

178. Benchmarking & Survey Research/ABA, *Target Breach Impact Survey*.

179. Elaine Pofeldt, "Keeping Customers on Contracts Amid Credit Card Churn," CreditCards.com, June 30, 2014, https://www.creditcards.com/credit-card-news/keeping-customers-contracts-amid-churn-1585.php.

For many banks and credit unions in the Northwest United States, Target wasn't their biggest headache in late 2013. It was a company called URM, which processed payments for hundreds of stores in the region. Suddenly, on the week of Thanksgiving, customers got in line at the grocery store and were told to pay by cash or check. The payment processor had been breached, and POS systems for hundreds of stores were shut down on some of the busiest shopping days of the year.

"We didn't take many losses from Target even though there were *way* more compromised cards. The losses were from URM, because they were using that information right away," said Jason Kolberg, director of ERM and data management at Missoula Federal Credit Union. According to Kolberg, the smaller, more localized URM attack resulted in quicker fraud that hit local financial institutions especially hard.

There are ways to reduce the risk of fraud besides PIN changes, of course. Financial institutions and payment processors monitor cards for signs of fraud, such as sudden use outside the cardholder's region or other unusual patterns of behavior. These methods, of course, are not bullet-proof, but banks must weigh the uncertain risks of fraud if they do not reissue the card with the definite costs and hassle for the consumer if they do.

7.5 Chip and Scam

After the Target breach, there was widespread public anger. Consumers were upset. Merchants were upset. Banks and credit unions were upset.

Retailgeddon triggered widespread scrutiny of payment card system security. Recall that the payment card system is fundamentally insecure: You have a long number that you're supposed to keep very secret, but then you have to give it to lots of people in order to use it. The problem is obvious. For years, fraud had skyrocketed, and the card brands had continually pushed responsibility (and liability) down to banks and merchants, using the PCI DSS and contractual obligations.

At the same time, alternate payment solutions were taking off. PayPal was rapidly expanding its merchant services offerings, enabling consumers to pay at brick-and-mortar stores using their phones.[180] Less than a year after the Target breach, ApplePay was publicly launched, followed quickly by Samsung Pay and Android Pay. These solutions used tokenization and therefore removed the need for merchants to process payment card numbers. That meant that if alternate payment solutions were widely implemented, payment card breaches could become a thing of the past—at least, for merchants—and so would PCI DSS compliance.

The card brands moved swiftly to establish a different dialogue. In the aftermath of the Target breach, Visa and Mastercard proclaimed vehemently that the problem was that the United States was not using chip-and-PIN (EMV) cards like Europe. However, as we will see, EMV technology would not actually have helped Target or other retailers avoid a data

180. Verne G. Kopytoff, "PayPal Prepares to Expand Offline," *Bits* (blog) *New York Times*, September 15, 2011, https://bits.blogs.nytimes.com/2011/09/15/paypal-prepares-for-a-move-offline.

breach. The card brands owned the EMV technology and many patents related to it, and so they benefited from widespread adoption of "the chip."

Merchants poured their money into new POS terminals that supported EMV, instead of focusing on PayPal, ApplePay, and other alternative solutions that actually would reduce their risk of a breach (not to mention their compliance requirements).

To this day, the effects of the post-Target EMV push still linger. In this section, we will show how Retailgeddon led to the mass adoption of EMV technology, which in turn redirected funds that might otherwise have gone towards alternate payment solutions. As a result, payment card data breaches remain a widespread problem.

7.5.1 Alternate Payment Solutions

The best way to prevent payment card data breaches from occurring is to get rid of payment card data in the first place. Far from being a pipe dream, this was already being put into practice by PayPal and others at the time that Target was breached. Apple was preparing for the global rollout of ApplePay, which was poised to change the game.

When ApplePay launched in September 2014 (just weeks after the giant Home Depot breach), CEO Tim Cook called attention to the security benefits, saying: "We're totally reliant on the exposed numbers, and the outdated and vulnerable magnetic interface—which by the way is five decades old—and the security codes which all of us know aren't so secure."[181]

ApplePay and similar products allow consumers to pay by tapping their phone to the merchant's POS system. The phone and POS system communicate wirelessly via near-field communication (NFC). There is no need for the cardholder to swipe a terribly insecure magnetic stripe or hold up the line by waiting for a long EMV transaction. The merchant never receives the card number at all, so there is nothing to be stolen from the local POS system.

Logically, a mass migration to mobile payment systems that leveraged tokenization would have been smart. Merchants would no longer have to bear the risk of processing credit card numbers since they would never receive them. Consumers could even be protected by biometric authentication (such as TouchID on the iPhone), and conveniently they could use their phones to pay with any number of accounts.

7.5.2 Card Brands Push Back

The card associations had a different plan. Instead, they pushed harder for the world to adopt EMV (widely known as "the chip").

EMV cards are a type of "smart card" used to provide increased security and additional feature options for credit card transactions, such as improved support for offline transactions. "Smart cards" are what they sound like: cards that are "smarter" than old-fashioned magnetic stripe cards. They have a small computer chip built in. When used with a reader, the smart card can perform complex processes, such as cryptographic authentication.

Traditionally, in the United States credit cards included a magnetic stripe with encoded information. Magnetic stripe cards are quite easy to copy, and criminals routinely steal data

181. Shirley Li, "Apple Pay Might Just Make Mobile Wallets Finally Happen," *Atlantic*, September 9, 2014, https://www.theatlantic.com/technology/archive/2014/09/apple-pay-coin-softcard-google-wallet-might-just-make-mobile-wallets-finally-happen/379899/.

from the stripe and copy it onto new cards. This is particularly easy in restaurants, where the server can walk into a different room with the customer's card and copy it onto a machine. Criminals can also install credit card "skimmers" on top of the normal credit card slot at gas stations and other endpoint purchase devices.

EMV is widely used throughout Europe and has recently been more widely adopted in the United States. There are two common ways that users authenticate themselves with EMV cards: "chip-and-PIN" or "chip-and-signature."

- **Chip-and-PIN:** When a smart card is configured to use "chip-and-PIN," the user has to enter a PIN in addition to swiping the card at the time of purchase. The card cryptographically checks that the PIN is correct.
- **Chip-and-Signature:** With the "chip-and-signature" system, users do not have a PIN. They verify their identity (in theory) using a signature. However, since most merchants do not check the validity of the user's signature, this is a less secure method of authentication compared with chip-and-PIN.

7.5.3 Changing the Conversation

Just a few weeks after the Target breach was announced, Mastercard executive Chris McWilton released a statement:

"In the wake of the recent reported merchant data breach, chip technology has gained even greater interest and rightfully so. . . . Mastercard continues to believe that now is the time to migrate to EMV in the U.S."[182]

Visa, too, chimed in. "Visa is committed to ensuring our network operates at the highest level of security available and will continue to move the industry toward the adoption of new safeguards including EMV chip technology," said Visa's CEO, Charlie Scharf.

The card brands had already announced an October 1, 2015, deadline for U.S. merchants to switch to EMV-capable POS devices. After the Target breach, they advertised it with renewed vigor. The "liability shift," they emphasized, was not a mandate. Rather, any merchant that had not switched to using EMV would find themselves liable for certain types of fraud.

For example, if a criminal copied a card number to the magnetic stripe of a new card and swiped it in a merchant's non-chip-enabled terminal, the merchant would be liable for the fraud—not the banks. The rationale was that if there was fraud that EMV terminals could protect against, then the merchant would be left holding the bag since he or she chose not to use the available technology to prevent it.

7.5.4 Preventing Data Breaches . . . Or Not

EMV cards are far more difficult to clone than magnetic stripe cards because they contain a tiny computer chip. As a result, they can help to reduce certain types of fraud in which criminals make fake copies of cards and use them for in-store purchases.

182. Chris McWilton, "Customer Letter," Mastercard, January 8, 2014, https://newsroom.mastercard.com/wp-content/uploads/2014/01/C-McWilton-Customer-Letter-01-07-14.pdf.

However, *EMV does not reduce the risk of a data breach.* Criminals can still steal payment card information from the memory of a POS system, as was the case for Target and Home Depot. Once the card data is stolen, the number can be used for card-not-present purchases, and the data can still be copied onto a non-EMV card and used to make fraudulent purchases at retailers that accept magnetic stripe cards (which they all do).

As Krebs bluntly put it: Zero is "[t]he number of customer cards that Chip-and-PIN-enabled terminals would have been able to stop the bad guys from stealing had Target put the technology in place prior to the breach (without end-to-end encryption of card data, the card numbers and expiration dates can still be stolen and used in online transactions)."[183]

Studies have shown that EMV does not reduce fraud in general. In European countries, card-present fraud declined after EMV deployment—but card-not-present fraud went up.[184] Criminals simply used stolen card data to make online purchases instead of committing in-person fraud.

"EMV doesn't really help in any way regarding a data breach,"said Greg Buzek, president of IHL Group, a technology research firm that focuses on retail and hospitality. "EMV also does nothing to help keep online transactions secure."[185]

This begs the question: If EMV doesn't actually prevent data breaches or reduce fraud overall, then why did the card associations want it to be adopted after the Target breach?

7.5.5 Who Owns the Chip?

The card brands had another reason to push merchants to EMV: They owned it. The acronym itself stands for "Europay, Mastercard, and Visa," which were the three card brands that originally developed the standard. The brands formed a company, EMVCo, LLC (registered in the state of Delaware), to develop and manage the EMV standards. Today, EMVCo is owned by American Express, JCB, Mastercard, Discover, UnionPay and Visa. According to EMVCo's website, "EMV is a registered trademark or trademark of EMVCo, LLC in the United States and other countries around the world. Dating back to 1999, EMV refers to all of the specifications administered by EMVCo."[186]

According to a study published by IPWatchdog, as of 2015 Mastercard held the most EMV-related patents (22.3%). Visa held 4.5%. These card brands had a vested interest in forcing a mass deployment of EMV in the United States.

7.5.6 Public Opinion

Visa's and Mastercard's statements following the Target breach left the public with the mistaken impression that EMV would have helped prevent the breach and that Target was remiss by

183. Brian Krebs, "The Target Breach, By the Numbers," *Krebs on Security* (blog), May 6, 2014, https://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/.

184. Benjamin Dean, "What You Will Pay for a More Secure Credit Card," *Fortune*, October 1, 2015, http://fortune.com/2015/10/01/pay-secure-credit-card.

185. Glenn Taylor, "EMV 'Money Pit' Set to Cost Retailers $35 Billion," *Retail Touch Points*, July 24, 2015, https://www.retailtouchpoints.com/topics/pos-payments-emv/emv-money-pit-set-to-cost-retailers-35-billion.

186. "The Trademark Centre," EMVCo, accessed January 17, 2018, https://www.emvco.com/about/trademark-centre.

not having deployed it. "Consumers are also looking to EMV for renewed confidence in the payments system," reported CreditCards.com after the Target breach.[187]

Target itself was quick to perpetuate the EMV myth, spinning it as a nationwide failing. "I think what we've seen is vulnerability in our system," said the company's CEO, in his first interview following the breach. "In the United States, we're using mag-stripe technology. And that's old technology . . . there's a better way and it's called EMV technology. . . . And we think it's time for America to make that commitment to get to that standard."[188]

Under fire, Target quickly reacted by announcing that it would spend $100 million upgrading its POS systems to support EMV. "Still pushing to right itself after an enormous data breach by cybercriminals, Target announced on Tuesday that it would switch its debit and credit cards over to a more secure technology by early next year, most likely making it the first major retailer in the country to do so."[189]

Even though EMV wasn't an effective remedy for data breaches, the public bought the card associations' story hook, line, and sinker. This gave Target a straightforward way to proclaim its infrastructure "secure," thereby regaining the public's trust. It jumped on the bandwagon, spent the money, and "upgraded" to EMV.

7.5.7 Worth It?

Many observers questioned whether the shift to EMV was worth the cost. The National Retail Foundation estimated that the total cost to the industry would be $30 to $35 billion.[190] This included the costs of new equipment, software, certification fees, installation, and training, as well as the cost of $1.2 billion for new chip cards.[191]

EMV also hit merchants in the wallet in other ways. It took longer for consumers to pay using an EMV card, slowing the checkout process. "On average, it takes between seven to 10 seconds to pay using a chip card versus two to three seconds to pay using a traditional swipe credit card," explained Jared Isaacman, founder and CEO of Harbortouch, a POS system vendor.[192]

Merchants pushed back at the whole prospect of transitioning from magstripe to EMV, fearing longer lines and loss of sales. At ADA Bar in Chicago, server Michelle Szot broke down the numbers. "At a 300 [customers] a night blues bar, that's gonna suck . . . every four cards adds

187. Tamara E. Holmes, "Data Breaches Turn Spotlight on EMV Cards," CreditCards.com, February 7, 2014, https://www.creditcards.com/credit-card-news/data_breaches-spotlight-EMV_chip_cards-1273.php.

188. CNBC, "CNBC Exclusive."

189. Elizabeth A. Harris, "After Data Breach, Target Plans to Issue More Secure Chip-and-PIN Cards," *New York Times*, April 29, 2014, https://www.nytimes.com/2014/04/30/business/after-data-breach-target-replaces-its-head-of-technology.html.

190. David French, "Hearing on the EMV Deadline and What it Means for Small Businesses," *NRF*, October 7, 2015, https://nrf.com/sites/default/files/ChipAndPin-2015-SmallBusiness-HearingStatement.pdf.

191. "Retail's $35 Billion 'Money Pit': Product Overview," IHL Group, accessed January 17, 2018, http://www.ihlservices.com/product/emv.

192. Stacey Wescoe, "EMV Cards Could Slow Holiday Shopping Lines," LVB.com, accessed January 17, 2018, November 30, 2015, http://www.lvb.com/article/20151130/LVB01/311259997/emv-cards-could-slow-holiday-shopping-lines.

up to a minute," she said. "Every couple of seconds that gets tacked on is another drink you can't get served. . . . It's money that you could've made—it's money the bar could've made."[193]

Retailers were wary, to the point where many purposefully disabled chip readers during peak shopping times. The week before Christmas in 2015, just two months after the liability shift deadline, CVS disabled its EMV systems during checkout. "CVS probably wasn't the only retailer to do that," reported *Quartz* magazine. "[T]he solution for longer lines wasn't to make checkouts faster but to completely bypass the new security feature during the busiest shopping season of the year."[194]

PIN vs. Signature

Chip-and-PIN cards are very effective at reducing fraud because two-factor authentication is required for purchases. Criminals may steal the card data, but if they don't have users' PINs, they're out of luck. However, many U.S. businesses have valid concerns about implementing chip-and-PIN.

Many consumers find the added PIN annoying, particularly given that the average card owner has about three cards in his or her wallet, and many have multiple PINs to track.[195] More critically, at restaurants the gratuity has to be added to the total *before* the chip-and-PIN card is run, utterly changing the United States' long-standing dining custom. "With a traditional EMV device, the server will generally need to ask for the gratuity to be entered in advance of the card transaction," said Dave Miller, senior vice president of marketing at Buzztime. "This process eliminates the fraud potential of the server entering a higher tip amount after the patron signs their check, but can also be uncomfortable for the server and patron, diminishing the guest experience."[196]

The result is that most EMV cards issued in the United States are chip-and-signature, not chip-and-PIN—and as famously illustrated by writer John Hargave in 2006, a signature isn't good for much. Hargrave (co-creator of the early Internet humor site Zug.com) decided to test whether anyone was actually looking at his signature. Hargrave turned the signature block on this credit card receipt into a series of art projects, including Shamu the whale, a detailed picture of human intestines, and the phrase "I stole this card" (all of which were accepted, until a visit to Circuit City when he tried to buy a $16,800 television and signed in large letters, "NOT AUTHORIZED").[197]

(*Continues*)

193. Matthew Sedacca, "Chip Cards are Going to Ruin Your Night Out at the Bar," *VinePair*, August 17, 2016, https://vinepair.com/articles/the-new-credit-card-chips-are-a-disaster-for-bartenders-and-customers.

194. Ian Kar, "The Chip Card Transition in the US Has Been a Disaster," *Quartz*, July 29, 2016, https://qz.com/717876/the-chip-card-transition-in-the-us-has-been-a-disaster.

195. Stefani Wendel, "State of Credit: 10 Year Lookback," *Experian* (blog), May 20, 2019, https://www.experian.com/blogs/insights/2019/05/state-of-credit-2018-2/.

196. Sedacca, "Chip Cards."

197. John Hargrave, "How Crazy Would I Have to Make My Signature Before Someone Would Actually Notice?" Zug.com, April 28, 2007, https://web.archive.org/web/20070428090930/http://www.zug.com:80/pranks/credit.

(*Continued*)

Chip-and-signature is about as effective as just "chip" alone—essentially single-factor authentication (something you have), whereas chip-and-PIN provides two-factor authentication (something you have and something you know). Fraud rates will always be higher on chip-and-signature as a result—but in the United States, the customer experience is more important.

7.5.8 No Chip, Please Swipe

Consumers watched in confusion as retailers across the nation purchased new POS systems that sat on their counters, with little cards in the EMV slot that read "No Chip" or "Please Swipe." In many cases, these new devices sat, dysfunctional, for months or years.

This was especially perplexing because the new POS systems were expensive. Deploying a new POS infrastructure required investing in new equipment and labor. There was also apparently a shortage of equipment; retailers that ordered new POS devices in advance of the deadline found that there was a four-month wait simply to receive the devices.[198] Once the liability deadline passed, merchants were liable for certain fraudulent transactions that were conducted without EMV, and so they had strong incentive to immediately put the new features to use.

Mysteriously, thousands of new POS devices still sat on counters, with their EMV capabilities unused. They sat for so long that a new industry sprang up: manufacturers peddled cards to fit into EMV reader slots that said "Chip reader coming soon," and "Please swipe card instead!" These were touted as a "[s]imple reminder to customers that the chip reader is not functional."[199] Some vendors even offered customized cards featuring the merchant's logo.

Why?

7.5.8.1 EMV Certification Bottleneck

It turned out that upgrading to EMV systems wasn't so simple because every POS system had to be certified by EMVCo—which, not coincidentally, was owned by six major card brands. There were three levels of certification, the first two of which could be completed by the manufacterer of the POS device. Many merchants with more complex setups needed to be "level 3" certified, in which each of the card brands tests the integrated setup.

Certification itself could be an expensive process. "Usually, EMV certification involves an administrative fee (charged by acquirers), ranging between $2,000 and $3,000 for every formal test script run," explains online payment blog *Paylosophy*. "An average cost of EMV toolkit (which is used in every EMV certification) ranges from $10,000 to $30,000 per user license."[200] Each acquirer that processes cards charges its own fees and accepts only certain toolkits, so merchants can end up paying these fees multiple times.

198. Kar, "Chip Card Transition."

199. Chip Reader Messages, "Chip Reader Messages - 20 Card Set," Amazon, accessed October 1, 2018, https://www.amazon.com/Chip-Reader-Messages-Card-Set/dp/B01HSUF5Y0/.

200. "EMV Certification in a Nutshell," Paylosophy, accessed January 17, 2018, http://paylosophy.com/emv-certification-nutshell.

All of the POS manufacturers and software providers had to get their terminals certified, and the only company that did the certification was EMVCo. The result was a widespread backlog of certification requests. Providers also had to pay hefty fees to EMVCo just to start the process—fees that undoubtedly were passed along to merchants in the price of the products. The provider must also pay additional "renewal" fees to EMVCo regularly. The fee structures are listed in obscure PDF "bulletins" buried within EMVCo's website. As an example, currently the approval and renewal fees range from $5,500 to $6,000.[201]

After the devices themselves were certified, merchants then had to apply for their own level 3 certifications. In this complex process, merchants negotiate with each card brand and acquirer. The cost of level 3 certification varies depending on the size and complexity of each merchant's infrastructure, but reportedly can range from hundreds up to tens of thousands of dollars.[202]

Fuming about Gas Pumps

The EMV transition was tough enough for stores with checkout counters, but for businesses that had invested in more expensive devices such as ATMs or gas pumps, the price was exhorbitant. The deadline for ATM upgrades was eventually pushed to October 2016, and gas pumps to October 2017.

Many security professionals expressed concerns about the extension: "Because gas pumps are outside, exposed, and unattended, it's easy for criminals to attach card skimming devices and unobtrusively collect cardholder data. . . . Postponing the use of more secure EMV technology will allow fraudsters to continue victimizing consumers."[203]

7.5.8.2 Time Takes Its Toll

As merchants waited for EMVCo, card brands, and acquirers to slowly process the large volume of certification requests, the EMV liability shift deadline came and went. In California, two retailers filed a lawsuit against the card brands, claiming that "[c]ard fraud continued as merchants awaited certification. But because the EMV deadline shifted liability to the noncompliant party, that means that any fraudulent transaction in which a chip card was swiped because of a non-activated terminal fell on the shoulders of the merchants. The two plaintiffs complained they faced 88 chargebacks worth over $9,000 on top of a $5-per-transaction fee—a significant financial burden."[204]

---

201. EMVCo, "Card Approval Fee Change Notification," *EMVCard Type Approval Bulletin* 26, 4th ed., (October 2018), https://www.emvco.com/wp-content/uploads/documents/CTA_Bulletin_No_26_4th_Ed_-_CA_ApprovalFeeChangeNotification_20181005.pdf (accessed July 31, 2019).

202. "EMV Costs, Certifications and More: What You Need to Know Before the Migration," QuickBooks, accessed January 17, 2018, https://quickbooks.intuit.com/r/emv-migration/emv-costs-certifications-and-more-what-you-need-to-know-before-the-migration.

203. "Delayed EMV Liability Shift Brings More Harm Than Help," Chargeback911.com, December 9, 2016, https://chargebacks911.com/delayed-emv-liability-shift-brings-more-harm-than-help.

204. BI Intelligence, "Small Businesses are Moving Ahead with an EMV Lawsuit," *Business Insider*, October 10, 2016, http://www.businessinsider.com/small-businesses-are-moving-ahead-with-an-emv-lawsuit-2016-10.

In the spring of 2016, U.S. Senator Richard Durbin wrote a scathing letter to EMVCo, saying that "[t]he 2015 transition to EMV in the United States has been plagued by problems that have burdened retailers and consumers and hampered EMVCo's goal of reducing fraud. For example, many merchants that have purchased EMV card reader technology have been unable to use it because of backlogs in the EMV software certification process. Also, many consumers have been discouraged from using EMV cards because of the long amount of time the transactions take at the retail counter."

Senator Durbin cited the lack of "diverse stakeholder representation" in EMVCo's leadership as the underlying issue. "[C]onsumers, financial institutions, merchants, processors, technology companies, and smaller payment networks . . . do not have a meaningful vote in any EMVCo decisions," he wrote. In fact, in order for diverse stakeholders to have any representation at all, they have to sign up for the EMVCo subscriber service, which costs $750 for individuals or $2,500 for companies.[205]

"It appears that EMVCo is currently run by the big card networks for the big card networks," Durbin concluded.[206]

7.5.8.3 Draining Resources

A long-term effect of Retailgeddon was to spur the adoption of EMV technology. Ironically, the EMV rollout actually did little to reduce the risk of payment card data breaches. Instead, it redirected resources and attention away from technologies that might have actually helped.

"[Twelve] years ago when EMV was introduced into Europe it made tremendous sense," said Greg Buzek, founder of research firm IHL Group. "Today, it stands in the way of real data security by stealing critical budget away from focusing on the risks that retailers face from online hackers."[207]

By moving quickly and forcefully to push the adoption of EMV, the card brands successfully shifted public attention (and dollars) away from the alternative payment solutions. "Mobile commerce provides merchants with the opportunity to communicate with their customers and target and serve their most profitable and desirable consumers better with a solution that is potentially more secure than what exists today at the physical point of sale," observed Karen Webster, CEO of Market Platform Dynamics. "The deployment of EMV only forces them to divert attention and resources away from something that adds value to the consumer as well as the merchant and the overall payments system."[208]

---

205. "EMVCo Subscriber Programme," EMVCo, accessed January 17, 2018, https://www.emvco.com/get-involved/subscribers.

206. Dick Durbin, "Durbin Questions Whether Credit/Debit Card Chip Technology Rollout Is Adequately Protecting Competition & Consumers," Dick Durbin, U.S. Senator, Illinois (website), press release, March 17, 2016, https://www.durbin.senate.gov/newsroom/press-releases/durbin-questions-whether-credit-/-debit-card-chip-technology-rollout-is-adequately-protecting-competition-and-consumers; Dick Durbin, "Letter from Senator Durbin to Director of Operations Brian Byrne," Dick Durbin, U.S. Senator, Illinois (website), May 11, 2016, https://www.durbin.senate.gov/imo/media/doc/Letter%20from%20Senator%20Durbin%20to%20EMVCo%20Director%20of%20Operations%20Brian%20Byrne%20-%20May%2011,%202016.pdf.

207. "EMV: Retail's $35 Billion 'Money Pit,'" *BusinessWire*, June 3, 2015, http://www.businesswire.com/news/home/20150603006366/en/EMV-Retails-35-Billion-Money-Pit (accessed January 17, 2018).

208. Karen Webster, "6 Reasons to Call an EMV 'Time Out,'" PYMNTS.com, March 23, 2014, https://www.pymnts.com/news/2014/6-reasons-to-call-an-emv-time-out.

In October 2015, on the threshold of the EMV liability shift deadline, the National Retail Federation submitted a blistering statement to Congress, calling attention to the fact that the transition financially benefited the card brands and threatened their competitors:[209]

> If businesses can be forced to quickly install, at significant expense, the kinds of equipment that is most compatible with EMV Co.'s and the card companies' future business plans (EMV Card Personalization; Chip-based contact specifications—near field communications technology, etc.) then competitive alternatives, such as new mobile platforms (e.g. Starbucks-style payment programs) may effectively be locked out of the market.

It was clear that there was a conflict of interest within the payment card governance system that at times may have caused profits to supercede security.

7.6 Legislation and Standards

Retailgeddon spurred a flurry of legislative activity. Six congressional committees held hearings on data security and data breaches in the months following the Target breach. Due in part to the intense public scrutiny of Target's notification delay, there was a great deal of discussion regarding the lack of a national data breach notification law in the United States, which had resulted in a confusing patchwork of state laws. Several bills were introduced in the U.S. House and Senate that sought to establish proactive security standards, as well as a national data breach notification regulation.

Attorney General Eric Holder gave Congress a big push, publishing a video statement in which he called for national legislators to act.[210] The Federal Trade Commission, which opened an investigation of the Target breach, took the opportunity to push for an expansion of its authority to regulate cybersecurity. In March 2014, Chair Edith Ramirez testified before the Senate Committee on Commerce, Science, and Transportation. "Legislation in both areas—data security and breach notification—should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking authority under the Administrative Procedure Act," said Ramirez.[211]

None of the proposed federal legislation passed. Cybersecurity regulation had the potential to significantly increase risks and costs for businesses. While there was widespread support from consumers, businesses were tepid about the prospect. A federal breach notification standard

209. French, "Hearing on the EMV Deadline."

210. Tom Risen, "FTC Investigates Target Data Breach," *US News*, March 26, 2014, https://www.usnews.com/news/articles/2014/03/26/ftc-investigates-target-data-breach.

211. Federal Trade Commission, *Data Breach on the Rise: Protecting Personal Information From Harm* (Washington, DC: U.S. Senate, April 2, 2014), https://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.

could have greatly simplified breach response, but there were many questions about conflicts with existing state laws.[212]

The National Retail Federation, which was in a delicate position, reiterated its support for a national data breach notification standard[213] but cautioned that it was "wary of legislation that would create 'over-notification' standards that could desensitize the public from the most significant threats."[214]

Still, the move toward a national cybersecurity standard inched forward. In February 2014, the Obama administration announced the release of the Framework for Improving Critical Infrastructure Cybersecurity, developed by the National Institute of Standards and Technology (NIST).[215] The new framework was the result of a year-long initiative, which was launched a year prior with Obama's Executive Order on Improving Critical Infrastructure Security.[216]

The framework was not a federal regulation. It was not mandatory for any organization. Rather, it was an act of leadership that established a "common language to address and manage cybersecurity risk in a cost-effective way based on business needs."[217]

While the new NIST Cybersecurity Framework (as it was commonly referred to) had been "in the works" long before the Target breach was announced, its release in February 2014 could not have been better timed. There was widespread public support for cybersecurity initiatives and a clear need for a national standard. Over the next few years, many entities—from regulatory bodies such as the Securities and Exchange Commission and the Federal Financial Institutions Examination Council, to private businesses and nonprofits—began referring to the NIST Cybersecurity Framework and encouraging their communities to leverage it.

7.7 Conclusion

The Target breach represented a turning point for payment card data breaches. Whereas once merchants could expect their breaches to remain under wraps for weeks, months, or more, now they could be publicly exposed by the mainstream media even before they themselves knew what had happened. This shift was driven in large part by investigative journalist Brian Krebs, who

212. N. Eric Weiss and Rena S. Miller, *The Target and Other Financial Data Breaches: Frequently Asked Questions* (Report R3496, Congressional Research Service, February 4, 2015), https://fas.org/sgp/crs/misc/R43496.pdf.

213. Alina Selyukh, "New Hopes for U.S. Data Breach Law Collide with Old Reality," *Reuters*, February 11, 2014, https://www.reuters.com/article/us-usa-security-congress/new-hopes-for-u-s-data-breach-law-collide-with-old-reality-idUSBREA1A20O20140211.

214. Risen, "FTC Investigates Target Data Breach."

215. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* v.1.0 (Framework Paper, NIST, Washington, DC, February 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

216. Office of the Press Secretary, "Executive Order Improving Critical Infrastructure Cybersecurity," The White House, President Barack Obama (website), February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

217. NIST, *Framework*.

paved the way for reporting based on dark web research and tips from a cadre of banks and credit unions. This new model drove savvy retailers to adopt stronger crisis communications programs and invest in data breach prevention and response. Those that did not often paid a heavy price.

The massive fraud and card replacement costs caused by the Retailgeddon breaches triggered a widespread public outcry. The card brands quickly pushed the adoption of EMV as a solution, even though there was no evidence that it reduced the risk of large-scale data breaches. Instead, EMV drained resources from merchants who otherwise might have invested in newer payment technologies that were genuinely more secure. As a result, payment card data breaches remain an epidemic today. Ultimately, consumers paid the price and businesses suffered.

On the plus side, Retailgeddon brought cybersecurity to the forefront of public dialogue and spurred support for initiatives such as the NIST Cybersecurity Framework. It also brought to light the risks posed by supplier vulnerabilities and breaches, which we will discuss further in the next chapter.

Chapter 8

Supply Chain Risks

Google shocked the world in early 2010 when the seemingly invincible company announced that it had been hacked. "In mid-December, we detected a highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google," wrote Chief Legal Officer David Drummond. "However, it soon became clear that what at first appeared to be solely a security incident—albeit a significant one—was something quite different."

According to Drummond, Google wasn't alone. "[A]t least twenty other large companies from a wide range of businesses—including the Internet, finance, technology, media and chemical sectors—have been similarly targeted," he wrote. Sources close to the investigation later described how Google traced their stolen data to exfiltration servers in Taiwan, where data belonging to the other companies was also discovered.

Over the next few weeks, major tech giants including Adobe, Yahoo, Rackspace, Symantec, and Intel, as well as defense contractors Northrup Grumman and Dow Chemical, were publicly implicated as victims.[1] There was evidence that at least 34 companies were targeted.[2] The series of attacks was dubbed "Operation Aurora" based on the presence of the word "Aurora" in the malware.

The Aurora breaches exposed the deep risks inherent in a highly interconnected world. The tech giants that reportedly fell victim supplied countless organizations with software and IT services. They were ubiquitous suppliers for all sectors: military, government, financial, health, manufacturing, and more. By compromising these tech companies, attackers could, in theory, threaten the security of an entire society.

Once the Aurora attackers wormed their way inside a tech giant, they sought access to repositories of intellectual property. Source code was reportedly chief among the stolen loot. This had serious implications not just for the hacked tech companies but for their customers. Attackers could use stolen source code to identify even more vulnerabilities or create copycat (perhaps infected) versions of products. Even more frightening, a malicious actor with access to a tech giant's source code repository could potentially *inject* malicious code, which, if undetected, could be deployed to customers worldwide. The thought was chilling.[3]

1. Ariana Eunjung Cha and Ellen Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say," *Washington Post*, January 14, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

2. Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies," *Wired*, January 13, 2010, https://www.wired.com/2010/01/google-hack-attack/.

3. Zetter, "Google Hackers."

As if to illustrate the point, the Aurora attackers had leveraged software supply chain weaknesses to break into the tech giants. They hacked into their targets using zero-day exploits for Adobe Reader and Internet Explorer—two software programs that were deployed on countless systems around the world. (Scandalously, it emerged that Microsoft had known of the vulnerability in Internet Explorer months earlier but chose not to issue a patch immediately, exposing customers to seemingly unnecessary risk.)[4]

The zero-day exploits were technically advanced and likely took deep pockets to develop. At the same time, they were delivered using common social engineering tactics: The attackers sent spear phishing messages to victims through email or chat. When a victim clicked a link or opened an infected attachment, it automatically installed a backdoor on his or her computer, giving attackers remote access.[5]

Google strongly implied that China was behind the attacks. In support, U.S. Secretary of State Hillary Rodham Clinton issued a pointed statement: "We look to the Chinese government for an explanation." By that time, China already had a well-known history of engaging in successful, highly funded, long-running cyberattacks, largely focused on government agencies and defense contractors.

As an early cloud storage provider, Google held data on behalf of its *customers*, including email, documents, personally identifiable information (PII), and far more. The Aurora attackers gained access to Google's intellectual property, as well as a small amount of *customer* data—a fact that could have resulted in major reputational damage had Google not taken an utterly brilliant approach to public relations.

Transcending a Breach

In a rare example of the "transcendence" image repair strategy, Google spun the breach as an international human rights issue. "A new approach to China," read its headline. According to Google's announcement, the attackers successfully accessed data associated with two Gmail accounts, although they obtained only limited information such as the email subject lines. Furthermore, Google reported that dozens of Gmail accounts belonging to "advocates of human rights in China" had been regularly accessed by unauthorized intruders—not (Google emphasized) because of a breach of Google's systems but because of malware or phishing scams aimed at the account holders, which presumably resulted in stolen passwords.

Dramatically, Google's announcement went on to describe how the wide-ranging cyberattack "goes to the heart of a much bigger global debate about freedom of speech" and made clear that Google was "no longer willing to continue censoring our results on Google.cn." As a result, Google ultimately shut down its operations in China.

(*Continues*)

4. Kim Zetter, "Microsoft Learned of IE Zero-Day Flaw Last September," *Wired*, January 22, 2010, https://www.wired.com/2010/01/microsoft-zero-day-flaw.

5. Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," *Wired*, January 14, 2010, https://www.wired.com/2010/01/operation-aurora.

(*Continued*)

In the eyes of the public, Google was a patriot, fighting the repressive Chinese regime and supporting human rights activists. Instead of seeing its reputation tarnished, Google emerged from its data breach unscathed—perhaps even better off.

Years later, a very different picture of the Google hack emerged. According to David Aucsmith, the senior director of Microsoft's Institute for Advanced Technology in Governments, the Aurora hackers (who also targeted Microsoft) were not motivated by "issues of human rights and repression." Instead, said Aucsmith, "[w]hat we found was the attackers were actually looking for the accounts that we had lawful wiretap orders on." The hack was likely part of a counterintelligence operation, which enabled the Chinese government to determine which of its spies had been detected by the U.S. government.[6]

Until Aurora, companies outside of the defense sector largely considered themselves immune from nation-state attacks. The fact that the technology sector had been targeted sent shock waves throughout the global IT community. Suddenly, everyone felt more vulnerable. "All I can say is wow. The world has changed," wrote George Kurtz, chief executive officer of McAfee. "These attacks have demonstrated that companies of all sectors are very lucrative targets."[7]

Operation Aurora was just the beginning of a rising tide of attacks on technology providers. It illustrated that:

- Supply chain risks are critically impactful; a single hacked company can threaten the security of all of its customers.
- Software vulnerabilities in a single product can lead to cascading compromises throughout the globe.
- Powerful technology companies are not invincible: indeed, far from it.
- Everyone is at risk.

Today, technology underlies every aspect of our global society, connecting suppliers and their customers in a massive, complex web. Supplier security risks can trickle down to customers, at times resulting in widespread data breaches. In this chapter, we will discuss how risks are transferred as a result of service provider access to customer IT resources and data. Then, we will analyze the risks introduced throughout the technology supply chain, including software and hardware vendors, and provide tips for minimizing the risk of a breach.

---

6. Kenneth Corbin, "'Aurora' Cyber Attackers Were Really Running Counter-Intelligence," *CIO*, April 22, 2013, https://www.cio.com/article/2386547/-aurora{cyber-attackers-were-really-running-counter-intelligence.html; Robert McMillan, "Google Attack Part of Widespread Spying Effort, *Computerworld*, January 13, 2010, https://www.computerworld.com/article/2522519/google-attack-part-of-widespread-spying-effort.html.

7. George Kurtz, "Operation 'Aurora' Hit Google, Others," *Security Insights Blog*, McAfee, January 14, 2010, https://web.archive.org/web/20100118082207/http://siblog.mcafee.com/cto/operation-"aurora"-hit-google-others/.

8.1 Service Provider Access

Service providers often have access to sensitive customer data or supporting IT resources in order to do their jobs. This access may be co-opted by criminals, or simply mismanaged, resulting in a data breach. Breaches of this type typically occur through one of the following vectors:

- **Data Storage** - Breach of the customer's data while it is stored in a service provider repository. (Note that discussion of cloud data breaches will be reserved for Chapter 13, "Cloud Breaches.")
- **Remote Access** - Misuse of third-party remote access credentials, or a breach that spreads across a third-party connection (such as a virtual private network [VPN]).
- **Physical Access** - Theft or unauthorized access to sensitive information, typically in the form of papers or storage media.

We will discuss each of these vectors in turn.

8.1.1 Data Storage

Nearly every organization relies on outside service providers that store and process data on their behalf. This includes attorneys, accountants, sales and marketing firms, IT providers, and more. When one of these service providers is breached, it jeopardizes the data of customers, as well.

The "Panama Papers" breach is a perfect example. At 2.6 TB, it was the largest data leak in history when it was first publicized in 2016. The documents were stolen from the Panamanian law firm Mossack Fonesca, which specialized in offshore financial services. The law firm's records contained the dirty secrets of many prominent world leaders, including politicians, celebrities, and business moguls, dating as far back as the 1970s. The exposed data contained more than 11.5 million documents (including emails, contracts, bank statements, databases, and more). "This is pretty much every document from this firm over a 40-year period," said Gerald Ryle, the director of the International Consortium of Investigative Journalists (ICIJ).[8]

The Panama Papers exposure breach was a wake-up call for the legal industry, which had largely skirted cybersecurity oversight up to that point. Suddenly, attorneys in firms around the world imagined the nightmare scenario where all *their* client data was leaked. Clients began scrutinizing firms more carefully, asking tough questions about their cybersecurity programs. Many organizations suddenly ramped up their supplier vetting programs, requiring law firms and other service providers to produce the results of security assessments and demonstrate that they were appropriately controlling risk.

8. J. Garside, H. Watt, and D. Pegg, "The Panama Papers: How the World's Rich and Famous Hide Their Money Offshore," *Guardian*, April 13, 2016, https://www.theguardian.com/news/2016/apr/03/the-panama-papers-how-the-worlds-rich-and-famous-hide-their-money-offshore; Andy Greenberg, "How Reporters Pulled Off the Panama Papers, the Biggest Leak in Whistleblower," *Wired*, April 4, 2016, https://www.wired.com/2016/04/reporters-pulled-off-panama-papers-biggest-leak-whistleblower-history.

Tip: Vet Your Suppliers

The risk of a breach trickles through your supply chain. To minimize this risk, make sure to carefully vet your suppliers' cybersecurity practices, both in the initial contract phase and on a regular basis (e.g., annually). Ideally, supplier assessments should be conducted as part of a formal program that includes the following components:[9]

- Establish supply chain risk management processes.
- Identify, prioritize, and assess suppliers using the established processes.
- Use contracts to implement appropriate measures.
- Evaluate suppliers to ensure they meet contractual requirements.

Today, many suppliers routinely undergo cybersecurity assessments, including both technical and nontechical components, in order to minimize the risk of a breach. Organizations may choose to conduct their own in-depth assessment of critical suppliers or require suppliers to conduct their own and provide results (in which case, the cost may be passed along to the customer in the form of higher prices). To minimize the effort involved in supplier vetting, consider requesting copies of vendors' existing third-party assessments or summaries.

8.1.2 Remote Access

Many suppliers have remote access to a customer's systems. In some cases, this access is fairly limited, for the purposes of submitting invoices or time sheets. However, as illustrated by the case of Target's HVAC vendor, Fazio Mechanical (described in Chapter 7, "Retailgeddon"), even limited access to IT resources can allow criminals to leap from one network to another and cause a data breach.

Some suppliers have extensive remote access to their customers' networks, in order to provide IT services or support equipment that they installed. Unfortunately, this access can be abused by criminals who steal the supplier's credentials or pivot through its network. For example, healthcare providers Athens Orthopedic and Midwest Orthopedic discovered they were breached in 2016, when a criminal gang held their data for ransom. According to the Midwest Orthopedic patient notification letter, "hackers . . . likely gained access into our secured database system through a third party contractor."[10] The Athens Orthopedic press release stated that "[t]he breach occurred when a hacker used the credentials of an outside contractor who performed certain services for the Clinic."[11]

---

9. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity* v.1.1 (April 16, 2018).

10. "Local Medical Group Involved in Computer Hack Identified," *Daily Journal Online*, July 27, 2016, http://dailyjournalonline.com/news/local/local-medical-group-involved-in-computer-hack-identified/article_1dfafa55-d3d5-54ba-98cf-bdccafeed7a0.html.

11. Athens Orthopedic Clinic, "Important News for Patients," accessed January 18, 2018, http://athensorthopedicclinic.com/important-news-patients.

Criminals may be able to use one hacked supplier to trivially breach many customers, using stolen passwords or targeted phishing attacks. Passwords stored in plain text files are, unfortunately, a common sight on computers of many service providers since they are an easy way to manage credentials for numerous customer networks. Suppliers may not have a better system for tracking and managing passwords for multiple customer accounts. The results can be devastating for the customers they serve.

Athens Orthopedic and Midwest Orthopedic are examples of how one supplier's insecurity can place many customers at risk of a breach. Security researcher "Dissent Doe" received a tip linking both clinics' data breaches to an "inadequately secured Quest Records LLC file on Dropbox," which contained passwords for all of the supplier's customer networks. Quest Records, in turn, admitted that it had suffered a "data security incident" and stated that the organization was cooperating with the FBI.

"[H]ow many other clients of Quest Records LLC may have had their patient information hacked or may still be at risk?" wrote Dissent, noting that "at least two previously unnamed entities are investigating whether that vendor's breach resulted in compromise of their patient information."[12]

Tip: Assess Supplier Remote Access

Supplier remote access is the single biggest cybersecurity risk for many organizations. To reduce the risk of a breach due to supplier remote access:

- **Ensure that suppliers have a secure password management system** to minimize the risk of password theft or insecure practices such as reuse.
- **Require suppliers to use two-factor authentication.** That way, a stolen password alone will not give criminals direct access.
- **Log and monitor vendor remote access** to quickly detect misuse or stolen account credentials.

8.1.3 Physical Access

Long before the term "data breaches" existed, suppliers introduced security risks due to physical access. Cleaning staff often have unsupervised access to sensitive information after regular staff have gone home. Security guards, delivery personnel, and other providers may have greater access to information than most people realize, often during times they are largely unsupervised. Daytime employees may forget that third parties have extensive access to their desks and cabinets at night and leave sensitive information unlocked or visible.

In a classic example of a physical data breach, police arrested seven members of an identity-theft ring in March 2010, after they stole the identities of up to 250 patients of

12. Dissent, "Quest Records LLC Breach Linked to TheDarkOverlord Hacks; More Entities Investigate If They've Been Hacked," *DataBreaches.net* (blog), August 15, 2016, https://www.databreaches.net/quest-records-llc-breach-linked-to-thedarkoverlord-hacks-more-entities-investigate-if-theyve-been-hacked.

Northwestern Medical Faculty Foundation in Chicago. A janitor who worked at night stole personal information from patient files and passed it along to her conspirators. According to Cook County Sheriff Tom Dart, the thieves would then "go online and either apply for credit cards or request that person's credit report be mailed." Ultimately, the criminals made more than $300,000 of fraudulent purchases using patient accounts, including furniture, electronics, appliances, and jewelery.

Tip: Manage Physical Access

Physical data breaches are a long-standing problem that information security teams often overlook. As NIST cautions: "There should be no gap between physical and cybersecurity."[13] To reduce the risk of a physical breach caused by a supplier:

- **Implement a "clean desk/clear screen" policy** to ensure that sensitive information is inaccessible when unattended.
- **Take appropriate physical security precautions, even within the interior of facilities.** Lock up sensitive data, make sure keys and other access devices are properly secured, and install cameras and other monitoring systems where appropriate.
- **Conduct background checks of suppliers with access to facilities.** All third-party personnel with trusted access should be individually identified and carefully vetted.

8.2 Technology Supply Chain Risks

As we have seen, technology can act as a conduit for risk, allowing threats to spread from service providers to their customers. At the same time, technology *itself* can introduce risk. Software and hardware can contain exploitable vulnerabilities, backdoors, and malware, which are unknowingly installed in customer organizations around the world. Malicious actors may deliberately hack into technology companies to introduce vulnerabilities or malware into products at the source. What's more, technology companies depend on *other* technology companies, resulting in risk that cascades throughout the supply chain.

In this section, we will explore the complex topic of technology supply chain risks, including software and hardware vulnerabilities, and targeted attacks on technology companies.

8.2.1 Software Vulnerabilities

Software is ubiquitous and global. All software has bugs; some bugs lead to vulnerabilities; and some vulnerabilities lead to data breaches. Many software products are deployed on a massive

13. National Institute of Standards and Technology (NIST), "Best Practices in Cyber Supply Chain Risk Management," U.S. Department of Commerce, September 2015, https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf.

scale, meaning that a single software vulnerability can result in a data breach of countless organizations around the world.

8.2.1.1 Bugs and Breaches

Industry experts estimate that programmers introduce, on average, 15 to 50 bugs for every 1,000 lines of code.[14] Strong training and testing processes can reduce the number of bugs that actually make it into production software, but at significant cost—so the number of bugs is rarely, if ever, zero. These remaining bugs lurk in production software, undetected, until someone (friend or foe) discovers them.

A certain percentage of these vulnerabilities can be leveraged by criminals to gain unauthorized access to system resources. When a new vulnerability is publicized, "black hat" developers spring into action and quickly develop modules and malware that leverage it. This new functionality can make existing exploit kits more potent or spur the development of wholly new malware.

Exacerbating the issue is the fact that some cybercriminals specialize in uncovering software vulnerabilities for profit. Highly technical hackers around the world search constantly for "zero-day" vulnerabilities (vulnerabilities that are not yet known). When found, zero-day vulnerabilities may be sold to the highest bidder or stockpiled for use in a later attack.

Tip: Prepare for Zero-Day Attacks

Breach response teams should treat all systems as though they contain zero-day vulnerabilities because they almost certainly do. While a proactive, patch-forward approach is ideal, a strong monitoring and network-based detection process is key to addressing risk. Ideally, you want to detect potential breaches in the prodromal phase, or at least nip them in the bud as early as possible. To accomplish this, you should:

- **Implement network-based detection mechanisms and monitoring** to detect exploits for systems you may not even know are vulnerable.
- **Coordinate closely with IT administrators and risk management teams** to help determine software patching priorities and develop compensating controls.
- **Ensure that there is a software inventory and patch management system in place** for all applications, and third-party vendor updates are proactively tracked and managed.
- **Receive alerts regarding critical vulnerabilities and updates** that affect your organization's risk.

8.2.1.2 Scaling Up

Vulnerabilities are all the more powerful when they exist in software that is replicated on a massive scale, in millions of computers, phones, and Internet of Things (IoT) devices around

14. Steve McConnell, *Code Complete: A Practical Handbook of Software Construction*, 2nd ed. (Seattle: Microsoft Press, 2004).

the world. In these cases, a single bug can result widespread, cascading data breaches. The issue of cascading security failures first came to light in the early 2000s, when malware such as Slammer and Nimda spread across millions of computers at lightening speed, overloading networks and causing widespread outages. Security experts sounded the alarm. "[T]hese worms did not have to guess much about the target computers because nearly all computers have the same vulnerabilities," observed Dr. Dan Geer and his colleagues in their famous "monoculture" paper.[15]

Fast-forward nearly two decades, and the same problems exist today. The "EternalBlue" exploit, which was leaked from an National Security Agency (NSA) cyberweapons arsenal, was quickly leveraged by attackers to spread the WannaCry ransomware through critical networks in more than 74 countries. "[WannaCry] is reportedly causing disruptions at banks, hospitals, telecommunications services, train stations, and other mission-critical organizations in multiple countries," reported Dan Goodin of *Ars Technica*.[16] The same single exploit was later used to spread the infamous Emotet banking Trojan, the "NRSMiner" cryptominer, and countless other malware infections that in many cases led to data breaches.

Tip: Prepare for Large-Scale Vulnerabilities

Large-scale vulnerabilities quickly translate into large-scale attacks when they become publicly known. Reduce your risk of a breach after a large-scale vulnerability (such as EternalBlue) is announced by taking the following steps:

- **Expect attackers to quickly develop sophisticated payloads.**
- **Fast-track your organization's response.**
- **Patch affected systems as quickly as possible.**
- **If you can't patch right away, make sure your response team is aware of elevated risk.**
- **Implement additional network-based detection and protection mechanisms to identify attacks on vulnerable systems.**

8.2.1.3 Patch Problems

The solution to preventing breaches due to software vulnerabilities may seem simple—patch affected systems—but it isn't that straightforward. First, vulnerabilities have to be discovered and reported to the vendor before they can be patched. This alone may be a challenge, particularly when a strong underground market exists for finding zero-day vulnerabilities.

---

15. Dan Geer et al., "CyberInsecurity: The Cost of Monopoly," *Computer & Communications Industry Association Report*, September 24, 2003, https://www.schneier.com/essays/archives/2003/09/cyberinsecurity_the.html.

16. Dan Goodin, "An NSA-Derived Ransomware Worm Is Shutting Down Computers Worldwide," *Ars Technica*, May 12, 2017, https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/.

Even if a vulnerability is known to a vendor, that doesn't mean a patch exists (as the public found out when it was discovered that Microsoft had known about the Aurora vulnerability for months without issuing a patch). Vendors need to devote significant resources to diagnosing reported flaws and developing software patches. Software vendors have limited resources, like all organizations, and must prioritize their responses. The result is that there is always a delay between the time a bug is known and the time a patch exists. Hospitals, manufacturers, transit authorities, and many other types of organizations rely heavily on specialized third-party vendors, who can take months or years to evaluate and test a patch before pushing it out to customer systems. In some cases, a patch may never exist.

Even when a vendor has developed and distributed a software patch, vulnerable organizations may not deploy it right away, often due to resource constraints, compatibility concerns, or process issues. For example, nearly a year after Microsoft patched the "EternalBlue" vulnerability, Proofpoint discovered a cryptomining botnet containing more than 500,000 infected Windows computers, which still successfully used EternalBlue to spread. This is because IT teams around the world have to test patches and ensure they work with all of their software before deploying. In operationally sensitive environments, where uptime is critical, the risk of system changes may be high, and scheduling downtime to update systems can be a challenge.

The result is that when a widespread vulnerability is revealed, it is common for large numbers of computers to remain vulnerable for an extended time. Meanwhile, criminals use this delay to compromise systems around the world.

Tip: Patch Management

Everyone knows that patch management is important—but there are many hurdles to deploying them quickly and safely. Here are some tips for managing software updates:

- **Assign responsibility for receiving alerts** of critical patches for both operating systems and applications.
- **Prioritize software patches based on risk.**
- **Ensure that you have a formalized, effective process** for installing software patches throughout your organization.
- **Audit regularly** in order to catch systems that are missing patches, and verify that your program is working.
- **Consider moving away from complex or difficult-to-maintain onsite software** in favor of cloud applications that are maintained by a third party (when appropriate).
- **Segment your network** so that sensitive equipment and other systems that may be behind on patches are separated. This will reduce the risk of malware spreading from common workstations to vulnerable, more specialized devices.

8.2.2 Hardware Risks

Hardware devices, too, can be used to spread malware. For example, in 2015, Kaspersky Labs revealed that a shadowy organization known as the "Equation Group" (widely rumored to be the NSA's hacking team) had hacked popular hard drive firmware manufactured by Seagate, Western Digital, IBM, Toshiba, Samsung, and others. Infected drives were found in more than 30 countries. Targets included "government and military institutions, telecommunication companies, banks, energy companies, nuclear researchers, media, and Islamic activists."[17]

Once installed in a hard drive's firmware, the malware was capable of persisting even through hard drive reformatting and reinstallation. "The hardware will be able to infect the computer over and over," said Kaspersky researcher Costin Raiu. Furthermore, the malware could prevent disk sectors from being deleted or return malicious code instead of normal instructions upon boot.[18]

According to the researchers, one Equation Group hard drive worm was designed to map air-gapped networks and save data for exfiltration in a hidden area of the infected hard drive. When the hard drive was connected to a system that had access to the Internet, the worm would upload data to the attacker's command-and-control server.

In order to create the malware, Raiu insisted that the Equation Group must have had access to the manufacturers' proprietary source code. "There is zero chance that someone could rewrite the [hard drive] operating system using public information," he said. The NSA could have gained access to source code in a variety of ways, including through U.S. government software audits. The revelation also reignited concerns about the Aurora attacks in which the source code of major manufacturers was exposed.[19]

8.2.3 Hacking Technology Companies

Operation Aurora and subsequent attacks on Silicon Valley demonstrated that technology companies themselves could be targeted, raising the spectre that popular software could be compromised and used to gain access to many other organizations. Indeed, Operation Aurora seemed to indicate a new strategy for nation-state cyberwarfare, where technology suppliers were specifically targeted as part of long-term, well-funded, multistage attacks.

The effectiveness of this strategy was demonstrated shortly thereafter, when a breach of the popular security company, RSA, was linked directly to subsequent, successful hacks of the defense sector. At the time, RSA was the leading provider of two-factor authentication tokens. Its "SecurID" products were used to protect login interfaces used by 40 million organizations around the world, including U.S. Department of Defense (DoD) contractors and corporate banking customers. Since hardware tokens were more costly and labor-intensive

17. Joseph Menn, "Russian Researchers Expose Breakthrough U.S. Spying Program," *Reuters*, February 16, 2015, https://www.reuters.com/article/us-usa-cyberspying/russian-researchers-expose-breakthrough-u-s-spying-program-idUSKBN0LK1QV20150216.

18. Kaspersky Labs, "Kaspersky Lab Discovers Equation Group: The Crown Creator of Cyber-Espionage," press release, February 16, 2015, https://usa.kaspersky.com/about/press-releases/2015_equation-group-the-crown-creator-of-cyber-espionage.

19. Menn, "Russian Researchers."

to use than single-factor authentication, users of RSA's SecureID product typically had high-value accounts and were therefore willing to invest more in cybersecurity defense.[20]

RSA announced that it had been hacked in March 2011—but not in so many words. Then-CEO Art Coviello published an "Open Letter to RSA Customers" on the company's website. The letter's generic title belied its dramatic revelation: The renowned security company had been breached. Exactly what the attackers pilfered was a mystery; Coviello's letter vaguely revealed that the attackers "extracted" data that was related to the SecurID product line. Customers were left to wonder whether the core SecurID intellectual property had been compromised—and whether their own systems could be at risk as a result.[21]

In a painful blow, U.S. defense contractor Lockheed Martin was hacked two months later—and publicly blamed RSA. Lockheed confirmed to the press that its forensic analysts had concluded that the RSA breach was a "direct contributing factor" to the subsequent breach, allowing attackers to calculate or guess the six-digit one-time PIN that served as the second factor of authentication for a user's login.[22] Shortly thereafter, another major DoD contractor, L-3 Communciations, announced that it, too, had been targeted by attackers who were "leveraging the compromised information" from the RSA attacks.[23] It became painfully clear to the world that RSA's two-factor authentication products were compromised.

The future looked grim for RSA, as customers lost confidence in the company's flagship product line. Within days, RSA released another "Open Letter," offering to replace or monitor tokens for "customers with concentrated user bases typically focused on protecting intellectual property and corporate networks."[24]

This desperate move came at an enormous expense. "It was hell to live through what we did," said President Tom Heiser, months later. The company had to increase its production sevenfold in order to meet the demand for replacement tokens. The monitoring program alone cost $66 million.[25] RSA's outreach team implemented a crisis communications strategy, in which it contacted more than 60,000 customers, including more than 15,000 customers reached by phone, and more than 5,000 customers reached by conference calls and in-person meetings.

At the same time, highly targeted military units, government agencies, DoD contractors, and financial institutions scrambled to reissue tokens for all of their users—and meanwhile worked to manage their exposure.[26]

---

20. Riva Richmond, "The RSA Hack: How They Did It," *Bits* (blog), *New York Times*, April 2, 2011, https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it.

21. Dan Goodin, "RSA Breach Leaks Data for Hacking SecurID Tokens," *Register*, March 18, 2011, https://www.theregister.co.uk/2011/03/18/rsa_breach_leaks_securid_data.

22. Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *New York Times*, June 3, 2011, http://www.nytimes.com/2011/06/04/technology/04security.html.

23. Kevin Poulsen, "Second Defense Contractor L-3 'Actively Targeted' with RSA Secured Hacks," *Wired*, May 3, 2011, https://www.wired.com/2011/05/l-3.

24. Art Coviello, "Open Letter to RSA SecurID Customers," RSA, 2011, https://web.archive.org/web/20110701042640/www.rsa.com/node.aspx?id=3891.

25. Hayley Tsukayama, "Cyber Attack on RSA Cost EMC $66 Million," *Washington Post*, July 26, 2011, https://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html.

26. Nelson D. Schwartz and Christopher Drew, "RSA Faces Angry Users After Breach," *New York Times*, June 7, 2011, http://www.nytimes.com/2011/06/08/business/08security.html.

Extremely "Sophisticated" Cyber Attacks

Struggling to explain how they had been hacked, the Aurora victims, including Google, Adobe, and others, seized upon a common tactic: emphasize the extremely advanced, highly skilled nature of the attacks. In the ensuing media blitz, one word stood out: "sophisticated." As an image repair strategy, this served to effectively shift the burden of responsibility, making the breach seem like an uncontrollable event rather than the result of any negligence or oversight on the part of the victims. While this strategy had been used by some hacked organizations in the past, it became status quo in the Aurora attacks—and it was largely successful.

The concept of "advanced persistent threat" (APT) burst into the mainstream at the same time. Tech companies and journalists embraced it. The term was new to the public, it made commentators sound savvy, and it neatly fit with the key image repair strategy of portraying the attackers as extremely "sophisticated" adversaries.

A year later, RSA seized upon the same tactics following its breach. "Recently, our security systems identified an extremely sophisticated cyber attack in progress being mounted against RSA," wrote Coviello in the public notification. "Our investigation has led us to believe that the attack is in the category of an Advanced Persistent Threat (APT)." Yet again, the words "sophisticated" and "advanced persistent threat" had found their way into a data breach announcement. The attackers, the message implied, were so advanced that even a security company was no match for their powers.

8.2.4 Suppliers of Suppliers

The technology supply chain isn't really so much of a *chain*; it's more of a complex web, with technology providers highly dependent upon each other. Risk flows throughout the system in a nonlinear way. Aurora illustrated this poignantly; the tech giants were hacked using vulnerabilities in software they relied upon, which was in turn produced by other tech giants.

Software configuration management (SCM) systems are one example of a popular product that many tech giants rely on. Major software developers use SCM systems to manage and secure their source code repositories. The security of these systems is critical since source code is one of the crown jewels for many tech companies. Attackers who gain access to a tech company's source code can potentially make counterfeit or competing products, identify zero-day vulnerabilities to be used in future attacks, or insert backdoors for distribution to the victim's customers.

After the Aurora attacks, researchers from McAfee pointed out the importance of SCM systems in establishing risk throughout the entire software supply chain. A handful of SCM vendors are used by many tech giants. The researchers conducted a security analysis of the popular Perforce software, used by *Fortune* 1,000 companies.

Their findings were eye-opening. McAfee's researchers found major vulnerabilities in the widely used SCM software, including authentication bypass issues, lack of encryption, and other serious security issues.[27] The software giants' reliance on the same, widely deployed,

27. McAfee Labs and McAfee Foundstone Professional Service, "Protecting Your Critical Assets: Lessons Learned from 'Operation Aurora'" (white paper, McAfee, Santa Clara, CA, 2010), https://www.wired.com/images_blogs/threatlevel/2010/03/operationaurora_wp_0310_fnl.pdf.

vulnerable code management software introduced risks throughout the technology supply chain that most people had never considered before.

Tip: Implement Cascading Risk Management

When evaluating suppliers, ensure that each supplier manages risk of *its* suppliers. This may seem like a challenge, but it has been made easier now that supplier management is built into common cybersecurity and information management standards such as the NIST Cybersecurity Framework, ISO 27001, COBIT, and more.

Your organization can require suppliers to adhere to a common framework that includes risk management of their supply chain. By doing so, you can help reduce the risk introduced by your suppliers' suppliers.

8.3 Cyber Arsenals

Over the years, as technology matured and spread, exploits and vulnerabilties became a valuable commodity. It became clear that data breaches could be used to gain military, economic, financial, or political advantages. Governments, organized crime groups, and hacker consultants began to stockpile "cyberweapons" in order to facilitate hacking—only to discover that these dangerous caches, too, could be breached. When "cyber arsenals" were exposed, the effects rippled around the world.

The NSA's breach was a catastrophic example. Few people realized that the U.S. government maintained an arsenal of cyberweapons—until 2016, when a mysterious group called the "Shadow Brokers" emerged online, claiming to have hacked the Equation Group (recall from earlier that the Equation Group is commonly believed to be the NSA's hacking team). Over the coming months, the attackers dumped multiple caches of stolen data, including very effective exploits (such as the soon-to-be-infamous "EternalBlue,"), and "FuZZbuNch," a user-friendly tool that made it easy to launch exploits—similar to the publicly available Metasploit framework.[28]

The hackers weren't done. In the weeks that followed, the Shadow Brokers announced a subscription service that enabled buyers to receive new releases regularly. Prices started at approximately $21,000 per month.[29]

8.3.1 Weapons Turned

Cybercriminals greedily gobbled up the newly available hacking tools and incorporated them into the latest malware. Within weeks of the Shadow Brokers' releases, more than 200,000

28. Shadow Brokers, "Lost in Translation," *Steemit*, February 2017, https://steemit.com/shadowbrokers/@theshadowbrokers/lost-in-translation.

29. Swati Khandelwal, "Shadow Brokers Launches 0-Day Exploit Subscriptions for $21,000 Per Month," *Hacker News*, May 29, 2017, https://thehackernews.com/2017/05/shadow-brokers-exploits.html.

computers worldwide were already infected with malware based on the leaked cyberweapons. "Created at huge expense to American taxpayers, those cyberweapons have now been picked up by hackers from North Korea to Russia and shot back at the United States and its allies," reported Joseph Cox of *Motherboard* magazine.[30]

The leaked exploits weren't quite zero-days; Microsoft had released an update in March that patched the last four vulnerabilities. (Many speculated that Microsoft received an early heads up about the leaked material and rushed to close the holes in their software.) Still, multitudes of organizations didn't have time to test and deploy the new patches before virulent new malware emerged. Many systems remained vulnerable months and years later.

"The bloodbath will continue," said security professional Dan Tentler, CEO of Phobos Group. "It's going to get worse."

8.3.2 Calls for Disarmament

Tech companies were infuriated by the revelation that the NSA had stockpiled vulnerabilities rather than disclosing them to vendors. These vulnerabilities could be leveraged not just by the NSA but by any attacker that similarly uncovered them. Furthermore, when stockpiles of cyberweapons were leaked, as occurred with the NSA's cache, there was no easy way to deploy a fix that would protect the masses. The whole world was more vulnerable as a result.

Microsoft, as the manufacturer of the world's most popular operating system for PCs, stood in the crossfire of nation-state attacks. The worst of the NSA's leaked exploits affected the Windows platform, which undoubtedly caused massive headaches (and financial consequences) for Microsoft.

At the RSA conference in February 2017, Microsoft's president and chief legal counsel, Brad Smith, called on governments around the world to protect civilians from cyberweapons.

"What we need now is a Digital Geneva Convention," Smith said. "We need a convention that will call on the world's governments to pledge that they will not engage in cyberattacks on the private sector, that they will not target civilian infrastructure, whether it's of the electrical or the economic or the political variety. We need governments to pledge that, instead, they will work with the private sector to respond to vulnerabilities, that they will not stockpile vulnerabilities, and they will take additional measures."[31]

Smith laid out a six-point plan for such a convention:[32]

1. **No targeting of tech companies, private sector, or critical infrastructure.**
2. **Assist private sector efforts** to detect, contain, respond to, and recover from events.
3. **Report vulnerabilities to vendors** rather than stockpile, sell, or exploit them.

30. Joseph Cox, "Your Government's Hacking Tools Are Not Safe," *Motherboard*, April 14, 2017, https://motherboard.vice.com/en us/article/d7bvxa/your-governments-hacking-tools-are-not-safe.

31. Brad Smith, Transcript of Keynote Address at the RSA Conference 2017 "The Need for a Digital Geneva Convention" (Moscone Center, San Francisco, CA, February 14, 2007), 10, https://blogs.microsoft.com/wp-content/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

32. Smith, "Need for a Digital Geneva Convention."

4. **Exercise restraint in developing cyberweapons** and ensure that any developed are limited, precise, and not reusable.
5. **Commit to nonproliferation** activities to cyberweapons.
6. **Limit offensive operation** to avoid a mass event.

Despite the pressure from Silicon Valley, the call for disarmament did not appear to result in any significant cyber arms control agreement. The stockpiling of cyberweapons—and risk of breaches—continued.

Cyber Disarmament

The public debate over cyber arsenals in many ways mirrors the older debate regarding nuclear weapons. Global superpowers once rushed to develop nuclear weapons to defend against adversaries. Once developed, the weapons had to be carefully secured and managed—at great expense. Their simple existence increased the risk of mass destruction.

Ed Grothus was a key figure in the debate over nuclear disarmament. A former weapons technician who worked at Los Alamos National Laboratories (LANL) for 20 years, Grothos struggled with the ethics of his work developing nuclear weapons. After retiring from LANL, Grothos founded the Black Hole salvage yard. Here, he devoted much of his time to turning discarded lab equipment into art projects, such as a giant metal flower made out of discarded warheads. At the entrance to the Black Hole, vistors were greeted by a sign that read:

"No One is Secure Unless Everyone is Secure."

Grothos's sign was a powerful reminder that the existence of nuclear weapons increases risk for all. In much the same way, the existence of cyber arsenals increase risk for all. While stockpiles of cyberweapons can afford their owners a powerful advantage, it is not without cost.

Cyber arsenals are difficult to control. If one group has discovered a vulnerability, then it is possible others will stumble across the same flaw and take advantage of it. Furthermore, the risk of a data breach applies to all systems, including caches of malware and exploits. There is always a risk that such cyberweapons will be stolen or otherwise leaked, and used in unintended ways—perhaps even turned against their creators.

8.4 Conclusion

In today's interconnected world, the risk of a breach flows throughout our supply chain. Service providers transfer risks to their customers by storing and accessing data on their behalf. Technology providers, such as software vendors and hardware manufacturers, may unwittingly introduce vulnerabilities, backdoors, and malware into their supply chain. Cybercriminals, recognizing the power of upstream attacks, have engaged in long-term, multistage, targeted attacks on technology providers.

Organizations can no longer afford to ignore the risks posed by suppliers. To manage the risk of a breach, it's important to establish formal processes for vetting suppliers and ensure that they, too, formally manage cybersecurity risks.

Even the most mature vetting programs, however, are no match for nation-state-funded cyber arsenals. The breach of the NSA's cyberweapons cache fundamentally changed the risk of data breaches around the globe, releasing powerful cyberweapons that criminals immediately used to hack into computers around the world. Stockpiling vulnerabilities and exploits creates risk for all. Common organizations—from schools to hospitals to businesses—have been breached due to the release of nation-state cyberweapons, and this trend will continue as long as cyber arsenals exist.

In the next chapter, we will delve into healthcare breaches. Due to the specialized nature of medical equipment, healthcare organizations rely heavily on third-party suppliers for cybersecurity. They have also been hit hard by ransomware and data-stealing malware, in many cases due to EternalBlue and other leaked NSA cyberweapons—illustrating how supply chain cybersecurity breaches can have direct consequences for all of us.

This page intentionally left blank

Chapter 9

Health Data Breaches

Imagine if a photograph from your medical record was tweeted out onto the Internet, revealing your latest medical problem to everyone in the world. That's exactly what happened to NFL football player Jason Pierre-Paul after he injured his right hand in a fireworks accident.

After ESPN journalist Adam Schefter received a photograph of Pierre-Paul's hospital chart, he tweeted: "ESPN obtained medical charts that show Giants DE Jason Pierre-Paul had right index finger amputated today." The corresponding photos showed the operating room schedule and an excerpt of Pierre-Paul's medical record from Miami's Jackson Memorial Hospital.[1]

Pierre-Paul's team was unaware of his amputation until ESPN's tweet. Rumors of Pierre-Paul's accident and hand injury had been circulating for days, and as a result the New York Giants had retracted its offer of a long-term $60 million contract.

After the tweet with Pierre-Paul's medical record, a media storm ensued, with fans and journalists alike questioning the ethics—and legality—of Schefter's decision to publish the photographs.[2] Suddenly, the Health Insurance Portability and Accountability Act (HIPAA) was trending. Fans posted angry messages accusing Schefter of violating the federal law:[3]

> "@AdamSchefter WHAT are you doing with someone's confidential medical records? HIPAA might suggest you and @espn broke the law. #JPP #toofar"—Dane Oldridge (@TheREALCrankie1) July 9, 2015
>
> "@adamschefter Dumb move man. You better get your blog ready because you're not going to be on ESPN much longer. #HIPAA #Violation"—Aaron Stanley King (@trendoid) July 9, 2015

1. Matt Bonesteel, "Jason Pierre-Paul, Adam Schefter and HIPAA: What It all Means," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/early-lead/wp/2015/07/09/jason-pierre-paul-adam-schefter-and-hipaa-what-it-all-means.

2. Erik Wemple, "Twitter Stupidly Freaks about ESPN, Jason Pierre-Paul and HIPAA," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/blogs/erik-wemple/wp/2015/07/09/twitter-stupidly-freaks-out-about-espn-jason-pierre-paul-and-hipaa.

3. Eliot Shorr-Parks, "Did ESPN Violate HIPAA Rules by Posting Jason Pierre-Paul's Medical Records?" NJ.com, July 8, 2015, http://www.nj.com/giants/index.ssf/2015/07/did_espn_violate_hippa_rules_by_posting_jason_pier.html.

9.1 The Public vs. the Patient

Was Schefter's tweet a HIPAA violation?

For Jackson Memorial Hospital, the incident *was* almost certainly a HIPAA violation. HIPAA protects the privacy and security of protected health information (PHI). The groundbreaking federal legislation was passed in 1996, and subsequently the HIPAA Privacy Rule and HIPAA Security Rule were issued, with compliance dates of 2003 and 2005, respectively. HIPAA has dramatically improved the security and confidentiality of PHI held by "covered entities": heathcare providers, health plans, healthcare clearinghouses, as well as their "business associates" (people or organizations that work on behalf of a covered entity).

Jackson Health System took quick action. Chief Executive Officer Carlos A. Migoya immediately released an open letter stating: "[M]edia reports surfaced purportedly showing a Jackson Memorial Hospital patient's protected health information, suggesting it was leaked by an employee. An aggressive internal investigation . . . is underway. . . . If we confirm Jackson employees or physicians violated a patient's legal right to privacy, they will be held accountable, up to and including possible termination."[4]

9.1.1 Gaps in Protection

Yet Schefter and ESPN actually *hadn't* violated the federal law. "HIPAA doesn't apply to media who obtain medical records of others," said Michael McCann, legal analyst for *Sports Illustrated*. "Invasion of privacy does, but 1st Amendment offers a good legal defense"—particularly in cases involving public figures.

HIPAA's protections are limited—more so than most people realize. HIPAA and its cousin, the Health Information Technology for Economic and Clinical Health (HITECH) Act, are "downstream" data protection models, as described by Nicolas P. Terry, executive director of the Center for Law at Indiana University. "[W]hile upstream data protection models limit data collection, downstream models primarily limit data distribution after collection," writes Terry.[5] HIPAA/HITECH apply specifically to "covered entities" involved in the treatment and payment for healthcare services. They extend by contract to these entities' "business associates." The data by itself is not protected. Once health information escapes the confines of this very specific list of organizations—say, because of a data breach—there is little a patient can do to stop others from buying, selling, trading, or using it.

In Florida, Pierre-Paul sued ESPN and Schefter, citing violations of the Florida medical privacy statute. However, the defendents pointed out that "Florida's medical privacy law does not apply to the general public, including members of the media—it does not, as Plaintiff contends, essentially impose a world-wide prior restraint on the speech of any person who

4. Jackson Health Systems (@jacksonhealth), "This is a Statement from Carlos A. Migoya, President and CEO of Jackson Health System in Regards to Current Events," Twitter, July 9, 2015, 12:01 p.m., https://twitter.com/jacksonhealth/status/619219877518290951/photo/1.

5. Nicholas P. Terry, "Big Data Proxies and Health Privacy Exceptionalism," *Health Matrix* 24 (2014): 66.

allegedly learns some medical information from a Florida-based health care provider."[6] The district court concurred.

Pierre-Paul himself knew better than to accuse Schefter and ESPN of inappropriately reporting the *fact* of his amputation, proactively acknowledging that the information may have been "of legitimate public concern." However, he alleged that "the Chart itself was not," and that the publication of the actual photo from his medical record was an invasion of privacy.

"If the hospitalization of a public figure constituted authorization for the publication of that person's medical records, then the right to privacy would be non-existent," wrote Pierre-Paul's legal team in court documents. "Indeed, public figures would hesitate to seek medical treatment, or be less likely to share certain information with health care professionals, out of fear that hospital personnel would sell their medical records to those who want to profit from the publication thereof (as ESPN did here), thereby negatively impacting their health." Ultimately, Pierre-Paul and ESPN settled out of court, leaving several questions from their case unresolved.

9.1.2 Data Breach Perspectives

For Jackson Memorial Hospital, the Pierre-Paul disclosure was shameful, illegal, and cost two employees their jobs. For Schefter, tweeting Pierre-Paul's medical information was considered by many to be accurate, timely, and relevant journalism—particularly given the importance of Pierre-Paul's medical condition to his high-profile, public role. Regarding the photo of Pierre-Paul's medical chart, Schefter said, "[I]n a day and age in which pictures and videos tell stories and confirm facts, in which sources and their motives are routinely questioned . . . this was the ultimate supporting proof."[7]

In other words, the definition of a "data breach," and the repercussions that follow, depend not just on what specific data was leaked but where it came from and how it came to be disclosed. Typically, there is a *path of disclosure* along which successive custodians—some authorized, some not—obtain and transfer protected data. In many cases, the path looks more like a tree because a single custodian may transfer the data to many others.

The question of who is an authorized or unauthorized custodian is tricky. A hospital might consider a third-party IT provider to be an authorized custodian, even though a patient might object. In some cases, the good of the public or a third party might outweigh the importance of the data subject's privacy. The law often differs from the expectations of individuals along the path. As we will see, as data gets passed along, it can often seem like a game of telephone, where each data custodian imposes slightly different rules on the next party, and no one truly seems to be in control.

This has strange and confusing implications for data breach management. The same data may be exposed by two different organizations, but because they each have different

6. Jason Pierre-Paul v. ESPN, Inc, No. 1:16-cv-2156 (S.D. Fla. 2016), http://thesportsesquires.com/wp-content/uploads/2014/05/307369385-Espn-s-Finger.pdf.

7. Kevin Draper, "Jason Pierre-Paul Is Suing ESPN Because Its Reporting Was Too Accurate," *Deadspin*, September 8, 2016, https://deadspin.com/jason-pierre-paul-is-suing-espn-because-its-reporting-w-1785963477.

relationships with the data subject, one is a data breach and one is not (as in the case of Jason Pierre-Paul, Jackson Memorial Hospital, and ESPN). Responders need to carefully consider not just *how* to respond to a data breach but whether a specific event "counts" as a data breach at all. When it comes to health information, this has become a very complicated question.

In this chapter, we'll begin by covering the digitization of health information, which has paved the way for an increasing number of data breaches. We'll touch on relevant parts of the HIPAA/HITECH regulations, which define prevention and response requirements for certain types of health-related breaches. (For simplicity, the discussion in this chapter is focused primarily on the U.S. HIPAA/HITECH laws, but many of the same issues apply to health data protection regulations in other jurisdictions.)

Later in this chapter, we'll discuss the way data can escape from HIPAA/HITECH regulation or bypass it in the first place. We'll analyze challenges specific to the healthcare environment that contribute to the risk of data breaches, including complexity, vendor-managed equipment, a mobile workforce, and the emergence of the cloud. Finally, we'll enumerate the negative impacts of a breach and show how lessons learned from handling medical errors can help us resolve data breaches, too.

Personal Health Data

In this book, we define "personal health data" as any information that describes or can be used to deduce information relating to a person's health. This includes any kind of health-related data collected from an individual, including "protected health information" formally defined by HIPAA, as well as any medical information covered under state laws and health-related data that people share or collect using mobile apps, online health communities, and other personal health management tools.

"Health data" exists far outside the healthcare information ecosystem. Health data can be generated by:

- **Healthcare providers**, who share it with pharmacists, insurers, software providers, and other business associates
- **Subjects** who use wearable fitness trackers, health apps, social media sites such as WebMD, etc.
- **Third parties** who deduce health information about subjects from information such as shopping histories, geolocation data, etc.

9.2 Bulls-Eye on Healthcare

In 2017 alone, 5 million medical/healthcare records were breached, according to the Identity Theft Resource Center's (ITRC) data breach report.[8] In 2015, that number was a whopping

8. Identity Theft Resource Center, *2017 End of Year Report* (San Diego: ITRC, 2018), https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf.

121.6 million, thanks to megabreaches in the health sector, such as the Anthem and Premera cases.[9]

"[S]ince late 2009, the medical information of more than 155 million American citizens has been exposed without their permission through about 1,500 breach incidents," reported the Brookings Center for Technology Innovation.[10]

That means that nearly half of all Americans may have had their protected health information exposed—and this is only based on incidents that were actually detected and reported to the U.S. government.

Why are healthcare entities and business associates so commonly breached? The health industry has seen enormous changes in all five of the data breach risk categories: liquidity, access, retention, value, and proliferation. As we will see, a push to extract value from personal health information in bulk has dramatically increased the risk of data breaches—and created critical questions about what constitutes a "breach" in the first place.

9.2.1 Data Smorgasbord

Healthcare organizations store almost every kind of sensitive information imaginable: Social Security numbers (SSNs), billing data, credit card numbers, driver's license numbers (and often high-resolution scans of IDs), insurance details, and, of course, medical records. In fact, healthcare providers are an excellent source of "fullz" (see § 5.3.1) since they tend to store a wide range of identification information, financial data, and contact details all in one place.

"The medical record is the most comprehensive record about the identity of a person that exists today," says Robert Lord, founder of Protenus, which offers privacy monitoring software for healthcare organizations.[11]

Criminals can split up the information contained within medical records and sell different pieces separately. For example, "[o]n the underground market forum AlphaBay, the user Oldgollum sold 40,000 medical records for $500 but specifically removed the financial data, which was sold separately," reported McAfee Labs in 2016. "Oldgollum is essentially double-dipping to get the most from both markets." McAfee's team pointed out that the price of medical data is "highly variable," in part because sellers can break up stolen data and sell the pieces for different purposes.[12]

When the health insurance giant Anthem reported a breach of 78.8 million records in 2015, the stolen data included "names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data." Anthem was careful to report that no evidence indicated that "medical information such as claims, test results, or diagnostic

9. Identity Theft Resource Center, *Data Breach Reports: December 29, 2015* (San Diego: ITRC, 2015), http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.

10. Center for Technology Innovation at Brookings, *Hackers, Phishers, and Disappearing Thumb Drives: Lessons Learned from Major Health Care Data Breaches* (Washington, DC: Brookings Institution, May 2016), https://www.brookings.edu/wp-content/uploads/2016/07/Patient-Privacy504v3.pdf.

11. Mariya Yao, "Your Electronic Medical Records Could Be Worth $1000 to Hackers," *Forbes*, April 14, 2017, https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#4be095ad1856.

12. C. Beek, C. McFarland, and R. Samani, *Health Warning: Cyberattacks are Targeting the Health Care Industry* (Santa Clara: McAfee, 2016), https://www.mcafee.com/us/resources/reports/rp-health-warning.pdf.

codes were targeted or obtained."[13] Even so, the company was hit with a record $115 million settlement for the ensuing class-action lawsuit. The settlement fund was established to cover costs of credit monitoring and out-of-pocket expenses for victims.[14]

Anthem is a prime example that illustrates how healthcare providers and business associates are on the hook not just for potential breach of health data, but also the identification and financial data that is typically bundled with it.

Due to the volume and value of the data that healthcare providers hold, they must contend with many of the same risks as financial institutions and government agencies—plus, they carry the additional risk of handling extensive volumes of personal health data.

9.2.2 A Push for Liquidity

Health data has become increasingly "liquid," stored in compact, structured formats that facilitate transfer and analysis. Once upon a time, healthcare providers stored your information in filing cabinets and accessed it when needed for treatment purposes. Now your data has been converted to electronic bits and bytes.

In the past two decades, healthcare has witnessed a technology revolution. Today, healthcare providers' computer systems are increasingly interconnected; many people have access to health-related data for purposes of treatment, cost/risk analysis, or medical research. Data is copied over and over, scattered throughout the world, often without the knowledge of the care provider, let alone the patient.

The digitization of personal health data and widespread adoption of electronic medical record (EMR) systems set the stage for large health data breaches. In 2009, the U.S. government passed the HITECH Act, which provided strong financial incentives for shifting to electronic systems. Beginning on January 1, 2015, healthcare providers were required to demonstrate "meaningful use" of EMR systems in order to maintain their Medicare reimbursement levels. As a result, many clinics rushed to transition from paper to electronic records in order to meet deadlines—and overlooked security.

When the HITECH Act passed, technology advocates celebrated, saying that electronic health records could save "tens of billions of dollars each year from reduced paperwork, faster communication and the prevention of harmful drug interactions." Data mining could also lead to better decision making and treatment.[15]

"Finally, we're going to have access to millions and millions of patient records online," said Harvard professor and physician Blackford Middleton—a statement that undoubtedly sent chills down the spine of any cybersecurity professional who read his quote in the *Washington Post*.[16] Nearly a decade later, the digitization of health records has spurred the development of groundbreaking healthcare technologies—and eroded the privacy of hundreds of millions of data breach victims.

---

13. Anthem, "Statement Regarding Cyber Attack against Anthem," press release, February 5, 2015, https://www.anthem.com/press/wisconsin/statement-regarding-cyber-attack-against-anthem.

14. Beth Jones Sanborn, "Landmark $115 Million Settlement Reached in Anthem Data Breach Suit, Consumers Could Feel Sting," *Healthcare IT News*, June 27, 2017, http://www.healthcareitnews.com/news/landmark-115-million-settlement-reached-anthem-data-breach-suit-consumers-could-feel-sting.

15. Robert O'Harrow Jr., "The Machinery Behind Health-Care Reform," *Washington Post*, May 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/05/15/AR2009051503667.html.

16. O'Harrow, "Machinery Behind Health-Care Reform."

9.2.3 Retention

Medical records stick around. While there are no universal guidelines for medical record retention, most states have a minimum retention requirement of five to ten years.[17] It is safe to say, however, with the conversion from paper to electronic format, many care providers have little incentive to clean out their file repositories. Indeed, with the emergence of the big data analytics industry, many organizations retain personal health data indefinitely since it can be sold or traded for valuable goods and services.

9.2.4 A Long Shelf Life

Stolen health data can be useful for years after a breach—even a lifetime. "The value of a medical record endures far beyond that of a card," says Douville. So can the harm, as illustrated by the case of "Frances."

"PPL WORLD WIDE," announced a Facebook post in January 2014. "FRANCES . . . IS HPV POSITIVE!" The posting included Frances's full name and date of birth, "along with the revelation that she had human papillomavirus, a sexually transmitted disease that can cause genital warts and cancer," reported NPR. "It also . . . ended with a plea to friends: 'PLZ HELP EXPOSE THIS HOE!' "[18]

Poor Frances had been treated at a local hospital, where a technician who knew her had access to her record and posted her diagnosis on Facebook. After Frances reported the incident to the nursing supervisor, the hospital sent her a letter of apology. But for Frances, the damage was done: "It's hard to even still deal with it," she said. "I'll spend that extra gas money to go into another city to do grocery shopping or stuff like that, just so I don't have to see anybody from around the neighborhood."[19]

Once stolen, health information can't be changed or quickly devalued like other forms of data. You can change your payment card number after a data breach, but you can't change your medical records.

In short, a data breach involving personal health information can come back to haunt patients for their entire lives.

9.3 HIPAA: Momentous and Flawed

In the United States, data breach prevention and response is regulated by federal law, at least when it comes to PHI. The HIPAA regulations include proactive cybersecurity requirements, while the HITECH Act (which was enacted many years later) specifically address breach

17. Health Information & the Law, *Medical Record Retention Required Health Care Providers: 50 State Comparison*, accessed January 17, 2018, http://www.healthinfolaw.org/comparative-analysis/medical-record-retention-required-health-care-providers-50-state-comparison.

18. Charles Ornstein, "Small Violations of Medical Privacy Can Hurt Patients and Erode Trust," NPR, December 10, 2015, http://www.npr.org/sections/health-shots/2015/12/10/459091273/small-violations-of-medical-privacy-can-hurt-patients-and-corrode-trust.

19. Ornstein, "Small Violations."

response and notification. HIPAA/HITECH are among the few existing federal regulations that address cybersecurity and data breach response at a national level in the United States.

The HIPAA/HITECH regulations are far from perfect. Even for security professionals, understanding the requirements—let alone complying with them—can be a daunting challenge. In this section, we will show how HIPAA emerged and developed, in order to understand the original intent (and how that led to many of the "gaps" in HIPAA/HITECH coverage later on). Then, we will discuss the passage of the Breach Notification Rule and show how the implementation of fines and penalties led to increased breach reporting.

9.3.1 Protecting Personal Health Data

Our instinct to protect the privacy of health information goes back to the very founding of Western medicine. For more than two thousand years, physicians have sworn to keep patient health information secret. The earliest versions of the Hippocratic Oath included the line:

"Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private."[20]

The obligation to protect patient confidentiality remains today and is explicitly included in the AMA Code of Medical Ethics and similar documents used by medical schools.

At the same time, personal health information can be valuable for researchers, employers, and society at large—as well as media outlets, data brokers, and businesses seeking to make a profit. Greater connection and access to medical records can lead to better treatment for patients, but it has also introduced grave privacy concerns.

In 1997, the secretary of the U.S. Department of Health and Human Services (HHS), Donna E. Shalala, gave an impassioned—and timely—speech at a National Press Club luncheon:[21]

> Until recently, at a Boston-based HMO, every single clinical employee could tap into patients' computer records and see detailed notes from psycho-therapy sessions. In Colorado, a medical student copied countless health records at night and sold them to medical malpractice attorneys looking to win easy cases. And, in a major American city, a local newspaper published information about a congressional candidate's attempted suicide. Information she thought was safe and private at a local hospital. She was wrong.
>
> What about the rest of us? When we give a physician or health insurance company precious information about our mood or motherhood, money or medication, what happens to it? As it zips from computer to computer, from doctor to hospital, who can see it? Who protects it? What happens if they don't?
>
> . . . We are at a decision point. Depending on what we do over the next months, these revolutions in health care, communications, and biology could bring us great promise or even

20. Michael North trans., "The Hippocratic Oath," National Library of Medicine, 2002, https://www.nlm.nih.gov/hmd/greek/greek oath.html.

21. "Health Care Privacy," *C-SPAN video*, 53:05 min, posted, July 31, 1997, https://www.c-span.org/video/?88794-1/health-care-privacy&start=1629.

> greater peril. The choice is ours. We must ask ourselves, will we harness these revolutions to improve, not impede, our health care? Will we harness them to safeguard, not sacrifice, our privacy? And will we harness these revolutions to strengthen, not strain, the very life blood of our health care system, the bond of trust between a patient and a doctor?
>
> The fundamental question before us is: Will our health records be used to heal us or reveal us? The American people want to know. As a nation, we must decide.

Secretary Shalala presented recommendations for protecting healthcare information, which were based upon five key principles:

- **Boundaries:** Health information should be used for health purposes, with a few carefully controlled exceptions.
- **Security:** Entities that create, store, process, or transmit health information should take "reasonable steps to safeguard it" and ensure it is not "used improperly."[22]
- **Consumer Control:** Individuals should have access to their personal health records, including the ability to review the content and access records, and the ability to correct any errors.
- **Accountability:** Entities that misuse or fail to properly safeguard personal health information should be held accountable, through "real and severe penalties for violations . . . including fines and imprisonment."
- **Public Responsibility:** Personal health information can and should be disclosed in a controlled manner for the purposes of public health, research, and law enforcement purposes.

The balance between security and public disclosure has been particularly tricky, as we will see in the sections on deidentification and reidentification.

Ultimately, due to the efforts of Secretary Shalala and many others, the HIPAA Security Rule and Privacy Rule were issued and became the foundation for health information security, privacy, and breach response in the United States.

9.3.2 HIPAA Had "No Teeth"

The HIPAA Security Rule went into effect on April 1, 2005 (or a year later for smaller entities). It required all covered entities to establish administrative, technical, and physical controls designed to safeguard the security of PHI. This sounded good, but in practice, HIPAA was not effectively enforced. Moreover, it carried no requirement to notify affected persons in the event of a data breach. As a result, healthcare breaches were common but rarely reported or even discussed outside tight-knit information security circles.

---

22. U.S. Department of Health and Human Services, "Testimony of Secretary of Health and Human Services, September 11, 1997," *ASPE*, February 1, 1998, https://aspe.hhs.gov/testimony-secretary-health-and-human-services-september-11-1997.

In this section, we'll discuss the impact of HIPAA on data breach preparation and response, from the period between 2005 and 2009 (prior to the implementation of the HITECH Breach Notification Rule). This will set the stage for discussing the impacts of the rule in the next section.

9.3.2.1 Lack of Enforcement

"Even though over 19,420 HIPAA complaints/violations have been officially lodged since HIPAA went into effect, it has resulted in zero fines," reported Roger A. Grimes of *InfoWorld* in 2006. "This is amazing, but unfortunately, not surprising. Other than two criminal prosecutions on specific individuals, there appears to be no penalties for organizations violating the HIPAA Act."[23]

Security and privacy professionals around the country began to say that HIPAA had "no teeth." Even if HHS were to impose a fine for a HIPAA violation, the penalties were fairly low, ranging from $100 to a maximum of $25,000 per calendar year for all violations "of an identical requirement or prohibition."[24] Many executives of healthcare organizations saw the potential fines as significantly less than the funds required to bring a healthcare facility's network and processes in compliance with HIPAA.

9.3.2.2 No Breach Notification Requirement

The HIPAA Security Rule did not include any reference to the term "breach." Although the term appeared in the proposed rule, the authors removed it in favor of the more general term "security incident," defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."

Covered entities were required by law to "[i]dentify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes." Seem a little vague? Before the rule was finalized, commenters wrote in to request more specific guidance from HHS, but the authors responded that the details would be "dependent upon an entity's environment and the information involved."[25]

There was little pressure to report health data breaches, even to parties that could be affected. HIPAA did not include an explicit notification requirement. Instead, "[w]hen an improper disclosure (a 'breach') occurred, the responsible party [was] required to take available

23. Roger A. Grimes, "HIPAA has No Teeth," CSO, June 5, 2006, http://www.infoworld.com/article/2641625/security/hipaa-has-no-teeth.html.

24. U.S. Department of Health and Human Services, "HIPAA Administrative Simplification: Enforcement," 70 Fed. Reg. 8389 (Feb. 16, 2006), https://www.federalregister.gov/documents/2006/02/16/06-1376/hipaa-administrative-simplification-enforcement.

25. U.S. Department of Health and Human Services, "45 CFR Parts 160, 162, and 164: Subpart-C," 68 Fed. Reg. 8377 (Feb. 20, 2003), https://www.cms.gov/Regulations-and-Guidance/Regulations-and-Policies/QuarterlyProviderUpdates/Downloads/cms0049f.pdf.

steps to 'mitigate' the harm of disclosure, which may mean notifying the individual whose information was disclosed."[26]

There was no federal requirement to report breaches to any authority or to the public. This made it difficult for even the HHS to evaluate the extent of the problem. "There is no national registry of data breaches that captures all data breaches," noted HHS in 2009. Since healthcare organizations also stored sensitive personal information such as SSNs, they were sometimes required to notify affected persons due to a breach of personal information under state laws. Some health data breaches were also reported to state health agencies under state law; many were tracked by public websites such as the Data Loss database maintained by the Open Security Foundation, which (surprisingly) HHS itself turned to for statistics.[27]

9.3.2.3 Lack of Detection

Security incidents could lead to only more work, liability, angry patients, and possibily fines—so no one *wanted* to uncover one. When healthcare entities discovered a "security incident," typically legal and compliance advisors would ask whether there was any evidence that PHI or other regulated data was accessed or acquired. If no evidence existed, then more often than not, no one would be notified and the incident would not be classified as a breach.

For example, if a system administrator detected that attackers had broken into a hospital server through an unpatched web interface, but the hospital did not retain file access logs or network logs that would indicate that sensitive data had (or had not) been touched, typically the legal team would conclude that there was no clear evidence of a breach, and it would not be reported to anyone. Case closed.

As a result, healthcare organizations had little incentive to invest in cutting-edge intrusion detection systems (IDS), detailed logging systems, or other advanced network monitoring technologies. Absent evidence, they usually assumed a breach had *not* occurred.

Practically speaking, in the early days of the HIPAA Security Rule, ignorance was bliss.

9.3.2.4 Lack of Economic Incentive

Even when word did get out about a healthcare data breach, there was little chance of it impacting a healthcare clinic's bottom line.

"Patients are unlikely to change their doctor if they are impacted by a data breach," wrote Niam Yaraghi of the Brookings Institution. "Most people choose their health care provider based on proximity to their residence. There is a limited supply of such providers in a given geographical area. In many instances, there is only one specialist, testing center, or hospital within miles of a patient's home. The scarcity of specialized medical services means most patients have no choice. In a market where such major security breaches have little to no effect on the revenue stream of the organizations, there is no economic incentive to invest in digital security and prevent a data breach."[28]

---

26. Frost Brown Todd LLC, "HIPAA Breach Notification Rules," October 6, 2009, https://www.frostbrowntodd.com/resources-New_HIPAA_Breach_Notification_Rules_10-06-2009.html.

27. U.S. Department of Health and Human Services, "Breach Notification for Unsecured Protected Health Information," 74 Fed. Reg. 42739, 42761 (Aug. 24, 2009), https://www.gpo.gov/fdsys/pkg/FR-2009-08-24/html/E9-20169.htm.

28. Center for Technology Innovation at Brookings, *Hackers*.

In short, the economic incentives for HIPAA security compliance—and breach notification—simply did not exist for the healthcare industry before 2009.

In the meantime, some healthcare security teams made progress on HIPAA initiatives, forming incident response programs, setting up central logging servers, and establishing individual computer accounts for each user. Others, however, largely ignored the new rules or made cursory efforts to gradually move forward on compliance.

"If I was the CIO at one of our nation's hospitals, I might actually decrease my HIPAA compliance budget this year," said Grimes in 2006. "If it's a law without any teeth, why waste the funds when there are so many other competing objectives?"[29]

9.3.3 The Breach Notification Rule

That changed in 2009, with passage of the HITECH Act. Among other things, HITECH introduced the HIPAA Breach Notification Rule.[30] An interim rule was released in 2009 and finalized with the release of the Omnibus HIPAA Rulemaking in early 2013. The final rule includes the definition of a "breach," explicit notification requirements, and (in some cases) public disclosure requirements.

9.3.3.1 Definition of a Breach

The Breach Notification Rule defines "breach" as follows:[31]

> Breach means the acquisition, access, use, or disclosure of protected health information . . . which compromises the security or privacy of the protected health information.

The term "breach" under HITECH explicitly excludes scenarios in which PHI was unintentially accessed by a workforce member of the covered entity and similar situations.

9.3.3.2 Notification Requirements

The HIPAA Breach Notification Rule is the first federally created notification requirement for health data breaches. It requires:

- **Notification to Individuals** - Organizations must notify each affected individual within 60 days of discovering a data breach.
- **Notification to the Media** - For breaches "involving more than 500 residents of a state or jurisdiction," organizations must notify "prominent media outlets." HHS cautioned that simply updating the organization's website did not sufficiently meet the requirements of notification.
- **Notification to the Secretary** - Organizations must notify the HHS secretary after discovering a breach. For breaches involving more than 500 individuals, organizations must

29. Grimes, "HIPAA Has No Teeth."

30. 45 C.F.R. §§164.400–414.

31. U.S. Department of Health and Human Services, "Part 164 Security and Privacy: 164.402 Definitions," 78 Fed. Reg. 5566, 5695 (Jan. 25, 2013), https://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/FR-2013-01-25.pdf.

notify the secretary within 60 days of discovering the breach. For smaller breaches, each organization must keep a log and provide notification to the secretary within 60 days following the end of the calendar year.

The Breach Notification Rule applies to all breaches discovered on or after September 23, 2009, but the HHS does not "impose sanctions for failing to provide the required notification for breaches discovered before February 22, 2010."[32]

9.3.3.3 The Wall of Shame

The HITECH Act requires the HHS secretary to "post a list of breaches of unsecured protected health information affecting 500 or more individuals."[33] The list is currently posted as a searchable web application, which lists (among other things) the name of each covered entity, breach submission date, number of individuals affected, and a brief summary of the breach. Now, in addition to financial penalties and potential media attention, organizations that experience a breach are immortalized on what security professionals colloquially referred to as the "Wall of Shame," as shown in Figure 9-1.

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Brooke Army Medical Center	TX	Healthcare Provider	1000	10/21/2009	Theft	Paper/Films
Business Associate Present: No **Web Description:** A binder containing the protected health information (PHI) of up to 1,272 individuals was stolen from a staff member's vehicle. The PHI included names, telephone numbers, detailed treatment notes, and possibly social security numbers. In response to the breach, the covered entity (CE) sanctioned the workforce member and developed a new policy requiring on-call staff members to submit any information created during their shifts to the main office instead of adding it to the binder. Following OCR's investigation, the CE notified the local media about the breach.						
Mid America Kidney Stone Association, LLC	MO	Healthcare Provider	1000	10/28/2009	Theft	Network Server
Alaska Department of Health and Social Services	AK	Healthcare Provider	501	10/30/2009	Theft	Other, Other Portable Electronic Device
Health Services for Children with Special Needs, Inc.	DC	Health Plan	3800	11/17/2009	Loss	Laptop
Mark D. Lurie, MD	CA	Healthcare Provider	5166	11/20/2009	Theft	Desktop Computer
L. Douglas Carlson, M.D.	CA	Healthcare Provider	5257	11/20/2009	Theft	Desktop Computer
David I. Cohen, MD	CA	Healthcare Provider	857	11/20/2009	Theft	Desktop Computer
Michele Del Vicario, MD	CA	Healthcare Provider	6145	11/20/2009	Theft	Desktop Computer
Joseph F. Lopez, MD	CA	Healthcare Provider	952	11/20/2009	Theft	Desktop Computer
City of Hope National Medical Center	CA	Healthcare Provider	5900	11/23/2009	Theft	Laptop
The Children's Hospital of Philadelphia	PA	Healthcare Provider	943	11/24/2009	Theft	Laptop

Figure 9-1. Office for Civil Rights' list of "Breaches Affecting 500 or More Individuals." Source: "Cases Currently Under Investigation," Dep't of Health & Human Services, Office for Civil Rights, accessed October 14, 2016, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

32. GBS Directions, "HIPAA Privacy Breach Notification Regulations," *Technical Bulletin* 8 (2009), 8, https://www.ajg.com/media/850719/technical-bulletin-hipaa-privacy-breach-notification-regulations.pdf.

33. U.S. Department of Health and Human Services, "Cases Currently Under Investigation," Office for Civil Rights, accessed October 14, 2016, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

9.3.3.4 Presumption of a Breach

Critically, the final Breach Notification Rule flips the breach definition process on its head. It states:

> [A]n impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised.

This change (released in January 2013) had far-reaching consequences. Absence of evidence no longer meant that organizations could sweep potential breaches under the rug. Covered entities and business associates now have *strong* incentives to implement file system access logging, network monitoring, and similar tools that allow them to *rule out* a breach. Combined with the dramatic increases in penalties, healthcare organizations now have a solid business case for investing in security infrastructure.

Tip: Collect Extensive Evidence

Under the HIPAA Breach Notification Rule, your healthcare organization must assume that a data breach has occurred and react accordingly, unless it can demonstrate otherwise.

If you have HIPAA-regulated health data on your network, make sure to collect extensive records of cybersecurity-related events, including network logins/logouts, access to regulated data, intrusion detection reports, and more. Without evidence, you may be left having to assume an entire data set was compromised. This can lead to unnecessary and expensive overnotification, as well as reputational damage.

Test your evidence collection systems regularly so that you know you have the evidence you need when a suspected breach does occur. That way, you can quickly rule out a breach or at least define the scope as narrowly as possible.

9.3.3.5 The Four Factors

According to HHS, an affected entity must conduct a risk assessment to determine whether a suspected breach has compromised PHI. This risk assessment should include at least the following four factors:[34]

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of reidentification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

34. U.S. Department of Health and Human Services, "Breach Notification Rule," accessed January 18, 2018, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

If an entity concludes that there was a "low probability" of compromise based on this risk assessment, then it is permissible to conclude that a breach did not occur. Regardless, the entity is required to maintain documentation of the risk assessment.

HHS points out that notifications are required only if the breach involves *unsecured* PHI, or PHI that "has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance."

In the United States, HITECH-regulated data is currently one of the few instances where data is presumed to be breached unless an organization can demonstrate otherwise. Under most U.S. state and federal regulations, there is little guidance regarding how to practically determine that a breach has occurred, particularly when the evidence does not exist or is inconclusive. As a result, organizations that maintain health data now have *greater* incentive to monitor and collect evidence than their peers in most other industries. In the next section, we'll discuss how this can skew data breach statistics.

Tip: Conduct a Four-Factor Risk Assessment

Even when electronic PHI has been exposed or subject to unauthorized access, you do not necessarily have to declare a breach. Take the time to conduct a formal risk assessment using at least the four factors described by HHS. In many cases, organizations that complete this risk assessment legitimately determine a low risk of PHI compromise, making notification unnecessary.

Consider leveraging outside counsel to oversee this effort. Attorneys who specialize in healthcare data breaches see many cases and can draw from experience helping other organizations in similar positions. Also, having a qualified third party in charge gives in-house leadership some protection in the event that their decisions are later questioned by a board, regulators, investigators, or the media.

9.3.4 Penalties

The HITECH Act also requires HHS to issue a dramatic increase in financial penalties for violations and to impose penalties for willful neglect. "Prior to the enactment of the HITECH Act, the imposition of [civil money penalties] under HIPAA was limited to a maximum of $100 per violation and $25,000 for all violations of an identical requirement or prohibition occurring within the same calendar year," advised the law firm McGuire Woods in a legal alert. "[T]he amount of the penalty increases with the level of culpability, with maximum penalties for violations of the same HIPAA provision of $1.5 million per year."[35] (Note that the penalties were further increased over time.)

The HITECH Act establishes four categories of culpability:

- Unknowing
- Reasonable cause

35. McGuire Woods, "HIPAA Omnibus Final Rule Implements Tiered Penalty Structure for HIPAA Violations," *McGuire Woods Legal Alert*, February 14, 2013, https://www.mcguirewoods.com/Client-Resources/Alerts/2013/2/HIPAA-Omnibus-Final-Rule-Implements-Tiered-Penalty-Structure-HIPAA-Violations.aspx.

- Willful neglect - corrected within 30 days of discovery
- Willful neglect - not corrected within 30 days of discovery

There are also four corresponding tiers of penalties, which increase based on the level of culpability. "Our observation has been that HHS tends to give bigger fines when people are not trying. You'd better be trying, or you're going to get in big trouble," said Michael Ford, information security officer for the Boston Children's Hospital.[36]

The Office for Civil Rights (OCR), charged with actually conducting investigations and levying fines, met with shocking pushback in one of its first investigations. Cignet Health of Temple Hills, Maryland, was reported to the OCR after refusing to release the medical records of 41 patients, in accordance with HIPAA requirements. Moreover, when the OCR contacted Cignet to investigate, "They failed to appear, they ignored us, they refused to engage with us to have us understand why they were doing this," said OCR Director Georgina Verdugo. The agency bestowed Cignet Health with the dubious honor of the first HIPAA fine to be imposed on a covered entity, announced on February 22, 2011: $4.3 million total, which included $1.3 million for failing to release the patient medical records, and a whopping $3 million because "Cignet failed to cooperate with OCR's investigations on a continuing daily basis from March 17, 2009, to April 7, 2010, and that . . . failure to cooperate was due to Cignet's willful neglect to comply with the privacy rule."[37]

Just two days later, the OCR announced a settlement agreement with Massachussetts General Hospital, which required the hospital to pay $1 million after an employee left documents containing PHI on the subway.[38] The OCR said in its press release:

> We hope the health care industry will take a close look at this agreement and recognize that OCR is serious about HIPAA enforcement. It is a covered entity's responsibility to protect its patients' health information.[39]

By 2016, the media was reporting that the OCR had "stepped up its enforcement activities in recent years" and had become "more aggressive in enforcing HIPAA regulations." In 2016 alone, the agency received payments in excess of $22 million, including a record $5.5 million penalty on Advocate Health System for three data breaches that affected millions of patients.

"When you start seeing multiple-million-dollar fines . . . you get the feeling there's teeth there," said Ford.[40]

---

36. Michael Ford, interview by the author, June 20, 2017.

37. "HHS Imposes a $4.3 Million Civil Money Penalty for Violations of the HIPAA Privacy Rule," *BusinessWire*, February 22, 2011, https://www.businesswire.com/news/home/20110222006911/en/HHS-Imposes-4.3-Million-Civil-Money-Penalty.

38. Shannon Hartsfield Salimone, "HIPAA Enforcement Escalates: What Does This Mean for the Healthcare Industry?" *ABA Health eSource* 7, no. 8 (April 2011), https://www.americanbar.org/content/newsletter/publications/aba_health_esource_home/aba_health_law_esource_1104_salimone.html.

39. Chester Wisniewski, "HIPAA Fines Prove the Value of Data Protection," Naked Security by Sophos, February 25, 2011, https://nakedsecurity.sophos.com/2011/02/25/hipaa-fines-prove-the-value-of-data-protection.

40. Ford interview.

Tip: Be Polite and Responsive

When the OCR comes knocking, it's important to be polite and responsive. Inquiries from regulators can be stressful, of course, but there is plenty of evidence that cooperation leads to a better outcome for affected organizations.

Keep in mind the four categories of culpability. If you are able to demonstrate that any issues occurred because of lack of knowledge or reasonable cause, the penalties will be lower than if there was willful neglect (i.e., problems were reported but simply not addressed). Even if there was willful neglect, remember that you can reduce your culpability by remediating issues within 30 days of discovery—so a quick response can save your organization money and headache in the long run.

9.3.5 Impact on Business Associates

The HITECH Act dramatically changed the requirements for "business associates" of covered entities. Suddenly, attorneys, IT firms, and vendors around the country were themselves required to comply with HIPAA security and privacy rules, report breaches of PHI to the covered entities that they served, and make sure that any subcontractors *they* leveraged were contractually obligated to do the same.

It was an important leap forward for patient privacy—but the estimated 250,000 to 500,000 business associates of covered entities were not ready. According to a survey conducted by the Healthcare Information and Management Systems Society (HIMSS) in December 2009: "[B]usiness associates, those who handle private patient information for healthcare organizations—including everyone from billing, credit bureaus, benefits management, legal services, claims processing, insurance brokers, data processing firms, pharmacy chains, accounting firms, temporary office personnel, and offshore transcription vendors—are largely unprepared to meet the new data breach-related obligations included in the HITECH Act."[41]

In fact, many business associates had no idea that they were suddenly required to adhere to this new regulation. The HIMSS study revealed that "[o]ver 30 percent of business associates surveyed did not know the HIPAA privacy and security requirements have been extended to cover their organizations."[42]

At the time, HIMSS found that more than half of the healthcare entities surveyed said that they would "renegotiate their business associate agreements" as a result of the HITECH Act, and nearly half "indicated that they would terminate business contracts for violations." However, in the years immediately following passage of the HITECH Act, business associates were rarely subjected to audits, and oversight was limited.

---

41. HIMSS Analytics and ID Experts, *Evaluating HITECH's Impact on Healthcare Privacy and Security* (Burlington, VT: HIMSS Analytics, November 2009), https://web.archive.org/web/20111112031528/http://www.himssanalytics.org/docs/ID_Experts_111509.pdf.

42. HIMSS Analytics and ID Experts, *Evaluating HITECH's Impact*.

9.4 Escape from HIPAA

Since HIPAA, and many similar laws, apply only to certain entities such as healthcare providers, the question of who generated the data is core to determining what laws apply and whether a data exposure event constitutes a "breach" under the law.

There are primarily three ways that regulated data "escapes" the confines of HIPAA/HITECH:

- **Data Breach:** Breached information can be traded and sold, or used to make derivative data products.
- **Mandated Information Sharing:** State regulations may require healthcare entities to provide information to third parties for purposes of public interest, such as tracking and managing epidemics. State Prescription Drug Monitoring Programs (PDMPs) are one such example.
- **Deidentification/Reidentification:** Under HIPAA, data can be "deidentified" and released without restriction. However, reidentification is always a risk, and the emergence of big data analytics and data brokers has made reidentification much easier.

In addition, certain personal health information bypasses HIPAA from the very beginning because it is created outside the typical caregiver/patient relationship. Data subjects are often surprised to learn that "noncovered entities" that hold their data are not, in fact, bound by federal HIPAA/HITECH regulations.

9.4.1 Trading Breached Data

In the United States, health information is protected by HIPAA only when it is in the hands of a "covered entity" or "business associate." News outlets such as ESPN, for example, aren't included, as the vignette at the beginning of the chapter showed.

While the legality of leveraging stolen data is questionable at best, the lack of global legal standardization means that there are many jurisdictions where U.S. data protection laws simply would not apply. Furthermore, an increasingly complex web of data brokers facilitates *data laundering*, which can enable stolen data to reenter legitimate markets. See Chapter 2, "Hazardous Material," for details.

9.4.2 Mandated Information Sharing

PDMPs are a prime example of how legally mandated information sharing increases the risk of data breaches. These databases are treasure troves of health information that are designed to be widely accessible for the purposes of reducing drug abuse. Forty-nine states and the District of Columbia and the territory of Guam have a PDMP. While the details vary from state to state, typically doctors and pharmacists are required to report prescriptions of schedule II-IV or II-V drugs to the state. The state maintains a database that includes extensive details of each person, along with detailed prescription records.

Doctors and pharmacists are required to check the PDMP database prior to prescribing or dispensing medication. This means that the state PDMP databases are typically available online

to tens of thousands of doctors, pharmacists and their staff, and often law enforcement agencies, state Medicaid administrators, and others. The database may also be accessible to practitioners in neighboring states, such as Maryland's PDMP, which is available to prescribers in Delaware, Washington, DC, West Virginia, Virginia, and Pennsylvania. In the New York State, the Bureau of Narcotic Enforcement advertises that it "provides millions of secure Official New York State Prescriptions annually to over 95,000 prescribing practitioners across the State."[43]

The fact that PDMPs are so widely accessible leaves them at high risk of unauthorized access. Consider that any medical practitioner around the state who has a PDMP password stolen or a computer infected with malware can be a gateway to this extensive database. By their nature, the PDMP databases are directly accessible via the web and typically protected only by single-factor authentication (username and password) chosen by the practitioner.

Virginia residents discovered in 2009 that their records had been accessed when the state Prescription Monitoring Program (PMP) website was defaced, and the hacker left the following message:[44]

> In *my* possession, right now, are 8,257,378 patient records and a total of 35,548,087 prescriptions. Also, I made an encrypted backup and deleted the original. Unfortunately for Virginia, their backups seem to have gone missing, too. . . . For $10 million, I will gladly send along the password. You have 7 days to decide. If by the end of 7 days, you decide not to pony up, I'll go ahead and put this baby out on the market and accept the highest bid. Now I don't know what all this s—is worth or who would pay for it, but I'm bettin' someone will. Hell, if I can't move the prescription data at the very least I can find a buyer for the personal data (name, age, address, social security #, driver's license #).

Virginia's governor, Tim Kaine, elected not to pay the ransom. Two months later, the state formally sent breach notification letters to more than 530,000 people whose SSNs may have been stored on the system.[45]

At the time, Virginia had a breach notification law that applied to SSNs, credit card numbers, and similar data, but it did not include health or medical data (a breach notification law for medical information was subsequently passed in 2010, although it applies only to state government agencies or organizations "supported . . . by public funds").[46] As a result, the state did not notify all patients with data in the hacked system. Instead, only persons who had their SSNs in the database were notified. An FAQ on the state's website explained, "If you do have a prescription record in the PMP and it did not contain a nine-digit number that could be a Social Security number, you will not be sent a letter."[47]

---

43. New York State Department of Health, Bureau of Narcotic Enforcement, accessed January 18, 2018, https://www.health.ny.gov/professionals/narcotic (accessed January 18, 2018).

44. Cary Byrd, "Stolen Files Raise Issues About Prescription Drug Monitoring Programs," *eDrugSearch*, May 11, 2009, https://edrugsearch.com/stolen-records-raise-questions-about-prescription-drug-monitoring-programs.

45. Bill Sizemore, "Virginia Patients Warned about Hacking of State Drug Web Site," *Virginia Post*, June 4, 2009, http://hamptonroads.com/2009/06/oficials-hacker-may-have-stolen-social-security-numbers.

46. Va. Code Ann. § 32.1-127.1:05, Breach of Medical Information Notification (2010), https://law.lis.virginia.gov/vacode/title32.1/chapter5/section32.1-127.1:05.

47. Virginia Department of Health Professionals, "Questions and Answers: Updated June 5, 2009," accessed January 18, 2018, https://web.archive.org/web/20090618021638/http://www.dhp.virginia.gov/misc_docs/PMPQA060509.pdf.

9.4.3 Deidentification

The HIPAA Privacy Rule allows covered entities and business associates to "deidentify" PHI and subsequently share the resulting data with anyone, *sans* HIPAA regulations. "Deidentification" in this context refers to the process of modifying data sets of medical information so that there is a low risk that individual subjects can be identified.

Under HIPAA, PHI can be deidentified in one of two ways, as illustrated in Figure 9-2 and described in the following list:

- **Expert Determination:** An expert uses "statistical and scientific principles" to determine that the risk of individual identification is very low.
- **Safe Harbor:** Eighteen types of identifying information are removed from the record. Examples include names, email addresses, facial photographs, SSNs, and more.

Theoretically, deidentifying data enables organizations to retain much of the value of medical datasets, while reducing the risk of privacy injury for individual subjects. According to the HHS, "the Privacy Rule does not restrict the use or disclosure of de-identified health information, as it is no longer considered protected health information."[48]

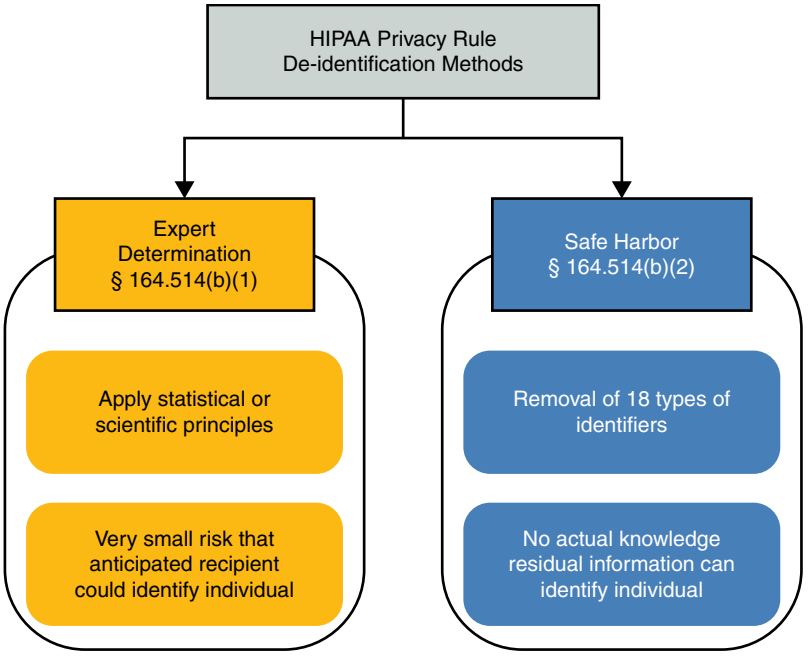


Figure 9-2. Illustration of the two methods of deidentification acceptable under HIPAA Privacy Rule. Source: HHS, *Guidance Regarding Methods for De-identification*.

48. U.S. Department of Health and Human Services, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, accessed January 18, 2018, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html.

The OCR specifically refers to deidentification as one of the factors to be considered in evaluating whether a cybersecurity incident is a breach (and therefore subject to the breach notification laws). When assessing the risk of a breach, organizations are required to consider the "types of identifiers" and "likelihood of re-identification."[49] Since a breach under the HITECH Act is defined as "an impermissible use or disclosure of protected health information" held by a covered entity or business associate, unauthorized access to de-identified information is not typically considered a breach.

Deidentification is one of the ways that health data can "escape" the HIPAA-regulated environment. Deidentified data can be freely sold, transferred, or exposed to the world without regulation under HIPAA. However, the HHS website clearly explains that "de-identified data . . . retains some risk of identification. Although the risk is very small, it is not zero, and there is a possibility that de-identified data could be linked back to the identity of the patient to which it corresponds."[50] If sensitive data were deidentified, transferred to a third party, and subsequently reidentified, then the original sensitive data could potentially exist outside of a HIPAA-regulated organization.

9.4.4 Reidentification

"Reidentification," is the process of adding identifying data back to previously deidentified data sets. Reidentification may be done for a variety of reasons: for example, to match up records across two or more data sets; for ethical notification of subjects in the event that a research study turns up important findings; or for less ethical concerns such as marketing and personal data mining. To support reidentification, HIPAA explicitly permits entities to replace identifying information with a code. The OCR is clear that "[i]f a covered entity or business associate successfully undertook an effort to identify the subject of de-identified information it maintained, the health information now related to a specific individual would again be protected by the Privacy Rule, as it would meet the definition of PHI."[51]

While explicit identifiers can be removed, the very factors that make data sets valuable for researchers (and commercial entities) can also be used to define unique profiles, and ultimately reidentify users. Researchers have demonstrated that reidentification can be much easier than people realize. Specific health conditions, treatment dates and times, names of physicians, location of treatment, and prescription histories function like a digital health fingerprint.

"Health information . . . from sleep patterns to diagnoses to genetic markers . . . can paint a very detailed and personal picture that is essentially impossible to de-identify, making it valuable for a variety of entities such as data brokers, marketers, law enforcement agencies, and criminals," said Michelle De Mooy, the director of the Privacy & Data Project at the Center for Democracy & Technology.[52]

---

49. U.S. HHS, "Breach Notification Rule".

50. U.S. HHS, *Guidance*.

51. U.S. HHS, *Guidance*.

52. Adam Tanner, "The Hidden Trade in Our Medical Data: Why We Should Worry," *Scientific American*, January 11, 2017, https://www.scientificamerican.com/article/the-hidden-trade-in-our-medical-data-why-we-should-worry.

9.4.5 Double Standards

Reidentification is not a crime. While a few states require purchasers to sign or acknowledge a "data use agreement" in order to receive "deidentified" information, HIPAA does not require it for transfer of deidentified data. The result is that a covered entity (or business associate) can deidentify data in compliance with the law and transfer it to a third party without restriction. The third party could then attempt to reidentify the data. If successful, the third party would then be in possession of the same data as the covered entity, *sans* HIPAA/HITECH regulation.

Imagine that you suddenly discover, to your horror, that your organization accidentally posted people's names and known medical problems on the web. Is that a data breach? It depends. If you work for a healthcare provider, then HIPAA/HITECH applies to you, and you would need to consider the definition of a breach in HIPAA/HITECH. On the other hand, if you work for a marketing firm that has re-identified data, it might be that no relevant law applies to you.

That means that two different organizations could expose the exact same data, and in one case it would be a "breach," and in the other case it wouldn't—simply by virtue of how the databases came to exist.

9.4.6 Beyond Healthcare

Fitness trackers, mobile health apps, paternity tests, social media sites, and many other emerging technologies typically fall outside the bounds of the caregiver/patient relationship, and therefore are not covered by regulations such as HIPAA. These "noncovered entities" (NCEs) often collect extensive health and medical-related details about individuals, which they can share or sell it with few restrictions.

The proliferation and spread of health information through NCEs increases the risk of personal health data exposure. NCEs are typically not bound by specific regulations that require them to safeguard health data. The HHS reported in 2016 that "NCEs have been found to engage in a variety of practices such as online advertising and marketing, 139 commercial uses or sale of individual information, and behavioral tracking practices, all of which indicate information use that is likely broader than what individuals would anticipate."[53]

Absent regulations and oversight requiring specific cybersecurity safeguards, NCEs can be particularly high-risk environments. Since there are no standard requirements for incident detection methods and oversight, a high percentage of potential breaches may simply go undetected in these environments. A 2012 study of personal health record (PHR) vendors by Maximus Federal Services found that "[o]nly five of the [41] PHR vendors surveyed referenced audits, access logs, or other methods to detect unauthorized access to identifiable information in PHRs."[54]

Subjects often do not realize that NCEs have great freedom to share or sell their health information. For example, in May 2017 attorney Joel Winston pointed out that by submitting DNA

53. U.S. Department of Health and Human Services, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA* (Washington, DC: HHS, June 2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

54. Maximus Federal Services, *Non-HIPAA Covered Entities: Privacy and Security Policies and Practices of PHR Vendors and Related Entities Report*, December 13, 2012, https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf.

samples to the popular service AncestryDNA for analysis, users "grant[ed] AncestryDNA and the Ancestry Group Companies a perpetual, royalty-free, world-wide, transferable license to use your DNA . . . and to use, host, sublicense and distribute the resulting analysis to the extent and in the form or context we deem appropriate on or through any media or medium and with any technology or devices now known or hereafter developed or discovered."[55]

"[H]ow many people really read those contracts before clicking to agree? And how many relatives of Ancestry.com customers are also reading?" asked Winston. AncestryDNA changed its terms of service shortly thereafter.

Health information persists as an asset—and a risk—even after a company merges, liquidates, or is acquired. AncestryDNA itself takes pains to point this out in its current privacy statement:[56]

> [A]s our business continues to grow and change, we might restructure, buy, or sell subsidiaries or business units. In these transactions, customer information is often one of the transferred assets, remaining subject to promises made in then prevailing privacy statements. Also, in the event that AncestryDNA, or substantially all of its assets or stock are acquired, transferred, disposed of (in whole or part and including in connection with any bankruptcy or similar proceedings), personal information will as a matter of course be one of the transferred assets.

NCEs are not bound by the HIPAA Breach Notification Rule, and therefore are not required to report a "breach" of health-related data under HIPAA/HITECH. However, the Federal Trade Commission's Health Breach Notification Rule, which went into effect in 2010, does apply to vendors of personal health records, their service providers, or "related entities." This rule requires organizations to notify affected U.S. citizens or residents, the FTC, and in certain cases, the media, when there has been "unauthorized acquisition of PHR-identifiable health information that is unsecured and in a personal health record."[57] The FTC may also investigate when a suspected breach indicates that an organization may have engaged in "unfair or deceptive acts or practices" since that is part of the FTC's core mandate.[58]

9.5 Health Breach Epidemic

Suddenly, in 2010 healthcare data breaches began popping out of the woodwork. Many professionals concluded that meant healthcare breaches were on the rise. Statistics reported

55. Ancestry.com, "AncestryDNA Terms and Conditions (United States)," accessed January 18, 2018, https://web.archive.org/web/20170521230901/https://www.ancestry.com/dna/en/legal/us/termsAndConditions.

56. Ancestry.com, "Ancestry Privacy Statement," accessed January 18, 2018, https://www.ancestry.com/dna/en/legal/us/privacyStatement#3.

57. Federal Trade Commission, "Health Breach Notification Rule: 16 CFR Part 318," accessed January 18, 2018, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/health-breach-notification-rule.

58. Thomas Rosch, *Deceptive and Unfair Acts and Practices Principles: Evolution and Convergence* (Washington, DC: FTC, May 18, 2007), 1, https://www.ftc.gov/sites/default/files/documents/public_statements/deceptive-and-unfair-acts-and-practices-principles-evolution-and-convergence/070518evolutionandconvergence_0.pdf.

by the Identity Theft Resource Center seemed to indicate that the number of healthcare data breaches more than doubled between 2009 and 2010.[59]

The American Bar Association published an insightful analysis by attorney Lucy Thomson, who began: "Massive data breaches are occurring with alarming frequency. An analysis of data breaches by industry should provide a wake-up call for the health care industry. . . . Health care breaches have increased steadily from fourth place in 2007 through 2009 to second place behind only the business sector in 2010 and 2011."[60]

And yet, was it really the case that the number of *breaches* in healthcare increased so dramatically? Or were there other factors at play?

9.5.1 More Breaches? Or More Reporting?

The website InformationIsBeautiful.net has an interactive page called "World's Biggest Data Breaches & Hacks: Selected Losses Greater Than 30,000 Records." As shown in Figure 9-3, the chart illustrates data breaches by year, filtered in this case to show only healthcare industry breaches. The size of each bubble indicates the approximate number of exposed records.

What's striking is the absence of major breaches reported before 2009: The earliest major breach was the Virginia PMP, discussed earlier in the chapter. After that, AvMed, Inc. reported a theft of two laptops that occurred in December 2009 and affected 1.2 million patients, and subsequently Affinity Health Plan, Inc. reported in April 2010 that the data of more than 400,000 patients may have been exposed on an office copier hard drive that was not properly wiped before reuse.

Of course, prior to September 23, 2009, there was no legal definition of a "breach" of protected health information, at least under federal law. There was no Breach Notification Rule that explicitly required organizations to notify affected persons. There was no requirement to notify the media or HHS. There was no "Wall of Shame" where the public could view reported breaches. There was no threat of a fine if an organization did not notify affected parties quickly enough.

September 2009 (the effective date of the Breach Notification Rule) and February 2010 (the date after which organizations could be sanctioned for failing to provide proper notice) introduced massive regulatory changes. These changes almost certainly triggered a substantial rise in the number of health data breaches that were *reported*. Furthermore, the *presumption of a breach* incentivized many organizations to invest in network monitoring and logging in a way they never had before, giving these organization new capability to detect data breaches themselves.

In other words, the number of healthcare data breaches that *occurred* did not necessarily rise. Instead, for the first time, the health industry had defined what a breach *was* and gave organizations incentives to detect and report data breaches. Suddenly, the public had a glimpse of the *rest* of the iceberg.

---

59. Identity Theft Resource Center, *ITRC Breach Statistics 2005–2016*, accessed January 18, 2018, https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf.

60. Lucy L. Thomson, *Health Care Data Breaches and Information Security: Addressing Threats and Risks to Patient Data* (Chicago: American Bar Association, 2013), 253–67, https://www.americanbar.org/content/dam/aba/publications/books/healthcare data breaches.authcheckdam.pdf.

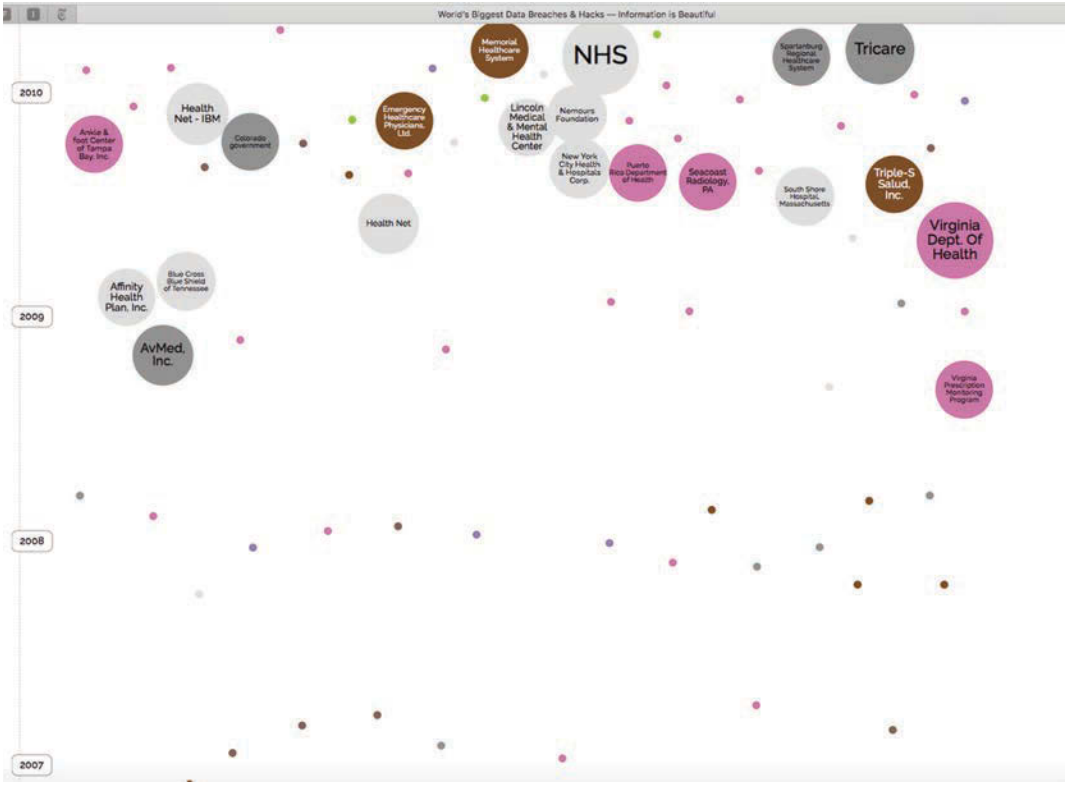


Figure 9-3. Major health care sector data breaches reported over time, 2007–10. Each bubble representing a reported breach is placed randomly within the year it occurred. Image courtesy of InformationIsBeautiful.net.

9.5.2 Complexity: The Enemy of Security

Why so many healthcare breaches? As the issue erupted into the public spotlight, industry cybersecurity professionals wrestled with a myriad of challenges. "There are two things that make health care such an attractive target," explained Larry Pierce, manager of information security and enterprise management at Atlantic Health System. "One is the value of the data, and two is that safeguards and protections are sometimes not in place to protect these environments."[61]

"The worst enemy of security is complexity," wrote Bruce Schneier, the renowned security expert, in 1999.[62] If that's the case, then healthcare organizations have a powerful enemy, indeed.

61. Larry Pierce, interview by author, June 20, 2017.

62. Bruce Schneier, "A Plea for Simplicity: You Can't Secure What You Don't Understand," *Schneier on Security*, November 19, 1999, https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html.

In the next few sections, we will explore specific factors that contribute to the epidemic of healthcare data breaches: the complexity of their IT environments, third-party dependencies, the lack of a perimeter, a mobile workforce, the emergence of personal mobile devices and social media, increasing reliance on the cloud, and more. Technological advances in each of these areas have increased the risk of data breaches and also changed how we respond.

From a veritable jungle of specialized software applications to unique staffing issues and the emergence of Internet of Things (IoT), healthcare technology has become wildly complex. As we will see, it's hard for security professionals to keep up.

9.5.2.1 Specialized Applications

Modern healthcare facilities are fantastically complex environments, from an information management perspective. Hospital networks typically have admission-discharge-transfer (ADT) software systems to track patients from the time they step into the facility to the time they are discharged. The ADT interfaces with the central EMR, used throughout the organization.

Individual departments maintain specialized applications, such as radiology, laboratory, or pharmacy systems. All of these applications need to be integrated with the ADT and the EMR in order to maintain up-to-date, accurate information on patients. Data is transferred between software applications via interface engines using the international Health Level-7 (HL7) protocol.

"Remote organizations receive and send data back to the EMR," described Michael Ford, Information Security Officer at the Boston Children's Hospital. "Prescriptions go out to a pharmacy somewhere using HL7." Data is also shared with researchers and data warehouses, often in real time.

"There is patient data flowing back and forth between hundreds of systems," said Ford. "It looks like a giant brain. It's very difficult to map it all."[63]

Pierce pointed out that "environments within health care [are] significantly more complex than what you'd find in the banking industry or even the government. Most health care systems have in excess of 300 applications and programs that they have to support—all with remote access."[64]

9.5.2.2 Staff and Services

When you compare healthcare environments to those of banking or other industries, it's easy to see why security is a challenge. Like banks, hospitals store highly sensitive financial and identification data, in addition to medical details. Unlike banks, hospitals are open to the public 24/7. This simple fact makes it challenging to find windows of time for installing software patches or running disaster recovery tests.

Banks employ a clearly defined set of personnel: tellers, loan officers, managers, to name a few. Hospitals, however, include full-time and part-time staff, doctors who may rotate through multiple facilities, researchers employed by academic institutions, and more. Care providers who rotate shifts all need access to patient data, and it is not possible to predict in advance precisely who will need access to a specific patient's medical record. This has a major impact on

63. Ford interview.

64. Pierce interview.

access control models in hospitals. Rather than place granular restrictions on which staff can access a particular patient's record, healthcare facilities tend to invest more in post treatment analytics to detect inappropriate access and deter future issues.

9.5.2.3 Patients

At a hospital, when a patient is wheeled in from an ambulance, he or she may not possess an ID card or even the ability to speak—but hospital staff still need to accurately identify the patient, pull up the right medical record, and provide treatment. Contrast this with a bank, where it's normal to require that customers provide identification or answer authentication questions in order to receive service. According to Pierce, Atlantic Health System addressed the issue of patient identification by installing palm scanners in the emergency room department—yet another high-tech (and pricey) system that must be integrated into the hospital's IT environment.

9.5.2.4 Internet of Things

The complexity of healthcare technology only increases as technology advances. Today, smart refrigerators track breast milk expiration dates using barcode readers and transmit temperature monitoring data across the Internet to cloud apps, which can be accessed via a mobile phone app. Patients wander through the halls, implanted with lifesaving devices such as cardioverter defibrillators, which can be remotely controlled via radiofrequency signals. The emergence of IoT and the ubiquitous permeation of cellular networks means that healthcare facilities are literally crawling with networked devices that are attached to patients in their care—yet many of these devices are outside the control of local IT staff.

9.5.2.5 Hospital Infections

Attackers develop malware designed to quietly siphon information out of healthcare networks without impacting operations, in order to retain longer-term footholds. "Botnets" of infected devices can be sold to criminal groups and used to quietly steal valuable information from affected systems. "Stealthy" malware of this kind typically does not impact hospital operations and can remain undetected indefinitely.

Researchers at security firm TrapX discovered a classic example after they installed their security product at a healthcare organization. The researchers noticed alerts from their software indicating that a picture archive and communications systems (PACS) used by the radiology department had been hacked. The initial source of the compromise was a user workstation elsewhere in the hospital; the user had surfed to a malicous website and triggered a classic "drive-by download" attack. Once the PACS was infected, the attackers moved laterally through the facility's network, infecting a nurse's workstation.

"Confidential hospital data was being exfiltrated to a location within Guiyang, China," detailed TrapX. "It is uncertain how many data records in total were successfully exfiltrated. Communications went out encrypted using port 443 (SSL) and were not detected by existing cyber defense software."[65]

65. Trapx Labs, *Anatomy of an Attack: Industrial Control Systems Under Siege* (San Mateo, CA: Trapx Security, 2016), 16–18, http://www.trapx.com/wp-content/uploads/2017/07/TrapX-AOA-Manufacturing.pdf.

According to the *Verizon Data Breach Investigations Report*, 24% of healthcare breaches in their study were discovered months or years after the fact. While more than half were discovered in days or less, the researchers noted that "[u]nfortunately . . . we found out that the majority of them were breaches involving misdeliveries of information or stolen assets." Cases of improper access to electronic health records were simply not detected as quickly, due to lack of effective internal monitoring systems.[66]

"Most organizations tend to focus on perimeter defenses only, but the most effective security strategies need to include . . . the whole network, machine analytics, behavioral analytics." says Pierce. He cites tight budgets throughout the health care industry as a major obstacle. "Health care operates on very, very slim margins. . . . There are monitoring tools, but most organizations with the money they have tend to focus on perimeter defenses only."[67]

In the complex 24/7 hospital environment, it can be challenging to successfully deploy automated IDS without generating a constant barrage of false positive alerts. The traditional reliance on perimeter defenses is no longer effective.

Tip: Invest in Organization

Healthcare environments are massively complex, and complexity breeds insecurity. The good news is that many software tools and products track and organize data, IT assets, clinical equipment, IoT devices, and other equipment used in healthcare environments. However, healthcare entities often do not invest enough in *organization*—an oversight that can lead to expensive security problems (not to mention inefficiencies).

Effective organization is closely tied to effective security. Invest in software that can track and manage sensitive data and equipment throughout your network. Regularly audit documentation and ensure it is up-to-date. If necessary, bring in outside consultants to help with an enterprise-wide organization project. These tasks are often last on a security team's list, but affect the security of your entire enterprise.

9.5.3 Third-Party Dependencies

Healthcare organizations rely heavily on third parties to supply, manage, and maintain specialized software and equipment. As a result, they inherit security risks introduced by outside manufacturers and vendors. In this section, we will review the risks introduced by clinical equipment and vendor remote access, and highlight critical inconsistencies between the way the HHS and the Food and Drug Administration (FDA) regulate data breaches. Along the way, we will provide tips for reducing security risks introduced by third parties and discuss the impact of these organizations on data breach response.

66. "Verizon's 2017 Data Breach Investigations Report," Verizon Enterprise, 2017, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf.

67. Pierce interview.

9.5.3.1 Frozen in Time

Clinical equipment and software can pose a huge cybersecurity risk for healthcare providers. Often, manufacturers prioritize functionality over security, and once a product is released, security updates may be few and far between. Even when security is a priority in the development phase, once a system is deployed, all bets are off.

It's not always clear who is responsible for managing system security (the manufacturer or the purchaser's IT staff). If the purchaser is responsible for handling security, this can be an overwhelming task. Healthcare providers rarely have the staff or intimate knowledge of the equipment to properly secure all of their clinical devices on an ongoing basis (especially given the large number of clinical devices at any one healthcare facility).

A study by the Center for Technology Innovation at Brookings reported that "[t]he manufacturers of these devices . . . sign contracts with medical providers in such a way that removes all of their responsibility in regards to the security of such devices. Thus, medical providers themselves should bear the responsibility of securing these devices. Many smaller medical providers do not have the capability to do this and thus remain very vulnerable to potential cyberattacks."[68]

What's more, vendors may not guarantee that their software will work on an updated system. Whenever a software update is installed, there is a risk that the new code can "break" the functionality of a vendor's custom-written software, sometimes in unexpected ways. This creates a disincentive for local IT staff to modify the devices, even for the purposes of installing important security updates. As a result, clinical equipment often remains unpatched long after exploitable vulnerabilities are widely publicized.

Even in the best-case scenario, there are still delays between the time that a new patch is released and the time that administrators are able to test and install it. Busy healthcare providers rely on expensive clinicial devices to treat patients around the clock, and they may have difficulty carving out the down time required to test and install software patches.

In cases where the manufacturer does provide security updates, there are still many challenges. Manufacturers often have different security standards and priorities than the healthcare professionals who rely on them. Ideally, manufacturers would remain on constant alert, proactively test for new vulnerabilities, and continually ensure that their software is updated to work with the latest updates. In practice, this would require an expensive (perhaps exhorbitant), ongoing investment by the manufacturer, which many cannot or will not make.

Furthermore, over the years many vendors installed their software on various operating systems and versions at different healthcare facilities, without a strong patch management program. It is difficult to bring all of these varied platforms up-to-date, particularly when the equipment is used for day-to-day patient care.

Given that clinical devices are often riddled with security holes, it's not surprising that they are easy to hack. Unfortunately, investigating a potential breach of a clinical device is similarly challenging. Researchers at the security firm TrapX, upon identifying malware-infected clinical devices, noted that "[i]t could take weeks to handle these security incidents because of both

68. Center for Technology Innovation at Brookings, *Hackers*.

scheduling and access to the manufacturer's resources. Once the malware was removed, we found the medical devices could be re-infected fairly quickly." The researchers also pointed out that cyber defense software products, such as antivirus and host-based IDS, are typically not designed for installation on medical devices.[69]

Ultimately, clinical devices often remain on the network without critical security patches, long after a vulnerability is widely known. These fragile systems are typically placed on network segments separated from the rest of the hospital network, in the hopes that the internal segmentation will reduce the chances of a malware infection. In practice, however, segmentation is not always effective because clinical devices still need to interface with other healthcare provider systems. Once infected, clinical equipment is difficult to "clean" and susceptible to re-infection.[70]

The FDA has spoken out about the problem, strongly encouraging device manufacturers to adopt "a proactive, rather than reactive, postmarket cybersecurity approach." In December 2016, the agency released guidance clearly stating that manufacturers should include cybersecurity vulnerabilities in their postmarket device management programs.

For years, medical device manufacturers have claimed that they cannot issue security updates because this would require an FDA recertification of the device.[71] The FDA, however, worked hard to dispell that myth, repeatedly emphasizing that manufacturers *can* apply routine security patches without going through a recertification process, as long as the update does not "significantly affect the safety or effective performance of the medical device."[72]

Tip: Preventing Clinical Device Breaches

Clinical equipment can be very challenging for healthcare facilities to manage because each device is highly specialized and typically produced by a third-party vendor. It is very difficult, if not impossible, for healthcare IT staff to effectively manage the dizzying array of clinical equipment that is used to treat patients. As a result, these devices often pose an enormous security risk for healthcare facilities.

(*Continues*)

69. Steve Ragan, "Attackers Targeting Medical Devices to Bypass Hospital Security," CSO, June 4, 2015, https://www.csoonline.com/article/2931474/attackers-targeting-medical-devices-to-bypass-hospital-security.html.

70. Trapx Labs, *Anatomy of an Attack*, 9.

71. J. M. Porup, "Malware in the Hospital," *Slate*, January 25, 2016, http://www.slate.com/articles/technology/future_tense/2016/01/malware_not_malicious_hackers_is_the_biggest_danger_to_internet_connected.html.

72. U.S. Food and Drug Administration (FDA), *Postmarket Management of Cybersecurity in Medical Devices* (Silver Spring, MD: CBER, December 28, 2016), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.

(*Continued*)

Here are some rules of thumb for reducing the risk of a breach:

- Explicitly assign responsibility for clinical equipment security in the purchasing contract.
- Whenever possible, ensure that the manufacturer is responsible for issuing software patches and updates in a timely manner. Specialized clinical devices require IT staff to invest a lot of time and resources to individually test and secure, and so placing this burden solely on the healthcare facility's IT staff does not scale.
- Make sure that clinical equipment is included in cybersecurity tests, and provide feedback to vendors if their devices are insecure.
- Communicate with industry peers regarding clinical device management, and consider working together with colleagues to address the security of especially challenging devices.

9.5.3.2 The FDA vs. HIPAA

The FDA recommends that manufacturers take a risk-based approach to managing cybersecurity vulnerabilities and updates for medical equipment. According to the agency:[73]

> [A] manufacturer should establish, document, and maintain throughout the medical device lifecycle an ongoing process for identifying hazards associated with the cybersecurity of a medical device, estimating and evaluating the associated risks, controlling these risks, and monitoring the effectiveness of the controls. . . . [I]t is recommended that such a process focus on assessing the risk of patient harm.

There's a catch: The "loss of confidential information, including compromise of protected health information (PHI)" is not considered "patient harm," according to FDA guidelines at the time of this writing.[74] This means that, based on FDA guidelines, device manufacturers do not need to consider the risk of a data breach when they assess vulnerabilities and decide whether to issue security patches. In contrast, healthcare providers are required by HIPAA to conduct a risk assessment that *does* include evaluation of risks to confidentiality of PHI.

Healthcare providers are between a rock and a hard place when it comes to clinical equipment security. On the one hand, HIPAA requires that they maintain the confidentiality of patient data. On the other hand, the FDA does not consider "loss of confidential information" a priority risk for the manufacturers of clinical equipment. This creates a big gap between the risk management programs required for healthcare entities and those required for the medical device manufacturers that they rely on and whose equipment permeates healthcare environments. This gap directly affects the risk of a data breach.

In October 2018, the FDA issued draft guidance for premarket submissions of medical devices, in which the definition of "patient harm" included loss of confidentiality. For further updates that occurred after this book was printed, see the author's website: hackeralien.com.

73. FDA, *Postmarket Management*, 15.

74. FDA, *Postmarket Management*, 10.

Responding to Clinical Device Breaches

When clinical devices get hacked, it can be hard for investigators to get access in a timely manner in order to contain the damage and gather evidence. Sometimes this is because expensive clinical devices are often critical for patient care, and planned outages can be difficult to schedule. Other times, it's because a vendor controls access to the device or holds specialized knowledge, and it may be difficult to get the right resources in place. Here are some tips for making sure your response to a data breach of a clinical device goes as smoothly as possible:

- Ensure that your data breach plans explicitly include clinical devices.
- Keep a record of the types of data that are handled by each device. Different clinical devices contain different types of data; many have PHI, but some do not.
- Plan for outages to accomodate evidence collection and cleanup in the event of a potential breach.
- Make sure that you know how to quickly get access to an infected device in order to preserve evidence. Remember, when it comes to PHI, you may need evidence to demonstrate that there is a low risk of a breach. The faster you act to collect evidence, the more likely it is that the records you seek will exist.
- Maintain contact information for experts who have specialized knowledge of each type of device, and make sure it is readily accessible in the event of a potential breach.

9.5.3.3 Vendor Remote Access

Countless healthcare breaches can be traced back to a vendor-related security issue. Why? For starters, healthcare providers rely on many types of vendor-provided equipment, which connect to the facility network to support remote administration and maintenance. In addition to common devices such as HVAC systems (all-too-often configured with default passwords), hospitals maintain a bevy of expensive clinical equipment, from MRIs to ultrasound equipment to X-ray machines. Equipment such as drug-dispensing systems, refrigerators, drug infusion pumps, ventilators, and more are connected to the network. Specialized software used by different departments must be deployed and maintained, often with the help of contracted vendor support teams.

Healthcare facilities typically have many, many holes poked in the firewall to allow vendors to connect remotely and facilitate automated device commmunication. "They have to get in to manage their equipment—they have on-premises devices," explains Ford. "Often, their equipment is going to phone home. All that equipment sends telemetry to the Internet, like refrigerators and medical devices. . . . Now all your vendors are bypassing your front door."[75]

75. Ford interview.

9.5.4 The Disappearing Perimeter

"The classic [security] model of an organization is that you have a single connection to the Internet, and you have a firewall. You open the ports for the things you want to allow, and you close the ports that you don't want to allow. You open the gate to the castle, and you close the gate to the castle," Ford explained during our interview. "Now, that concept is gone."

Ford was referring to the *perimeter security* model, pioneered by information security experts Bill Cheswick and Steve Bellovin, in their seminal 1994 book, *Firewalls and Internet Security: Repelling the Wiley Hacker*. In their book, the duo lay out a clear model for securing networks by establishing a strong *perimeter*. "If it is too difficult to secure each house in a neighborhood, perhaps the residents can band together to build a wall around the town," they wrote. "Alert, well-trained guards can be posted at the gates while the people go about their business. . . . This approach is called *perimeter security*." Essentially, network administrators build a virtual wall around an organization's network by restricting the flow of traffic, and install a firewall to function as the gate. "To be effective," the authors caution, "the wall should go all the way around the town, and be high enough and thick enough to withstand attack. It also must not have holes or secret entrances that allow an attacker to creep in past the guards."[76]

The perimeter security model has been used as the basis for securing many organizations over the years, and it is still used today. However, Ford's argument is that the model is no longer effective for large segments of the healthcare industry, particularly hospital networks, because the "perimeter" in these environments no longer exists. He cites "the disappearing perimeter" as one of the key drivers behind health industry data breaches.

To start, healthcare providers have long had a porous physical perimeter: They host patients throughout their facilities, including exam rooms, in-patient wards, cafeterias, operating rooms and laboratories (again, compare this with banks, which have specific, limited areas that are accessible to the public). While this physical pourousness is nothing new, the access to *data* in these environments has expanded exponentially over the years.

Sensitive data is instantaneously accessible from laptops attached to rolling carts, tablets, and workstations distributed over a large geographical area. Network jacks throughout the facilities are designed to connect medical equipment, clinical systems, security cameras, and more—and potentially provide a point of access for unauthorized persons. Ubiquitous wireless networks facilitate the use of mobile devices for clinicians, as well as guest access for patients and their families.

The virtual perimeter has become increasingly porous, too. Staff members constantly receive emails that may contain malicious attachments or links. "The user opens it [and gets infected], and now there's a beachhead internally which opens a command-and-control channel out," explains Ford.[77]

Multiple healthcare facilities are connected using site-to-site virtual private networks (VPNs), enabling care providers to share data and network resources. Vendor networks, too, are connected, through site-to-site VPNs or other remote connections.

---

76. W. R. Cheswick, S. M. Bellovin, and A. D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker*, 2nd ed. (Boston: Addison-Wesley Professional, 2003), 11.

77. Ford interview.

In this manner, the "village" of a hospital has grown to encompass so many other villages and towns that the perimeter security model no longer makes sense. Indeed, Cheswick and Bellovin themselves called attention to this issue: "The perimeter approach is not effective if the town is too large."[78]

Tip: An Integrated Approach

Perimeter security alone is no longer an effective way to secure a healthcare organization. Instead, security needs to be woven throughout the enterprise, including mobile devices, IoT, and the cloud. Consider leveraging enterprise-quality security products that integrate mobile devices, IoT, cloud providers, and other sources of data. Make sure to take advantage of automated discovery tools, which detect systems in your environment without any manual intervention. In today's complex organizations, this is the only way to keep up.

9.5.4.1 Mobile Workforce

Hospital environments, in general, must support a high level of mobility and flexibility for employees. Medical staff routinely work at multiple facilities or remote offices. Modern employees want—and sometimes need—to be able to work at home, at odd hours, or while commuting. This is especially important in healthcare, where patients expect 24/7 access to care providers, and specialists serve multiple organizations.

Technology such as personal mobile devices, home computers, and email has become ingrained in the fabric of our everyday lives, and it facilitates the mobile workplace that is so desperately needed for today's healthcare providers. At the same time, the rise of mobile workers spreads sensitive information, increasing the risk of data exposure.

In some cases, healthcare systems issue mobile devices that practitioners can carry with them. In other cases, practitioners install special apps to store health data, or they may even access health information remotely from personal devices.

Storing information on users' home computers or other personal devices presents a serious risk since the healthcare organization cannot control access to users' personal computers. Furthermore, when the employees separate from the organization, there is no guarantee that any data on their personal devices will be appropriately returned or destroyed.

"[Imagine] I'm a doctor, home at my beach house, and I'm on call," suggested Ford during our interview. "I need to download some patient data, so I login to the VPN and download it to my laptop to do a consult for a patient. Now the patient data is outside the hospital and on this device."

When PHI ends up on personal devices, including home computers or cell phones, it can constitute a data breach, leading to massive fines and reputational damage for the healthcare facility.

78. Cheswick, Bellovin, and Rubin, *Firewalls and Internet Security*, 11.

9.5.4.2 BYOD . . . Or Not

Many healthcare systems have a policy that explicitly forbids staff members from capturing PHI on personal mobile devices. Doctors and nurses are prohibited from texting fellow staff members about patient cases or taking photographs of patients using their own personal smartphones or tablets. (In fact, since SMS messaging is not encrypted, texting PHI is often prohibited regardless of the device owner.)

Some healthcare providers go so far as to provide "secure" text message alternatives, such as Imprivata Cortext, which includes both a desktop application and smartphone app. Nurses can log into workstations and message doctors, who then receive notifications on their phones.

Even in environments where such tools exist, clinicians often circumvent security controls—at times, with good reasons. Apps may have issues that seem minor to developers but add delays for already burdened care providers, such as extra passwords (easy to forget when providers juggle multiple accounts) or significant drains on device battery use. In the middle of the night, a nurse might find the only option to reach the doctor on call is a text message from a personal phone—and subsequently receive instructions to text a photo of the patient, a task impossible from the hospital-owned workstation. In this all-too-common scenario, the nurse is forced to choose between providing the best possible data to the doctor or avoiding a HIPAA violation.

"You have to think about the user experience," says Sherri Douville, CEO of Medigram. Her company offers a HIPAA-compliant communications app that healthcare practitioners can install on their own devices. "If the clinician won't use it, it's not secure."[79]

9.5.4.3 Email and HIPAA Violations

Even a single instance in which an employee emails PHI to a home computer can be classified as a data breach. For example, in 2014, Penn State Hershey hospital notified nearly 2,000 patients of a data breach after a clinicial technician downloaded their personal health information to a USB and connected it to his home computer. In addition, he also sent patient information through his personal email to two physicians.[80] *HIPAA Journal* explained that "[t]he employee's home system was outside of the control of the medical center, and potentially the information could have been exposed or viewed by external parties."[81]

Even when healthcare management establishes a clear policy prohibiting transfer of PHI to personal devices, staff members often attempt to bypass these restrictions in order to work remotely. Physicians in particular often struggle with sanctioned remote access systems, juggling passwords for multiple healthcare system VPNs and email systems. Many doctors routinely transfer PHI to their personal systems for later use, typically by sending email attachments from a healthcare provider's workstation to their own personal accounts. For example, in 2010 Geisinger Health System notified approximately 3,000 patients of a breach,

79. Sherri Douville, interview by author, June 20, 2017.

80. Erin McCann, "Staff Blunder Leads to HIPAA Breach," *Healthcare IT News*, June 9, 2014, http://www.healthcareitnews.com/news/staff-blunder-leads-hipaa-breach.

81. "Penn State Hershey Medical Center Announces HIPAA Breach," *HIPAA Journal*, June 22, 2015, http://www.hipaajournal.com/penn-state-hershey-medical-center-announces-hipaa-breach-7092.

after "a gastroenterologist . . . e-mailed to his home computer patient names, medical record numbers, procedure indications and brief impressions regarding the care provided."[82]

The incident was classified a HIPAA violation for two reasons:

1. Since the email itself was unencrypted, the PHI was not encrypted in transit.
2. The PHI was then stored on insecure systems outside the control of the healthcare organization and could have been inappropriately accessed.

Data Loss Prevention (DLP) Systems

Healthcare providers can, and do, install data-loss prevention (DLP) systems to block emails containing PHI, but these have several weaknesses. First, health information can be stored in many formats. Structured text data—such as SSNs and medical record IDs—is easy to detect and block using automated tools. Unstructured data such as provider notes is harder to detect using automated tools. Images, such as screenshots of EMRs or radiology scans, are challenging to analyze and often left out of text-based software rules.

Furthermore, DLP systems may block legitimate traffic, triggering unhappy calls to IT from care providers and overwhelming (notoriously understaffed) IT departments. The "tighter" the rules on a DLP system, the more false positive results are likely to occur. As a result, many healthcare providers invest in a DLP system and set it up to block only obvious violations or simply configure it to generate alerts that IT staff rarely have time to review. In the latter case, the DLP system is a liability rather than a helpful security tool.

Individual practitioners can also leverage encrypted email systems to bypass DLP systems, by sending PHI through secure portals to their own personal email accounts. While the data is encrypted in transit (typically a good thing), depending on the specifics of the setup, the encryption can prevent the DLP system from inspecting the contents of the message, thereby allowing PHI to escape the environment undetected.

9.5.4.4 The Cloud

Today, healthcare providers are moving to the cloud, increasingly leveraging software-as-a-service (SaaS) platforms such as Amazon Web Services, Azure, Office365, and more. "Basically, you have infrastructure virtualized outside your network," commented Ford when I interviewed him. "How do you put a perimeter around that?"

Cloud-based services enable staff members and clinicians to access data remotely—and may also increase the risk that data will spread outside the controlled healthcare systems. The risk varies depending on the controls in place. For example, clinicians may be instructed to access cloud resources only from devices owned by the healthcare provider or affiliates, but in practice they may have the ability to violate the policy and access cloud resources from personal devices. As a result, sensitive information may end up on personal devices.

82. Howard Anderson, "Unencrypted E-Mail Leads to Breach," *Data Breach Today*, December 28, 2010, http://www.databreachtoday.com/unencrypted-e-mail-leads-to-breach-a-3213.

In other cases, access to cloud resources is partially restricted through technical means: Staff may have the ability to check work email from personal devices, for example, but not download attachments. This can still place sensitive information at risk because the contents of the messages can be copied or captured as screenshots.

Finally, there are low-risk configurations where access to cloud resources is limited only to specific, carefully controlled devices and restricted using strong authentication, such as client certificates.

We will discuss cloud data breaches further in Chapter 13, "Cloud Breaches."

9.5.4.5 Social Media

"I'm walking away from the hospital now because I have to leave the premises," sobbed nurse Katie Duke, outside the New York Presbyterian Hospital "I made an online social media post . . . that has gotten me fired." After seven years employed at the hospital's emergency room, Duke snapped a photo of a messy trauma room and published it on Instagram, with the caption, "#Man vs 6 train." Later that day, her employment was terminated. In a classic social media twist, Duke claimed that she hadn't even taken the photograph in the first place—instead, she had reposted a physician's Instagram post.[83] While the photo reportedly wasn't a HIPAA violation, Duke's supervisor told her that she was "fired for being insensitive."[84]

Some cases of inappropriate sharing are not so subtle. For example, at Northwestern Memorial Hospital in Chicago, a young female patient was undergoing treatment for overintoxication when a doctor snapped photos of her. The doctor posted the pictures on his Facebook and Instagram social media accounts, with comments such as "#bottle #service #gone #bad."[85] The patient later sued both the hospital and the doctor.

In another instance, an employee in the emergency room at Spectrum Health (Grand Rapids, Michigan) snapped a photo of a female patient's bare buttocks and posted it to Facebook, with the comment, "I like what I like." The woman's face was not visible, and she was not identified by name in the post. Multiple employees "liked" the photo on Facebook, and some posted comments. The associate medical director of emergency services posted "OMG. Is that TB?" and was fired, along with the physician himself, a registrar, and an assistant. The associate medical director later sued the hospital for wrongful termination.[86]

In both cases, an instantaneous error of judgment by staff led to significant potential for liability due to a data breach and the ensuing fallout, as well as negative media attention for the healthcare facility.

Doctors, nurses, janitors, and other healthcare staff routinely walk through the most sensitive areas of healthcare facilities carrying personal smartphones and tablets. Whereas once the four walls of an operating room provided reliable security from prying eyes, now the physical security perimeter can be bypassed by tiny recording devices belonging to staff members. Even

---

83. Liz Neporent, "Nurse Firing Highlights Hazards of Social Media in Hospitals," *ABC News*, July 8, 2014, http://abcnews.go.com/Health/nurse-firing-highlights-hazards-social-media-hospitals/story?id=24454611.

84. Neporent, "Nurse Firing Highlights Hazards."

85. "Woman Sues Northwestern after Doctor Posted Drunk Photos," *CBS Chicago*, August 21, 2013, http://chicago.cbslocal.com/2013/08/21/woman-sues-northwestern-after-doctor-posted-drunk-photos.

86. Sue Thoms, "Physician Terminated after Facebook Comment Sues Spectrum," *MLive*, March 15, 2014, http://www.mlive.com/news/grand-rapids/index.ssf/2014/03/physician_terminated_after_fac.html.

in facilities where staff are prohibited from carrying smartphones, patients themselves may bring devices onsite. Healthcare providers and their staff are struggling with this new reality, in which cameras are ubiquitous and patient privacy can be undermined with the click of a button.

9.5.4.6 Medical Crowdsourcing

Many healthcare providers use social media to share case studies and "crowdsource" opinions from peers regarding patient treatment. By 2011, one study found that more than 65% of physicians used social media "for professional purposes."[87] Since then, a plethora of information-sharing communities have emerged that encourage practitioners to join. In addition to general purpose social media services such as Facebook and Twitter (where healthcare professionals may choose to discuss patient cases with their personal connections), doctor-specific socal network sites have emerged.

One popular example is SERMO, which advertises itself as the "#1 social network for doctors in the US and now globally." The site provides a forum where doctors can engage in medical crowdsourcing ("Help your peers by sharing and solving challenging cases!"), review treatment options, access discussion forums, and even receive "honoraria"—financial payments—in exchange for taking surveys. Case details provided by physicians become part of SERMO's permanent database, which can be accessed by other members around the world. The materials uploaded by doctors include "anonymous information about the patient, including images, text results and other relevant information."[88]

Of course, this begs the question of just how "anonymous" specific cases can be, particularly when lab images and other unique data are posted. Patients are not informed that their data has been uploaded to the social media site, and in many cases the healthcare provider may have no oversight or involvement in the process either. If the data is uploaded without a HIPAA business associate agreement, the social media provider may well have no federal legal requirement to report a breach. Furthermore, the act of uploading the data might well constitute a HIPAA violation, depending on precisely what data the individual practitioner chooses to upload.

But who would find out?

9.5.4.7 Patient-Managed Data

As patients gain access to more tools to monitor their health and access their data, they also gain more responsibility for their own security. Patients and care providers increasingly leverage wearable monitors that track glucose levels, heart rate, oxygen levels, or other factors. Rather than relying on data collected in a healthcare facility, more patients are collecting data at home and giving providers access via the cloud.

As an example, Ford describes a scenario: "Johnny goes to the hospital and the doctor says, 'Here's a sensor. You can wear it at home. [The sensor] interfaces through your mobile devices and home wireless connection, and sends data to the cloud. . . . Johnny and his parents are the

87. M. Modahl, L. Tompsett, and T. Moorhead, *Doctors, Patients & Social Media* (Waltham, MD: Quantia MD, September 2011), 1, http://www.quantiamd.com/q-qcp/social_media.pdf.

88. "FAQ: How Does SERMO Crowdsourcing Work?" SERMO, accessed January 18, 2018, http://www.sermo.com/what-is-sermo/faq.

ones creating the data. The hospital is not liable for your data [in the event of a breach] because it didn't put it there."[89]

Many healthcare providers are also introducing patient portals, designed to give patients remote access to their appointment schedules, health records, and lab results. Patient portals, of course, can get hacked because of flaws in the provider's application. This was the case with Molina Healthcare, a top Medicaid and Affordable Care Act insurer, which reported a breach in May 2017 that allowed anyone to access arbitrary patient accounts in its online patient portal. The company has more than 4.8 million customers.[90]

But what if a patient's account is breached because his or her own personal computer is infected or an account password was stolen? Many patients prefer simple authentication strategies and short, easy-to-remember passwords, which are convenient but woefully insecure. Hardware tokens are expensive and inconvenient. Modern "apps" that provide a second factor of authentication—such as a code or confirmation button—are promising, especially given that as of 2019, 81% of adults in the United States carry smartphones. However, relatively few patients understand how to leverage these tools.[91]

"It's no longer a technical perimeter. It's a responsibility perimeter," says Ford. For now, healthcare providers are pulled in different directions, by patients who want hassle-free, remote access to their health data, and at the same time demand strong security and privacy.

9.6 After a Breach

A breach involving personal health data, such as diagnoses, prescriptions and procedures, can cause harmful ripple effects for individual victims, their families, and the wider community. Breached organizations struggle to reduce harm and compensate victims, although in many cases the damage cannot be undone (or even fully understood). At the same time, court rulings in health data breach cases are not yet consistent.

Absent a clear path to resolution, healthcare providers might consider applying techniques from medical error cases (which they already handle) to data breaches. A clear apology, openness and a commitment to improvement are sometimes the best medicine.

9.6.1 What's the Harm?

Health data breaches fuel crimes such as:

- **Medical identity theft**, where people obtain fraudulent medical care, insurance coverage, or prescriptions using the personal information of a victim. In addition to financial loss

89. Ford interview.

90. Chad Terhune, "Molina Healthcare, Top Obamacare Insurer, Investigates Data Breach," *Orange County Register*, May 26, 2017, http://www.ocregister.com/2017/05/26/molina-healthcare-top-obamacare-insurer-investigates-data-breach.

91. Pew Research Center, "Mobile Fact Sheet," *Pew Internet and Technology*, 2019, http://www.pewinternet.org/fact-sheet/mobile.

and further data disclosure, this can result in mistakes in the victim's medical records, such as the addition of another person's ailments or physical characteristics. In one study conducted by the Ponemon Institute, a majority of healthcare providers did not have any process for correcting errors in medical records.[92]

- **Insurance fraud** specifically refers to misuse related to a victim's health insurance coverage. This type of fraud can result in victims being denied coverage when they need it. "Patients who have private health insurance often have lifetime caps or other limits on benefits under their policies. So every time a false claim is paid in a patient's name, the dollar amount counts toward that patient's lifetime or other limits," reports the National Health Care Anti-Fraud Association. "This means that when a patient legitimately needs his or her insurance benefits the most, they may have already been exhausted."[93] In the United States, where medical treatment and insurance is decentralized, fraud is especially difficult to detect and prevent.
- **Drug fraud**, which is a specific outcome of medical identity theft, can have a widespread impact on society, resulting in addiction, overdoses, and increased healthcare costs.
- **Extortion**, in which criminals demand a ransom in exchange for not releasing sensitive information. In some cases, criminals attempt to extort money from the patients; other times they approach the breached organization.
- **Sale or unauthorized use of personal health information**, in which criminals sell information about medical treatments, diseases, prescription details, and more to organizations such as news outlets, marketing firms, or data brokers.

In addition, health breaches have negative impacts on victims and society at large that may not be classified as crimes per se but that raise ethical and legal concerns.

- **Economic exploitation** is one negative consequence that is difficult to track. In addition to the potential for direct extortion, patients with specific diseases or problems can be targeted by corporations seeking profit. "Marketers and other people monetize data by categorizing people based on their health information," says Sherri Douville, CEO of Medigram Mobile Intelligence.[94]
- **Discrimination** is one of the most insidious and difficult-to-measure consequences. Your medical records can reveal your sexual orientation, genetic risks, job attendance, and more. Throughout the course of human history, health information has been used to make discriminatory decisions in marriage and dating, employment, politics, and endless other areas. The United States has developed some laws protecting against disability

92. Ponemon Institute LLC, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* (research report sponsored by ID Experts, May 2016), https://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf.

93. National Health Care Anti-Fraud Association, "The Challenge of Health Care Fraud," accessed January 17, 2018, https://www.nhcaa.org/resources/health-care-anti-fraud-resources/the-challenge-of-health-care-fraud.aspx.

94. Douville interview.

and gender-based discrimination, but there are many loopholes—and discriminatory decisions that are quietly made behind closed doors often go undetected.

"Every company would like the perfect employee who has never had a mental health problem, never had an addiction, never had high blood pressure," added Douville during our interview. "They want the perfect little robot."

"People can lose out on jobs, pay more for insurance, fare poorly in custody battles and suffer personal embarrassment," reported *Bloomberg* Business.[95]

It is impossible to enumerate all of the potential negative consequences of health data breach, particularly as the laws and technology evolve. Breaches of confidentiality can lead to employment difficulties, embarrassment, harassment, discrimination, and more. Victims may never even know that their health information was stolen and used against them.

9.6.2 Making Amends

Since personal health information has the potential to impact lives in so many ways, it is difficult to imagine compensation or corrective action that could truly repair the open-ended risks for affected data subjects. While breached organizations often try to compensate victims, offers that are common in other industries may fall flat when it comes to health data breaches.

For example, in March 2015, Premera Blue Cross, a large health insurance provider based out of Washington State, announced a data breach in which criminals "may have gained access" to "name, date of birth, email address, address, telephone number, Social Security number, member identification numbers, bank account information, and claims information, including clinical information."[96] Reportedly, the criminals had access to Premera's systems for nearly a year. As with most health data breach announcements, "clinical information," was buried at the end of the list—but people noticed.

As compensation, Premera provided access to "two years of free credit monitoring and identity protection services" to affected persons. Of course, while credit monitoring and identity theft protection can help mitigate risk of financial fraud, it doesn't address the long-term risk of harm due to PHI exposure. U.S. Senator Patty Murray, ranking member of the Senate Health, Education, Labor, and Pensions Committee, drafted a letter to Premera Blue Cross in the days following the breach announcement. In it, she expressed:

"I understand that Premera has now started to notify each of the affected individuals regarding the attack, and to offer two years of credit monitoring to those customers. I am glad that Premera is taking action on behalf of their customers. However, I remain concerned about the potential harm resulting from this enormous breach and what efforts that Premera will make to ensure that any harm is remedied."[97]

---

95. Jordan Robertson, "States' Hospital Data for Sale Puts Privacy in Jeopardy," *Bloomberg*, June 5, 2013, https://www.bloomberg.com/news/articles/2013-06-05/states-hospital-data-for-sale-puts-privacy-in-jeopardy.

96. Premera, "Premera Has Been the Target of a Sophisticated Cyberattack," accessed January 17, 2018, https://web.archive.org/web/20150330101405/http://www.premeraupdate.com.

97. U.S. Senate Comm. on Health, Education, Labor & Pensions, "Murray Demands Answers from Premera Blue Cross Following Cyberattack that Impacted Millions of Washington State Residents," press release, March 20, 2015, https://www.help.senate.gov/ranking/newsroom/press/murray-demands-answers-from-premera-blue-cross-following-cyberattack-that-impacted-millions-of-washington-state-residents.

Unfortunately, it's not clear that there *is* an effective way to mitigate the potential harm that can be caused by the exposure of private health information. The healthcare industry as a whole has struggled with the problem.

"For breaches involving health care data, credit monitoring doesn't address potential embarrassment or discrimination that can come as a result of exposed medical details," said Ford during our interview. Once private health information is stolen from a hospital, insurer, or third-party provider, there may be no way to put the genie back in the bottle.

9.6.3 Health Breach Lawsuits

Ironically, the open-ended nature of the risk in health data breaches is precisely what makes it difficult for victims to successfully sue. "HIPAA . . . [does] not have a private right of action that you can sue under the statue," explained data breach attorney David G. Ries, counsel at Clark Hill, "but in a lot of states, if there's a law that's intended to protect you and somebody breaches their duty to protect you, you can bring a tort action against them."[98]

In order to gain standing in court, victims must typically demonstrate that they have been harmed or are at risk of impending harm due to the data breach. This can be challenging in data breach cases, particularly with health data. Harm such as discrimination or loss of job opportunities can be difficult to connect with a specific breach, especially when information is distilled, sold, and resold by intermediary data brokers. How would a job seeker know that he or she was rejected because the employer leveraged an employability "score" produced by a data broker, which in turn was based on data that should have been private? What's more, since health data retains its value, actual harm may come years or decades down the road, long after data breach cases are settled or dismissed.

In the case of Health Net of California, Inc., the provider's vendor, IBM, lost servers that contained personal data of approximately 2 million people, including medical and financial data. Within weeks, ten victims filed a punitive class-action lawsuit against Health Net and IBM, alleging that both companies had violated California's Confidentiality of Medical Information Act (CMIA), and that Health Net had violated the Customer Records Act (CRA).

The district court dismissed the case, stating that "[a]ny harm stemming from their loss thus is precisely the type of conjectural and hypothetical harm that is insufficient to allege standing." (Interestingly, the district court also drew a distinction between *theft* versus *loss* of data, pointing out that there was also no evidence that third parties accessed the data.)

"The named plaintiff must himself actually suffer an injury and that injury cannot be hypothetical," summarized attorney Bridget A. Purdue Riddell of Bricker & Eckler LLP.[99]

On the flip side, Health Net victims successfully filed a class-action lawsuit in California's Superior Court and reached a settlement in 2014.[100]

---

98. Dave Ries, interview by author, December 3, 2018.

99. Bridget A. Purdue Riddell, "California Class Action over Loss of Server Drives Storing Personal and Medical Information Dismissed for Lack of Standing," *Lexology*, February 7, 2012, https://www.lexology.com/library/detail.aspx?g=51aec218-acc1-4797-9975-4883182b4dbd.

100. Marianne Kolbesuk McGee, "Health Net Breach Lawsuit Settled," *Data Breach Today*, July 24, 2014, https://www.databreachtoday.com/health-net-breach-lawsuit-settled-a-7099; Shurtleff v. Health Net of California, Inc., No. 34-2012-00121600 (County of Sacramento, CA, 2013), https://eclaim.kccllc.net/caclaimforms/HBS/Documents/HBS_Preliminary%20Approval%20Order.pdf.

Ries is quick to point out that federal and state court rulings on data breaches are complex and not always consistent. "It's still developing," he says.

9.6.4 Learning from Medical Errors

Mistakes that cause permanent harm are nothing new in the healthcare industry. A team of researchers from Johns Hopkins found that "medical errors" result in 251,000 deaths each year, making them the third-leading cause of death in the United States.[101]

How do providers deal with these terrible situations? Many take the "deny and defend" approach, clamming up and releasing as little information as possible.[102] That's standard procedure for data breach disclosure today, as well: patients receive a tersely worded notification letter, if required by law, and little else.

As with medical errors, there are serious downsides to keeping quiet in a data breach response. Lack of transparency leads to perpetuation of mistakes. Trust between patients and health providers may be damaged, causing patients to withhold information from care providers, which in the long term leads to public health concerns. Angry victims are more likely to file lawsuits.

A new approach has emerged in medical error response. Instead of "deny and defend," many healthcare providers are now establishing programs designed "to circumvent litigation by offering prompt disclosure, apology and compensation for mistakes as an alternative to malpractice suits," reported the *Washington Post*.[103] One example is the Communication and Optimal Resolution (CANDOR) approach, which features "prompt investigation of errors whose findings are shared with the victims, as well as an apology and compensation for injuries."[104]

Healthcare providers—and their breach response teams—might consider taking a page from the industry's own playbooks. "You have to normalize honesty to create a culture of continuous improvement," said Richard C. Boothman, chief risk officer for the University of Michigan Health System.[105]

Even as data breaches become more common, healthcare security teams continue to struggle in isolation and silence. "When there's a data breach . . . you read about it in the news but after that it's only speculation," says Pierce. "Nobody is willing to throw out, 'here's what happened' so you can learn lessons from that. That would go a long way from an awareness and education perspective, for organizations to learn from each other's misfortune."[106]

---

101. Ariana Eunjung Cha, "Researchers: Medical Errors Now Third Leading Cause of Death in the United States," *Washington Post*, May 3, 2016, https://www.washingtonpost.com/news/to-your-health/wp/2016/05/03/researchers-medical-errors-now-third-leading-cause-of-death-in-united-states.

102. Sandra G. Boodman, "Should Hospitals—and Doctors—Apologize for Medical Mistakes?" *Washington Post*, March 12, 2017, https://www.washingtonpost.com/national/health-science/should-hospitals{and-doctors–apologize-for-medical-mistakes/2017/03/10/1cad035a-fd20-11e6-8f41-ea6ed597e4ca.

103. Boodman, "Should Hospitals and Doctors."

104. Boodman, "Should Hospitals and Doctors."

105. Boodman, "Should Hospitals and Doctors."

106. Pierce interview.

As with medical errors, there is great fear surrounding data breach disclosure—but transparency and openness can help to reduce long-term risk throughout the system.

9.7 Conclusion

Healthcare data breaches are an epidemic. The very same technical advances that have fueled better information sharing, advances in medical equipment, and sophisticated clinical decision making also create extremely high risks for data breaches.

Health data is accessed by many providers involved in a patient's care; it has therefore become extremely liquid. Copies of personal health data proliferate and are retained for long periods of time. Incredible advances in artificial intelligence and data analytics have created new markets for patient health data and derivative data products. Judging by the rapid pace of development in healthcare technology, none of these risk factors are likely to decline any time soon.

A lack of resources within the healthcare industry adds to the challenge. Cash-strapped healthcare providers are often forced to choose between investing in better equipment, hiring more staff, improving facilities—or implementing cybersecurity measures.

While HIPAA/HITECH and similar state laws provide disincentives for data breaches in the form of fines and public shaming, the regulatory and legal system surrounding health data breaches is extraordinarily complex and inconsistent. The patchwork of regulations and inconsistent legal opinions dramatically slow down the breach response process, creating uncertainty and conflicts within response teams. Furthermore, it's difficult to justify financial investments in cybersecurity when the costs of noncompliance vary wildly.

Current breach notification regulations, which typically penalize institutions that disclose breaches, clearly disincentivize transparency and openness in breach response. When a breach happens, healthcare providers are hesitant to share details, even with industry peers, due to concerns about reputational damage and patient outrage. This leaves healthcare cybersecurity practitioners isolated, facing the daunting challenge of cybersecurity without access to a strong industry-wide knowledge base. Patients, too, are often in the dark, given only a bare thread of information about a breach involving their most personal details.

At the same time that the OCR has stepped up enforcement efforts and increased fines for breaches, personal health data is increasingly proliferating outside the healthcare industry. Fitness trackers, social media, software companies, and data brokers all gather, distill, and disseminate health information. Ironically, while already-strapped healthcare organizations are fined for breaches, the very same sensitive data can be exposed by other organizations without penalty. There is an increasingly expanding and rich pool of identifible health information that is not covered by breach notification laws and therefore remains in the realm of dark matters.

What's the solution? Data breaches will remain an enormous problem for the healthcare industry for a long time to come. The risk of breaches can be reduced only through a combination of changes designed to provide more resources and clear incentives for healthcare cybersecurity. This could include legal changes that require more proactive audits and public accountability, supply chain cybersecurity improvements for medical devices (which could

be spurred by the FDA), greater community emphasis on openness and transparency with respect to cybersecurity issues and breach response, and technical advances to help manage cybersecurity throughout the lifecycle of patient health information.

Data will still escape. Healthcare systems are pourous. While we can certainly develop more effective controls, the five data breach risk factors will continue to place healthcare organizations at elevated risk.

Ultimately, the best solution may be to admit that healthcare data breaches will continue to happen and to regulate the *use* of health information—not just within the healthcare industry, but also after it inevitably escapes.

This page intentionally left blank

Chapter 10

Exposure and Weaponization

"*Someone has your password*" warned the email subject line. On Saturday, March 19, 2016, John Podesta, chair of Hillary Clinton's presidential campaign, received a security notification that appeared to come from Google. By then, the U.S. presidential election was in full swing. Clinton had won 19 primaries; but her opponent, Bernie Sanders, was picking up steam. Every day mattered on the campaign trail.

"Hi John," read the notification, which was sent to Podesta's personal Gmail account.[1] "*Someone just used your password to try to sign in to your Google Account john.podesta@gmail .com. . . . Google stopped this sign-in attempt. You should change your password immediately.*" This was followed by a clickable button that said "CHANGE PASSWORD." Instead of linking to Google's actual site, however, the button linked to a shortened URL service, which in turn forwarded the reader to a strange domain that had the country code of Tokelau (a New Zealand territory).[2] It wasn't really from Google.

Podesta didn't click immediately. His chief of staff forwarded the email to the campaign's IT help desk manager, Charles Delavan. "This is a legitimate email," Delavan responded, incorrectly. "John needs to change his password immediately, and ensure that two-factor authentication is turned on his account." Following the help desk manager's assurance, Podesta (or someone assisting him) clicked on the link.

It was a mistake that would cost the Clinton campaign dearly. Unbeknownst to the campaign staff, hackers stole Podesta's emails and shared them with WikiLeaks, an international organization dedicating to publishing "censored or otherwise restricted official materials."[3] WikiLeaks was far from a neutral third party. Its founder, Julian Assange, had made no secret of his anti-Clinton stance, and even published a statement on WikiLeaks in February 2016 saying that "[a] vote today for Hillary Clinton is a vote for endless, stupid war."[4]

The WikiLeaks hackers didn't release the Podesta emails right away. They waited.

---

1. Podesta Emails, "Re: Someone has your password," *WikiLeaks*, accessed March 14, 2018, https://WikiLeaks .org/podesta-emails/emailid/36355.

2. Bitly, accessed March 14, 2018, https://bitly/1PibSU0+.

3. "What Is WikiLeaks?," WikiLeaks, November 3, 2015, https://WikiLeaks.org/What-is-*WikiLeaks*.html.

4. Julian Assange, "A Vote Today for Hillary Clinton is a Vote for Endless, Stupid War," WikiLeaks, February 9, 2016, https://WikiLeaks.org/hillary-war.

Just one month before the U.S. presidential election, on October 7, 2016, WikiLeaks released the first 2,050 of "The Podesta Emails." The dump was posted less than an hour after the *Washington Post* published the bombshell "Access Hollywood" tape showing Donald Trump caught on a hot mic making crude remarks about women. Podesta himself speculated that the timing "might not have been a coincidence."[5]

The emails were organized in a searchable, indexed database that gave the public full access to 58,660 emails from Podesta's personal Gmail account. Podesta had clearly used his personal account extensively for work, and the emails contained extensive—at times embarrassing—internal conversations, phone numbers, passwords, as well as donor Social Security numbers (SSNs), and personal details.

Instead of releasing all 58,660 emails at once, WikiLeaks broke the data into 36 chunks. Over the next four weeks, it stoked the media's attention by releasing one or two parts each day. It wasn't just a data breach; it was a full-fledged media campaign based on stolen data—every organization's worst nightmare.

"The drip, drip, drip of the hacked emails . . . makes it all but impossible to measure their effect precisely," wrote political commentator Harry Enten. "But we can say two things: (i) Americans were interested in the WikiLeaks releases, and (ii) the timeline of Clinton's fall in the polls roughly matches the emails' publishing schedule."[6]

Podesta was not alone. He was one of many officials who succumbed to hacking during the 2016 presidential campaign within the Hillary for America campaign, the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and other political and high-profile organizations. U.S. intelligence agencies accused the Russian government of launching the cyberattacks as part of a formal campaign to "influence" the outcome of the 2016 presidential elections. Others disagreed, pinning the blame variously on an independent hacker, CrowdStrike (a forensics firm involved in the investigation), and even Democrats themselves.[7]

Whoever the hackers were, and whatever their motive, one thing was clear: The 2016 U.S. presidential election breaches illustrated a fundamental shift in the way stolen data was leveraged. Many politicians and high-ranking officials had been hacked over the past decades. Traditionally, the hackers stole data quietly like mice in the night, furrowing out breadcrumbs of data and secretly using it to their advantage. Suddenly, the criminals brazenly dumped their stolen goods out into the open, leveraging sophisticated public relations (PR) tactics.

In this chapter, we'll discuss different motivations for data exposure and analyze response tactics. Along the way, we will show how information exposure technology has evolved. Finally,

---

5. Aaron Sharockman, "It's True: WikiLeaks Dumped Podesta Emails Hour after Trump Video Surfaced," PolitiFact, December 18, 2016, http://www.politifact.com/truth-o-meter/statements/2016/dec/18/john-podesta/its-true-WikiLeaks-dumped-podesta-emails-hour-afte.

6. Harry Enten, "How Much Did WikiLeaks Hurt Hillary Clinton?" *FiveThirtyEight*, December 23, 2016, https://fivethirtyeight.com/features/WikiLeaks-hillary-clinton.

7. Eric Bradner, "Trump: DNC Hacked Itself," *CNN*, June 16, 2016, http://www.cnn.com/2016/06/15/politics/dnc-hack-donald-trump.

we'll examine the emergence of the "megaleaks" phenomenon and discuss how it affects breach response strategies.

10.1 Exposure Breaches

Data exposure has become a major risk for all kinds of organizations. Recall from Chapter 5, "Stolen Data," the definition of *exposure*:

> Exposure - Data is revealed to the world, thereby damaging the target's reputation, unmasking illicit or objectionable activities, or reducing the value of an information asset.

In this section we will discuss the motivation for data exposure and the evolution of key technologies and tactics.

10.1.1 Motivation

Everyone—from teenagers to CEOs—has to worry about the threat of data exposure. Stolen data is deliberately exposed for a variety of purposes, including:

- Hacktivism
- Whistleblowing
- Politics
- And more

(There are also cases of accidental exposure, which we discuss more in Chapter 13, "Cloud Breaches.")

10.1.2 Doxxing

The concept of "doxxing"—revealing sensitive details about a person on the Internet—was one of the earliest forms of weaponized data exposure. Publishing a victim's SSN, birth date, and other details could subject victims to identity theft and frustrating financial consequences. Cyberbullying is also facilitated by doxxing, since exposed contact information could be leveraged to make prank calls, send harassing messages, or even initiate death threats.

Any site that is used to host data can be leveraged for doxxing. For example, "pasting" sites allow anyone in the world to post arbitrary text; such sites are often used to doxx victims or leak sensitive data. Pastebin.com is one popular mainstream pasting site. There are plenty of legitimate uses for pasting sites, and many (including Pastebin.com) do not condone data leaks.

Over time, doxxing tactics became more sophisticated. "Hacktivists," took the concept of doxxing and wielded it against corporations and other entities as a weapon. "Hacktivists have gone after everyone from foreign governments and corporations to drug dealers and

pedophiles," reported the *Huffington Post*. "Police departments, hospitals, small towns, big cities and states also have come under attack. Online activists have successfully frozen government servers, defaced websites, and hacked into data or email and released it online."[8]

Whistleblowers leveraged data exposure in order to incite change. Disgruntled employees leaked data to damage corporations and government agencies. Political operatives around the world published stolen data to impact diplomatic relations and influence elections.

Perpetrators quickly found that data exposure was an effective tool for influencing their targets, fueling even more breaches.

10.1.3 Anonymous

The "Anonymous" movement popularized the use of data exposure as a tool for driving change or exacting revenge.

In 2003, the earliest inklings of "Anonymous" emerged out of the 4chan imageboard website. (Particularly popular was 4chan's "/b/" board, the host of random postings that was the genesis for "lolcats," "rickrolling," and countless other Internet memes.) On 4chan, users were free to post images, thoughts, and ideas under arbitrary usernames—or no name at all. If a person didn't enter a specific name, his or her post would be automatically attributed to "Anonymous."

As a result, countless posts on 4chan were attributed to the same name, "Anonymous," giving a label to a wide and varied collection of postings produced by thousands of users. "Anonymous is not a single person, but rather, represents the collective whole of 4chan," explains the site's FAQ. "He is a god amongst men."[9]

Anonymous grew to be a powerful god. Over the years, 4chan's users joined forces to take collective action against other organizations online—often for political or social causes.

Anonymous rose to international fame in early 2008, when the collective launched its "Project Chanalogy" attacks against the Church of Scientology, after the church attempted to force YouTube to remove a leaked video featuring Tom Cruise. Incensed by the concept of Internet censorshop, Anonymous declared war and engaged in a variety of attacks, including doxxing. Hacktivists released stockpiles of the church's "secret" internal documents, as well as contact information of key figures, subjecting the church leadership to endless prank calls and faxes.[10]

As Anonymous gained followers and unleashed its wrath against a growing list of targets, the public struggled to wrap their minds around what, exactly, "Anonymous" *was*: A group? A movement? "It's more like a stampeding herd," observed the *Guardian*'s technology editor,

---

8. Jenni Bergal, "'Hacktivists' Increasingly Target Local And State Government Computers," *Huffington Post*, January 11, 2017, https://www.huffingtonpost.com/entry/hacktivists-increasingly-target-local-and-state-government_us_587651e8e4b0f8a725448401.

9. "FAQs: Who Is 'Anonymous'?," 4Chan.org, accessed March 16, 2018, https://www.4chan.org/faq#anonymous.

10. Tony Ortega, "DOX: The FBI's 2008 Investigation of Anonymous and its Attacks on the Church of Scientology," *Underground Bunker*, August 26, 2017, https://tonyortega.org/2017/08/26/dox-the-fbis-2008-investigation-of-anonymous-and-its-attacks-on-the-church-of-scientology; Ryan Singel, "War Breaks Out Between Hackers and Scientology: There Can Be Only One," *Wired*, January 23, 2008, https://www.wired.com/2008/01/anonymous-attac; Mark Schliebs, "Internet Group Declares War on Scientology," *News.com.au*, January 25, 2008, https://web.archive.org/web/20080128185211/http://www.news.com.au/technology/story/0,25642,23107452-5014239,00.html.

Charles Arthur, "not quite sure what it wants but certain that it's not going to put up with any obstacles, until it reaches an obstacle which it can't hurdle, in which case it moves on to something else."[11]

The herd—or whatever it was—frequently took up causes relating to equality and the free exchange of information, lashing out against perceived inequality, censorship, and antipiracy movements. Data exposure was a common tactic, often used alongside denial-of-service attacks to damage targets.

10.1.4 WikiLeaks

Exposed data may also be hosted by websites that are specifically designed to publish stolen data. WikiLeaks is one such service. Founded in 2006 by Julian Assange, WikiLeaks broke new ground in data exposure, incorporating new methods for hosting and marketing breached information. In an interview with *Der Spiegel*, Assange refers to the site as "a giant library of the world's most persecuted documents. We give asylum to these documents, we analyze them, we promote them and we obtain more."[12]

Over the years, WikiLeaks grew from a nascent, Wikipedia-style site where anyone could submit or edit leaked material, to a sophisticated, redundant, highly connected global publishing syndicate. It gave anonymous sources confidence to share and expose documents that might otherwise have remained buried; it then fed breached data to reporters all over the world, bridging the arcane world of Internet geeks and the mainstream media. Within just a few years, WikiLeaks grew into a global powerhouse, used by data leakers all over the world to expose governments, corporations, politicial entities, and more.

Today, WikiLeaks offers would-be leakers:

- Anonymous submissions
- Reliable, resilient hosting platform
- Connections with the mainstream media
- Searchable database that enables readers to analyze information efficiently

Since WikiLeaks burst into the public spotlight, many similar sites have followed its example, leveraging similar techniques to spread large volumes of breached data around the globe.

10.1.5 Weaponization

Over time, data exposure perpetrators became increasingly savvy. Instead of releasing data all at once, they found they could expose data in small, carefully timed chunks, effectively creating a bad news campaign for their chosen target. Furthermore, they learned to create derivative data products that highlighted the most damaging information and presented it in ways that

11. David Leigh and Luke Harding, *WikiLeaks: Inside Julian Assange's War on Secrecy* (London: Guardian, 2013), 207.

12. Michael Sontheimer, "We Are Drowning in Material," *Spiegel Online*, July 20, 2015, https://www.spiegel.de/international/world/spiegel-interview-with-wikileaks-head-julian-assange-a-1044399.html.

were attractive to the mainstream media and general audiences. The results were powerful and painful.

Sony Pictures Entertainment is one example of how a series of timed data releases can turn a nasty data exposure case into a PR nightmare.

10.1.5.1 Sony Pictures Entertainment 2014 Breach

Walking into the office on Monday, November 24, 2014, employees of Sony Pictures Entertainment (SPE) were greeted with a shocking sight: their computers were locked up, and the normally benign screen had been replaced by a frightening image of a skull. "We've already warned you, and this is just a beginning" read the note that was plastered across their screens. "We've obtained all your internal data including your secrets and top secrets. If you don't obey us, we'll release data shown below to the world." The message was followed by a deadline and then a list of data links.[13]

SPE's operations were totally down. The attackers had installed malware that totally wiped the data on half the company's workstations and servers, thousands of systems in all. Employees had no access to email or critical files. "The studio was reduced to using fax machines, communicating through posted messages, and paying its 7,000 employees with paper checks." SPE's team set up a "war" room, holding meetings twice daily and working around the clock to restore operations. The hackers' deadline loomed, and then passed, without any major development—or so it seemed.[14]

In those painful first days, few could have imagined it was only the beginning of the hackers' payback.

10.1.5.2 Internal Data Dumps

By the end of the week, the hackers had dumped five unreleased Sony films onto the Internet. The following week, the hackers published the salaries of top Sony executives, as well as thousands of employees. This triggered a massive debate over gender pay gap, when it was discovered that male employees were paid significantly more than their female counterparts at the studio.

Next, the hackers leaked a spreadsheet that contained names, SSNs, and birth dates for nearly 4,000 Sony employees, triggering state data breach notification laws—and a human resources crisis. "Employees lined up to get help with credit protection and fraud alerts, and with setting up new e-mail and phones," reported *Vanity Fair*. "The F.B.I. came in to give victim counseling and seminars on identity theft."[15] The hackers also published hundreds of passwords for internal servers, bank account details, internal incident reports, and extensive volumes of additional data.

---

13. Kim Zetter, "Sony Got Hacked Hard: What We Know and Don't Know So Far," *Wired*, December 3, 2014, https://www.wired.com/2014/12/sony-hack-what-we-know.

14. Mark Seal, "An Exclusive Look at Sony's Hacking Saga," *Vanity Fair*, March 2015, https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg.

15. Seal, "Exclusive Look."

Rumors began circulating that North Korea was behind the hack.[16] At the time, Sony was preparing to release *The Interview*, a comedy about two journalists who are recruited by the CIA to assassinate Kim Jong-Il. North Korea had expressed strong concerns regarding the film, referring to it as an "act of war."[17] Representatives for North Korea denied responsibility for the hack but referred to it as a "righteous deed."[18]

10.1.5.3 Email Exposure

In the early days of data exposure cases, security teams focused on securing personally identificable information, payment card data, protected health information, and other regulated data. Most people shrugged off the idea of email hacking. "Who cares if someone gets into my email?" was a common refrain. "I don't have anything an attacker would want."

The SPE breach illustrated the extensive damage that can be done when an executive's email inbox is exposed to the world. On December 9, the hackers posted yet another data dump, which contained the full internal emails of Amy Pascal, chair of SPE's Motion Pictures Group. The emails contained inflammatory comments, including a racial remark regarding the president of the United States, and bitter rants about actors such as Angelina Jolie.

Some commentators were shocked that the executives would even put such inflammatory statements in writing. "What were they thinking?" wrote Donna Rosato of *Time* magazine. "Companies routinely monitor worker communications. Email is regularly used as evidence in lawsuits and criminal investigations. Now hacking is another threat. Email isn't private. Everyone knows that."[19]

The fallout continued into early 2015. Pascal was forced to resign. Sony had attempted to put the genie back in the bottle by sending takedown notices to websites hosting its stolen data and sending threatening letters to media outlets that published stories on it. But Sony's attempts were ineffective. In April 2015, the company was thwarted entirely when WikiLeaks posted hundreds of thousands of stolen documents and emails. "This archive shows the inner workings of an influential multinational corporation," explained Assange. "It is newsworthy and at the center of a geopolitical conflict. It belongs in the public domain. WikiLeaks will ensure it stays there."[20]

The SPE data breach represented a landmark development in data breaches, demonstrating to executives everywhere that exposure of *emails* could lead to the downfall of a well-respected executive, as well as worldwide negative media attention. Reading the news headlines, managers

---

16. Arik Hesseldahl, "Sony to Officially Name North Korea as Source of Hack Attack," *Recode*, December 3, 2014, https://www.recode.net/2014/12/3/11633486/sony-to-offcially-name-north-korea-as-source-of-hack-attack.

17. Aly Weisman, "A Timeline of the Crazy Events in the Sony Hacking Scandal," *Business Insider*, December 9, 2014, http://www.businessinsider.com/sony-cyber-hack-timeline-2014-12.

18. Weisman, "Timeline."

19. Donna Rosato, "Why Smart People Send Stupid Emails That Can Ruin Their Careers," *Time*, December 15, 2014, http://time.com/money/3632504/smart-people-stupid-email-pascal-rudin.

20. Brett Lang, "WikiLeaks Publishes Thousands of Hacked Sony Documents," *Variety*, April 16, 2015, https://variety.com/2015/film/news/wikileaks-sony-hack-1201473964; WikiLeaks, "Sony," press release, April 16, 2015, https://wikileaks.org/sony/press.

everywhere shuddered at the thought of what might be in *their* email accounts. After SPE, many more people thought twice before putting controversial thoughts in email and hitting "send."

10.2 Response

Data exposure breaches can be effectively managed using the DRAMA model of data breach management, as described in Chapter 4, "Managing DRAMA":

- **Develop** your data breach response function.
- **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
- **Act** quickly, ethically, and empathetically to manage the crisis and perceptions.
- **Maintain** data breach response efforts throughout the chronic phase, and potentially long-term.
- **Adapt** proactively and wisely in response to a potential data breach.

In data exposure cases, there are distinct tasks that response teams must handle during the "realize" and "act" phases, including:

- **Verify that the data is authentic.**
- **Investigate the breach**, in order to identify the perpetrator, prevent further leaks, and help scope the breach.
- **Remove the data from the Internet as soon as possible.**
- **Conduct an effective public relations campaign** to minimize the reputational or political fallout from the exposure.

In the early days of data exposure cases, accomplishing these goals was often relatively straightforward and within the reach of an effective response team. Since then, however, distribution systems such as WikiLeaks have made it very difficult to identify the source or remove data from the Internet.

In this section, we will analyze response tactics for data exposure cases, including verification, data removal, source identification, public relations tactics, and more.

10.2.1 Verify

The first step for responders in any potential data exposure case is to check that the exposed data is *authentic* and *originated from your organization*. If not, then the victim organization can simply point out that the data is not legitimate, which is a very strong defense. There is no reason to spend time, money, and effort on a data breach investigation if a breach never occurred in the first place.

Verification strategy varies depending on the type and volume of data stolen. Typically responders take a sample of the exposed data and compare it with internal databases to determine whether there is a match. Comparison can involve examining any or all of the following characteristics of the exposed data:

- Structure and format of stolen data (e.g., fields in databases, order, etc.)
- Filenames
- Cryptographic checksums
- Content

The trickiest cases are when exposed data dumps contain *some* legitimate content, in addition to some fake or doctored content. In the modern day and age, a few clicks can produce realistic-looking documents or alterations. Leaked data may be altered in subtle ways, to more effectively fuel media interest or incite public anger.

When appropriate, consider asking forensic analysts or IT staff to audit the leaked data using cryptographic checksums or other techniques, in order to proactively detect alterations. In some cases, exposed documents may even contain cryptographic signatures that can help reviewers authenticate them. For example, many mail servers (such as those run by Google) use DomainKeys Identified Mail (DKIM) signatures to cryptographically sign sent emails. DKIM signatures are included in the headers of received emails. Reviewers can use the signatures, along with the signer's public key, to verify that the contents of the message were not altered and the email did actually originate from the sender's listed domain.

Cryptographic signing can be a double-edged sword for anyone wishing to communicate off the record: On the one hand, it enables people to remotely verify the sender and content of messages, which is important for everyday decision making. On the other hand, messages that are cryptographically signed are difficult to repudiate for anyone who wishes to deny a statement after the fact.

Cryptography Bites Back

Lack of authenticity is a go-to defense for organizations that suffer damaging data leaks—but it is important to use this argument only if it is true. In the case of the 2016 Hillary Clinton campaign email breach, CNN commentator Donna Brazile was accused of sending a debate question to the Clinton campaign in advance. Accused of bias, Brazile told an interviewer that "[y]our information is false" and implied that the emails were "doctored."[21]

Cryptography was not on Brazile's side. While Brazile's emails were not DKIM-enabled, the HillaryClinton.com responses were, and the verified responses clearly showed that the Clinton

(*Continues*)

21. Ian Schwartz, "Megyn Kelly vs. Donna Brazile: Did You Receive Debate Question Beforehand?; Brazile: I Will Not Be 'Persecuted,'" *Real Clear Politics*, October 19, 2016, https://www.realclearpolitics.com/video/2016/10/19/megyn_kelly_vs_donna_brazile_did_you_receive_debate_question_beforehand_brazile_i_will_not_be_persecuted.html.

(*Continued*)

campaign had exchanged emails with Brazile which demonstrated advance knowledge of the questions.[22] Brazile was fired from CNN.[23]

Data breaches are a test of character. In a crisis, it is important to maintain and repair trust, something that can be accomplished only by sticking to the truth.

If the authenticity of exposed data has not been confirmed, then it may be wise for the organization to publicly point this out. Remember that journalists have an uphill battle determining whether leaked material is authentic, particularly when it is provided by an anonymous source with no reputation. Unlike the breached organization itself, reporters have no data source to compare with the leaked data in order to determine whether it is legitimate. Forensic analysis of documents *can* reveal evidence of forgery or modification, but typically cannot rule either one out.

Even if the exposed data is authentic, consider whether it is unique to your organization. In cases involving intellectual property or email, this may be obvious. Other times, the exposed data may consist of personally identifiable information or other records that could exist at any number of institutions. The data could also have been stolen from a supplier or affiliate. Don't assume that a database originated from a specific organization just because it is labeled as such; attackers may try to fool people into believing a breach has occurred in order to accomplish their own objectives.

Tip: Verify the Breach

When exposed data is attributed to your organization, it can set off a frenzy of reactions. Make sure to verify that the exposed data is *authentic* and *actually originated from your organization* before responding to it as a breach. Detecting fake or altered data early on in a data exposure case can save an enormous amount of time and headache in the long run.

10.2.2 Investigate

Investigating a data exposure breach is important for identifying the perpetrator, preventing future leaks, and scoping the breach. Response teams need to preserve evidence as quickly as possible, especially because perpetrators may be actively working to hide their tracks.

Knowing who perpetrated a data exposure breach can help responders properly scope the breach and ensure that it has truly been stopped. Strategies for response differ wildly depending

22. Podesta Emails, "Re: From time to time I get the questions in advance," WikiLeaks, March 12, 2016, https://wikileaks.org/podesta-emails/emailid/5205.

23. Michael M. Grynbaum, "CNN Parts Ways with Donna Brazile, a Hillary Clinton Supporter," *New York Times*, October 31, 2016, https://www.nytimes.com/2016/11/01/us/politics/donna-brazile-wikileaks-cnn.html.

on who caused a breach and how it occurred. For example, if the source of the data was an authorized insider, then HR/legal should be engaged in order to remove access and potentially take legal steps. On the other hand, if the leak was caused by an outside hacker, then responders might need to clean malware off the network, change passwords, and focus on other technical response measures.

When tracking down the perpetrator, there are two obvious places to start: the origin or the hosting provider(s) used to publish the data.

10.2.2.1 Origin

Investigators can analyze evidence from the organization that was breached, in order to determine who had access to the data and how it was exfiltrated. This may include the organization's network logs, intrusion detection system alerts, web surfing history, hard drive evidence, physical access records, and any other details. Many organizations outsource data storage or analytics to third-party suppliers (who, in turn, may outsource to fourth- or even fifth- party suppliers). In this case, coordination with the supplier's IT team may be necessary.

Typically, management of the breached organization is highly motivated to invest resources in gathering internal evidence and identifying the cause of the breach. However, breached organizations often do not collect or retain enough evidence to conclusively pinpoint the culprit—and even when evidence *is* collected, it may be scattered in many different places or too voluminous to analyze quickly, leading to delays. In cases where the data was stolen from a supplier's system, aquiring evidence can be a slow and difficult process.

10.2.2.2 Host

Investigators can analyze evidence from the hosting provider(s) used to expose the data, in order to identify the individual or group that submitted the data to the provider's site and ultimately trace it back to the initial culprit. Useful evidence may include details such as account name and IP address.

Getting evidence from a hosting provider can be a challenge. Reputable providers often require a subpoena before they release data that can identify users, which requires filing a court case. Legal action takes time, and while the clock ticks, critical evidence may be overwritten or deleted. In the United States, if litigation is anticipated, you can send a preservation order to the hosting provider. This obligates the hosting provider to preserve digital evidence that may be relevant to the case. (See Chapter 13, "Cloud Breaches," for a more detailed discussion of evidence aquisition from cloud providers.)

The international nature of data breaches is another challenge: a crime in one nation may be business as usual in another. If data is stolen from one country and hosted in another, navigating the legal process of a foreign country can be slow and painful. Language differences alone can create barriers for response teams, law enforcement, and legal counsel—not to mention actual differences in laws and culture. Finally, the hosting provider may sympathize with the perpetrator (or even *be* the perpetrator), in which case a request for evidence could result in no response (at best) or trigger escalation (at worst).

Even when response teams are able to obtain evidence that identifies the person or group that uploaded data to a hosting provider, there is no guarantee that this was the same entity that *stole* the data in the first place. As we have seen, breached data is routinely bought and

sold on the criminal underground. A hacker or inside attacker may steal and sell data to a buyer, who in turn exposes it to damage the victim organization. Although it can be useful to identify the entity that chose to expose the data to the world, this does not in and of itself enable investigators to determine how the data was stolen or conclusively scope the breach.

10.2.2.3 Anonymous Submissions

Anonymizing communications technology can make it virtually impossible for investigators to trace exposed data back to the person or group that uploaded it. Often, perpetrators deliberately use an anonymizing proxy to leak data to a hosting provider, journalist, or other intermediary. Depending on the context, perpetrators of data exposure may be at risk of prosecution, reputational damage, physical violence, or other harm. Anonymity is a cloak that can defend against all of these.

WikiLeaks advertises that it "records no source identifying information and there are a number of submission mechanisms available to deal with even the most sensitive national security information."[24] This enables people around the world to submit data without fear of reprisal.

"[W]e took the position that we would need to have a publishing system where the only defense was anonymity," Assange explained, in a rare interview with Eric Schmidt (executive chairman of Google).[25]

WikiLeaks uses the Tor onion routing software for anonymous submissions (see Chapter 5, "Stolen Data," for details on onion routing). Leakers are encouraged to upload data to WikiLeaks via a TLS-encrypted Tor submission form, to maintain confidentiality as well. More technically savvy users can use WikiLeaks' public PGP key to wrap the data in strong end-to-end encryption prior to submission.[26]

For organizations concerned about potential data leaks, the presence of Tor traffic can be an instant red flag (although there are many legitimate uses for Tor, depending on the environment). That said, many leakers exfiltrate breached data in other ways (such as using USB drives or remote hacking tools), and then submit the data via Tor using personal or public networks, where it is outside the view of the breached organization.

WikiLeaks: Origin Story

Ironically, WikiLeaks' original "submissions" may have been captured involuntarily due to a loophole in the Tor onion router security. Tor is designed to provide users with anonymous communication across the Internet. It does not, however, include built-in support to ensure

(*Continues*)

24. "WikiLeaks: Submissions," WikiLeaks, accessed June 1, 2019, https://wikileaks.org/wiki/WikiLeaks:Submissions.

25. Julian Assange, *When Google Met WikiLeaks* (New York: OR Books, 2014), 73–74.

26. "Submit Documents to WikiLeaks," WikiLeaks, accessed March 16, 2018, https://wikileaks.org/#submit.

(*Continued*)

confidentiality. Reportedly, Assange or one of his associates ran a Tor exit node (a server that routes Tor users' traffic to a final destination) and discovered that they could read the contents of users' traffic.

Tor was (and is) used for a wide variety of purposes—from cybercriminals seeking to hide their origins to intelligence agents transmitting sensitive materials back to their home offices. Assange realized that, by running a Tor exit node, he could fish highly sensitive documents out of the prolific streams of data. "Hackers monitor chinese and other intel as they burrow into their targets, when they pull, so do we," gushed Assange in early 2007 to his colleague John Young, who ran the peer site Cryptome. "Inexhaustible supply of material. Nearly 100,000 documents/emails a day. We're going to crack the world open and let it flower into something new. . . . Dozens of political parties and consulates, worldbank, opec, UN sanctions, trade groups, tibet and falun dafa associations and . . . russian phishing mafia who pull data everywhere. We're drowning. We don't even know a tenth of what we have or who it belongs to."[27]

From Tor's fountain of data, Assange began siphoning off confidential material. WikiLeaks published its first exposed document in December 2006: a "secret decision" signed by Somali rebel leader Sheik Hassan Dahir Ahweys.[28] This breached data was only the beginning of a flood that would change the world.

10.2.3 Data Removal

When data is exposed, most responders immediately attempt to remove it from the Internet as quickly as possible. As we will see, this can be a quick and easy process or nigh impossible, depending on how the data has been published.

10.2.3.1 Takedown Requests

Mainstream sites such as Pastebin routinely take down stolen data when it is reported. Pastebin.com, one of the oldest and most popular sites for data exposure, includes a "report" link above every post that gives readers the opportunity to report abuse and request removal. Since data leaks have become more common, Pastebin has hired staff to proactively monitor the site for stolen data in order to distance itself from hackers.[29] In response, similar Pastebin-style sites proliferated, such as Doxbin, which is designed to host illegal and stolen data. (Doxbin

27. Leigh and Harding, *Julian Assange's War on Secrecy*, 55.

28. Kim Zetter, "WikiLeaks Was Launched with Documents Intercepted from Tor," *Wired*, June 1, 2010, https://www.wired.com/2010/06/wikileaks-documents.

29. Adi Robertson, "Pastebin Hiring People to Proactively Remove 'Sensitive Information,' Says Owner," *Verge*, April 3, 2012, https://www.theverge.com/2012/4/3/2922151/pastebin-hiring-people-to-proactively-remove-sensitive-information.

was taken down by law enforcement in 2014, but quickly resurfaced under new leadership and spawned many clones after its source code was published in 2016.)

Tip: Ask Nicely First

Many sites that are used for data exposure will actually take down the offending material in response to a simple request. If you are in the unfortunate position of discovering that your sensitive data has been posted online, make a list of the sites where it appears and contact any *reputable* service providers to request removal. (Be careful—it may be unwise to contact administrators of websites affiliated with criminals or hacktivist groups.) Reputable service providers typically have a form or email address that you can use to automatically file a takedown request.

10.2.3.2 Legal Action

In many jurisdisctions, there is a straightforward legal process that requires service providers to remove damaging material from the Internet. What's more, service providers may be obligated (via legal mechanisms) to turn over evidence that could help track down the source of a breach, such as account information, IP addresses, and other potentially identifying details.

Not in Sweden. The neutral Nordic nation's constitution defends the rights of journalists and media outlets, including strong (although not bulletproof) protections against uncovering the identity of sources. For this reason, in 2007, WikiLeaks moved its servers to a Swedish ISP owned by founders of the media piracy site, The Pirate Bay.[30] "There's just no one that bothers less about lawyers harassing them about content they're hosting," said early WikiLeaks organizer Daniel Domscheit-Berg.[31]

In addition to jurisdiction, the effectiveness of legal action often depends upon precisely what type of breached data was stolen. For example, in the United States, copyrighted information is protected by the Digital Millennium Copyright Act of 1998 (DMCA), and due to this hosting providers routinely receive and process requests to remove protected data from the Internet. However, as we saw in the case of football player Jean Pierre-Paul and ESPN (see Chapter 9, "Health Data Breaches"), third parties may be under no legal obligation to refrain from spreading other types of information, such as personal health data (although by policy many organizations voluntarily choose not to host stolen data).

Even when the law is on your side, one problem for breached organizations is that legal action can take time. While the wheels of justice turn the offending data may remain visible online for days, weeks, months, or years.

30. David F. Gallagher, "BITS; WikiLeaks Has Friend in Sweden," *New York Times*, February 25, 2008, https://query.nytimes.com/gst/fullpage.html?res=9B01E5D7173CF936A15751C0A96E9C8B63.

31. Leigh and Harding, *Julian Assange's War on Secrecy*, 51.

Tip: Copyrighted Material

In the United States, the DMCA protects copyrighted material. Organizations that are grappling with exposure of copyrighted data can often invoke the DMCA and trigger a speedy removal. Reputable sites such as Pastebin, GitHub, and other forums have standard DMCA claims forms, which are quickly and routinely processed.[32]

10.2.3.3 Free Speech vs. Stolen Data

There is a big difference between *hosting* breached data and *stealing* data in the first place. Journalists and media outlets enjoy special protections in many countries, giving them leeway to republish material regardless of the source. Laws designed to protect freedom of speech can also protect hosting providers that publish breached data. This has significant consequences for organizations that are trying to remove their exposed data from the Internet: You may have legal recourse against hackers but not the third parties that redistribute your stolen information.

This important distinction was illustrated long before the Internet during the 1971 "Pentagon Papers" breach. In this landmark federal case, military analyst Daniel Ellsberg, employed at the time by RAND Corporation, leaked a top-secret U.S. Department of Defense (DoD) study of the government's decision-making process during the Vietnam War. Revelations from the documents—dubbed the "Pentagon Papers"—were published by the *New York Times* and the *Washington Post* in June 1971.[33] The Nixon administration sought to muzzle the newspapers, but the Supreme Court quickly ruled that the First Amendment protected the right of the newspapers to republish the leaked, classified information, unless the government could demonstrate that such publication would cause "grave and irreparable" danger.[34]

In contrast, Rupert Murdoch and his U.K. tabloid, *News of the World* learned the hard way that actual involvement in hacking could be disastrous for a media company. The newspaper was dogged by accusations that reporters hacked into the phones of celebrities and civilians, starting in 2006 when two of the paper's affiliates were arrested for hacking into the voicemail of the royal family.

Far from being an isolated incident, hacking was secretly a routine practice within the news organization. Over the next few years, more victims came forward and accused the tabloid of invasion of privacy. In 2011, the *Guardian* published an exposé of the practice, alleging that the media corporation hired private investigators to hack into "thousands" of phones, including those of British elected officials.[35]

---

32. "Digital Millenium Copyright Act Form," Pastebin.com, accessed November 11, 2018, https://pastebin.com/dmca.php.

33. "Washington's Culture of Secrets, Sources and Leaks," *Frontline*, PBS, February 13, 2007, https://www.pbs.org/wgbh/pages/frontline/newswar/part1/frankel.html.

34. New York Times Co. v. United States, 403 U.S. 713 (1971), https://www.oyez.org/cases/1970/1873.

35. Nick Davies, "Murdoch Papers Paid £1m to Gag Phone-Hacking Victims," *Guardian*, July 8, 2009, https://www.theguardian.com/media/2009/jul/08/murdoch-papers-phone-hacking.

The scandal blew up. Rebekah Brooks, the CEO of News International, which published *News of the World*, stepped down under pressure and was subsequently arrested.[36] Upon investigation, a British parliamentary panel issued a report that concluded owner Murdoch had "exhibited willful blindness to what was going on in his companies and publications" and was "not a fit person to exercise the stewardship of a major international company."[37] On July 10, 2011, after 168 years in business, *News of the World* shut its doors forever.

Media organizations walk a fine line. Republishing leaked data is one thing; engaging in hacking (or even encouraging it) is quite another.

10.2.3.4 Technical Action

Sites that publish breached data can be taken down through technical means. One common method involves working through the domain's registrar (the organization that manages information about registered domains). With sufficient documentation (such as a court order), registrars can transfer a domain away from the current owner and give control to another entity such as law enforcement. The new owner can choose whether to keep the website running ("seize and operate"), suspend DNS resolution so that visits are unsuccessful ("seize and take down"), or cause the URL of the site to redirect to a notification page ("seize and post notice").[38]

Although not typically recommended, it may also be technically possible to remove data from the Internet by hacking into the host's servers or launching a denial-of-service attack. While it can be tempting to fight fire with fire, most of the time these activities violate laws and can harm innocent third parties. Organizations that engage in illegal hacking or denial-of-service attacks risk legal jeopardy or the threat of escalation.

The Streisand Effect

Attempting to remove leaked data from the Internet can backfire terribly, as singer Barbra Streisand discovered. In 2003, Streisand sued the California Coastal Records Project after discovering that aerial photographs of her Malibu home were published online as part of the project's extensive archive of the state's coastline. The singer claimed that the photographs violated her privacy and demanded $50 million in damages.[39]

(*Continues*)

36. "Rebecca Brooks Arrested by Hacking Police," *BBC News*, July 18, 2011, http://www.bbc.com/news/uk-14178051.

37. John F. Burns and Ravi Somaiya, "Panel in Hacking Case Finds Murdoch Unfit as News Titan," *New York Times*, May 1, 2012, http://www.nytimes.com/2012/05/02/world/europe/murdoch-hacking-scandal-to-be-examined-by-british-parliamentary-panel.html.

38. Dave Piscitello, "Guidance for Preparing Domain Name Orders, Seizures & Takedowns," Internet Corporation for Assigned Names and Numbers (ICANN), March 2012, https://www.icann.org/en/system/files/files/guidance-domain-seizures-07mar12-en.pdf.

39. Allan J. Goodman, "Case No. SC 077 257, Ruling on Submitted Matters, Tentative Decision and Proposed Statement of Decision," Superior Court of the State of California, County of Los Angeles, West District, December 3, 2003, https://www.californiacoastline.org/streisand/slapp-ruling-tentative.pdf.

(*Continued*)

Streisand's lawsuit caused a sensation. Before the lawsuit, the photograph of Streisand's property had been downloaded a total of six times (two of which were attributed to Streisand's attorney). In the ensuing media storm after Streisand filed her lawsuit, more than a million visitors downloaded the image. It was also picked up by the Associated Press and replicated in innumerable news stories around the world.[40]

"If you want to hide something from the internet—you're only likely to make it more widely available, so you're often better off not stirring the hornet's nest," wrote Mike Masnick, founder of the blog *TechDirt*. "[A]s the case gets closer to trial, it's pretty clear that there's no way the photo will ever disappear from the internet—as everyone is checking it out and downloading their own copy."[41]

Ultimately, the judge threw out the lawsuit and ordered Streisand to pay the defendant's legal fees. Two years later, after yet another organization filed a cease-and-desist in an attempt to have data removed from the Internet, Masnick cemented Streisand's place in data breach history. "How long is it going to take before lawyers realize that the simple act of trying to repress something they don't like online is likely to make it so that something that most people would never, ever see . . . is now seen by many more people?" he quipped. "Let's call it the Streisand Effect."[42]

10.2.4 Public Relations

Data exposure is by nature a public affair. Typically, perpetrators seek to damage the victims' reputation, and so having a proactive communications campaign is key.

In exposure cases, PR teams should consider:

- **Victims:** Which individuals or organizations are primarily impacted by the exposure? All too often, it is not just the breached organization that suffers negative publicity and reputational damage.
- **Spin:** The interpretation of the data. Often, attackers are seeking to sway public opinion by selectively publishing or modifying the data. They may also carefully time data releases to influence events.
- **Attacker Reaction:** How attackers may react to press releases or other responses by the victim organization. In some cases, the attackers may have no way to publicly speak after releasing the data. In other cases, they may taunt, threaten, or further embarrass the organization.

40. Stacy Conradt, "How Barbra Streisand Inspired the 'Streisand Effect,'" Mental Floss, August 18, 2015, http://mentalfloss.com/article/67299/how-barbra-streisand-inspired-streisand-effect.

41. Mike Masnick, "Photo of Streisand Home Becomes an Internet Hit," *TechDirt* (blog), June 24, 2003, https://www.techdirt.com/articles/20030624/1231228.shtml.

42. Mike Masnick, "Since When Is It Illegal to Just Mention a Trademark Online?," *TechDirt* (blog), January 5, 2005, https://www.techdirt.com/articles/20050105/0132239.shtml.

In this section, we will provide tips and examples for handling victim communications, spin, and attacker reactions. (For a detailed discussion of data breach crisis communications, see §§ 3.2 and 3.3.)

10.2.4.1 Victims

Data exposure cases typically affect many people, not just the breached organization. Customers, patients, employees, and other parties may be hit with the shrapnel. The impact depends on the precise content that was exposed, and victims may suffer embarrassment, fraud, financial loss, or physical violence. It is not always clear what responsibility the breached organization has to make things right, particularly in cases where the damage is irreparable. When the breach exposes unethical or illegal activity, the organization may be held liable for keeping the information secret in the first place.

In the Panama Papers case (introduced in Chapter 8, "Supply Chain Risks,"), the law firm Mossack Fonesca was breached, resulting in the exposure of 2.6 TB of highly sensitive data. Many of the firm's clients were seriously impacted. For example, the leaks exposed shady financial dealings of world leaders, such as David Cameron, who was then prime minister of the United Kingdom. Cameron was scrutinized for accepting a £200,000 "gift" from his mother, which was widely perceived as a tax evasion scam. In response, thousands of people swarmed the streets outside the U.K. government headquarters, calling for Cameron's resignation.[43]

Journalists combing through the Panama Papers also uncovered a complex web of shady companies and financial transactions that led back to Russian president Vladimir Putin. Media outlets such as the *Guardian* produced reader-friendly diagrams that laid out the money trail, naming specific friends, family members, banks, and corporations that were reportedly involved in money laundering schemes.

Tip: Proactively Contact Victims

When data exposure occurs, victims may include not just the breached organization but anyone associated with the leaked data: clients, patients, employees, and more. To reduce the potential harm, consider contacting victims as soon as possible to enable them to prepare their own responses.

10.2.4.2 Spin

People who deliberately leak data do it for a reason. Often, "spin" is the name of the game. Recordings, videos, documents, and conversations can be selectively edited to support a particular angle and then exposed. Intermediaries and sources of leaked data routinely filter the caches of data that they obtain, choosing to release only a portion. Recipients, such as the mainstream media, aim to present a balanced picture but rarely raise the question of what might have deliberately been left *out* of the exposed data stockpiles.

---

43. Simon Walters and Glen Owen, "Cameron's Tax Bill Dodge on Mother's £200,000 Gift," *Mail Online*, http://www.dailymail.co.uk/news/article-3531822/Cameron-s-tax-bill-dodge-mother-s-200-000-gift-New-row-historic-decision-publish-PM-s-tax-return-revealed-family-avoided-70-000-bill-father-died.html.

In the Panama Papers case, the data was reportedly leaked by an anonymous source, who claimed that he dumped the data for ethical reasons. "I want to make these crimes public." Then, a month after the leak went public, the International Consortium of Investigative Journalists (ICIJ) published an 1,800-word manifesto written by the source, which provided an explanation and attempted to justify the leak. "Income inequality is one of the defining issues of our time," it began. In effect, the author claimed that he exposed the Panama Papers for the noble cause of shining a light on widespread systemic corruption.

Yet there were other, less inspiring (and less reported) theories for the leak. A spokesman for Putin dismissed the leak as an attempt to "destabilise the situation in Russia ahead of elections." (Russia's parlimentary elections took place in September 2016.)[44]

"You journalists all know what an information product is," said Putin himself, at a media forum in St. Petersburg. "So they went through this offshore [material]. Your humble servant was not there, but they don't talk about that. But there's still a job to be done. So what did they do? They make an information product—they found acquaintances and friends."

WikiLeaks—which had reportedly been contacted by "John Doe" but did not respond—was quick to point the finger at the U.S. government, tweeting "#PanamaPapers Putin attack was produced by OCCRP which targets Russia & former USSR and was funded by USAID & Soros."[45] (By then, questions had surfaced regarding the relationship between WikiLeaks and Putin, with many accusing Assange of a bias toward Russia.) The Organized Crime and Corruption Reporting Project (OCCRP) was one of the media partners involved in reporting the leak, however, and was not named as the actual source.

The U.S. State Department confirmed that it provided funding for OCCRP (as did various other organizations), but insisted that the U.S. government was not "in any way involved in the actual leak."[46] Still, it was hard to rule out that the leak could have been politically motivated and professionally produced.

Tip: Hire a PR Professional

More and more often, data is exposed in order to accomplish a specific agenda. Attackers have become increasingly savvy and in some cases enlist the help of professional PR specialists in order to accomplish their goals. The true motive behind data exposure may differ wildly from the publicly presented story. Any organization can be caught in the crossfire of a well-funded political or economic cyber conflict.

If your organization is impacted by data exposure (whether as the breached organization or because your data was affected), don't assume you can handle PR on your own. Immediately engage a professional PR team that has experience handling cybersecurity-related cases.

---

44. Luke Harding, "Kremlin Dismisses Revelations in Panama Papers as 'Putinphobia'," *Guardian*, April 4, 2016, https://www.theguardian.com/news/2016/apr/04/kremlin-reaction-putin-dmitry-peskov-panama-papers-putinphobia.

45. WikiLeaks (@wikileaks), "#PanamaPapers Putin attack was produced by OCCRP which targets Russia & former USSR and was funded by USAID & Soros," Twitter, April 5, 2016, 2:05 p.m., https://twitter.com/wikileaks/status/717458064324964352/photo/1.

46. Irina Titova and Vladimir Isachenkov, "Putin Says Panama Papers Part of U.S. Plot to Weaken Russia," AP News, April 7, 2016, https://apnews.com/b2e8d290404b40478cd4198b86d6adf2/putin-says-panama-papers-part-us-plot-weaken-russia.

10.2.4.3 Attacker Reaction

In many data exposure cases, the perpetrator publicly taunts or threatens the victim organization to get a reaction, increase publicity, or simply out of twisted enjoyment. For example, "hacktivists" have historically engaged in extensive public communications with their victim organizations to build momentum for their cause or make demands. The victim's public response (or lack thereof) can dramatically affect the perpetrators' behaviors, either escalating the fight or causing momentum to fizzle.

A golden rule of responding to data exposure is to not publicly engage with the attackers. The once-respected security firm, HB Gary Federal, learned this the hard way when its CEO, Aaron Barr, began publicly bragging that he knew the names of key leaders of the Anonymous movement. As the media caught wind and began publishing Barr's story, Anonymous members began to leave negative comments on the stories and launched a distributed denial-of-service attack on the corporation.[47] In response, Barr's approach was to escalate the public fight. "I am planning on releasing a few names of folks that were already arrested," he wrote in an email to colleagues. "This battle between us will help spur publicity anyway."

It did indeed spur publicity. Shortly thereafter, Anonymous broke into HB Gary Federal and HB Gary's Inc.'s servers and stole more than 60,000 emails and documents (including troves of sensitive correspondence with clients), dumped the breached data on The Pirate Bay dark website, defaced HB Gary Federal's website and left a copy of the data there for the world to download. The stampeding herd also deleted more than a terabyte of HB Gary's backup files, and reportedly even wiped Barr's iPad for good measure.[48]

The HB Gary breach revealed sensitive, and at times shocking, correspondence relating to the firm's clients, which included a law firm working on behalf of Bank of America and the U.S. Chamber of Commerce. Within days the HB Gary brand had become "toxic," according to *Forbes*.[49] A year later, HB Gary Federal was shut down, and its sister company HB Gary, Inc. was sold.

Tip: Don't Feed the Hackers

Attackers often taunt and threaten organizations and data subjects in order to get what they want. Most of the time, a direct public response will fuel media attention and increase the attacker's sense of power.

Refrain from directly addressing the attacker or engaging in debates. Focus instead on image repair tactics such as bolstering, which can help to rebuild your image without drawing more attention to the attacker.

---

47. Jaqui Cheng, "Anonymous to Security Firm Working with FBI: 'You've Angered the Hive,'" *Ars Technica*, February 7, 2011, https://arstechnica.com/tech-policy/2011/02/anonymous-to-security-firm-working-with-fbi-youve-angered-the-hive.

48. Nate Anderson, "How One Man Tracked Down Anonymous–and Paid a Heavy Price," *Ars Technica*, February 9, 2011, https://arstechnica.com/tech-policy/2011/02/how-one-security-firm-tracked-anonymousand-paid-a-heavy-price/.

49. Andy Greenberg, "HBGary Execs Run for Cover as Hacking Scandal Escalates," *Forbes*, February 15, 2011, https://www.forbes.com/sites/andygreenberg/2011/02/15/hbgary-execs-run-for-cover-as-hacking-scandal-escalates.

10.3 MegaLeaks

Today, megaleaks are a threat to every high-profile organization. A megaleak is a large-scale data exposure case, typically involving a high volume of data and widespread distribution through the mainstream media. The impact of a megaleak can reverbrate throughout a breached organization's ecosystem and cause deep financial, legal, and social consequences not only for the organization itself, but customers, affiliates, investors, suppliers, and more. Once a megaleak is released, it can't ever be erased.

Megaleaks were not always possible. Exposing large volumes of data is more difficult than it sounds. First, simply finding a place to *host* a large volume of sensitive data can be a challenge for attackers, especially when powerful organizations want to see it removed. Gaining the attention of the mainstream media typically requires existing relationships and a good story. Picking out juicy nuggets of information from a vast trove of data requires teams of people, in some cases with specific expertise.

It was the 2010 Bradley Manning data breach that made megaleaks possible. Bradley Manning, an intelligence analyst for the U.S. Army, stole hundreds of thousands of classified documents and leaked them to WikiLeaks, which (after extensive effort) was ultimately able to expose them to the world. Due to the enormous volume of highly sensitive data that Manning leaked, innovation was necessary in order to analyze and disseminate it. New developments included:

- Collaboration with mainstream media partners.
- Analysis and authentication of large, complex data repositories.
- Redaction standards and methods for large volumes of leaked data.
- Presentation tactics for communicating key points to the public.
- Timed releases designed to maximize attention and reduce risk.
- Strong social media following for WikiLeaks.

In this section, we will step through the innovations that WikiLeaks and its mainstream media partners pioneered during the Manning breach and discuss how these changed defenders' response strategies.

10.3.1 Manning's Crime

In January 2010, Army intelligence analyst Bradley Manning[50] sat at a keyboard at a U.S. military base outside Baghdad, lip-syncing to Lady Gaga. Little did anyone know that as the pop music played, Manning quietly copied hundreds of thousands of secret documents from the classified military network to the rewritable CD in the drive of his government-owned laptop.

50. Later, Manning transitioned to female and renamed herself Chelsea Manning. For the purposes of this book, we will refer to Manning with the name and gender that she portrayed at the time of the events described, to match documentation from the time.

As an intelligence analyst, Manning analyzed all sources of available information to create "work products," such as "maps and charts to conduct predictive analysis based on statistical trends."[51] Manning therefore had unlimited access to databases containing detailed Iraq and Afghanistan war records, including the "Significant Activities" (SIGACTs) records, which he described as essentially a "daily journal" of events.[52]

Over time, Manning became increasingly disturbed by the information he digested. Ultimately, he decided he needed to release it to the public. "I believed that if the general public, especially the American public, had access to the information . . . this could spark a domestic debate on the role of the military and our foreign policy in general, as well as it related to Iraq and Afghanistan," Manning later explained. "I also believed a detailed analysis of the data over a long period of time, by different sectors of society, might cause society to re-evaluate the need, or even the desire to engage in . . . operations that ignored the complex dynamics of the people living in the affected environment each day."

Manning had direct access to the U.S. military's classified network, SIPRNet. For security purposes, SIPRNet was "air gapped," meaning that it was not connected to the Internet. However, it soon became clear that, with physical access, a privileged insider could exfiltrate practically anything.

Due to dust and heat, computer equipment at the Iraqi military bases was often unreliable. Manning and his fellow analysts experienced frequent crashes that had caused them to lose information.[53] The analysts were instructed to keep backups of their work product. As a result, Manning developed a process in which he copied the data he frequently needed, as well as his work product, to multiple locations, including CD-RW disks that he kept in a conference room.

At the end of his shift on January 8, 2010, Manning took a backup CD-RW from the conference room, put it in the cargo pocket of his uniform, and walked out of the secure military facility. "The air gap has been penetrated," Manning later confessed. The CD-RW contained more than 482,832 reports from the Iraq and Afghanistan wars. Manning didn't have a specific plan at the time, but he copied the stolen data to his personal computer and ultimately brought it to the United States while on a two-week leave.

After reaching out unsuccessfully to reporters at the *New York Times* and the *Washington Post*, Manning visited a Barnes and Noble store, where he used the public wireless network and uploaded the documents to WikiLeaks, a site dedicated to publishing leaked and stolen data. Manning later described a feeling of relief: "I felt I had accomplished something that allowed me to have a clear conscience based upon what I had seen, read about and knew were happening in both Iraq and Afghanistan every day."[54]

The volume of classified data that Manning stole was unprecedented, at least in the public eye: 391,832 reports on the Iraqi war (2004–9),[55] 91,000 documents on the war in Afghanistan

51. Bradley Manning, "PFC Manning's Statement Redacted," Google Docs, January 29, 2013, at 6, https://docs.google.com/file/d/0B_zC44SBaZPoQmJUYURBUnBycUk/edit.

52. Manning, "PFC Manning's Statement," 4.

53. Manning, "PFC Manning's Statement," 7.

54. Manning, "PFC Manning's Statement," 14.

55. "The Iraq War Logs," WikiLeaks, accessed March 16, 2018, https://wikileaks.org/irq (accessed March 16, 2018).

(2004–10),[56] hundreds of files on Guantanamo Bay detainees,[57] and 251,287 U.S. diplomatic cables.[58]

10.3.2 Caught!

Manning was caught—but not because investigators successfully tracked down the source of the leak. Although the military network was reportedly monitored, Manning later described a culture of pervasive apathy: "I even asked the NSA guy if he could find any suspicious activity coming out of local networks . . . he shrugged and said . . . 'its [*sic*] not a priority.'"[59]

Manning might have gotten away with his crime, but, feeling isolated, he reached out to reformed cybercriminal Adrian Lamo online and confessed. Shortly thereafter, Lamo reported Manning to the DoD.[60] Days later, Manning was arrested in Iraq and sent to a U.S. military prison.

The Insider Threat

For the U.S. military, Manning's identification was an important turning point. Once Manning's access to the classified military network was removed, he could no longer gather additional materials to leak. Responders had the opportunity to interrogate him directly and determine precisely what information had been stolen so that they could prepare for publication (or try to prevent similar breaches from occurring).

The realization that an insider had leaked the data also caused the military to seriously reevaluate its information access control policies. In the preceding years, the U.S. military had worked to expand access to information so that personnel could operate more effectively and efficiently. "We want those soldiers at a forward operating base to have all the information necessary, not just for their own security, but to accomplish their mission," said Defense Secretary Robert Gates. "Should we change the way we approach that or do we continue to take the risk?"[61] Manning's actions triggered an investment in internal cybersecurity. Shortly

(*Continues*)

56. "Afghanistan," WikiLeaks, accessed March 16, 2018, https://wikileaks.org/afg.

57. D. Leigh, J. Ball, I. Cobain, and J. Burke, "Guantánamo Leaks Lift Lid on World's Most Controversial Prison," *Guardian*, April 25, 2011, https://www.theguardian.com/world/2011/apr/25/guantanamo-files-lift-lid-prison.

58. "Cablegate: 251,287 Diplomatic Cables, Nearly All from 2003 to 2010," WikiLeaks, accessed March 16, 2018, https://wikileaks.org/plusd/?qproject[]=cg&q=#result.

59. Evan Hansen, "Manning-Lamo Chat Logs Revealed," *Wired*, July 13, 2011, https://www.wired.com/2011/07/manning-lamo-logs.

60. Ed Pilkington, "Adrian Lamo on Bradley Manning: 'I Knew My Actions Might Cost Him His Life,'" *Guardian*, January 3, 2013, https://www.theguardian.com/world/2013/jan/03/adrian-lamo-bradley-manning-q-and-a.

61. Spencer Ackerman, "Top U.S. Officer: WikiLeaks Might Have Blood on Its Hands," *Wired*, July 29, 2010, https://www.wired.com/2010/07/top-military-officer-wikileaks-has-blood-on-its-hands/.

(*Continued*)

thereafter, the Defense Advanced Research Projects Agency (DARPA) announced funding for the "Cyber Insider Threat" (CINDER) program, designed to root out insider threats within government and military networks.[62]

10.3.3 Cooperation: A New Model

WikiLeaks suddenly found itself under heavy pressure from the world's largest military power—and it was wildly unmatched. Manning's arrest sparked an international manhunt for Julian Assange, who now held a treasure trove of classified U.S. military records and was hell-bent on releasing it.

Investigative journalist Nick Davies observed that Assange "was facing four separate lines of attack":[63]

> The first was physical—that someone would beat him up or worse. The second was legal—that Washington would attempt to crush WikiLeaks in the courts. The third was technological—that the US or its proxies would bring down the WikiLeaks web site. The fourth and perhaps most worrisome possibility was a PR attack—that a sinister propaganda campaign would be launched, accusing Assange of collaborating with terrorists.

Convinced that the yet-to-be-revealed cables were "the biggest story on the planet," Davies reached out to WikiLeaks, hoping to convince Assange to partner with the *Guardian*. Under normal circumstances, Assange viewed the media with suspicion and as competitors. Davies knew that Assange would not be inclined to simply hand over his biggest scoop to the much-derided "mainstream media." But he also knew that Assange was vulnerable. Partnering with major media outlets would provide WikiLeaks with legitimacy, as well as access to more resources.

The *Guardian* itself was also vulnerable. Headquartered in the United Kingdom, it was subject to "hostile" media laws. By publishing the leaked U.S. cables, the *Guardian* could find itself facing an injunction by the U.S. embassy, which would halt publication. As Assange revealed the full extent of the leaked databases—including the Iraq and Afghanistan war logs, as well as the Guantanamo files—the risk of pressure or retaliation by the United States seemed ever more real.[64]

---

62. Defense Advanced Research Projects Agency (DARPA), "DARPA-BAA-10-84, Cyber Insider Threat (CINDER) Program," FedBizOps.gov, August 25, 2010, https://www.fbo.gov/index?s=opportunity&mode=form&id=cf11e81b7b06330fd249804f4c247606; Spencer Ackerman, "DARPA's Star Hacker Looks to WikiLeak-Proof Pentagon," *Wired*, August 31, 2010, https://www.wired.com/2010/08/darpas-star-hacker-looks-to-wikileak-proof-the-pentagon/.

63. Leigh and Harding, *Julian Assange's War on Secrecy* (London: Guardian, 2013), 96–97.

64. Leigh and Harding, *Julian Assange's War on Secrecy*, 97–101.

Weighing the options, Davies proposed that WikiLeaks partner with the *Guardian* and other respected papers to publish the material simultaneously. Assange agreed, and the group pulled in the *New York Times* and (eventually) Berlin-based *Der Spiegel*. Assange requested that the *New York Times* publish five minutes ahead of the other papers, to reduce the risk of Manning being convicted of espionage.[65]

Thus began an unlikely partnership: the international desperado Assange, working with three of the most respected global media outlets. As described by the *Guardian* staff, it was "a new model of cooperation aimed at publishing the world's biggest leak."[66] And it worked.

10.3.4 Drowning in Data

Manning's leak was a vast and detailed record of war events and diplomatic correspondence. It was far more than any one person could possibly digest, and much of the material required specialized knowledge to fully understand. The reporters quickly discovered that having possession of data wasn't the same as actually *knowing* anything.[67] In addition to making sense of the material, the media outlets also had to authenticate and redact it.

The mainstream media brought in experts who analyzed the data and uncovered shocking, previously unknown facts about both wars, as well as scandalous diplomatic correspondence. They established teams of analysts, including experts in the Iraq and Afghanistan wars, in order to verify the authenticity of the data and digest it. The *Guardian* set up a "war room" at its London headquarters. It quickly built a searchable database to facilitate internal analysis. Reporters flew in from around the world, including Islamabad, New York, and Germany. Manning didn't know it, but as he suffered in prison, world-renowned journalists pored over the documents he had leaked.

The *New York Times* likewise set up a war room at its facilities and provided assistance analyzing the data. *Der Spiegel*'s reporters turned out to be vital, as they had access to the German federal parliament's investigation into Afghanistan and were therefore able to confirm the authenticity of many of the details in the leaked documents.[68]

The sheer volume of data that WikiLeaks and its partners analyzed and published was unprecedented. "In Ellsberg's day, it took nearly a year to photocopy the 7,000-page Pentagon papers and most of another year to get excerpts published," reflected *Time* magazine. "The push-button model of WikiLeaks compresses the timeline radically and permits the universal broadcast of voluminous archives in full, so much so that leak hardly seems to suffice as a metaphor." Indeed, it wasn't so much a leak as a flood.[69]

The teams of analysts distilled the material into powerful articles, infographics, and catchy sound bites, which were powerful media products.

---

65. Leigh and Harding, *Julian Assange's War on Secrecy*, 100–101.

66. Leigh and Harding, *Julian Assange's War on Secrecy*, 98.

67. Leigh and Harding, *Julian Assange's War on Secrecy*, 106.

68. Leigh and Harding, *Julian Assange's War on Secrecy*, 104–10.

69. Barton Gellman, "Person of the Year 2010: Runners-Up: Julian Assange," *Time*, December 15, 2010, http://content.time.com/time/specials/packages/article/0,28804,2036683_2037118_2037146,00.html.

10.3.5 Redaction

Much of the data leaked in the Manning breach contained identifying information that could place war informants or other civilians at risk of harm. The reporters were deeply concerned about the safety of people mentioned in the leaked documents, such as Iraqi and Afghani informants who had worked with U.S. operatives—especially because the leaked databases were simply reports written up by U.S. military personnel, who themselves were fallible. "I thought about the American bases I'd visited, the Afghan characters I'd met in little villages and towns," said *New York Times* reporter Declan Walsh. "There was no way I'd like to put them at risk on the basis of a document prepared by some wet-behind-the-ears American GI, who may or may not have correctly understood the information they were receiving."

While the mainstream media was planning to publish only a handful of documents, Assange at first made it clear that WikiLeaks would publish the entire contents of the leak. The reporters had a hard time convincing him that redaction was important "Well, they're informants," Assange once said callously at a dinner. "So, if they get killed, they've got it coming to them."[70]

Eventually, however, the reporters convinced Assange of "the logic of redaction." Assange refrained from publishing 15,000 files from the Afghanistan war logs that were "most likely to contain identifying details." After WikiLeaks was called to task for not fully redacting the material that it did publish, Assange used a software program to automatically redact names from the Iraqi war logs.[71]

The result was that WikiLeaks developed new technical processes for redacting large volumes of material. Unfortunately, the redaction was undermined when the full archive was accidentally exposed—but it nonetheless established a precedent for future breaches.

The Leakers' Leak

Assange had agreed to publish only a fraction of the U.S. cables (which had been redacted by the mainstream media partners), and did so at first. However, this effort was later undermined, accidentally, as a consequence of his interactions with the mainstream media. WikiLeaks had locked the entire compendium of unredacted, leaked U.S. cables in an encrypted, password-protected file and circulated it widely online. The rationale was that if WikiLeaks were shut down, the password to unlock the file could be revealed, enabling continued access to the information.

Assange provided the encrypted file and password to the *Guardian* team in order to give them access to the data—but the *Guardian* team unwisely published the password in a header of its 2011 book, with the label "Assange's 58-character password." In defense, the *Guardian* staff said that Assange had told them that the password would be valid for only a few hours—to which WikiLeaks clapped back (via Twitter): "Changing a sent file's encryption password

(*Continues*)

70. Leigh and Harding, *Julian Assange's War* on Secrecy, 111.

71. Leigh and Harding, *Julian Assange's War on Secrecy*, 112–13.

(*Continued*)

is just as impossible as it is for a writer to change the text of a book after printing."[72] Since the cat was already out of the bag, on September 1, 2011, WikiLeaks published all 251,287 unredacted cables.

"In the end, all the efforts at confidentiality came to naught," reported *Spiegel Online*, in a play-by-play description."For many people in totalitarian states this could prove life-threatening. . . . [N]o potential whistleblower would feel comfortable turning to a leaking platform right now." This, of course, turned out not to be true.[73]

10.3.6 Data Products

In order for the public to understand the significance of the exposed data, it had to be digested and turned into data products. Reporters around the globe worked tirelessly to distill the vast volumes of data into bite-sized chunks that could be absorbed by a mainstream audience. The result was a series of pointed articles that highlighted key findings from analysis of the exposed data. The *Guardian* even pulled in a "data visualizer" to produce an interactive graphical display for readers.[74]

At the same time, WikiLeaks prepared to publish a massive, searchable database of the redacted source material, which the public could examine themselves. This searchable database is an important feature of WikiLeaks that facilitates widespread and ongoing analysis of the data to this day.

10.3.7 Timed and Synchronized Releases

When the material was finally released (in a series of synchronized campaigns), it triggered protests and debate within the United States, sparked anger around the world, and caused what one foreign minister referred to as "the 9/11 of world diplomacy."[75]

But publishing the cables was no easy feat. WikiLeaks and its partners deliberately synchronized releases to minimize risk to any one party, while maximizing attention. The global media partners coordinated extensively to synchronize their launch time, but tripped up when early copies of *Der Spiegel* were accidentally distributed.

Despite the chaotic launch, the publication was a massive success, from a readership standpoint. The *Guardian* experienced "remarkable traffic—the 4.1 million unique users clicking on

72. R. Mackey, J. Harris, R. Somaiya, and N. Kulish, "All Leaked US Cable Were Made Available Online as WikiLeaks Splintered," September 1, 2011, *New York Times*, https://thelede.blogs.nytimes.com/2011/09/01/all-leaked-u-s-cables-were-made-available-online-as-wikileaks-splintered.

73. Mackey, Harris, Somaiya, and Kulish, "All Leaked US Cable"; Christian Stöcker, "A Dispatch Disaster in Six Acts," *Spiegel Online*, September 1, 2011, http://www.spiegel.de/international/world/leak-at-wikileaks-a-dispatch-disaster-in-six-acts-a-783778.html.

74. Leigh and Harding, *Julian Assange's War on Secrecy*, 104–6

75. Leigh and Harding, *Julian Assange's War on Secrecy*, 202.

it that day was the highest ever. Record numbers would continue, with 9.4 million browsers viewing WikiLeaks stories between 28 November and 14 December."[76]

On July 25, 2010, WikiLeaks published the Afghan war documents. The *Guardian*, the *New York Times*, and *Der Spiegel* all published reports on the same day. The data dump, which The *Guardian* hailed as "one of the biggest leaks in US military history," painted a day-by-day picture of the Afghanistan conflict as it unfolded, for a six-year period between 2004 and 2009.[77]

Then, on October 22, 2010, WikiLeaks published the Iraq war logs, after having proactively shared them with The *Guardian*, the *New York Times*, *Der Spiegel*, *Le Monde* (French), and others. The trove of documents—which at 391,832 cables was four times as large as the Afghan war logs—was once again hailed as the "[b]iggest document leak in history" by the Bureau of Investigative Journalism.[78] The media highlighted juicy revelations, such as the discovery that the total number of deaths was 30,000 higher than the official figures reported by the United States.[79]

The impact of the Iraq and Afghanistan war logs was dwarfed, however, by "Cablegate," the subsequent publication of more than a quarter of a million U.S. diplomatic cables. Released on November 28, 2010, the cables contained the "unvarnished" internal reports from U.S. diplomats around the world. "Hillary Clinton and several thousand diplomats around the world are going to have a heart attack," predicted Manning.

"The German chancellor is referred to as Angela 'Teflon' Merkel. Karzai is said to be 'driven by paranoia.' North Korean leader Kim Jong Il is said to suffer from epilepsy. Libyan leader Moammar Gadhafi's full-time nurse is called a 'hot blond,'" summarized NPR, after the cables' release.[80]

In addition to candid, often offensive observations of world leaders, the cables included startling revelations, such as the fact that U.S. diplomats were engaged in extensive spying operations, gathering intimate details on important geopolitical figures such as U.N. leadership, including highly personal information such as credit card numbers, passwords, fingerprints, and even DNA.[81]

Over the following years, WikiLeaks grew increasingly savvy and timed data dumps in order to create very effective media campaigns.

---

76. Leigh and Harding, *Julian Assange's War on Secrecy*, 202.

77. Nick Davies and David Leigh, "Afghanistan War Logs: Massive Leak of Secret Files Exposes Truth of Occupation," *Guardian*, July 25, 2010, https://www.theguardian.com/world/2010/jul/25/afghanistan-war-logs-military-leaks.

78. Rachel Oldroyd, "In Video: The Biggest Document Leak in History Exposes Real War," Bureau of Investigative Journalism, October 21, 2010, https://web.archive.org/web/20130429122404/http://www.iraqwarlogs.com/2010/10/21/the-leaked-us-files-and-what-they-mean/.

79. M. Chulov, C. McGreal, L. Eriksen, and T. Kington, "Iraq War Logs: Media Reaction Around the World," *Guardian*, October 28, 2010, https://www.theguardian.com/world/2010/oct/28/iraq-war-logs-media-reaction.

80. Dina Temple-Raston, "WikiLeaks Release Reveals Messier Side of Diplomacy," NPR, November 28, 2010, https://www.npr.org/2010/11/28/131648175/wikileaks-releases-huge-cache-of-u-s-diplomatic-cables.

81. David Leigh, "US Embassy Cables Leak Sparks Global Diplomatic Crisis," *Guardian*, November 28, 2010, https://www.theguardian.com/world/2010/nov/28/us-embassy-cable-leak-diplomacy-crisis.

Nothing Is Off the Record

Hillary Clinton and several thousand diplomats did appear to have heart attacks, as Manning had predicted. Years later, Clinton's reaction to Cablegate was ironically exposed to the world as part of the Podesta email leaks, which contained a transcript of her private speech to Goldman Sachs:[82]

> This is all off the record, right? You're not telling your spouses if they're not here. . . . Okay. I was Secretary of State when WikiLeaks happened," said Clinton, referring to Cablegate. "You remember that whole debacle. So out come hundreds of thousands of documents. And I have to go on an apology tour. And I had a jacket made like a rock star tour. The Clinton Apology Tour. I had to go and apologize to anybody who was in any way characterized in any of the cables in any way that might be considered less than flattering. And it was painful.

The lesson: In modern times, nothing is guaranteed "off the record" if it's recorded—and certainly not if it's sent via email.

10.3.8 Takedown Attempts Backfire

While publishing the Manning data, WikiLeaks was hit by a massive distributed denial-of-service attack, which swamped its servers. Assange and his team quickly moved WikiLeaks' main page into the Amazon cloud, which was capable of withstanding the attack. However, Senator Joe Lieberman called Amazon, pressuring the company into shutting down WikiLeaks' hosting. Amazon complied, canceling WikiLeaks' service with a terse note that stated the organization had violated Amazon's terms of service.[83]

"The dominoes then started to fall," described *Guardian* reporters Leigh and Harding.[84] WikiLeaks' DNS provider, EveryDNS, removed the organization's domain name (wikileaks.org) and email pointers from its systems, forcing WikiLeaks to switch to an alternate domain: wikileaks.ch.

The next day, PayPal suspended WikiLeaks' account, due to a "violation of the PayPal Acceptable Use Policy." Shortly thereafter, Assange's Swiss bank closed his accounts, on the basis that he did not actually live in Geneva, as required. Mastercard and Visa likewise shut down WikiLeaks' accounts. Without the ability to accept donations, WikiLeaks was cut off from its financial lifeline.[85]

"Whole sections of WikiLeaks' physical and human infrastructure kept disappearing," described Assange, years later. "[T]he banks placed us under extralegal financial blockades

---

82. CBS/AP, "Clinton's Goldman Sachs Speech Transcripts in Latest Podesta Email Dump," *CBS News*, October 15, 2016, https://www.cbsnews.com/news/clintons-goldman-sachs-speech-transcripts-in-latest-podesta-email-dump.

83. Leigh and Harding, *Julian Assange's War on Secrecy*, 205.

84. Leigh and Harding, *Julian Assange's War on Secrecy*, 206.

85. Leigh and Harding, *Julian Assange's War on Secrecy*, 206.

while communication companies, foreign governments, and our human networks were pressured by Washington."[86]

Under fire, WikiLeaks was forced to react quickly and build a more resiliant data distribution and hosting architecture, relying on web proxies and a network of mirror sites. "[WikiLeaks] had no financial defense; it had no legal defense; and it had no political defense," explained Assange. "Its defenses were purely technical. That meant a system that was distributed at its front with many domain names, and a fast ability to change those domain names, a caching system, and, at the back, tunneling through the Tor network to hidden services."[87] Shortly thereafter, WikiLeaks began accepting donations via Bitcoin, as a means of circumventing banking restrictions.[88]

Tip: It's Out There

Even the most well-connected and well-funded breach response teams cannot be certain of removing breached data from the Internet after it is leaked. While it's typically worth trying, it is also important to assume the data is out there permanently and focus on taking a proactive approach to public relations.

10.3.9 Distribution

As news of the Manning leaks spread, WikiLeaks gained supporters. Hordes of journalists followed WikiLeaks on social media, excitedly combing through new releases and distributing digests to the masses. Assange gained not only fame but inspired legions of passionate followers. As the embattled nonprofit was struggling to keep its servers up and running, John Perry Barlow, founder of the Electronic Frontier Foundation posted a resounding call to action on Twitter: "The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops."[89]

Anonymous heeded the battle cry. The stampeding herd echoed Barlow's words and issued their own call to action:[90]

> Julian Assage deifies everything we hold dear. He despises and fights censorshop constantly. . . . Now, Julian is the prime focus of a global manhunt. Governments across the world are baying for his blood, politicians are up in arms about his recent leak. . . . Anonymous has a chance to kick back for Julian.

86. Assange, *When Google Met WikiLeaks*, 14.

87. Assange, *When Google Met WikiLeaks*, 73–74.

88. Nermin Hajdarbegovic, "Assange: Bitcoin and WikiLeaks Helped Keep Each Other Alive," CoinDesk, September 16, 2014, https://www.coindesk.com/assange-bitcoin-wikileaks-helped-keep-alive.

89. John Perry Barlow (@JPBarlow), "The first serious infowar is now engaged. The field of battle is WikiLeaks. You are the troops," *Twitter*, December 3, 2010, 1:32 a.m., https://twitter.com/jpbarlow/status/10627544017534976.

90. Errisian Cacaphony, "A for Assange: Operation Avenge Assange," *YouTube*, 1:38 min, posted December 8, 2010, https://www.youtube.com/watch?v=fUfEoyxLJEQ; "4Chan Launches 'Operation Avenge Assange,' Targets Julia Gillard," Pedestrian TV, December 6, 2010, https://www.pedestrian.tv/news/4chan-launches-operation-avenge-assange-targets-julia-gillard.

The inspiring lead-in was followed by a seven-point list of specific action items. Supporters were called upon to boycott PayPal, spread the leaked cables, vote for Assange as the *Time* magazine Person of the Year, and organize community marches, among other activities.[91] Anonymous quickly pointed their cannons at Visa and Mastercard, crippling both companies' websites. They also targeted PayPal—with only limited success—and attacked the websites of WikiLeaks opponents Senator Joe Lieberman, Sarah Palin, and others.[92]

Due to the chaotic and disorganized nature of Anonymous, the group's assault on payment providers was short-lived. It did, however, garner international press and demonstrate support for WikiLeaks and Assange. "The event was something new," wrote the *Guardian* team, "the internet equivalent of a noisy political demonstration."[93] Although Anonymous had been "demonstrating" for years, Operation Avenge Assange took them—and WikiLeaks—to a whole new level of publicity.

Assange handily won the *Time* magazine readers' choice for Person of the Year in 2010.[94] Using his newfound power, he stoked the flames of media attention. He made it clear that more releases would follow and that he wasn't just targeting governments—he intended to aggressively go after corporate America.

"Early next year, Julian Assange says, a major American bank will suddenly find itself turned inside out," reported *Forbes* in late 2010. "Tens of thousands of its internal documents will be exposed on WikiLeaks.org with no polite requests for executives' response or other forewarnings. The data dump will lay bare the finance firm's secrets on the Web for every customer, every competitor, every regulator to examine and pass judgment on."[95]

WikiLeaks emerged from the Manning breach with a vastly expanded public profile and social media following. The result was a powerful new distribution model, in which WikiLeaks was able to feed information about new releases directly to legions of journalists and the public.

10.3.10 Punishment Backfires

The ensuing national debate illustrates how punishing the source of a data leak can have mixed consequences. The U.S. government sought to make Manning an example in order to discourage future leakers. He was moved to a high-security facility at Quantanimo, Virginia, where he was forcibly isolated for 23 hours a day, and barred access to clothing for extended periods of time.[96]

---

91. "4Chan Launches."

92. Esther Addley and Josh Halliday, "WikiLeaks Supporters Disrupt Visa and MasterCard Sites in 'Operation Payback'," *Guardian*, December 9, 2010, https://www.theguardian.com/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback.

93. Leigh and Harding, *Julian Assange's War on Secrecy*, p. 208.

94. Megan Friedman, "Julian Assange: Readers' Choice for TIME's Person of the Year 2010," *Time*, December 13, 2010, http://newsfeed.time.com/2010/12/13/julian-assange-readers-choice-for-times-person-of-the-year-2010.

95. Andy Greenberg, "WikiLeaks' Julian Assange Wants to Spill Your Corporate Secrets," *Forbes*, November 29, 2010, https://www.forbes.com/sites/andygreenberg/2010/11/29/wikileaks-julian-assange-wants-to-spill-your-corporate-secrets/.

96. "Bradley Manning Will Be Credited 112 Days for Horrendous Stay at Quantico," RT: US News, January 8, 2013, https://www.rt.com/usa/manning-wikileaks-sentence-pretrial-581.

Proponents of the press and civil rights activists condemned Manning's harsh treatment. "Bradley Manning deserves a medal," wrote *Guardian* reporter Glenn Greenwald, as Manning awaited trial.[97] "[T]hese proceedings reveal the US government's fixation with extreme secrecy, covering up its own crimes, and "intimidating future whistleblowers."

Ultimately, Manning was sentenced to 35 years in prison—the longest-ever sentence in the United States for a data leak. The ACLU's Ben Wizner remarked that it was "a sad day for all Americans who depend on brave whistleblowers and a free press for a fully informed public debate . . . When a soldier who shared information with the press and public is punished far more harshly than others who tortured prisoners and killed civilians, something is seriously wrong with our justice system."[98]

Others lauded the strong sentence. "The message won't be lost for everyone in the military," said Steven Bucci of the Heritage Foundation. "When you sign a security clearance and swear oaths, you actually have to abide by that. It is not optional."[99]

In January 2018, Manning's sentence was commuted by President Barak Obama—a parting gift as he left office. According to a senior administration official, the President took into account Manning's expression of remorse, and felt that the time already served was "sufficient punishment for the serious crimes she committed."[100] Manning (who changed her gender while in prison) took her first steps as a free woman on May 17, 2017.[101] In 2018, she ran for the U.S. Senate under her new name, Chelsea Manning.[102]

10.3.11 Copycats

The techniques leveraged by WikiLeaks and its mainstream media partners in the Manning breach served as a model for future data hosts and journalists who sought to publish sensitive data leaks. For example, years later the unprecedented Panama Papers breach was leaked to a German newspaper, *Suddeutsche Zeitung*. After reviewing a sample of the data, the newspaper reached out to the ICIJ, which had experience coordinating large data leaks. Much like in the Manning case, the ICIJ built a searchable database of the documents in order to facilitate analysis by experts. The ICIJ then shared the material with 370 journalists from more than

---

97. Glenn Greenwald, "Bradley Manning Deserves a Medal," *Guardian*, December 14, 2011, https://www.theguardian.com/commentisfree/2011/dec/14/bradley-manning-deserves-a-medal.

98. Julie Tate, "Bradley Manning Sentenced to 35 Years in WikiLeaks Case," *Washington Post*, August 20, 2013, https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd.

99. Tate, "Bradley Manning Sentenced."

100. Jordan Fabian, "Obama Commutes Chelsea Manning's Sentence," *Hill*, January 17, 2017, http://thehill.com/homenews/administration/314663-obama-commutes-chelsea-mannings-sentence.

101. Bill Chappell, "Chelsea Manning, Once Sentenced to 35 Years, Walks Free After 7 Years," NPR, May 17, 2017, https://www.npr.org/sections/thetwo-way/2017/05/17/528731790/after-serving-7-years-of-a-35-year-sentence-chelsea-manning-to-walk-free.

102. Ed Pilkington and Martin Pengelly, "Chelsea Manning Announces Run for US Senate with Video on Twitter," *Guardian*, January 14, 2018, https://www.theguardian.com/us-news/2018/jan/13/chelsea-manning-democrat-us-senate-maryland.

100 media outlets, based in 76 countries.[103] The *Guardian* and others established war rooms in order to analyze the monumental data trove.

The media partners distilled the Panama Papers leak into a myriad of powerful data products, including a searchable database, interactive relationship diagrams, and even a choose-your-own adventure game called "Stairway to Tax Heaven," which enabled readers to digest the exposed data in novel ways.[104] On Sunday, April 3, 2016, the ICIJ and partner organizations published the first articles based on the Panama Papers leak, in a media blitz that was carefully coordinated to maximize attention.

10.3.12 Consequences

When the dust had settled, one thing was clear: Bradley Manning changed WikiLeaks, and WikiLeaks changed the world.

The "megaleak" (as WikiLeaks founder Julian Assange later called it) jump-started WikiLeaks as a global distribution outlet. They say what doesn't kill you makes you stronger, and that certainly held true for WikiLeaks in the Manning case. Once WikiLeaks reached that critical level of fame, it had enough followers to easily command attention for future leaks.

"The government has recognized that WikiLeaks is not an event —it is a capability," said New York University scholar Clay Shirky. "[A]nybody who can get material out of a classified system can now publish it worldwide in a way that can't be redacted or removed."[105]

The leaks demonstrated that even a global powerhouse as mighty as the U.S. government couldn't stop the publication of leaked data. The world emerged with a new process for digesting and distributing stolen information, one that even large corporations and government agencies couldn't subvert. It set an example for future would-be leakers, as well as journalists and hosting providers seeking to expose information. The Manning leak represented a key turning point for data breaches because it:

- **Showed that data exposure could have a deep impact on a breached organization, as well as far-reaching consequences that rippled around the world.** This further encouraged would-be leakers (as well as extortionists, as we will see in Chapter 11, "Extortion").
- **Demonstrated that the "insider threat" was real.** No longer could organizations focus on securing their external perimeter (largely ignoring internal security, as so many organizations did). The Manning leak spurred a wave of investment to guard against inside attackers.

---

103. International Consortium of Investigative Journalists, "Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption," April 3, 2016, https://www.icij.org/investigations/panama-papers/20160403-panama-papers-global-overview.

104. Organized Crime Corruption and Reporting Project, "Offshore Leaks Database," accessed March 18, 2018, https://www.occrp.org/en/panamapapers/database; International Consortium of Investigative Journalists, "Interactive Game: Stairway to Tax Heaven," accessed March 18, 2018, https://www.icij.org/investigations/panama-papers/stairway-tax-heaven.

105. Gellman, "Person of the Year 2010."

- **Spurred WikiLeaks to develop resilient hosting and partnerships with the mainstream media.** This paved the way for the megaleaks phenomenon, which dramatically amplified the impact of exposure attacks.
- **Brought huge attention to WikiLeaks, significantly raising the profile of both the organization and its founder, Julian Assange.** This turned WikiLeaks into a powerful data distribution machine because mainstream reporters (and the general public) followed his communications and new releases in droves.

Suddenly, vast volumes of data could be leaked and picked apart by journalists around the world. Attackers could selectively release or highlight certain data in order accomplish specific objectives—whether political, economic, or financial. "These megaleaks . . . they're an important phenomenon," reflected Assange. "And they're only going to increase."[106]

For breach responders, the lessons from the Manning case were powerful:

- Any and all data stored digitally is at risk of exposure.
- Exposed data can spread *very* quickly to reach a mainstream audience.
- Large volumes of exposed information may be distilled into powerful *data products*.
- Redaction isn't guaranteed even when attempted.
- Attempting to take down the data against a hosting provider's will can result in greater publicity and empower the host (i.e., the Streisand Effect).
- Punishing the perpetrator can (surprisingly) build public sympathy for him or her.
- Once data is exposed, there is a good chance it will be available on the Internet permanently (particularly if it is interesting).
- Data leaks can have extensive and unpredictable consequences, not just for the breached organization but for anyone whose information has been included in the exposed repository.

10.4 Conclusion

In this chapter, we explored the motivations for data exposure and discussed important technologies that evolved to facilitate these types of breaches. We also outlined key response tactics, including verification, identification, data removal, and public relations. Finally, we discussed megaleaks and the role that the Manning leak played in the development of this phenomenon. In the next chapter, we will see how the maturation of data exposure tactics intertwined with cyber extortion to result in a new type of data breach.

106. Greenberg, "WikiLeaks' Julian Assange."

Chapter 11

Extortion

Hundreds of thousands of patient records went up for sale on "TheRealDeal" dark market in July 2016. There, a cybercriminal group that went by the name "TheDarkOverlord" (TDO) offered three databases to anyone who would pay the (hefty) price:[1]

- "Healthcare Database (48,000 Patients) from Farmington, Missouri, United States." Price: 151.96 bitcoins (approx. $97,000 at the time)
- "Healthcare Database (397,000 Patients) from Atlanta, Georgia, United States." Price: 607.84 bitcoins (approx. $388,000 at the time)
- "Healthcare Database (210,000 Patients) from Central/Midwest United States." Price: 321.71 bitcoins (approx. $205,000 at the time)

It was far from an isolated incident. TDO regularly hacked into organizations, stole their data, and then threatened to expose it to the world unless the victims paid a steep ransom. If an organization didn't pay, TDO would sell the data, wait for a period of time to give the buyer the opportunity to use it, and then ultimately publish it for the world to see.

Once the data was published, the hacked organization suffered painful consequences. Patients were angry and blamed the healthcare facility. Sordid news stories came out, embarrassing leadership and damaging organizations' reputations. In many cases, the exposure triggered a reportable data breach under state or federal laws, resulting in investigations and potential fines.[2] This, of course, made the criminals' future threats all the more credible.

"I delete everything I have once a victim pays," promised TDO in an interview. "I also supply a report regarding the results and the documentation of my attack. A little token of gratitude and support."[3]

1. Dissent, "Quest Records LLC Breach Linked to TheDarkOverlord Hacks; More Entities Investigate If They've Been Hacked," DataBreaches.net, August 15, 2016, https://www.databreaches.net/quest-records-llc-breach-linked-to-thedarkoverlord-hacks-more-entities-investigate-if-theyve-been-hacked.

2. Dissent, "Extortion Demand on Athens Orthopedic Clinic Escalates as Patient Data is Dumped," DataBreaches.net, August 3, 2016, https://www.databreaches.net/extortion-demand-on-athens-orthopedic-clinic-escalates-as-patient-data-is-dumped.

3. Dissent Doe, "655,000 Patient Records for Sale on the Dark Net after Hacking Victims Refuse Extortion Demands," *Daily Dot*, June 27, 2016, https://www.dailydot.com/layer8/655000-patient-records-dark-net; Dissent, "Quest Records."

True or not, many victims succumbed to TDO's extortion schemes, paying hefty fees in exchange for the criminals' promise of deletion and silence. Along the way, TDO took steps to frighten and cajole their victims into complying. Tactics included partial data dumps with threats of more, public jabs at the victim organization via Twitter, and even personal messages to staff and data subjects in the affected organizations.

The criminals leveraged knowledge of U.S. federal and state cybersecurity laws in their threats against victim organizations. For example, they knew full well that HIPAA-regulated executives feared the negative publicity, fines, and investigations that would result from a data breach. "We've recently had the pleasure of . . . acquiring 3.5k patient records that contain both PII [personally identifiable information] and PHI [protected health information]," wrote TDO, as they published a sample of stolen data from a small Manhattan dental clinic. "As proof that what we say is true, you will find below a link to sample of the data. Note that they contain PHI. Their records show that some patients have HIV, AIDS, Herpes Simplex, or Venereal Disease, and much more."

Unfortunately, the tormented dental clinic was hardly alone. In June 2017, TDO began "playing a game" called "A Business a Day," where they leaked data stolen from a different company each day. The criminals started by leaking 6,000 patient records from a Los Angeles medical practice and followed the next day with another 6,300 from a Beverly Hills optical clinic. "We love PII. Especially PII of celebrities" said the hackers' Twitter feed.[4]

TDO purposefully used the media as a means of pressuring victims into paying. Much like WikiLeaks, the group's Twitter followers quickly grew to include mainstream reporters, ensuring that every new data exposure was distributed to the mainstream media. "Every time I put a new listing up it gets reported without hesitation now," a TDO representative bragged to *Motherboard* magazine.

In addition to extorting healthcare providers, TDO terrorized school districts, IT companies, media distributors (famously including Netflix), law firms, accountants, manufacturers, police departments, and more.[5]

"The country is under siege right now," said Dr. Jay L. Rosen, CEO of the Tampa Bay Surgery Center (another TDO victim).[6]

The cyber extortion problem was even worse than news reports revealed. There was ample evidence that many of the victims paid to keep the breaches quiet and therefore remained uncounted.

---

4. Dissent, "They View It as 'Hollywood,' but TheDarkOverlord Hit Another Medical Entity (Update 2)," DataBreaches.net, June 21, 2017, https://www.databreaches.net/they-view-it-as-hollywood-but-thedarkoverlord-hit-another-medical-entity.

5. Dissent, "Irony: When Blackhats are Our Only Source of Disclosure for Some Healthcare Hacks (Update1)," DataBreaches.net, June 24, 2017, https://www.databreaches.net/irony-when-blackhats-are-our-only-source-of-disclosure-for-some-healthcare-hacks; @thedarkoverlord, "Tweets," *Twitter*, accessed October 13, 2018, https://twitter.com/tdo_hackers.

6. Tim Johnson, "How TheDarkOverlord is Costing U.S. Clinics Big Time with Ransom Demands," *Kansas City Star*, May 15, 2017, http://www.kansascity.com/news/nation-world/article150679092.html.

11.1 Epidemic

By 2016, cyber extortion was widespread. Ransomware—malicious software that encrypts data and holds it hostage until the victim pays a fee—affected more than 2.3 million users worldwide.[7] Criminal gangs routinely hacked into organizations, stole data, and then threatened to expose it, extracting large payments in exchange for keeping quiet.

11.1.1 Definition

Cyber extortion is when an attacker threatens to damage the confidentiality, integrity, or availability of information unless he or she receives a payment or other desirable outcome. Types of cyber extortion include:

- **Denial** - Data is rendered unavailable until the desired outcome is achieved.
- **Modification** - Attackers threaten to alter sensitive data unless the desired outcome is achieved.
- **Exposure** - Attackers impact the confidentiality of information, threatening to publish or share sensitive data unless the desired outcome is achieved.
- **Faux** - The extortion attempt is merely a ruse designed to obscure the attacker's true purpose.

Of these four types, denial and exposure extortions are by far the most common.

Modification extortion is still largely theoretical, but a frightening concept. "Imagine, mixing together all patients' medications in a hospitals, or their blood results or their radiology images," writes medical doctor and cybersecurity consultant Saif Abed, considering the potential for a "Clinical Integrity Extortion" attack. "[I]magine that clinicians often not having time to second guess what they see on their screens. . . . [I]t's a disaster."[8]

Each type of extortion requires a different response, as we will see throughout this chapter.

11.1.2 Maturation

Cyber extortion became an epidemic because of the maturation of specific technologies, laws, and cybersecurity standards, including:

- **Cryptocurrency**, which gave criminals an easy way to demand quick, anonymous payments in extortion cases.

7. "KSN Report: PC Ransomware in 2014-2016," Kaspersky Lab, June 22, 2016, https://securelist.com/pc-ransomware-in-2014-2016/75145/.

8. Saif Abed, "The Clinical Integrity Extortion (CIE) Attack: A Healthcare Cyber-Nightmare," *Medium*, September 14, 2018, https://medium.com/@s.abed86/the-clinical-integrity-extortion-cie-attack-a-healthcare-cyber-nightmare-3c74f61f5b5d.

- **Crimeware for exploitation and extortion**, which evolved to the point where even less-savvy users could purchase a commercial exploit kit or ransomware software and point-and-click their way to success.
- **Data breach laws and standards**. In the United States, by 2016, the Health Insurance Portability and Accountability Act (HIPAA) had teeth, and most states had data breach notification laws. Criminals used these regulations to incite fear in their victims, specifically targeting regulated data and highlighting it in extortion threats.

The result of these advancements was that cyber extortion became a quick and low-risk crime to commit. Furthermore, organizations that publicly reveal that they have been hacked can suffer devastating reputational damage and incite widespread anger—and some are willing to pay a hefty ransom to avoid that.

In the rest of this chapter, we will explore the three most common types of cyber extortion and discuss response strategies for each.

11.2 Denial Extortion

Denial cyber extortion occurs when an attacker prevents legitimate users from accessing information assets until they take action, such as paying a fee. In this section, we will focus on ransomware, the most common form of denial extortion.

11.2.1 Ransomware

Ransomware is software designed to lock up user files or entire operating systems in exchange for a fee. Modern ransomware outbreaks commonly begin in one of two ways:

- **Phishing:** The attacker sends a phishing email or social media message to an employee. The employee clicks on the link, which infects a workstation with malware.
- **Remote login:** Attackers scan the Internet searching for remote login interfaces with default or weak account credentials. Once obtained, they can access the systems themselves or sell access to other criminals.

Once the attacker installs ransomware, typically:

- **The ransomware encrypts files on the local computer**, as well as writable network shares and accessible cloud storage repositories. Depending on what files the user has access to, this can prevent him or her from accessing a large volume of valuable data, potentially crippling operations.
- **An electronic "ransom note" appears on the user's desktop or screen**, notifying the user of the encryption and providing the user with an opportunity to purchase decryption keys. Often, a deadline is included, after which the price for the decryption keys increases

substantially. Some strains of ransomware also permanently delete files periodically (e.g., every hour).

- **If the victim pays the ransom**, the criminal (theoretically) provides a decryption key, which will allow recovery of all or part of the volume of affected files.

Ransomware can wreak havoc, particularly if it spreads through an organization's network. In addition to denying access to the victim's data, attackers may steal or access sensitive information, which means that a ransomware infection may also constitute a data breach. Even if the operational impacts are short lived, the fallout from the data breach aspect may be long term and significant.

11.2.2 Encryption and Decryption

The first known ransomware, the AIDS Trojan, was released in 1989 by biologist Joseph Popp, who studied baboons in East Africa. He distributed the AIDS Trojan by mailing a floppy disk labeled "AIDS Information - Introductory Diskettes" to 20,000 AIDS researchers across 90 countries. After 90 reboots, the malware hid directories and encrypted filenames, and instructed victims to send $189 to a P.O. box in Panama in order to obtain a repair tool. The malware had a critical flaw, however: It used symmetric key cryptography, meaning the same key was used to encrypt and decrypt. Moreover, the key was the same for all victims, and defenders quickly developed decryption tools.[9]

In late 2004, modern ransomware emerged and began to spread via phishing and web-based attacks. This early ransomware was clunky and often had deficiencies that allowed savvy users to bypass the malicious software and regain access to their data without paying a fee. For example, Kaspersky[10] Labs reported encountering a new malware strain called GPCode, which encrypted files and left behind a ransom note that instructed the victim to "buy our decryptor" by contacting the attacker at a Yahoo email address. The researchers found that GPCode was likely of Russian origin and used a custom-written encryption algorithm that was easy to break. The author quickly fine-tuned the malware and released new, stronger variants, eventually switching to the strong RSA encryption algorithm.

Over the next several years, ransomware authors experimented with different models of extorting money from victims, including fake antivirus scans, which locked the user's computer and posted a warning on the screen requiring the user to call to "activate" the antivirus license. This evolved into law-enforcement-themed locker ransomware, which locked the victim's computer and posted a notice from law enforcement that accused the user of downloading pirated data or viewing pornography. The victim was told to "pay a fine" in order to have the computer unlocked. "[I]n the early days, attackers tricked victims into downloading fake tools to fix computer issues," wrote Symantec researchers. "Eventually, it dropped any pretense of

9. Alina Simone, "The Strange History of Ransomware," March 26, 2015, Medium.com, https://medium.com/un-hackable/the-bizarre-pre-internet-history-of-ransomware-bb480a652b4b.

10. Denis Nazarov and Olga Emelyanova, "Blackmailer: the story of Gpcode," SecureList, June 26, 2006. https://securelist.com/blackmailer-the-story-of-gpcode/36089 (accessed June 6, 2019).

being a helpful tool to just displaying a blatant request for payment to restore access to the computer."[11]

In some cases, ransomware strains delete but do not overwrite the original files, enabling forensic analysts to use common file recovery software to restore the original content. Another recovery tactic is to attempt to reverse-engineer the decryption key. If an analyst has access to both encrypted files and a sample of the original, nonencrypted files, then in some cases it may be possible to use cryptographic techniques to determine the key. However, this takes time and computing power, if it is possible at all.

Over time, ransomware developers refined their software and processes. Ultimately, they found that asymmetric cryptography was an effective means of rendering victims' files inaccessible. Attackers encrypted the victim's files with one key and held the corresponding decryption key hostage until they received payment. (See § 5.3.2 for details on asymmetric cryptography.) When implemented carefully, it is virtually impossible for victims to recover their files without a backup.

CryptoLocker was one widespread ransomware variant that emerged in 2013 and leveraged strong encryption (researchers observed it using the popular RSA algorithm with up to 2048-bit keys). It also overwrote the original files, rendering them impossible to recover even for forensics experts.[12] In 2014, a team of law enforcement agencies and security firms infiltrated the botnet used to spread CryptoLocker and captured a huge database of private keys, enabling many victims around the world to finally decrypt their data.

Today, many reputable security firms have released tools that can decrypt popular ransomware strains, either leveraging implementation issues or available private keys. Sites such as NoMoreRansom.org can help defenders determine their ransomware strain and quickly obtain decryption utilities. While there is no guarantee that these tools will be successful, it is often worth trying as a first step.

11.2.3 Payment

Before cryptocurrency existed, it was difficult for cybercriminals to extort payments over the Internet. Cybercriminals attempted to collect payment using wire transfers, payment voucher systems such as MoneyPak or paysafecard, or more creative methods such as text messages to premium phone numbers. All of these payment transfer systems were brokered by a third party and could potentially leave a trail that would help law enforcement track down the attacker. As a result, criminals typically used a money-laundering service in conjunction with a money transfer method.[13]

The rise of Bitcoin gave criminals a new, convenient option. When CryptoLocker erupted in 2013, it accepted payment using either Bitcoin or prepaid cash voucher. Victims in the United States were typically given 72 hours to pay the equivalent of $300. The ransom note warned

11. Kevin Savage, Peter Coogan, and Hon Lau, "The Evolution of Ransomware" (whitepaper, Symantec, Mountain View, CA, August 6, 2015), 10, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf.

12. "CryptoLocker: What Is and How to Avoid It," Panda Security, May 14, 2015, https://www.pandasecurity.com/mediacenter/malware/cryptolocker/.

13. Savage, Coogan, and Lau, "Evolution of Ransomware," 22–25.

that the victim's decryption key would be destroyed when the deadline passed, rendering the files permanently unrecoverable. However, victims reported that they could still purchase the key even after the deadline— at a much higher price.

Cryptocurrency dramatically reduced the risk of engaging in cyber extortion, which in turn caused the crime to proliferate. By 2014, a wide range of ransomware had sprung up that instructed bewildered victims to pay using cryptocurrency. Since most nontechie users were not familiar with Bitcoin, ransomers often left user-friendly, detailed instructions that walked the victim through the process of purchasing and transferring cryptocurrency.[14]

At first, the majority of cryptocurrency ransom demands were relatively small, on average about $300. Criminals soon realized, however, that when they locked up an organization (as opposed to an individual), they had leverage to extort far larger sums of money. For example, in 2015 the Swedesboro-Woolwich School District in New Jersey was held hostage for 500 bitcoins (approximately $124,000 at the time).[15] This trend became more widespread, particularly as more and more organizations purchased cyber insurance that covered large ransom payments.

In 2018, sophisticated ransomware evolved that encrypted individual file shares and devices with different keys ("key differentiation"). That meant criminals could charge victims money to recover each individual file share or storage device.[16]

11.2.4 World Domination

By the close of 2015, ransomware had become a dominant threat. "Never before in the history of human kind have people across the world been subjected to extortion on a massive scale as they are today," observed Symantec researchers in their 2016 *Internet Security Threat Report*.[17]

The Center for Internet Security dubbed 2016 "The Year of Ransomware."[18] In February 2016, Hollywood Presbyterian Hospital in Los Angeles was famously shut down by ransomware, generating an intense media storm. The hospital ended up paying $17,000 to the hackers in exchange for recovering its data.[19] The following month, Methodist Hospital in Kentucky was forced to declare an "internal state of emergency" after ransomware encrypted files throughout its IT infrastructure.

---

14. Brian Krebs, "2014: The Year Extortion Went Mainstream," *Krebs on Security* (blog), June 26, 2014, https://web.archive.org/web/20140702112204/http://krebsonsecurity.com/2014/06/2014-the-year-extortion-went-mainstream.

15. Rebecca Forand, "School District 'Bitcoin Hostage' Situation Continues; FBI, Homeland Security Investigating," NJ.com, March 24, 2015, http://www.nj.com/gloucester-county/index.ssf/2015/03/school_district_bitcoin_hostage_situation_continue.html.

16. Sherri Davidoff, "Cyber Alert: New Ransomware Holds Individual File Shares Hostage," LMG Security, May 16, 2018, https://lmgsecurity.com/cyber-alert-new-ransomware/.

17. Lucian Constantin, "New Ransomware Program Threatens to Publish User File," *Computerworld*, November 5, 2015, https://www.computerworld.com/article/3002120/security/new-ransomware-program-threatens-to-publish-user-files.html; Symantec, "2016 Internet Security Threat Report," *ISTR* 21 (April 2016): 58, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

18. Katelyn Bailey, "2016: The Year of Ransomware," *Center for Internet Security* (blog), 2016, https://www.cisecurity.org/blog/2016-the-year-of-ransomware/.

19. John Biggs, "LA Hospital Servers Shut Down by Ransomware," Tech Crunch, February 17, 2016, https://techcrunch.com/2016/02/17/la-hospital-servers-shut-down-by-ransomware.

As the ransomware epidemic spread, cybercriminals took over computer systems around the world, including hospitals, schools, police stations, and more. When a ransomware infection was found, local IT staff typically worked to clean off the malware and restore data as quickly as possible. Victims rarely reported ransomware incidents to the public voluntarily, but in severe cases where day-to-day operations were impacted, word spread.

Within a few years, commercial ransomware software became a popular product on the dark web. Criminals could purchase turnkey malware, distribute it using common exploit kits, and rake in profits. To make it even easier, many vendors peddled "ransomware-as-a-service," where customers on the dark web paid a fee to rent ransomware platforms, which often provided user-friendly dashboards and easy-to-understand instructions.

Targeting Healthcare

Ransomware is rampant within the healthcare industry. A 2016 study showed that over half of hospitals were hit with targeted ransomware attacks in the previous year.[20] Criminals have held healthcare providers around the world hostage, encrypting their files and refusing to release the key until the victim pays a hefty fee. Since healthcare providers depend on access to electronic medical records and intake/discharge systems in order to provide service, a ransomware infection has the potential to knock out operations, impacting patient care and quickly causing a public relations nightmare.

While severe cases of ransomware infection may make the news, most of the time affected organizations make an effort to keep incidents very quiet. As a result, the number of cases reported in the news likely represents just a small percentage of the actual incidents that occur. Since healthcare organizations depend so heavily on quick access to data (such as patient charts and prescriptions), they are prime targets for ransomware. Furthermore, the challenges involved in healthcare cybersecurity, previously discussed in Chapter 9, make healthcare providers particularly vulnerable. When ransomware affects patient operations, such as intake processes, EHR databases, or more, these cases can very quickly become big news.

11.2.5 Is Ransomware a Breach?

Victims traditionally took a "wishful thinking" approach to ransomware, assuming that even though attackers had locked up their data, they hadn't actually *taken* it. In the case of the Swedesboro-Woolwich School District, the superintendent reassured the public that the confidentiality of student data was not at risk. "Ransomware is more like an octopus," he said. "Its tentacles wrap around your data. There's no destruction or extraction."[21]

In keeping with this philosophy, most organizations treated ransomware exclusively as an operational issue. When an infected system was discovered, IT staff worked diligently to

20. Tom Sullivan, "More Than Half of Hospitals Hit with Ransomware in Last 12 Months," *Healthcare IT News*, April 7, 2016, https://www.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months.

21. Forand, "School District."

clean it, restore the data, and move on. "Because ransomware is so common, hospitals aren't reporting them all," said James Scott, senior fellow at the Institute for Critical Infrastructure Technology.[22]

Reality eventually caught up. Breach coaches who managed incidents realized that if an attacker had access to encrypt a victim's data, the cybercriminal could well have stolen it, too. And why not? Criminals could resell sensitive data on the black market *and* make money from denial extortion. To that end, ransomware developers added data-stealing capabilities to ransomware strains. For example, Cerber and Spora ransomware samples were updated to include keystroke loggers and password theft functionality. "By stealing credentials from victims, criminals are ensuring a double payday, because not only can they make money from extorting ransoms, they can also potentially sell stolen information to other criminals on underground forums," reported Danny Palmer of *ZDNet*.[23]

Ransomware is often the most visible sign of a compromise—but not the only component. Attackers frequently lurk in an organization's systems for months or years, stealing data or renting bots, before deciding to quickly monetize access by installing ransomware.

In 2016, the OCR caused waves throughout the healthcare industry by unequivocally stating that ransomware attacks should be treated as breaches. They published a "fact sheet" on ransomware and HIPAA, clearly stating that "when electronic protected health information (ePHI) is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired." That means that ransomware incidents should be treated as potential data breaches and must be reported unless the covered entity can demonstrate a "low probability" that PHI was compromised, as per the four-factor risk assessment outlined in the HITECH Breach Notification guidelines.[24] (For a detailed discussion about data breaches and the healthcare industry, see Chapter 9, "Health Data Breaches.")[25]

For other types of data, it's not always clear whether ransomware constitutes a data breach. The level of investigation and conclusions vary considerably based on the experience and risk tolerance of the breach coach and victim organization. It is always wise to retain a sample of the malware whenever possible, so that forensic analysts can assess its capabilities if needed.

11.2.6 Response

Responding to ransomware can be a painful and traumatic experience. There is typically little or no warning, and when ransomware hits, it can cause major damage. The DRAMA model of data breach management applies, as described in Chapter 4, "Managing DRAMA":

- **DEVELOP** your data breach response function.
- **REALIZE** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.

---

22. Jessica Davis, "Ransomware Rising, but Where Are All the Breach Reports?" *Healthcare IT News*, March 20, 2017, http://www.healthcareitnews.com/news/ransomware-rising-where-are-all-breach-reports.

23. Danny Palmer, "Ransomware 2.0: Spora Now Steals Your Credentials and Logs What You Type," ZDNet, August 24, 2017, http://www.zdnet.com/article/ransomware-2-0-spora-now-steals-your-credentials-and-logs-what-you-type.

24. U.S. Department of Health and Human Services, "Fact Sheet: Ransomware and HIPAA," accessed January 18, 2018, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es.

25. U.S. HHS, "Factsheet."

- **ACT** quickly, ethically, and empathetically to manage the crisis and perceptions.
- **MAINTAIN** data breach response efforts throughout the chronic phase and potentially long-term.
- **ADAPT** proactively and wisely in response to a potential data breach.

In ransomware cases, there are distinct issues that response teams should consider during the develop, realize, and act phases. These include:

- **Include ransomware in data breach planning.** All too often, organizations plan for the *operational* impacts of ransomware but forget to consider that it may also legally qualify as a data breach. A common result of this oversight is that critical evidence is not preserved during the immediate response to ransomware, making it impossible to rule out a data breach later.
- **Preserve evidence early on.** Make sure that first responders are trained to recognize ransomware as a potential data breach. Preserve important evidence such as the malware sample whenever possible, so that if needed, forensic analysts can later analyze it to determine whether the malware is capable of exfiltrating data or is designed to simply deny access. If ransomware is widespread and it is not feasable to perform a full forensic acquisition of all affected computers, prioritize based on volume and sensitivity of the data stored on each system.
- **Activate crisis communication plans quickly.** Since ransomware can have a sudden and dramatic impact on an organization's operations, news of the infection can become widely known very quickly. This is especially true for organizations that suffer a widespread infection that impacts public-facing services (as in hospitals and local government agencies).
- **Manage both the operational and data breach impacts of the crisis.** It can be challenging to manage a potential data leak while also working to restore operations. Consider, in advance, how to divide up the work and ensure that both issues are addressed.

In the "Act" phase, ransomware-specific crisis management steps include:

- **Assess the Damage** - Take an inventory of what data has been encrypted, and determine whether the organization can recover the data from backups, recreate missing data, or function without certain data sets.
- **Recover from Backups** - If available, restore as much data as possible from backups (after preserving appropriate evidence, of course).
- **Check for a Decryptor** - Technical experts can examine the encrypted systems to determine whether there is a known bypass—some way to unlock the files without paying to get the decryption key from the attackers.
- **Negotiate and Pay the Ransom** - If all else fails, then the organization may be stuck with a hard choice: pay to get the decryption key (which is not guaranteed to work) or fully rebuild, which in severe cases could threaten the viability of the organization. See the next section for a discussion of negotiation and payment in ransomware cases.

- **Fully Rebuild** - Many organizations choose (or are forced) to start from scratch, rebuild affected systems, and recreate lost data. This can be a painful, time-consuming, and expensive process.

11.2.6.1 Negotiation Tips

In ransomware cases, as in real-life hostage negotiations, you may need to come to an agreement with the extortionists regarding payment. Certain tactics can help increase your chances of a positive outcome. For example:

- **Demand "proof of data."** Before paying for a decryption key or tool to recover your data, make sure that the extortionists can actually deliver. Particularly in high-dollar cases, you can request that the ransomers send samples of decrypted files to ensure that they can actually fulfil their end of whatever deal you strike.
- **Act calmly, reasonablely, and logically.** Criminals are more likely to successfully negotiate with you if you build trust during your conversations and approach the discussion as a straightforward business deal rather than an emotionally charged situation.
- **Don't make unrealistic promises.** If you're not sure that you can pay or the dollar amount is genuinely too high, be straightforward. When criminals get annoyed by unmet expectations, they are more likely to retaliate or abandon the negotiation entirely.
- **Take a team approach.** As odd as it sounds, your organization and the extortionist have a mutual interest in reaching agreement. Leverage this in your conversations. Security consultant Hussam Al Abed recommends, "Use the word 'we' to encourage your captors to think of you as sharing mutual concerns. You do have a common interest in the outcome of this situation."[26]

At the same time, certain classic rules of hostage negotiation need to be rethought when it comes to ransomware. Unlike real-life hostage situations, the criminals behind ransomware do not have possession of a physical human being who needs to be fed, monitored, and kept alive in order to maintain leverage. Instead, perpetrators of ransomware can take over dozens of organizations and maintain their control with little ongoing effort.

The result is that cybercriminals have less incentive to close deals; they can store decryption keys for months or years if needed—or delete them on a whim. Consultants trained in real-life hostage negotiation tactics may be surprised to find themselves at a disadvantage in ransomware cases. Common wisdom is to reject the extortionists' first offer—a tactic that can backfire when dealing with cookie-cutter ransomware, where criminals may focus their time on easy money and ignore more complex discussions.

In addition, ransom notes often include a deadline after which files are automatically deleted or the ransom payment goes up. Victims that exceed this deadline due to negotiation attempts

26. Hussam A Al-Abed, "Extortion/Kidnapping Checklist," BankersOnline.com, July 21, 2003, https://www.bankersonline.com/qa/extortionkidnapping-checklist.

may find that they are unable to recover certain files as a result, or they end up paying a higher ransom due to the delay.

Should You Pay the Ransom?

When a victim is hit with a cyber extortion attack, often the most pressing question is, "Should I pay?" The answer is different for denial versus exposure extortion.

In denial ransomware, where the organization's data is inaccessible, this is a legitimate question that needs to be evaluated. Obviously, paying criminals is never a victim's preferred choice. Unfortunately, paying the ransom does sometimes make sense for victims of *denial* ransomware. The attackers have incentive to provide the key—otherwise, people would stop paying them. Once the organization has its data back, it can implement security procedures that will dramatically reduce the risk of a future attack.

In exposure cyber extortion, paying the ransom is never a winning strategy. Once criminals possess your data, you cannot trust them to delete it (and they may have already sold or shared it). What's more, paying the ransom signals to the criminals that you are susceptible to extortion, increasing the odds that you will be targeted in the future. There is nothing to stop the criminals from attempting to extort you over and over with the same stolen data. Some organizations may choose to pay an exposure ransom in an effort to demonstrate a good-faith effort at minimizing harm to data subjects. While this may work for a specific situation, it is certainly not guaranteed.

In all types of extortion, every ransom paid funds the extortionists' business model and therefore incentivizes crime.

11.3 Exposure Extortion

Just as ransomware reached epidemic proportions, criminals perfected modern data exposure tactics. For example, in 2016, the Panama Papers emerged as the largest data leak ever and was an important milestone in the development of the megaleaks phenomenon. That same year, the U.S. 2016 presidential elections were underway—and with them came a series of sophisticated, highly publicized data breaches that changed global politics forever.

Criminals realized that they could marry exposure and extortion tactics, resulting in a new type of data breach epidemic that struck fear in organizations around the globe: exposure extortion. They hacked into computers and threatened to publish sensitive information unless the victim paid a fee or took action. If the victim acquiesed, then (the criminals promised) they would delete the information and keep quiet. Of course, there was no guarantee that the criminals actually *did* delete the stolen data, and plenty of evidence to suggest that many sold it on the dark web while also holding the victim organizations for ransom.

Exposure extortion is almost always a data breach, in the colloquial sense if not the legal sense. Attackers typically obtain sensitive information by hacking into an organization's IT systems. Even if the victim pays the ransom and the stolen data remains unpublished, it is still

the case that an unauthorized party aquired it, and (depending on the data type) this fact alone can trigger state and national data breach notification laws. Because of this, organizations that choose to pay the ransom and remain quiet may place themselves in legal jeopardy and risk the wrath of regulators and consumers if the data breach is later uncovered.

To maximize impact, criminals often target data that is regulated (such as PHI or PII), intimate, or exceptionally valuable to an organization (such as a company's core intellectual property). In this section, we will discuss different types of exposure extortion cases, review strategies for response, and delve into a case study as illustration.

11.3.1 Regulated Data Extortion

Regulated data is typically regulated for a reason: because it is easy to use for fraud or to shame or embarrass an individual. Common types of regulated data in the United States include (but are not limited to):

- **Personally identifiable information (PII)** - Name, address, phone number, Social Security number (SSN), etc. "Personally identifiable information" and similar terms are defined in a variety of state and federal laws (there is no single universal definition).
- **Health information** - Medical records, treatment and diagnosis, healthcare billing information, and a variety of other personal details (see Chapter 9, "Health Data Breaches," for details on HIPAA and state health information laws).
- **Student educational records** - Grades, disciplinary records, student medical treatment, information about learning disabilities and other physical or psychological issues, and more. In the United States, the Family Educational Rights and Privacy Act of 1974 (FERPA) protects the privacy of education records for students of federally funded institutions.

As breach notification laws became widespread, it increased the likelihood that a data breach involving regulated information would result in fines, investigations, and widespread public outcry from the affected communities. This placed pressure on IT staff and management to invest in security.

Unfortunately, extortionists have learned to twist breach notification laws to their advantage, using the spectre of investigations, lawsuits, and angry stakeholders to frighten management of these organizations into caving to their demands. Ironically, as the public grew to better understand cybersecurity issues, the potential for reputational damage due to a data breach increased, putting even more pressure on organizations to sweep data breaches under the rug.

Given the high concentration of regulated data in hospitals and schools (and the relatively low budget for security compared with financial institutions), these organizations have become popular targets for extortionists.

11.3.1.1 School Districts

In 2017, TDO claimed responsibility for extorting school districts in Iowa, Montana, and Texas. (Many other cases may have occurred outside the public spotlight since cyber extortion cases are

often handled very quietly.)[27] "Imagine if we published all of your sensitive behavioural reports from your counselors and social workers on the open internet," they threatened in one school district's ransom note. "Imagine if we published student grades and even the shoddy student work. How about nurse reports and private health information? What would the parents have to say about this? What sort of lawsuits would they begin? What would happen if everyone found out the reason we closed down multiple districts and over thirty sites is due to your failure to secure your networks?"[28]

The criminals demanded a $150,000 ransom, payable in installments over a one-year period, or $75,000 if the school district paid the entire sum immediately.

To really turn the screws on their victims, TDO used stolen contact information to communicate directly with data subjects themselves. In the Iowa school district case, the criminals sent death threats to parents. One mother received a text from the cybercriminals that read, creepily: "The life of a precious young child is so precious." The communications often included detailed information, such as childrens' names and home addresses. In response, many parents kept their children home from school, and some school districts shut down in the days following the attack.

"I wanted the public to exist in a state of fear before I make my move," explained a spokesperson for TDO. "This will allow the government protecting your children to look poorly in the light of the public."[29]

11.3.1.2 Healthcare

The case of Athens Orthopedic Clinic (AOC) illustrates how cyber extortionists use sophisticated public relations tactics to stoke the public's anger and use it to pressure management into paying. This is especially effective when a case involves highly sensitive data such as health information. In June 2016, TDO hacked the clinic and demanded 500 bitcoins as ransom (approx. $329,000 at the time). Apparently AOC opted not to pay.

"[P]aying ransom does not guarantee any further criminal activity will not take place," a spokesperson for AOC later explained.[30]

In response, TDO turned up the heat—by going public. The criminals posted a sample of the stolen data—500 patients' records—on Pastebin, along with a public demand for payment.[31] Based on the leaked samples, the stolen databases included fields such as name and address,

---

27. Valerie Strauss and Moriah Balingit, "Education Department Warns of New Hacker Threat as 'Dark Overlord' Claims Credit for Attacks on School Districts," *Washington Post*, October 26, 2017, https://www.washingtonpost.com/news/answer-sheet/wp/2017/10/26/education-department-warns-of-new-hacker-threat-as-dark-overlord-claims-credit-for-attacks-on-school-districts/; Ms. Smith, "Dark Overlord Hacks Schools across U.S., Texts Threats against Kids to Parents," CSO, October 9, 2017, https://www.csoonline.com/article/3230975/security/dark-overlord-hacks-schools-across-us-texts-threats-against-kids-to-parents.html (accessed December 9, 2018).

28. "Cyberthreat Closes Schools," Petronella Technology Group, accessed June 3, 2019, https://petronellatech.com/cyberthreat-closes-schools/.

29. Smith, "Dark Overlord Hacks Schools."

30. Dissent, "Extortion Demand on Athens Orthopedic Clinic Escalates as Patient Data is Dumped," *DataBreaches.net*, August 3, 2016, https://www.databreaches.net/extortion-demand-on-athens-orthopedic-clinic-escalates-as-patient-data-is-dumped.

31. Dissent, "Extortion Demand on Athens."

gender, SSN, health insurance details, and more. Additional screenshots from the stolen data dumps showed that the criminals had access to full medical records, including diagnoses, prescription history, appointments, and surgeries.[32]

Days later, AOC publicly acknowledged the breach for the first time (despite the fact that AOC management had reportedly known about the breach for a month). "We did not make any public disclosure of the breach at that time so as not to interfere with their investigation or push the hacker into a mass public release of data," explained the clinic, in a statement on its website.[33] By late July 2016, AOC had reported the breach to the OCR and began mailing breach notification letters to affected patients.[34]

With the ransom demand still unpaid in early August, TDO leaked an additional 1,500 records, with a message directed personally at CEO Kayo Elliott: "Pay up, Kayo."[35]

The criminals were all too happy to disparage their victim in interviews and on social media. "It was like stealing candy from a baby," said a TDO representative, who revealed that the group had broken into a popular Electronic Health Record (EHR) software product and used it to download the patient records from AOC. According to the clinic, the hackers initially gained remote access using the credentials of a "third-party vendor" that was a "nationally-known healthcare information management contractor."[36] As we saw in Chapter 9, vendor remote access is often a weak spot in healthcare clinic security postures.

TDO publicly claimed it was still in AOC's systems throughout June and July, chastising clinic staff in emails that were later shared with a journalist:[37]

> You have done little to mitigate against an advanced attacker. . . . It is now over two weeks later, and the passwords are still not changed. Let's just use the PACS imaging system as an example here. We just logged in a few minutes ago. Even after telling you directly which systems were compromised, nothing has been done to correct the issue.

Unfortunately, the clinic was woefully unprepared to launch an effective public relations campaign in response. For example, in a surprising departure from the norm, AOC elected not to provide free credit monitoring for affected patients—a move that inflamed public ire. Elliott

---

32. Dissent Doe, "655,000 Patient Records."

33. "Important News for Patients," Athens Orthopedic Clinic, accessed January 18, 2018, http://athensorthopedicclinic.com/important-news-patients.

34. "Breach Notification," Athens Orthopedic Clinic, August 2016, https://web.archive.org/web/20171115112741/http://ath-cdn.com/sites/default/files/AOC%20letter.pdf; Dissent, "Athens Orthopedic Clinic to Begin Notifying Patients of Hack (UPDATE2)," DataBreaches.net, July 25, 2016, https://www.databreaches.net/athens-orthopedic-clinic-to-begin-notifying-patients-of-hack.

35. "Screenshot of Athens Orthopedic Clinic PII/PHI Leak #3," DataBreaches.net, August 17, 2016, https://www.databreaches.net/wp-content/uploads/Screenshot AOC2016-8-17.jpg.

36. Jim Thompson, "Athens Orthopedic Won't Pay for Extended Credit Monitoring in Data Breach," OnlineAthens, August 12, 2016, http://www.onlineathens.com/mobile/2016-08-12/athens-orthopedic-wont-pay-extended-credit-monitoring-data-breach.

37. Dissent, "Athens Orthopedic Clinic Incident Response Leaves Patients in the Dark and Out of Pocket for Protection," DataBreaches.net, August 15, 2016, https://www.databreaches.net/athens-orthopedic-clinic-incident-response-leaves-patients-in-the-dark-and-out-of-pocket-for-protection.

said, "We are not able spend the many millions of dollars it would cost us to pay for credit monitoring for nearly 200,000 patients and keep Athens Orthopedic as a viable business."[38] An attorney representing AOC stated that the organization did not have insurance that would cover "cyber-related losses."[39] The clinic recommended that affected patients place a fraud alert on their credit reports and provided a toll-free number patients could use to contact that clinic to discuss the breach.[40]

Patients were furious. "They are assuming no responsibility for this financially," said one client, Marianne Causey. "I guess I just trusted them to take care of us better."[41]

Many questioned AOC's reported lack of insurance coverage. By 2016, cyber insurance had become a well-established best practice for organizations that maintained extensive amounts of personal information. Even the criminals took AOC to task, with the following (sadly insightful) remark: "[T]he year is sixteen past two-thousand and that they should have already had the necessary insurance policies to cover such incidents as this one."[42] (Cyber insurance coverage will be discussed in depth in Chapter 12, "Cyber Insurance.")

In the AOC case, as in most exposure extortion cases, the criminals attempted to use public perception as a weapon against the breached organization. For this reason, a strong crisis communications plan is a critical part of the response. Since the public has come to expect compensation such as credit monitoring in data breach cases, it is important to have appropriate insurance coverage or budget for this offering, or an alternate, equally effective image repair strategy.

11.3.2 Sextortion

Sex-related information has emerged as a major driver behind extortion cases in recent years. This can take many forms, such as "webcam blackmail," where an attacker obtains risque or obscene photos or videos of a victim and threatens to publish the images or share them with the victim's friends or family unless he or she receives a fee.

Criminals soon realized they didn't actually need footage to extort money from victims. Instead, they sent widespread phishing emails that claimed to have obtained footage of sex acts from the recipient's webcam, and threatened to release it to all of their contacts. In a more recent twist, the criminals included the victims' passwords (stolen in other data breaches) in the emails. Many recipients, frightened and ashamed, quietly paid—not realizing the attackers had only their email address; the footage didn't actually exist.[43]

---

38. Thompson, "Athens Orthopedic Won't Pay."

39. Dissent, "Athens Orthopedic Clinic Incident Response."

40. John Fontana, "Clinic Won't Pay Breach Protection for Victims; CEO Says It Would Be Death Of Company," ZDNet, August 16, 2018, https://www.zdnet.com/article/clinic-wont-pay-breach-protection-for-victims-ceo-says-it-would-be-death-of-company/.

41. Fontana, "Clinic Won't Pay."

42. Dissent, "Athens Orthopedic Clinic Incident."

43. Brian Krebs, "Sextortion Scam Uses Recipient's Hacked Passwords," *Krebs on Security* (blog), July 12, 2018, https://krebsonsecurity.com/2018/07/sextortion-scam-uses-recipients-hacked-passwords/.

The Ashley Madison "cheating" website breach illustrated how both a breached organization and the data subjects themselves can become victims of sex-related extortion. The Ashley Madison site was designed to attract married men and women who sought to have affairs. "Thousands of cheating wives and cheating husbands signup everyday looking for an affair," advertised the site. "With Our affair guarantee package we guarantee you will find the perfect affair partner."[44]

Hackers broke into the site and demanded that Ashley Madison's owner, Avid Life Media, take the site offline permanently, or they would publish customer records, "including profiles with all the customers' secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails."[45] When Avid Life didn't comply, they published the data as two compressed files on the dark web, where the data was downloaded and circulated around the world.

Millions of users had their names, addresses, and other personal details exposed. The BBC reported that two individuals committed suicide as a result of the breach.[46] There were 1,200 email addresses with the suffix for "Saudi Arabia," where adultery is illegal and may be punished by death.[47]

After the lists of Ashley Madison users were published, third-party criminals began targeting them with extortion threats. For example, one criminal gang sent mass emails to Ashley Madison users advertising their new site, "Cheaters Gallery," which they claimed would feature each email recipient. "We will launch the site with a big email to all the friends and family of cheaters taken from Facebook, LinkedIn and other social sites," the criminals threatened. "This will include you if do not pay to opting out." The price for "opting out" was approximately $500, payable in bitcoins.[48]

One Ashley Madison user who received the email wisely pointed out that paying the ransom guaranteed nothing—in fact, doing so could make you more of a target. "[E]ven if you pay these guys off, they can come back in a couple of months . . . and hit you up again. Wouldn't surprise me if they sold lists of people foolish enough to pay up to other groups. Once you pay you've told them you're vulnerable to blackmail forever."[49]

As a result of the breach, Ashley Madison was hit with dozens of lawsuits; it ultimately settled its class-action case for $11.2 million.[50]

---

44. Kim Zetter, "Hackers Finally Post Stolen Ashley Madison Data," *Wired*, August 18, 2015, https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

45. Zetter, "Hackers Finally Post."

46. Chris Baraniuk, "Ashley Madison: 'Suicides' over Website Hack," *BBC News*, August 24, 2015, https://www.bbc.com/news/technology-34044506.

47. Philippe Lopez, "The Global Fallout of the Ashley Madison Hack," France24, August 20, 2015, https://www.france24.com/en/20150820-global-fall-out-ashley-madison-hack.

48. Robin Harris, "Ashley Madison Blackmail Roars Back to Life," ZDNet, April 24, 2017, https://www.zdnet.com/article/ashley-madison-blackmail-roars-back-to-life/.

49. Harris, "Ashley Madison Blackmail."

50. David Kravets, "Lawyers Score Big in Settlement for Ashley Madison Cheating Site Data Breach," *Ars Technica*, July 17, 2017, https://arstechnica.com/tech-policy/2017/07/sssshhh-claim-your-19-from-ashley-madison-class-action-settlement/.

11.3.3 Intellectual Property

Corporate data, too, is targeted by extortionists. Companies that rely heavily on digital intellectual property (such as online gaming vendors, software firms, or media companies) are particularly vulnerable since a sudden release of their intellectual property can threaten their profits or even undermine the value of the entire organization. In this section, we will examine two corporate extortion cases: the Hollywood "Netflix" hack and an early breach of Bloomberg.

11.3.3.1 The "Netflix" Hack

On Christmas morning in 2016, Hollywood's Larson Studios learned about cyber extortion the hard way when the company's husband-and-wife owners, Rick and Jill Larson, received an email from TDO threatening to expose all of their data. The small business handled audio postproduction for major networks, and the stolen data reportedly included dozens of movies and TV shows from ABC, NBC, E!, Fox, FX, IFC, the Disney Channel, Netflix, and more. The criminals demanded 50 bitcoins to keep quiet and destroy the stolen data—approximately $50,000 at the time. If the Larsons didn't pay, the criminals threatened, they would release the shows, starting with Netflix's *Orange is the New Black*.

Fearful of their livelihood, the Larsons filed a police report—and paid the ransom. One factor was TDO's reputation for upholding its end of the bargain. "They would return the materials, destroy the materials, and it was over," said Rick Larson. "This was the way they work." It was an attractive offer: If the Larsons paid the money, it would all be over.

But the Larson's nightmare was only beginning. By late March, the FBI called to report that the criminals were using the files stolen from Larson to blackmail major networks. The Larsons had never told their clients about the breach, apparently partially due to pressure from the hackers themselves to keep quiet. Suddenly, the business owners found themselves under heavy scrutiny by the security teams from the major studios that they served. It wasn't just the company's network that was breached; it was the trust they had built with their clients.

By April, TDO was publicly taunting Netflix on Twitter, demanding a ransom payment to prevent the group from leaking *Orange is the New Black*. When Netflix didn't bite, the criminals dumped ten episodes before the scheduled premier.

In the aftermath of the breach, some of the Larsons' clients left. Major studios that remained required extensive audits and additional security measures. Ironically, despite investing "six figures" on security in response to the breach, Larson Studios continued to fight the perception of insecurity long afterwards.[51]

11.3.3.2 Bloomberg's Early Breach

Exposure extortion is nothing new; it is simply that criminals' tactics have become more sophisticated over time. Many of the lessons from early cases apply today. For example, in 1999,

---

51. Janko Roettgers, "Netflix Hackers Could Have Three Dozen Additional TV Shows, Films from Other Networks and Studios," *Variety*, April 30, 2017, https://variety.com/2017/digital/news/netflix-hackers-additional-shows-movies-1202404171/; Janko Roettgers, "How Hollywood Got Hacked: Studio at Center of Netflix Leak Breaks Silence," *Variety*, June 20, 2017, https://variety.com/2017/digital/features/netflix-orange-is-the-new-black-leak-dark-overlord-larson-studios-1202471400/.

Bloomberg was hit was a cyber extortion attempt. A hacker from Kazakhstan, Oleg Zezev, used a small business to sign up for Bloomberg's services, which resulted in Bloomberg sending Zezev the software needed to access the company's systems. Once Zezev had the software, he used it to find vulnerabilities within the system and then gained unauthorized access to employee and customer accounts (including that of founder Michael Bloomberg).

Zezev gathered screenshots of the company's email inboxes, credit card numbers, and internal data, and then emailed samples of these to Michael Bloomberg. He threatened to disclose the vulnerabilities and theft to the media and Bloomberg's customers, unless Bloomberg paid him $200,000. "There a lot (sic) of clever but mean heads in the world who will use their chance to destroy your system to the detriment of your worldwide reputation," wrote Zezev, using the pseudonym "Alex." He concluded with "Your security and reputation are in your hands."[52]

Michael Bloomberg agreed to pay $200,000, on the condition that Zezev meet with him in London to explain how he hacked the system. Amazingly, the hacker agreed. After meeting with Bloomberg and his team, Zezev and one of his cohorts were arrested in London. Ultimately, they were extradited to the United States, where Zezev was convicted of extortion and computer intrusion, and sentenced to more than four years in prison.[53]

The Bloomberg case was a rare instance where a cyber extortionist was caught. As in the case of Larson Studios, criminals often pressure their victims not to report to law enforcement in the first place. Even in serious cases where law enforcement agents investigate, extortionists tend to be good at hiding their identities or may be based in nonextradition countries.

James Comey, who at the time was the U.S. attorney for the Southern District of New York, used the Bloomberg hacker conviction as an opportunity to generate positive PR for law enforcement. This was also unusual because cyber extortion is often kept secret. Victims, of course, do not want anyone to know that their systems were vulnerable or that an attacker had access to sensitive information. If the attacker is successful at extorting a payment, often no one finds out. This is especially true for cases where the affected data is not covered by a data breach notification regulation.

Perhaps because law enforcement had successfully captured the perpetrator, the Bloomberg case was publicized. "The Internet is a powerful communication tool in helping international commerce," Comey said. "This case demonstrates law enforcement's commitment to prosecute vigorously those individuals, wherever they are located, who seek to abuse this tool to their own ends."[54]

11.3.4 Response

The most effective response to exposure extortion is, essentially, to treat it as a data exposure case (see Chapter 10, "Exposure and Weaponization," for details). After all, once the data is

52. U.S. Department of Justice, "US Convicts Kazakhstan Hacker of Breaking into Bloomberg LP's Computers and Attempting Extortion," press release, February 26, 2003, https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/zezevConvict.htm.

53. U.S. Department of Justice, "Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion," press release, July 1, 2003, https://www.justice.gov/archive/criminal/cybercrime/press-releases/2003/zezevSent.htm.

54. U.S. Department of Justice, "US Convicts Kazakhstan Hacker."

in the hands of a criminal, it's out there. You never know when it might resurface or become public.

Key actions for response teams to consider include:

- **Verify** that the data is authentic and originated from your organization. As we have seen, in exposure extortion cases, criminals may include information gathered from other breaches as a means of tricking victims into thinking they have more data than they really do.
- **Proactively communicate** with affected stakeholders, such as the data subjects and data owners. This is especially important because the extortionists may reach out to them in order to put pressure on the breached organization to pay. Remember that if you remain quiet and don't tell affected stakeholders about the breach, you risk damaging trust and potentially place your organization in legal jeopardy. By proactively contacting stakeholders, you preserve more trust in the relationship, and you may have the opportunity to set the narrative if word has not already gotten out. This also gives stakeholders more time to prepare for any potential fallout.
- **Conduct an effective public relations campaign.** This is especially important because extortionists often publicly belittle their victims and attempt to damage their reputations. If the breach is not yet public, prepare a public relations campaign that you can launch immediately if and when it does.
- **Offer posttrauma counseling** for affected stakeholders, such as management, IT staff, and victims. Extortion can be a frightening and emotional experience. In exposure extortion cases, repurcussions often reverbrate throughout the organization and the surrounding community. For many, it is a painful experience that will never be forgotten. In much the same way that organizations hire grief counselors to work with team members after a death, it may be wise to offer third-party counseling services following exposure extortion.

11.4 Faux Extortion

Faux extortion, where the attacker does not actually want what he or she appears to demand, has occurred at a global scale (although it is not as prevalent as denial or exposure extortion).

11.4.1 Case Study: NotPetya

In June 2017, the "NotPetya" malware spread like wildfire. It started in the Ukraine, where employees at organizations across the country suddenly found themselves locked out of their computers, staring at ransom notes that read: "If you see this text, then your files are no longer accessible, because they have been encrypted. . . . We guarantee that you can recover all your files safely and easily. All you need to do is submit payment and purchase the decryption key."[55]

55. "NotPetya Technical Analysis—A Triple Threat: File Encryption, MFT Encryption, Credential Theft," *CrowdStrike* (blog), June 27, 2017, https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/.

NotPetya used two stolen National Security Agency exploits to infect victims—and it spread like wildfire. "Within hours of its first appearance, the worm raced beyond Ukraine and out to countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania," reported Andy Greenberg of *Wired* magazine. "It crippled multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser."[56]

But despite the reassurances of the ransom note, no one recovered their files. The malware wasn't ransomware at all. It was designed to destroy. Security analysts confirmed that the installation ID normally used to recover the decryption key was fake and randomly generated. "Do NOT pay the ransom," counseled technical analysts from the security firm CrowdStrike. "No files will be recovered if the ransom is paid."[57]

After extensive investigation, intelligence agencies concluded that NotPetya was a cyberweapon developed by the Russian military, designed to damage Ukrainian organizations. The ransom messages were "only a ruse" used to hide the malware's true purpose.[58]

11.4.2 Response

The appropriate response to faux extortion varies depending on the criminals' true motives and the impact of the crime. From a data breach management perspective, if there is evidence that criminals may have had access to an organization's sensitive data, then it should be treated as a potential exposure case.

Requiring proof of data can help responders quickly gauge whether the criminals actually want to negotiate. If the criminals ignore requests or refuse to demonstrate that the data can be decrypted, then responders can ignore demands and quickly move on to a different recovery strategy.

11.5 Conclusion

Cyber extortion has emerged as a dominant threat, fueled by the development of cryptocurrency and point-and-click crimeware. In this chapter, we discussed four different types of cyber extortion: denial, modification, exposure, and faux. In the next chapter, we will discuss how organizations can transfer their risk to insurers and leverage their help during a breach response.

56. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

57. "NotPetya Technical Analysis."

58. Greenberg, "Untold Story of NotPetya."

This page intentionally left blank

Chapter 12

Cyber Insurance

In May 2014, the Montana Department of Public Health and Human Services (DPHHS) announced one of the largest potential breaches of healthcare data reported to date. More than 1.3 million people's records may have been exposed—more than the population of the entire state, which had only a million residents at the time. A department server had been hacked in July 2013 and wasn't discovered until ten months later. According to the state's notification, the server may have contained names, addresses, birth dates, Social Security numbers (SSNs), as well as "information related to health assessments, diagnoses, treatment, health condition, prescriptions, insurance, and bank account numbers."[1]

Once the unauthorized access to the server was detected, the state's response was swift and effective—in large part because it had help. "We were the first state to have cyber insurance," said Lynne Pizzini, chief information security officer (CISO) of Montana. Pizzini, a 27-year veteran of the IT industry, founded the state's information security program (she became passionate about information security after a janitor unplugged her server one night to plug in a vaccum). In FY 2012, the state had added a $2 million breach response policy through a speciality insurer, Beazley.

The breach response insurance proved invaluable when the DPHHS incident occurred. "We immediately pulled the server off the network and contacted our insurance company," said Pizzini. "They immediately sent us a legal contact that met with us on a daily basis and developed the communications plan, based on requirements in all fifty states. We started having daily incident meetings with the Department of Health. [The attorney] flew out the next day after we notified the insurance company."[2] The insurer also connected the state with a forensics firm, which began the technical investigation.

Since the information on the server included personal information (as defined by state law), as well as protected health information, the clock was ticking with respect to notification. Montana's data breach law required notification "without unreasonable delay," and HIPAA had a 60-day notification requirement (beginning on the day of discovery).

Within ten days, the forensic investigation was complete—a quick turnaround for a forensics case, but still painfully slow for the state's management team. ("It was agonizing!" said Pizzini, of the wait.) Forensic investigators reportedly found no evidence that the data had actually been

1. Montana Department of Health and Human Services (DPHHS), "Notice Regarding DPHHS Computer Server," accessed January 19, 2018, http://web.archive.org/web/20150105200535/http://dphhs.mt.gov/Portals/85/Documents/ComputerServerNotice.pdf.

2. Lynne Pizzini, interview by the author, May 22, 2017.

accessed, but there was not enough evidence to rule it out. The state had to decide whether to notify the public.

Ultimately, said Pizzini, Governor Steve Bullock made the decision to notify the public "out of an abundance of caution." The state issued a press release describing the incident, along with a dedicated help line that individuals could contact between Monday and Friday, from 7 a.m. to 7 p.m. The insurer's breach response team "knew what frequently asked questions we should have answers to, because of the experience they had working with clients," explained Pizzini during our interview. "They set up a call center, an 800 number, and had people available to answer the phone with us. . . . It was immediately used. There's no way we could have had any of those things in a timely manner [without insurance], because we didn't have the contracts that provided those services."[3]

The Associated Press reported statements from key executives that were perfectly in line with the notification, illustrating a well-coordinated response. "There is no information, no indication, that the hackers really accessed any of this information or used it inappropriately," said Richard Opper, director of the DPHHS.[4]

Montana then faced the daunting challenge of mailing notification letters to 1.3 million people. "[The insurer] helped us with the notification," explained Pizzini. "We had seven different letters because of the data that was on that server." Included was an offer for credit monitoring. By late June, an approved notification letter template was sent to a mail processing center, along with names and addresses for delivery. On July 3, the mail processing center began sending letters to affected individuals, at a rate of 200,000 per day.[5]

The public relations impact was short lived, with a few news reports and relatively little attention given the number of affected people. There were no lawsuits. The state's policy covered the vast majority of forensics, legal, and notification costs. Just as with auto insurance, the state's premium for cyber insurance went up after the DPHHS breach, although Pizzini says it was "well worth it just to keep the insurance."

Cyber insurance had changed the game by the time Montana discovered the DPHHS incident in 2014. While many organizations struggled upon discovering a potential breach, trying to figure out what to do and how to handle the public relations fallout, those with access to breach response services found that they had an experienced team at their fingertips. The immediate support of a team of experts, as well as quick access to call centers, bulk mailing providers, and other important services, meant that Montana was able to respond quickly, meet legal requirements, and implement an effective crisis communications plan.

Pizzini is quick to point out that cyber insurance is not a substitute for preventative measures—although she says cyber insurance can help spur the development of good cybersecurity programs. "You can't get it until you have a good program in place!" she says. "We've evolved because the requirements weren't as stringent back when we first got it. You have to have a firewall. You have to have intrusion detection. You have to have policies, security training. It's

3. Pizzini interview.

4. Lisa Baumann, "Montana to Notify 1.3 Million of Computer Hacking," Associated Press, July 2, 2014, https://insurancenewsnet.com/oarticle/Montana-to-notify-13-million-of-computer-hacking-a-525670#.XPcPZxZKipo.

5. NASCIO, "Are You Ready? Disruptive Change Is the New Norm" (NASCIO Mid Year 2015 Conference, Alexandria, VA, April 16–29, 2015), https://www.nascio.org/dnn/portals/17/2015MY/Cybersecurity%20Insurance.pdf (accessed January 19, 2018).

all of those things that are part of a good security program . . . which is understandable, because they don't want to have to pay for an incident."[6]

12.1 Growth of Cyber Insurance

At the end of 2017, insurers wrote an estimated $4.52 billion in global premiums for cyber insurance annually. Researchers estimated that volume could balloon to $17.55 billion in 2023.[7] According to Price Waterhouse Cooper, "[a]s recognition of cyber threats increases, take-up of cyber insurance in under-penetrated industries and countries continues to grow, and companies face demands to disclose whether they have cyber coverage (examples include the US Securities and Exchange Commission's disclosure guidance)."[8]

The growth of cyber insurance is driven by increasing costs, regulations, and media attention on data breaches. As organizations scramble to reduce their risk, they face two options: mitigate or transfer. Risk mitigation is an important part of the cybersecurity puzzle, but much like car accidents, bad things are bound to happen. Insurance allows you to transfer that residual risk to third parties, to protect your organization.

Cyber insurance is typically designed to transfer risks associated with loss of confidentiality or availability of data. Since the topic of this book is "data breaches," we will primarily focus on the risks associated with loss of confidentiality, although these often go hand-in-hand with operational impacts and outages.

12.2 Industry Challenges

As alluring as cyber insurance is, the industry is fraught with challenges, both for insurers and consumers. Cyber threats are constantly changing. Whereas once a "cyber" policy might need to primarily cover losses due to network outages or data exposure, today's high-risk threats include ransomware, cryptojacking, and more.

IT infrastructures are changing, too—and the risks change with them. The insurance industry's CRO Forum cited five factors that influence the threat landscape:[9]

- The cloud
- Shadow IT ("when business functions procure IT solutions without involving the IT department")

6. Pizzini interview.

7. "Global Cyber Security Insurance Market 2018," *Reuters*, May 16, 2018, https://www.reuters.com/brandfeatures/venture-capital/article?id=36676.

8. PwC, *Insurance 2020 & Beyond: Reaping the Dividends of Cyber Resilience* (London: PwC, 2015), https://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

9. CRO Forum, *Cyber Resilience: The Cyber Risk Challenge and the Role of Insurance* (Amsterdam, Netherlands: CRO Forum, December 2014), 7, https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf.

- Mobile and flexible working
- Bring Your Own Devices (BYOD)
- Internet of Things (e.g., smart buildings, wearable devices, appliances, etc.)

Finally, coverage options are not standardized and are often unclear. Cyber coverage can overlap with standard property and liability coverage, leading to questions about who is responsible for covering a loss—or whether anyone is responsible at all. "Policy wordings are currently inconsistent, with evidence of some clear cyber exclusions, some explicit inclusion . . . and many policies which are not explicit either way."[10] The details of coverage vary widely, with certain types lumped together under different names depending on the provider, and significant variation in the definitions of common terms such as "personal information."

12.3 Types of Coverage

Cyber insurance can include both first-party and third-party coverage. First-party coverage insures against losses related to damage that affects the insured organization itself, such as data destruction, lost revenue due to operational outages, and other impacts that directly affect the policyholder. Third-party coverage involves liability related to other parties as a result of a cybersecurity incident or data breach, such as consumers affected by exposure of their personal data, banks and card brands that are impacted by a payment card data breach, or regulatory bodies that assess fines.[11]

Common coverage options include:

- **Information Security and Privacy Liability** - Claims and damages payable due to parties as a result of a data breach or failure of computer security. This can even cover explicit violations of privacy or security-related laws, including liability for failure to notify affected parties in a timely manner following a breach. The costs of legal fees and other investigation expenses are often included.
- **Response/Remediation Services** - This covers costs associated with breach response. In some cases, the insurer will provide breach response services. Covered services may include:
  - Forensics services
  - Legal counsel
  - Crisis management
  - Call center services
  - Public relations

10. CRO Forum, *Cyber Resilience*.

11. "A Buyer's Guide to Cyber Insurance," Law360, October 23, 2013, https://www.law360.com/articles/480503/a-buyer-s-guide-to-cyber-insurance.

  - Notification
  - Credit monitoring/identity theft protection offers

In some cases, items from this list may be split out into separate coverage. Insurers may also provide proactive breach response training at no charge, such as tabletop exercises, training videos, and more.

- **Regulatory Defense and Penalties** - Costs related to regulatory action such as investigation, assessment, or penalties due to a violation of privacy or security regulations. For example, this might cover fines assessed by the Office for Civil Rights (OCR) due to HIPAA violations or the legal fees associated with appealing a penalty.
- **Payment Card Industry (PCI) Fines and Expenses** - Since PCI is a contractual requirement and not a regulation, associated fines and expenses are typically not covered under regulatory defense and penalties. Many insurance policies explicitly exclude contractual obligations. Organizations that process or store payment card data should consider obtaining PCI-specific coverage.
- **Network Interruption** - Lost revenue due to a cyber event, such as a denial-of-service attack on a retailer's website.
- **Media Liability** - Costs that the policyholder is required to pay as a result of copyright infringement, plagiarism, defamation, libel, or other negligent acts relating to publication of media.
- **Public Relations/Reputation Management** - Public relations and crisis communications costs associated with managing a negative publicity event. This typically includes the costs of responsive advertising via digital media, television, and print; social media campaigns; and image monitoring. In some cases, proactive reputation management plans and training are included.
- **Information Asset** - Expenses to restore, repair, or recreate data after corruption, destruction, or other loss.
- **Cyber Extortion** - Ransom payments and other fees associated with an extortion involving digital assets. This type of coverage typically covers the costs of retaining security professionals to help resolve the incident.
- **Cyber Terrorism** - Coverage for damages as a result of an act of cyber terrorism, typically as defined by the federal Terrorism Risk Insurance Act (TRIA). This means losses must exceed $5 million in aggregate and result from a "violent act or an act that is dangerous to human life, property or infrastructure" and is committed "as part of an effort to coerce the civilian population of the United States or to influence the policy or affect the conduct of the United States Government by coercion."[12] Terrorism (and war) are often explicitly excluded from coverage, unless a cyber terrorism endorsement is purchased.

12. Terrorism Risk Insurance Act §102(1), 15 U.S.C. §6701 note (2002); see also Alex Reger, *Terrorism Risk Insurance Program* (Research Report 2016-R-0208, Connecticut General Assembly, Office of Legislative Research, November 1, 2016), https://www.cga.ct.gov/2016/rpt/pdf/2016-R-0208.pdf.

- **Proactive Risk Management** - A relatively new development in cyber insurance is the integration of risk management tools and services, combined with cyber coverage. This can include security controls assessments, enterprise risk management assessments, response readiness evaluations, vulnerability scans, and other offerings—in addition to standard breach response services.

From Coffee to Cyber

I stood on the second floor of Lloyd's of London, leaning over the glass railing. Down below, men and women in suits and ties busily conversed in polished wooden booths (or "boxes," as they are called), with gray signs above that read "Advent," "Chaucer," "Beazley," and more. Here and there, small groups of professionals stood conversing. Tiny printers and copiers dotted the floor.

"Lloyd's started out as a coffeeshop in the seventeenth century," my guide explained to me. To attract shippers and merchants to his establishment, proprietor Edward Lloyd provided news about ships that arrived, departed, sank, and other status updates. Groups of customers sat in wooden boxes, drank coffee, and conversed. A sunken ship could be devastating to ship owners and merchants, who would lose not only the vessel but the very expensive cargo as well. Over time, frequenters of Lloyd's Coffee House banded together, and groups began to insure each other so that if a ship sank, many people would chip in to cover the losses. Eventually, Lloyd's of London was born.

In the center of the main floor was the *Lutine* bell, a recovered remnant from the sunken HMS *Lutine*. In 1779, the German economy was on the verge of a crash. The HMS *Lutine* was loaded with an estimated $1.2 million in gold (worth more than $130 million in 2017 U.S. dollars) and sent to Germany to support the banks. A storm struck, and the ship sank, along with its valuable cargo. The ship and its cargo were insured through Lloyd's, and amazingly, the Lloyd's syndicate paid the full cost of the enormous claim, within two weeks. "It was the *Lutine* that created Lloyd's reputation for paying valid claims—and for having the financial wherewithal to withstand a loss of such legendary proportions."[13]

In 1858, a recovery operation yielded the ship's bell, which was hung in the center of Lloyd's. The bell is rung to indicate important news: once for bad news (such as a sunken vessel) and twice for good news (such as a returning ship).

Today, brokers on the floor don't just plan for the breach of a vessel—they plan for data breaches, too. Lloyd's syndicates specialize in specialty insurance, insuring many unusual risks such as kidnapping, political unrest, war, and even famous body parts, such as Keith Richard's fingers. It was the perfect place to learn about a new and rapidly changing type of policy: "cyber" insurance.

12.4 Commercial Off-the-Shelf Breach Response

Cyber insurance has changed the game when it comes to data breach response—and not for the reasons that most people think. While cyber insurance has existed for two decades in one form

13. "HMS Lutine," *Lloyd's*, https://www.lloyds.com/about-lloyds/history/catastrophes-and-claims/hms-lutine.

or another, the common thread through all policies is financial coverage for claims or expenses due to a cyber event. Around 2009 a groundbreaking change occurred: Insurers began offering data breach *response services*. Instead of simply covering the costs, insurers provide access to their own response teams that support thousands of policyholders. This may include breach response professionals directly employed by the insurer, as well as forensic analysis, attorneys, and other specialists from third-party vendors.

Mike Donovan, the global head of technology, media and business services for Beazley Group, came up with the idea for breach response insurance in 2007. At the time, data breach regulations had picked up steam. There were notification laws in many states, and breaches were on the rise.

But few organizations had access to the specialists required to provide experienced advice regarding data breach investigations and response, such as attorneys who were familiar with data breach notification laws in all 50 states or forensic investigators who knew how to preserve and analyze volatile, nonvolatile, and network-based forensic evidence. Even organizations that could afford these services without insurance typically did not have the time or connections to build their own panels of providers that specialized in data breaches.

Donovan and his team recognized that many organizations were struggling with cybersecurity incident response. "To be able to develop [breach response] capability was not easy," he reflected in an exclusive interview. "This was particularly true in the midmarket space. It was almost impossible. You're trying to line up credit monitoring after you've had a large breach when you have no relationship with anyone who provides it, you have no idea what the right price should be and you have to get it set up in a week. You have to mail [notifications] and you have no idea who to hire and you have to get them out."[14]

Mishandled data breaches were—and still are—far more costly and expensive than a breach where the response is quick, efficient, and tightly managed. Often, consumer lawsuits, negative PR attention, and regulatory fines are the result of delayed notification or lack of effective crisis communications (as the case of Target illustrates; see Chapter 7, "Retailgeddon"). There are even times where a "breach" might not have been declared a breach at all if evidence had been properly preserved.

Donovan and his team realized that their clients needed quick access to services in the event of a breach—and that insurers were uniquely positioned to help. "With normal insurance, an event happens and you insure the outcome of that event," Donovan explained. "A traffic event happens and the insurer responds to whatever damage exists at that time. The insurer is not in a position to do anything as the accident is happening. In the cyber space, the loss was happening in a very different way. These were crisis events. They were happening in real time."

Instead, Donovan envisioned a different model. His team would essentially act as a clearinghouse, connecting their clients with seasoned experts, right when they needed help the most. "When a breach happened, we already had talent experts," he explained. "We had call centers. We had credit monitoring. We had everything they needed to respond in an effective manner. We could bring it to them immediately." His goal was to reduce the losses for everyone. "If the breach is handled well, the chance that they'll suffer reputational damage, lawsuits is much less."[15]

---

14. Mike Donovan, interview by the author, May 25, 2017.

15. Donovan interview.

Today, many insurers offer breach response services (as do law firms, credit bureaus, and cybersecurity companies). When a policyholder contacts the insurer with a suspected breach, a team member quickly responds and brings in third-party specialists such as legal counsel or forensic investigators as needed. The insurers maintain panels of service providers, including forensic analysts, data breach attorneys, call centers, PR firms, and other vendors that specialize in breach response and are available on short notice to assist. For small to midsized organizations or any entity that does not manage data breach crises on a day-to-day basis, the services of an experienced third-party breach response team can prove invaluable.

When breaches are handled effectively, the response and liability costs are greatly reduced, and damage is minimized. By providing policyholders with quick and easy access to experienced providers in a time of crisis, insurers can elevate the quality and speed of data breach response and thereby reduce losses. This is a win-win for both the insurer and the insured.

12.4.1 Assessing Breach Response Teams

When choosing an insurance policy, consider the insurer's role in your breach response process. Will you be leveraging response services provided by the insurer or an approved provider? If so, ask the following questions:

- **Ease of Contact** - How easy is it to contact your insurer? Do you have 24/7 availability, or more limited hours?
- **Responsiveness** - What can you expect for the response time? Some insurers may respond in minutes, whereas others may take days or weeks to process your request and assign providers. Responsiveness can make a big difference in the outcome of a data breach investigation, especially given that evidence can spoil at any moment.
- **Approved Providers** - How experienced are the vendors on the insurer's panel? Some insurers carefully vet their providers based on quality of work to make sure they're hiring experts. Others may select vendors based on favorable rates, market position, or other relationships.

  Even if your insurer's panel is excellent, you may prefer to work with a different legal counsel or forensic investigator with whom you have an existing relationship or whose name you received from a trusted source. "Selection of counsel continues to be a delicate issue with insureds," writes risk consultant Richard S. Betterley, "but as we frequently see in other new lines of coverage, carriers typically reserve the right to select, or at least approve, counsel."[16]

  Make sure to address the issue of provider selection during the procurement phase—not in the heat of the moment when a suspected breach occurs. Carefully review the list of approved service providers, and find out what it would take to use your own selected vendor. Consider asking to get your vendors preapproved so that in the event of a suspected breach, you can hit the ground running.

16. Richard R. Betterley, *Cyber/Privacy Insurance Market Survey: 2017* (Sterling, MA: BRC, 2017), https://www.irmi.com/online/betterley-report-free/cyber-privacy-media-liability-summary.pdf.

12.4.2 Confidentiality Considerations

Be aware that when you purchase breach response coverage, you may be required to disclose ongoing details of the event with your insurance provider in order to receive coverage. The insurer is footing the bill, after all, and may have the right to review your service agreements, communications with providers, and reports. The vendors that you work with—including forensic investigators—may have contractual obligations to the insurer that require them to provide copies of your reports or other information about your case to the insurer.

As with any type of insurance, a negative event may affect your coverage and costs for future policies. For example, in the case of Sony Pictures Entertainment, when a breach occurred in 2011, the company made a $1.6 million claim against its policy with Hiscox. (Ironically, the details of Sony's insurance claims and negotiations were made public after its next major breach in 2014.) Steve Ragan of *CSO* magazine analyzed the leaked documents and determined that "due to exposures, as well as their $1.6 million claim, Hiscox didn't want to write a new policy, and thus declined to quote at renewal."[17]

12.5 How to Pick the Right Cyber Insurance

Cyber insurance isn't one-size-fits-all. A good policy can help you:

- Transfer risks to a third party
- Respond effectively to a breach
- Reduce the risk of a breach occurring in the first place

However, a policy that's not aligned with your risk profile or business needs will just be a waste of money. How do you choose the policy that's right for you? Here is a simple checklist:

Cyber Insurance Checklist

☑ Involve the Right People
☑ Inventory Your Sensitive Data
☑ Conduct a Risk Assessment
☑ Review Existing Coverage
☑ Obtain Quotes
☑ Review and Compare Quotes
☑ Research the Insurer
☑ Choose!

17. Steve Ragan, "Breach Insurance Might Not Cover Losses at Sony Pictures," CSO, December 15, 2014, http://www.csoonline.com/article/2859535/business-continuity/breach-insurance-might-not-cover-losses-at-sony-pictures.html.

Buying the Wrong Policy

"We had a really close call." It was Jenn, the office manager at a financial advising firm. Earlier that week, the firm had received a call from the bank notifying it that one of its money management computers had a virus. A staff member clicked on a link and accidentally downloaded malware, which was designed to steal banking credentials. Fortunately, the bank detected the suspicious activity—just in time.

The firm's executive team was spooked. "We manage a lot of money online," said Jenn. "We need insurance to cover a cash loss in case someone does break into one of our accounts." Within days, the firm's insurance agent sent over a quote. It was long and complex.

"Can you review it and tell us if it's the right coverage for us?" asked Jenn. The agent recommended the policy but the executive team wanted input from a cybersecurity professional.

After speaking with the agent, I reviewed the quote and concluded that it wasn't the right policy at all. The policy covered HIPAA violations, PCI violations, and breach response services appropriate for organizations bound by those regulations. However, the firm was not regulated by HIPAA and rarely handled credit card numbers.

After further research, we discovered that the firm's existing crime policy already covered the risk of money stolen from its online bank account. An in-depth discussion with its IT team revealed that the company had other critical risks that were not on the executive team's radar but that could be addressed by a different type of cyber insurance policy.

Time and time again, organizations ask their agents for "cyber" insurance, and the resulting quote is totally the wrong fit. Many organizations buy it anyway, not realizing until an issue comes up that they haven't covered their most critical risks.

Why does this occur? First, customers may not clearly communicate (or even understand) their coverage needs. Sometimes they just tell an agent they need "cyber" insurance and leave it at that.

On the flip side, agents often don't ask the right questions. They are not cybersecurity experts. Few agents have a strong understanding of the latest security threats or compliance requirements. Cyber policies themselves are so varied that it is hard for anyone to compare. The products are constantly evolving.

Know what risks you need to address, and get the right people involved in your cyber insurance selection process. That way, you can choose a policy that brings real value to your organization.

12.5.1 Involve the Right People

The first step in selecting your cyber insurance policy is to involve the right people, both inside and outside your organization. Cyber risk—and therefore cyber insurance—touches every part of your organization. Therefore, you need input from a variety of different functions during your decision-making process. Often, a cyber insurance policy is selected by management, finance, and legal, and then IT is told of its existence after the fact. This can result in insurance policy selections that don't reflect the true needs of the organization.

The exact persons you should involve will vary depending on your industry, size, and unique environment. Typically, it's wise to include people who handle the following business functions for you (either internal staff or outside service providers, depending on your organization):

- **Information Security** - If you have dedicated information security personnel, it's naturally a good idea to involve them so they can provide input regarding your key cybersecurity risks. Also, information security staff are responsible for implementing new security controls and tracking the changing threat landscape. You will need them to implement any technical requirements for maintaining coverage (such as mobile device encryption) and keep you updated if there are significant changes in your controls or the threat landscape that would require you to modify your coverage. Finally, information security staff are normally tasked with responding to potential data breaches, and so they need to be aware of insurance triggers and understand how and when to hand off to insurers and third-party service providers.
- **IT** - Your system administrators, help desk providers, and network engineers should have an intimate understanding of both the strengths and weaknesses of your network infrastructure. Much like information security staff, they may be involved in implementation of any technical requirements and have firsthand knowledge of changes to your IT infrastructure that would impact your risks. When a data breach occurs, your IT staff are often the first ones to see the signs, and they need to understand how to recognize indications of a breach and what information needs to be preserved and communicated in order to most effectively leverage your insurance policy.
- **Legal** - Your legal counsel will provide input on any risks that stem from contractual or regulatory requirements, such as PCI, state or federal breach notification or security laws, and more. While it's always wise to have your general counsel involved, it's also a smart idea to consult with a specialist attorney who has experience working with security and breach notification laws in all 50 states, and any specific industry or geographical region that's relevant to you.
- **Finance** - Your finance department can help you budget for cyber insurance, plan for payment of deductibles, and provide input on a cost/benefit analysis of your cyber insurance quotes. In addition, many cybersecurity risks relate directly to data that finance departments create, transmit, store, or process, including banking information, tax returns, employee SSNs, online banking credentials, and more.
- **Risk Management** - Your risk management personnel can help you prioritize risks, coordinate your risk assessment process, and define your coverage needs.
- **Human Resources** - Your HR department can help you evaluate and manage risks associated with theft of employee data (such as SSNs and W2s), insider attacks, and more. HR staff are often tapped with managing employee communications in the event of a breach, in order to ensure that employees have clear instructions and know how to respond to outside inquiries.
- **Public Relations** - Services such as crisis communications and reputation defense, often provided as part of a cyber insurance policy, naturally fall into your PR team's area of

expertise. Your PR team can help you vet insurance panel providers and evaluate your coverage needs.

- **Executive Team** - Typically the executive team has the bird's eye view of your organization and can oversee the cyber insurance selection process.
- **Board of Directors** - Ultimately, your board of directors should sign off on whatever policy you choose. Insurance is about transferring risk, and your board (or equivalent) should have the opportunity to understand and provide input on coverage choices, particularly when significant residual risk remains.
- **Insurance Agent** - You should always work through an experienced insurance agent who will review the policy in detail and advise you regarding coverage options.
- **Cybersecurity Specialist** - When it comes to cyber coverage, having an agent review your quotes is not enough. Use the buddy system when you buy cyber insurance. It is worth it to bring in an experienced cybersecurity professional who will work hand-in-hand with your agent to evaluate your risk, define your requirements, and review your quotes in detail. That way, you can make sure that the policy's coverage is truly in line with your organization's needs.

This is not to say that every person (or group) in this list should have an equal vote on your cyber insurance policy selection. Rather, the decision-making process should be designed to take input from all of these areas (and more, as needed) in order to accurately assess the organization's risk profile and evaluate the effectiveness of the proposed policy. Taking input from a wide field will help ensure that you are addressing cyber risks organization-wide, and it will also help you to obtain buy-in from the key stakeholders who will later be tasked with integrating and leveraging your cyber policy.

12.5.2 Inventory Your Sensitive Data

When you buy home insurance, it's wise to make an inventory of your property so that you know how much insurance to buy and what type of coverage you need. If you do need to make a claim, having the list readily available helps to expedite the process.[18]

Similarly, when you shop for cyber insurance, you should take an inventory of your data for much the same reasons. Refer to Chapter 2, "Hazardous Material," for guidance on taking an inventory of your data.

12.5.3 Conduct a Risk Assessment

Cyber insurance enables you to transfer risks to a third party. In order to pick the right insurance policy, you first need to enumerate and prioritize your risks. Too many organizations choose insurance coverage based on an executive's gut instinct about risk, rather than taking a methodical approach. Cyber insurance isn't cheap! Conducting a formal risk assessment will help ensure that your investment in cyber insurance is effectively spent.

18. "Home Inventory," Farmers.com, accessed January 19, 2018, https://www.farmers.com/inner-circle/home-tool-kit/how-to-create-a-home-inventory.

If you have sensitive information (and who doesn't?) chances are you should be routinely conducting risk assessments anyway, as per HIPAA, PCI, NIST Cybersecurity Framework guidelines. A word of caution, however: Many risk assessments are based on a subset of your network. For example, a HIPAA risk assessment may focus only on risks pertaining to ePHI. When you select cyber insurance, make sure you are basing your decisions on an enterprise-wide risk assessment.

Many people confuse risk assessments with controls assessments. These are not the same thing. A controls assessment is essentially a comparison of your existing controls with a known checklist, such as ISO 27001 or the NIST Cybersecurity Framework. You receive a report indicating controls in place and gaps.

In comparison, the NIST "Guide for Conducting Risk Assessments" (SP 800-30) states that "the purpose of a risk assessment is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring)."[19]

There are other effective models for assessing and communicating risk. For example, at Los Alamos National Laboratories, the security team uses an "attack tree" model. Threats and vulnerabilities are documented as leaves on a tree that interconnect, and the overall risk for a scenario is calculated based on the aggregate risk from all of the leaves. This model allows the team to evaluate the risk of the system as a whole, rather than individual parts in isolation.[20]

Once you have conducted a risk assessment, you can develop a risk management plan. A three- to five- year plan is common (you will want to update it at least annually in response to changes in your environment and the threat landscape). For each risk, determine whether you can mitigate or eradicate the risk. Some risks can be reduced or even eliminated with relatively little effort. Others cannot be addressed without a very large investment. Every organization has limited resources, and so there is a cost-benefit tradeoff to addressing risks. The organization will need to accept some residual risk.

The risks that the organization cannot eliminate but does not want to accept are prime candididates for *transfer* via insurance.

12.5.4 Review Your Existing Coverage

Before you reach out for quotes, make sure to review your existing coverage. Some cyber-related risks may be covered under your existing insurance. For example, commercial crime policies typically provide coverage for direct losses incurred by the policyholder as a result of malicious activity by third parties. So, if hackers break into your bank account and transfer $10,000 out,

---

19. National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments: Information Security*, Special Pub. 800–30, rev. 1 (Washington, DC: NIST, September 2012), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

20. Steven G. Howard, "Risk Based Information Security Model," Los Alamos National Laboratory, *National Laboratory Information Technology Conference (NLIT)*, June 15, 2011, https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-11-03062.

your commercial crime policy may well cover your cash loss. On the other hand, if the hackers also steal your employees' SSNs and open credit cards in their names, your crime policy would not cover your liability for any ensuing lawsuits or damages incurred by the employees or other third parties.

There are other areas where cyber-related risks *may* be covered by your existing insurance. "If there's a cyber attack that causes tangible damage to property, it could be covered under your property policy," said Kevin Kalinich, global practice leader for Aon Risk Solutions. "If there's an attack that causes tangible damage to a third party, your general liability policy could cover it."[21]

Once you identify your high-risk scenarios, review your existing policies to see if you already have insurance. Overlapping insurance policies mean that you're paying twice for the same coverage. Also, in the event that both policies are triggered, you could be faced with dueling insurers, which might slow down the process.

That said, tread carefully. There is often ambiguity in the ways that standard insurance policies apply to electronic data and breaches, which can lead to disputes between the policyholder and the insurance company. For example, in the case of *State Auto Property & Casualty Insurance Co. v. Midwest Computers* the defendant had insurance that covered "[p]hysical injury to tangible property." The court ruled that "[a]lone, computer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property." However, the coverage also included "[l]oss of use of tangible property that is not physically injured" and customers who had lost the *use* of their computers. Therefore, the court also stated that "[b]ecause a computer clearly is tangible property, an alleged loss of use of computers constitutes 'property damage' within the meaning of plaintiff's policy."[22]

Commercial general liability policies may provide some coverage for losses related to data breaches. For example, in 2013, two patients of Glen Falls Hospital discovered that their medical records turned up as the first result in a Google search for their respective names. Glen Falls had contracted a service provider, Portal Healthcare Solutions, LLC, to manage and store electronic patient health records. The patients initiated a class-action lawsuit. Portal attempted to trigger the company's commercial general liability insurance (provided by Travelers) to pay for the lawsuit, since it included coverage for "personal and advertising injury."[23] Travelers refused, arguing that "there was no 'personal injury' or 'publication' as defined by the policies because release of the records was not intentional and they were not viewed by a third party."

The federal appeals court in Virginia ruled against Travelers, stating that an unintentional publication is still publication. The court also said the definition of publication does not hinge on third-party access. Therefore, Travelers was required to cover Portal's legal defense costs

21. "Where Cyber Insurance Underwriting Stands Today," *Insurance Journal*, June 12, 2015, http://www.insurancejournal.com/news/national/2015/06/12/371591.htm.

22. American Online, Inc. v. St. Paul Mercury Insurance Co., 207 F. Supp. 2d 459, 470 (E.D. Va. 2002) (quoting State Auto Property & Casualty Insurance Co. v. Midwest Computers & More, 147 F. Supp. 2d 1113 (W.D. Okla. 2001), http://law.justia.com/cases/federal/district-courts/FSupp2/207/459/2346018.

23. Andrew G. Simpson, "Federal Court Rules CGL Insurance Covers Data Breach," *Insurance Journal*, April 12, 2016, http://www.insurancejournal.com/news/national/2016/04/12/404881.htm.

for the class-action lawsuit (since the commercial general liability [CGL] policy did not cover liability to third parties, so any resulting settlement or fines would be Portal's responsibility).

"What makes the decision important . . . is that they may have some data breach coverage that they didn't know they had," commented tech writer John P. Mello Jr., upon the announcement of the appeals court ruling in 2016.[24]

On the flip side, when the Sony Playstation network was hacked in 2011 and 77 million users' personal information was stolen, the company attempted to leverage the personal and advertising injury coverage in its CGL policy—and ultimately lost a battle with its insurer, Zurich American Insurance Co. "New York Supreme Court Justice Jeffrey K. Oing issued a bench ruling that the policy did not cover breach costs because the provision only covered confidential material published directly by Sony, not by the hackers who stole the information."[25]

Confused? You're not alone. "[S]everal courts had struggled with the definition of 'publication' . . . in recent years, with differing results," writes Jana Landon, data management attorney at Stevens & Young.[26]

As the cyber insurance industry matures, insurers have moved to explicitly exclude data breach and cyber-related coverage from CGL policies. "[U]nsurprisingly, given the confusion in the courts over these issues and the rapid uptick in third-party external hacking incidents, these standard CGL policies have now been updated to provide the insureds with further clarification," writes Landon. "For example, CGL policies now include the 2014 ISO form 'Access or Disclosure of Confidential or Personal Information Exclusion.' This exclusion expressly limits [Personal and Advertising Injury Liability Coverage] and excludes accessing or disclosure of, among other things, 'patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.' In other words, most of the information that is compromised during data breaches."[27]

If you have an older policy, it may include broader coverage for data breaches and related expenses than newer policies. However, if there's any ambiguity whatsoever, don't count on it.

You want your cyber insurance policies to be "harmonized" with your existing insurance. Understand which of your high-risk scenarios are—and are not—covered by your existing policies. Try to find coverage that will minimize overlaps while ensuring that your needs are met. Consider purchasing cyber insurance from the same companies that underwrite your CGL and/or property insurance, to minimize the risk of conflicts in the event that multiple policies are triggered by an event.

---

24. John P. Mello Jr., "Insurance Industry Buzzes Over Data Breach Ruling," *TechNewsWorld*, April 21, 2016, http://www.technewsworld.com/story/83403.html.

25. Latham & Watkins, "Cyber Insurance: A Last Line of Defense When Technology Fails," (Client Alert White Paper No. 1675, April 15, 2014), 7, https://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage.

26. Jana Landon, "Where Does Sony Settlement Leave CGL Insurance for Data Breaches?" *Legal Intelligencer*, May 13, 2015, https://www.law.com/thelegalintelligencer/almID/1202726345560/where-does-sony-settlement-leave-cgl-insurance-for-data-breaches.

27. Landon, "Sony Settlement."

Cyber Insurance Towers

At Lloyd's of London, my guide and I stood on the balcony, watching the tiny insurance brokers negotiate on the floor below. For small or midsized organizations, purchasing insurance is a fairly straightforward process: You talk with your broker, obtain quotes, and pick one. Large organizations, such as the retailer Target, need hundreds of millions of dollars in cyber insurance. Few, if any, insurers will provide that amount of cyber insurance all at once. Instead, the organization must build a "tower" of cyber insurance, made up of many layers.

When building a cyber insurance tower, one of the challenges is getting the upper layers of the policy to match the terms of the primary layer. This can involve coordinating with dozens of different underwriters. Ryan Gibney, assistant vice president at insurance brokerage firm Lockton Companies, shared that he was working with one "new-to-the-market" client that sought a $200 million tower. To build the tower, he was coordinating with 27 U.S. insurers, 9 in London, and 9 more in Bermuda. "So, we're speaking with 45 different underwriters with 45 different appetites in order to meet the capacity."[28]

"It's a lot easier to build a tower when you have everybody in the same room," said my guide. Sure, brokers can—and do—negotiate complex policies via phone and email. But as we watched, we could see brokers gather and move from box to box at Lloyd's. "A broker gets one insurer—say, Bob from Beazley—to underwrite the first $5 million. Then, he might go over to Sue from ACE and say, 'Hey, you know Bob, who you had lunch with yesterday? He's underwriting the first $5 million. Would you like to get the next $10 million?' It's easier to get things done when you can talk face to face. A lot happens right here in this room."

12.5.5 Obtain Quotes

Once you've identified your high-risk scenarios and understand your existing coverage, you're ready to get quotes. The process will vary depending on the type and amount of coverage you're seeking. Before you begin, take the time to define the coverage you seek in writing. This way everyone will be on the same page. Get input from both your insurance agent and a qualified cybersecurity professional.

Typically, you'll be asked to fill out an application designed to assess your needs and level of risk. This will include questions about the volume and type of data your organization stores, what policies you have in place (and whether you follow them), access control, backups, monitoring systems, and more.

As data breaches continute to proliferate, more organizations are seeking high-dollar coverage—and insurers are vetting them more carefully. "[U]nderwriters have begun asking more thoughtful questions," said Thomas Reagan, the cyber practice leader for Marsh insurance brokers. He added that underwriters are vetting applicants' risk management programs and asking specific questions about whether the applicants leverage risk management technologies such as encryption, chip-and-PIN cards, and tokenization. "Underwriters are just

28. Erin Ayers, "Higher and Higher: Cyber Insurance Towers Take Careful Construction," *Advisen*, September 24, 2015, http://www.advisenltd.com/2015/09/24/higher-and-higher-cyber-insurance-towers-take-careful-construction.

another example of how organizations have to tell their story about their cyber risk management process."[29]

It's very important to be accurate in your application. If your cybersecurity controls and risks are substantially different than what you state in your application, then your insurer may be justified in claiming that you have concealed or misrepresented material facts, and deny a claim accordingly. Insurers can also require audits of your cybersecurity infrastructure to assess and verify your risk profile.

In the case of Cottage Health System in southern California, a routine security audit turned into a nightmare when auditors discovered that 11,000 patient records were exposed on an Internet-facing server managed by a third-party vendor, inSync. Cottage's insurer, Columbia Casualty Company, denied the healthcare provider's claims, stating that Cottage "provided false responses" to a "Risk Control Self Assessment" that the company completed as part of the application process. The questions and Cottage's responses included:[30]

4. Do you check for security patches to your systems at least weekly and implement them within 30 days? *Yes*

5. Do you replace factory default settings to ensure your information security systems are securely configured? *Yes*

6. Do you re-assess your exposure to information security and privacy threats at least yearly, and enhance your risk controls in response to changes? *Yes*

11. Do you outsource your information security management to a qualified firm specializing in security or have staff responsible for and trained in information security? *Yes*

12. Whenever you entrust sensitive information to 3rd parities do you . . .

    a. contractually require all such 3rd parties to protect this information with safeguards at least as good as your own? *Yes*

    b. perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your standards (e.g., conduct security/privacy audits or review findings of independent security/privacy auditors)[?] *Yes*

    c. Audit all such 3rd parities [*sic*] at least once per year to ensure that they continuously satisfy your standards for safeguarding sensitive information? *Yes*

    d. Require them to either have sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality[?] *Yes*

13. Do you have a way to detect unauthorized access or attempts to access sensitive information? *Yes*

23. Do you control and track all changes to your network to ensure it remains secure? *Yes*

---

29. Ayers, "Higher and Higher."

30. Columbia Casualty Co. v. Cottage Health System, No. 2:16-cv-3759 (C.D. Cal. 2016), https://www.insideprivacy.com/wp-content/uploads/sites/6/2016/06/CNA-v-Cottage-Health-2016-complaint.pdf.

Columbia argued that these were "material misrepresentations and/or omissions of fact and that, consequently, Columbia is entitled to rescind the policy as void *ab initio*."[31] Ultimately, the case was dismissed for a different reason: because the policy required that the parties first attempt to resolve matters using alternative dispute resolution methods before turning to the courts.[32]

12.5.6 Review and Compare Quotes

Now, the fun part! Once you receive quotes from insurers, you can begin reviewing and comparing them. You may want to start by doing a high-level review of all the quotes that you receive and then, once you've narrowed it down, conduct a detailed examination of your top contenders. Make sure that both your insurance agent and your cybersecurity specialist review your quotes in detail. Then, involve key stakeholders within your organization when making the final decision.

12.5.6.1 Types of Coverage

Remember, you're rarely comparing apples to apples when reviewing cyber insurance policies. Sometimes it can feel like you're comparing apples to octopuses! What one underwriter calls "notification expenses" may mean something completely different in another policy.

For example, one cyber insurance policy covered "privacy notification expenses" in the event of a breach. However, the policy included "credit monitoring or other similar services" in the definition of privacy notification expenses. The sublimit for the "privacy notification expenses" was comparable to that of similarly named coverage offered by other insurers, but the other insurers separated credit monitoring into a different category. Given that credit monitoring is very expensive compared to simple notification costs, in the event of a breach the costs would have quickly exceeded the sublimit for privacy notification expenses.

12.5.6.2 Triggers

In order for you to receive payment or services under a cyber insurance policy, the policy must first be *triggered*. What is a trigger, in this context? According to the International Risk Management Institute, Inc. (IRMI), a *coverage trigger* is the "event that must occur before a particular liability policy applies to a given loss."[33]

---

31. *Columbia Casualty Co. v. Cottage Health System*.

32. Joe Van Acker, "Insurer's Failure to Mediate Kills Its $4M Data Breach Claims," Law360, July 20, 2015, https://www.law360.com/articles/680863/insurer-s-failure-to-mediate-kills-its-4m-data-breach-claims.

33. International Risk Management Institute (IRMI), "Coverage Trigger," accessed January 20, 2018, https://www.irmi.com/online/insurance-glossary/terms/c/coverage-trigger.aspx.

Pay careful attention to what types of events do—and don't—trigger your policy. For example, many cyber policies are not triggered until a formal lawsuit or request for monetary damages is filed. That means that any legal fees, fines, or work performed in response to government investigations or regulatory action may not be covered. The Cybersecurity by Chubb policy defines "claim" as:[34]

> A. any of the following:
>
> – 1. a written demand or written request for monetary damages or non-monetary relief;
>
> – 2. a written demand for arbitration;
>
> – 3. a civil proceeding commenced by the service of a complaint or similar pleading; or
>
> – 4. a criminal proceeding commenced by the service of an indictment,
>
> against an Insured for an Injury, including any appeal therefrom; or
>
> B. a written request received by an Insured to toll or waive a statute of limitations relating to a potential Claim described in paragraph A. above.

As you can see, a government investigation probably would not trigger coverage. Furthermore, even if a lawsuit were eventually filed, the policy specifically does not cover any expenses incurred prior to the time that an event meets the definition of a claim.

Attorney Steve Raptis of Manatt, Phelps & Phillipps LLP specializes in insurance advice and disputes. He recommends "[s]eeking trigger language that focuses on the insured's failure to protect confidential information, regardless of the cause (e.g., 'any failure to protect'), rather than language requiring an intentional breach."[35]

12.5.6.3 Retentions

Check the deductible and/or retention amounts on your policies carefully. Most people are familiar with deductibles since they are very common in car and health insurance. Your insurer is responsible for each claim, and the deductible is the monetary amount that you are responsible for.

A self-insured retention (SIR) is an amount that you are required to pay before one of your insurance policies kicks in. For example, in the case of Target, which reportedly was self-insured for the first $10 million of cyber coverage, the insurer would not get involved at all until the SIR was met.

---

34. "Cybersecurity by Chubb," Chubb.com, accessed January 20, 2018, https://web.archive.org/web/20180712175705/http://www.chubb.com/businesses/csi/chubb10308.pdf.

35. Steve Raptis, "Analyzing Cyber Risk Coverage," *Risk & Insurance*, March 13, 2015, http://riskandinsurance.com/analyzing-cyber-risk-coverage.

12.5.6.4 Covered Expenses

Make sure you understand exactly what expenses are covered in the event of a breach. For example, an AIG CyberEdge policy defines "loss" as specific "reasonable and necessary expenses and costs" incurred "*within one year of the discovery*" of a qualifying event, including coverage for forensics investigations, public relations, crisis management, notification, identity theft services, and more. The timing cutoff is buried in the definition itself and has huge implications for coverage, especially since data breach lawsuits can drag on for years. Also, the definition of "loss" explicitly excludes "internal charges"—meaning you may be better off hiring outside consultants whenever possible as opposed to conducting work in-house.[36]

A very common limitation, as expressed in a Beazley breach response policy, is that cyber insurance may cover "actual, reasonable and necessary costs and expenses incurred . . . to restore a Data Asset from back-ups or from originals or to gather, assemble and recollect such Data Asset from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction." It will not cover costs to "update, replace . . . or enhance a Data Asset or Computer System to a level beyond that which existed prior to the alteration . . . or damage of such Data Asset."[37]

12.5.6.5 Timing

Often, data breaches are discovered months or even years after the event actually took place—such as the Yahoo breaches publicized in 2016, which actually first occurred in 2013 and 2014. However, many cyber insurance policies will cover losses or claims due to breaches that occur only after the policy inception date or a "retroactive date" negotiated with the policyholder. Furthermore, the event typically must be discovered and reported to the underwriter during the period that the policy is in effect.

That means if a data breach occurred three years ago, before your insurance coverage took effect, but you discovered it today, your current cyber insurance might not cover the breach. Furthermore, if you switch insurers and later discover that a breach occurred while you had your previous policy, but you didn't detect or report it in time, you might not be covered.

What if a breach is ongoing, such as in the case of TJ Maxx, where hackers were accessing the company's network for a year and a half (see Chapter 6, "Payment Card Breaches")? Some insurers have specifically addressed these cases. For example, one Beazley Breach Response policy specifically states that "[a] series of continuing Security Breaches, related or repeated Security Breaches, or multiple Security Breaches resulting from a continuing failure of Computer Security, shall be considered a single Security Breach and be deemed to have occurred at the time of the first such Security Breach."[38]

Make sure to push the retroactive date as far back as you reasonably can, given your resources and coverage options. Also, be sure to understand the reporting requirements and

36. AIG CyberEdge, Security Failure/Privacy Event Management Insurance, December, 2013 (insurance policy, on file with author).

37. Beazley, *Beazley Financial Institutions and Breach Response Services Policy* (Report, Beazley, April 2014), 35, https://www.beazley.com/documents/Wordings/beazley-financial-institutions-and-breach-response-services-uk.pdf.

38. Beazley, *AFB Media Tech* (Report F00437, Beazley, September 2014), https://www.beazley.com/documents/TMB/Media%20Tech/MediaTechPolicy_SurplusLines_F00437092014ed.pdf.

have a strong detection program in place, so that you don't accidentally miss a reporting window and lose coverage.

12.5.6.6 Limits

Make sure that the limits of your insurance are in line with the volume and sensitivity of the data that you retain. When Anthem health insurance announced in 2015 that it had been hacked (see Chapter 9, "Health Data Breaches"), one of the most shocking aspects of the case was that it quickly smashed through the limits of its $100 million cyber insurance tower. Anthem's CEO, Joseph Swedish, confirmed that personal information of 78.8 million people had been exposed, including names, birthdates, medical IDs, SSNs, and more.

One hundred million dollars may seem like a lot of coverage—but not when the personal records of nearly *80 million* people are affected. "[T]his amount will not even be enough to cover the cost of postage, let alone cover damages due to the data breach," reported Presidio Insurance Solutions.[39] "And Anthem will have to spend millions more to fix its security problems and rebuild its reputation."

According to the *Insurance Insider*, Anthem's cyber insurance tower was built with Lexington (an AIG member) as the primary insurer, followed by eight upper layers, as illustrated in Figure 12-1. Note that these details are based on an anonymous source and have not been publicly confirmed by Anthem.

The total coverage limitation of a policy is important, of course, but pay attention to the sublimits as well. These are limitations for specific types of coverage within the policy. As illustrated earlier by the "privacy notification expenses" coverage, sublimits can have a big impact on the value of your policy.

There is a wide variation in the estimated cost of a breach per record, which adds to the challenge of calculating the potential costs of a breach (and thereby the appropriate insurance coverage, limits, and sublimits). According to the Ponemon Institute, the average per-capita cost of a breach in 2015 for U.S. citizens was $217. The same year, Verizon reported that the average per-capita cost of a breach was only 58 cents. That's a pretty huge difference, especially when you're calculating potential costs for almost 80 million people!

Some policies provide sublimits that are not tied to a specific dollar amount. For example, notification may be limited to 1 million individuals, or the call center services may be limited to 20,000 calls per day. These types of limits are less risky for the policyholder because they do not require it to translate the number of affected individuals into a specific dollar limit, which may fluctuate as breach response best practices, requirements, and services change.

Appropriate limits for your organization will necessarily depend, in part, on the sensitivity of the data that you hold, the potential for lawsuits, fines and long-term ("chronic") conflicts, and your risk appetite. Refer to the inventory of data that you created for your organization, and consider the costs of notification, credit monitoring, and other potential compensation for potential affected persons. Research fines or penalties for organizations that hold sensitive information that is similar to yours, such as medical files or payment card data. Make sure

39. Presidio Insurance Solutions, "What the Anthem Data Breach Means for Malpractice Insurance", http://www.presidioinsurance.com/news/anthem-data-breach (accessed January 20, 2018).

Figure 12-1. Illustration of Anthem's cyber insurance tower, based on unofficial details. Source: Adam McNestrie and Jenny Messenger, "Anthem Breach Could Exhaust $100mn Cyber Programme," *Insurance Insider*, February 16, 2015, https://web.archive.org/web/20150219100116/http://www.insuranceinsider.com/-1253434/10.

that you take into account all information that you hold, including archived data and employee records. Above all, remember that data is hazardous material, as Chapter 2 discusses.

As you compare the costs of various insurance policies, consider whether there is data that you can destroy, so that you don't have to wonder what it will cost in the event that is it exposed.

12.5.6.7 Exclusions

Cyber policies normally contain a laundry list of exclusions, which removes the insurer's obligation to provide coverage in certain scenarios. Many of these are straightforward and understandable, such as exclusions that explicitly carve out the insurer's obligation to cover

claims due to intentional crimes committed by the policyholder. However, there are some exclusions that dramatically change the value of your policy.

As an example, let's analyze the P. F. Chang's payment card data breach and subsequent insurance lawsuits, which hinged upon an exclusion for contractual obligations.

Contractual Obligations Exclusions

P. F. Chang's China Bistro is an Asian-style restaurant chain that processes more than 6 million payment cards each year. In 2014, P. F. Chang's purchased a Cybersecurity by Chubb policy through Federal Insurance Company ("Federal"), which was advertised as "a flexible insurance solution designed by cyber risk experts to address the full breadth of risks associated with doing business in today's technology-dependent world," including coverage for "direct loss, legal liability, and consequential loss resulting from cyber security breaches."[40] The owners paid an annual premium of $134,052 for the coverage.

On June 10, 2014, investigative reporter Brian Krebs broke the news that P. F. Chang's had suffered a major credit card breach. "On June 9, thousands of newly-stolen credit and debit cards went up for sale on rescator[dot]so, an underground store," reported Krebs. "Several banks contacted by KrebsOnSecurity said they acquired from this new batch multiple cards that were previously issued to customers, and found that all had been used at P. F. Chang's locations between the beginning of March 2014 and May 19, 2014."[41] Two days later, P. F. Chang's released a statement confirming the breach. Investigators later determined that 66,000 payment card numbers had been compromised.

P. F. Chang's immediately notified its insurer, Federal, which covered approximately $1.7 million in costs for forensic investigators and litigation defense stemming from lawsuits filed by customers and one issuing bank. In March 2015, P. F. Chang's also requested coverage for $1.9 million in fines and penalties assessed by Mastercard. The card brand imposed fees on P. F. Chang's payment processor, BAMS, which in turn sent the following letter to P. F. Chang's:[42]

> MasterCard's investigation concerning the account data compromise event involving [Chang's] is now complete. [BAMS] has been notified by MasterCard that a case management fee and Account Data Compromise (ADC) Operational Reimbursement and Fraud Recovery (ORFR) are being assessed against [BAMS] as a result of the data compromise. In accordance with your [Master Services Agreement] you are obligated to reimburse [BAMS] for the following assessments:
>
> - $ 50,000.00—Case Management Fee
> - $ 163,122.72—ADC Operational Reimbursement
> - $1,716,798.85—ADC Fraud Recovery 2
>
> $1,929,921.57

40. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co., No. CV-15-01322, 1 (D. Ariz. 2016), https://cases.justia.com/federal/district-courts/arizona/azdce/2:2015cv01322/934023/45/0.pdf.

41. Brian Krebs, "Banks: Credit Card Breach at P. F. Chang's," *Krebs on Security* (blog), June 10, 2014, http://krebsonsecurity.com/2014/06/banks-credit-card-breach-at-p-f-changs.

42. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co., No. CV-15-01322, 4 (D. Ariz. 2016), https://cases.justia.com/federal/district-courts/arizona/azdce/2:2015cv01322/934023/45/0.pdf.

P. F. Chang's paid the fees in order to maintain its ability to process credit cards and turned to Federal for reimbursement. Federal balked.

A federal judge analyzed the Cybersecurity by Chubb policy, which had an exclusion that stated: "With respect to all Insuring Clauses, [Federal] shall not be liable for any Loss on account of any Claim, or for any Expense . . . based upon, arising from or in consequence of any . . . liability assumed by any Insured under any contract or agreement."[43] The judge also analyzed the Master Services Agreement (MSA) between Chang's and its payment process, noting that "[i]n no less than three places in the MSA does Chang's agree to reimburse or compensate BAMS for any 'fees,' 'fines,' 'penalties,' or 'assessments' imposed on BAMS by the Associations, or, in other words, indemnify BAMS."[44]

Since the policy specifically excluded coverage for claims or losses due to contractual obligations, the court ruled that "the above referenced exclusions bar coverage for all three Assessments claimed by Chang's."

This is a very common exclusion, and since PCI-related fines are *not* assessed by regulatory bodies or a court of law, but instead are contractual obligations, organizations that seek coverage for credit card breaches should ensure that coverage for PCI-related fines and penalties are explicitly addressed.

Government-Sponsored Attack Exclusions

Another widespread exclusion that can have unexpected consequences involves "acts of war." It's standard practice to have some form of exclusion for claims or losses due to war—but these clauses can be quite broad and exclude any activity conducted on behalf of a government authority. Why is this a problem? Consider the following headlines:

- "Why the U.S. Was Sure North Korea Hacked Sony"—*CBS News* (2015)[45]
- "Google Reveals Gmail Hacking, Says Likely from China"—*Reuters* (2011)[46]
- "Russian Agents Were Behind Yahoo Hack, U.S. Says"—*New York Times* (2017)[47]

Many data breaches are perpetrated (or suspected to be perpetrated) by agents working for a government authority. For example, in February 2013, the forensics firm Mandiant published a famous research paper titled "APT1: Exposing One of China's Cyber Espionage Units." The researchers exposed a hacking group that they dubbed "APT1," and provided evidence to support the theory that the group was a government-sponsored unit of the People's Liberation Army (PLA). According to the report, "Our evidence indicates that APT1 has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of

43. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co.

44. P. F. Chang's China Bistro, Inc. v. Federal Insurance Co.

45. Bob Orr, "Why the U.S. Was Sure North Korea Hacked Sony," *CBS News*, January 19, 2015, https://www.cbsnews.com/news/why-the-u-s-government-was-sure-north-korea-hacked-sony.

46. Sui-Lee Wee and Alexei Oreskovic, "Google Reveals Gmail Hacking, Says Likely from China," *Reuters*, June 2, 2011, www.reuters.com/article/us-google-hacking-idUSTRE7506U320110602.

47. Vindu Goel and Eric Lichtblau, "Russian Agents Were Behind Yahoo Hack, U.S. Says," *New York Times*, March 15, 2017, https://www.nytimes.com/2017/03/15/technology/yahoo-hack-indictment.html (accessed January 20, 2018).

industries beginning as early as 2006. Remarkably, we have witnessed APT1 target dozens of organizations simultaneously. . . . We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has committed."[48]

If your organization detects a data breach, should it matter whether the intruders are government-sponsored, members of organized crime groups, or solo operators? Data breach notification laws still apply regardless of the perpetrators' motives and affiliations. Yet if a forensic investigation turns up evidence that your breach originated from an APT1-related IP address, you might not be covered.

Here are some examples of "war" exclusions from different cyber policies, underwritten by Beazley, Ascent, and AIG, respectively. All three are broadly worded and exclude government-sponsored attacks, which would exclude many breaches:

- "[T]his Policy does not cover Loss or Damage directly or indirectly occasioned by, happening through or in consequence of war, invasion, acts of foreign enemies, hostilities (whether war be declared or not) . . . or requisition or destruction of or damage to property by or under the order of any government or public or local authority."—Beazley Breach Response specimen, War and Civil War Exclusion, 2016
- "We shall not be liable for any claim directly or indirectly arising out of or in any way attributable to: . . . Strikes or similar labor actions, war, invasion, act of foreign enemy, hostilities or warlike operations (whether declared or not) . . . or requisition or destruction of or damage to property by or under the order of any government or public or local authority." –Ascent U.S. v2.3, 2015
- "The Insurer shall not be liable to make any payment for Loss: . . . arising out of, based upon or attributable to any seizure, confiscation, nationalization, or destruction of a Computer System or Electronic Data by order of any governmental or public authority." - AIG CyberEdge Security Failure/Privacy Event Management Insurance, p. 4, 2013

Given the prevalence of state-sponsored hacking, it's wise to carefully review the wording of any "war" exclusions in your policy quotes. Consider requesting edits to narrow the scope, so that breaches that stem from government-sponsored actions are still covered.

Security Practices Exclusions

Cyber insurance, in some cases, provides clear, specific financial incentive for implementing cybersecurity best practices. "Insurance can provide a lever to speed up companies' adoption of standard risk management practices," wrote a report produced by the CRO Forum, "by taking into account companies' cyber hygiene practices in the underwriting process."[49]

However, general exclusions for "failure to maintain security standards" are typically so broad that they don't provide clear incentives and can be leveraged as an "out" for the insurer in

48. Mandiant, *ATP1: Exposing One of China's Cyber Espionage Units* (Alexandria, VA: Mandiant, 2013) https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

49. CRO Forum, *Cyber Resilience: The Cyber Risk Challenge and the Role of Insurance* (Amsterdam, Netherlands: CRO Forum, December 2014), 8, https://www.thecroforum.org/wp-content/uploads/2015/01/Cyber-Risk-Paper-version-24-1.pdf.

the event of a major breach (as in the case of *Columbia v. Cottage Health*). "This is an extremely troubling exclusion as it adds an uncertainty to the coverage," writes Richard S. Betterley. "The problem is, what happens when the standards change, or there is a mistake, and the insured is out of compliance? For us, the exclusion is hard to accept and dangerous for the insured. An insurer may say that it would never apply the exclusion, but we would not be confident that it will never be applied in the future."[50]

In contrast, some policies specifically exclude coverage for claims that result from a lost or stolen device when it is *unencrypted*. In other words, if a laptop containing patient health information is stolen and the data was unencrypted, the resulting liability for data exposure would likely not be covered.

Exclusions of this type can dramatically reduce premium costs, but of course, they also leave the policyholder exposed to risk. The best approach is to ensure that portable devices are deployed with strong encryption and to implement an effective auditing program to prevent accidental lapses. For example, an analysis produced by Marsh for the Public Utility Risk Management Services said that the unencrypted device exclusion "can be removed with confirmation that the applicant stores data on portable devices in any encrypted format, or otherwise has procedures in place to prevent a loss of such data should a device be lost or stolen."[51]

In this way, insurers have become an important driver for implementation of cybersecurity best practices. For many organizations, there is no clear cost to insecurity. Boards and executives have a vague sense of risk, but there is no specific dollar figure associated with gaps in cybersecurity practices. Even when regulations protect sensitive data, such as patient health information or credit card numbers, fines and penalties are not consistently applied or calculated. As cyber insurance evolves, underwriters are becoming an important factor in developing cybersecurity best practices and providing incentive for adoption.

12.5.7 Research the Insurer

The value of your insurance policy depends on more than the words in the document itself. The quality of vendors on the insurer's panel impacts the level of service the policyholders receive in the event of a breach, which can directly impact the outcome. In addition, many insurers provide value-added services and resources for policyholders, which can help reduce cybersecurity risks.

12.5.7.1 Insurance Panels and Prior Consent

Make sure to review the providers listed on your insurer's panel of approved vendors. This can help ensure that you will be working with qualified, experienced service providers in the event of a breach.

As an example, in 2014, Sony Pictures Entertainment (SPE) negotiated new cyber insurance coverage (by expanding the broader Sony Corporation of America (SCA) coverage to include

50. Betterley, *Market Survey: 2017*.

51. Marsh, "PURMS: Summary of Cyber Coverage Policy Period: November 3, 2016," October 31, 2016, p. 3, http://www.purms.org/MeetingDocs/Board/Annual/2016/Marsh%20-%2010-31-16%20Cyber%20Proposal%20-%20Appendix%20D.pdf.

SPE). The director of risk management for SPE reviewed the list of approved attorneys and emailed SCA to make sure that SPE's providers were approved prior to signing, as shown below:[52]

> From: Tetzlaff, Donna
> Sent: Wednesday, August 13, 2014 6:39 PM
>
> . . .
>
> Hi Kathy:
>
> On the schedule of firms for SCA there is listed Ropes & Gray LLC, that is one of our firms as well. We also see on the AIG's Panel Counsel List are Alston Bird and Baker Hostetler. We use these firms too.
>
> We would like to add:
>
> Baker Mackenzie [*sic*]
>
> Thank you.
>
> Donna

> From: Turck Rose, Kathryn
> Sent: Thursday, August 14, 2014 1:22 PM
>
> . . .
>
> Hi Donna,
>
> We have been informed that AIG confirmed they can add Baker McKenzie to the panel counsel list, subject to the rates of $500/$250/$100 already listed on the SCA policy.
>
> Regards,
>
> Kathy Turck Rose
> Director, Risk Management
> Sony Corporation of America

That's the way to do it—check in before you sign a policy or any time you have a change in your preferred vendor. Make sure to review not just the list of attorneys, but any provider you may wish to use—forensic investigators, PR firms, and the like. If you do need to add a provider, note that the insurer may set the rate, as AIG did with Sony. Rate caps are typically reasonable, but you should clear any rate limitations and payment terms with your preferred provider to ensure that there are no issues. When a breach occurs, you want to be able to get help as quickly as possible, so there are no unnecessary negotiations or conflicts in an already sensitive time.

---

52. "EM from K Turck-Rose to DT 8-13-14 AIG accepted Baker-Mackenzie.docx," WikiLeaks, accessed August 8, 2019, https://wikileaks.org/sony/docs/03_03/RISKMGMT/POLICIES/E%26O-Media-Tech-Cyber%20Liab/14-15%20Renewal/Cyber/Correspondence/SCA/EM%20from%20K%20Turck-Rose%20to%20DT%208-13-14%20AIG%20accepted%20Baker-Mackenzie.docx.

12.5.7.2 Value-Added Services

Today's cyber insurers offer much more than coverage. Many also provide valuable resources and services, from employee training videos to vulnerability scans, which are offered free or at a discount to policyholders. This is a win-win for the insurer and the policyholder: By making proactive training and security products more accessible, the insurer reduces risk and, presumably, saves money on insurance payouts.

As you review quotes and pricing, check out each provider's value-added services. Some of them can save you money, which may make up for differences in pricing. For example, many insurers offer policyholders access to a web portal with resources designed to reduce risk. These may include:

- **Security Awareness Training** - online training videos and quizzes to educate employees
- **News Center** - timely updates on cyber risk, security and compliance, upcoming events, and helpful links
- **Risk Management Tools** - useful tools for assessing and managing risk, such as online self-assessments, breach cost calculators, and policy templates
- **Learning Center** - whitepapers, articles, and recorded webinars

Other proactive free or discounted services can include:

- Vulnerability Scans
- Proactive Legal Advice
- Tabletop Exercises
- And more

12.5.8 Choose!

You've done all the hard work—now it's time to decide! Choosing your cyber insurance provider, of course, is typically an iterative process. You may wish to have one or two people take the lead and narrow down the list. Before you pull the trigger, make sure to loop in your key stakeholders again, to verify that you haven't missed anything important and to ensure that you have their buy-in. It's also important to get executive or board-level approval for any residual risk that will not be covered.

12.6 Leverage Your Cyber Insurance

Don't just buy cyber insurance and let your policy get dusty on a shelf. Your cyber insurance policy is one of the key elements of your cybersecurity and data breach response program. To get the most out of your investment in cyber insurance, you'll want to integrate your insurer's services into your policies and procedures, and build relationships with key members of their team.

Recall that to manage a data breach, your organization must have the following capabilities:

- **Develop** your data breach response function.
- **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
- **Act** quickly, ethically, and empathetically to manage the crisis and perceptions.
- **Maintain** data breach response efforts throughout the chronic phase and potentially long-term.
- **Adapt** proactively and wisely in response to a potential data breach.

Let's discuss how your cyber insurance comes into play for each of these capabilities.

12.6.1 Develop

Once you sign a new cyber insurance policy, make sure to integrate it with your response function. Here are some key steps to take:

- Consider having a preliminary meeting with your insurer's breach response team, if available.
- Understand how and when to notify your insurer of a breach. Know what the insurer needs from you and what to expect in terms of response times and persons involved. Make sure that you carefully review any notification and documentation requirements, so you don't accidentally miss any notification deadlines!
- Note any contractual obligations required, such as documentation that you need to maintain with third-party providers, that you may need to provide to your insurer in the event of a breach. Make sure your legal counsel is aware of these requirements and has a plan for maintaining compliance.
- Develop a list of items that you will want to clearly agree upon in advance with your insurer, such as the names of approved providers for legal/breach response services, and any other items where advance approval would be appropriate. Ideally, you will already have your preferred vendors approved before you sign, but this list may change over time, and you need a process for keeping it up to date.
- Put together a list for your IT management that includes any technical requirements (for example, mobile device encryption) that you will need to have in place and documented for the insurance to be maximally effective.
- Review your insurer's cyber services and tools, and make a plan to take advantage of any training opportunities, policy templates, cybersecurity news alerts, or other resources.

12.6.2 Realize

When your first responders notice the signs and symptoms of a potential breach, you'll need to act quickly to notify both internal and external response teams. If your insurer also handles breach response services for you, then your team will need to reach out.

One tip for responders: In your internal communications, refer to a potential breach as an "incident" or an "event." Depending on state and federal laws, an event that might informally be referred to as a "breach" may not actually meet the legal definition. A common mistake that responders make early on is to refer to a "breach" in writing, even though actual data exposure has not been confirmed. In the event that you're subjected to regulatory investigations or lawsuits, the existence of email threads or documentation that refers to a "breach" can increase your liability.

The next step is investigation and scoping. Typically, you will work with a qualified attorney to manage the investigation and make the final call on whether notification is required. You may also need to engage the services of a digital forensics team to conduct evidence preservation and analysis. Your insurer may assign your service providers based on their panel, or you may be able to use your own provider, with prior approval.

12.6.3 Act

Take quick action to minimize reputational, financial, and operational damage. For example, actions may include working with a PR firm to issue a press release about a cybersecurity attack or outage. Your insurance may cover the costs of notification, call center services, credit monitoring, or other reparations.

12.6.4 Maintain

During the chronic phase of a data breach, coverage for legal fees and investigative response is particularly important. As you move into this phase, make a plan for managing potentially long-term expenses and human resources related to the breach. Will your insurer front the costs of ongoing legal fees, or will you need to plan for a reimbursement cycle? Will you be better positioned to leverage your insurance if you hire outside consultants, as opposed to leveraging in-house resources? Remember that lawsuits and investigations can last for years after a breach is announced. Make a plan early on for maintaining your response and working with your insurer long term.

12.6.5 Adapt

Review your coverage after a breach. What worked? What didn't? Do you need higher limits or a different type of coverage? Was your insurer easy to work with, or did you experience challenges?

12.7 Conclusion

Make sure to review and adjust your cyber insurance coverage at least annually and upon major changes to your environment or the threat landscape. New cyber threats emerge so quickly that a policy that was appropriate one year ago may need major changes to fit your current needs. Also, the cyber insurance landscape is changing very quickly, and new products may emerge that better suit your needs.

With cyber insurance, like technology itself, you shouldn't just "set it and forget it." Actively monitor your insurance and the state of the industry to ensure that you have the right coverage for today's risks.

Chapter 13

Cloud Breaches

Yahoo became the reigning data breach poster child in 2016, when the company grossly mishandled a massive breach of customer passwords. Rumors of a breach began circulating in July 2016, when *Motherboard* magazine reported that "[a] notorious cybercriminal is advertising 200 million of alleged Yahoo user credentials on the dark web." Yahoo acknowledged that it was "aware" of the rumor, but would neither confirm nor deny that the stolen data was legitimate.[1]

The struggling tech giant was in the process of negotiating an aquisition by Verizon. In July 2016, just as the stolen Yahoo passwords were being advertised on the dark web, the two companies announced that they had agreed to a purchase price of $4.83 billion.[2] Over the coming months, as details of Yahoo's massive breach emerged, it became an important case study that showed how a data breach can affect a major acquisition.[3]

At the time, Yahoo provided cloud services for approximately 3 billion users. In addition to serving consumers, Yahoo catered heavily to small businesses, offering domain hosting, business email, e-commerce sites, and marketing services.[4]

Ultimately, Yahoo disclosed multiple breaches that spanned several years. First 500 million, then 1 billion, and then ultimately all 3 billion accounts were included in the scope.[5] It was the world's largest known data breach—and it had taken the tech giant years to detect and report it.

The Yahoo breach immediately raised questions as to the effectiveness of Yahoo's security program. Hackers were able to penetrate the tech giant's security not once, but many times. Soon, more details emerged, revealing a pattern of poor security practices. Former employees dished about Yahoo's internal struggles (in a manner reminiscent of the Target breach—and

1. Joseph Cox, "Yahoo 'Aware' Hacker Is Advertising 200 Million Supposed Accounts on Dark Web," *Motherboard*, August 1, 2016, https://motherboard.vice.com/en_us/article/aeknw5/yahoo-supposed-data-breach-200-million-credentials-dark-web.

2. Todd Spangler, "Verizon Announces $4.83 Billion Yahoo Acquisition," *Variety*, July 25, 2016, http://variety.com/2016/digital/news/verizon-yahoo-acquisition-announcement-1201821960.

3. Richard Lawler, "Yahoo Hackers Accessed 32 Million Accounts with Forged Cookies," Engadget, March 1, 2017, https://www.engadget.com/2017/03/01/yahoo-hackers-accessed-32-million-accounts-with-forged-cookies/.

4. Julie Bort, "Yahoo Builds Ultimate Private Cloud," *NetworkWorld*, July 19, 2011, https://www.networkworld.com/article/2179359/yahoo-builds-ultimate-private-cloud.html; "Yahoo! Small Business," Yahoo, February 1, 2014, https://web.archive.org/web/20140201051421/http://smallbusiness.yahoo.com/.

5. Bob Lord, "An Important Message About Yahoo User Security," Yahoo, September 22, 2016, https://yahoo.tumblr.com/post/150781911849/an-important-message-about-yahoo-user-security.

equally damaging). According to *Reuters*, "the security team was at times turned down when it requested new tools and features such as strengthened cryptography protections, on the grounds that the requests would cost too much money, were too complicated, or were simply too low a priority."[6]

Then there was the swirl of ethical and legal questions surrounding the timing of Yahoo's notifications. Even after the Yahoo credentials were discovered on the dark web in July 2016, Yahoo made no public statement and did not provide details of the investigation for nearly two months. Meanwhile, users continued to log in using the same account passwords, unaware that cybercriminals could be accessing their accounts, too.

In September 2016 (two months after the initial rumors surfaced), Yahoo suddenly announced that half a billion users' account details had been "stolen from the company's network in late 2014," in a possibly unrelated case. This included names, email addresses, phone numbers, birthdates, encrypted passwords, and security questions and answers.[7]

Shockingly, Yahoo had just submitted an SEC filing, which stated that the company had no knowledge of "any incidents of, or third party claims alleging . . . unauthorized access" to customer personal data—less than two weeks before publicly confirming the breach. Further reports showed that Yahoo "knew of a large security breach in 2014, but the company did not reveal the security breach to users until September 2016."[8]

"[T]housands of users took to social media to express anger," reported *Reuters*.[9] U.S. senators called the lag "unacceptable." The day after Yahoo announced the breach, it was hit with its first lawsuit by a customer claming the company was "grossly negligent."[10] Dozens more lawsuits followed.

As if it couldn't get any worse for Yahoo, law enforcement officials approached the company in November 2016 with copies of stolen files that reportedly contained more breached Yahoo user data. After investigating, Yahoo subsequently disclosed in December that "an unauthorized third party, in August 2013, stole data associated with more than one billion user accounts."[11]

"The scale of a second Yahoo breach disclosed on Wednesday was staggering," reported the *Washington Post*. "But, perhaps even more staggering was that the theft happened three

---

6. Joseph Menn, Jim Finkle, and Dustin Volz, "Yahoo Security Problems a Story of Too Little, Too Late," *Reuters*, December 18, 2016, https://www.reuters.com/article/us-yahoo-cyber-insight/yahoo-security-problems-a-story-of-too-little-too-late-idUSKBN1470WT.

7. Reuters, "Some Furious Yahoo Users Close Accounts After Data Breach," *Fortune*, September 23, 2016, http://fortune.com/2016/09/23/yahoo-customers-data-breach.

8. U.S. Securities and Exchange Commission (SEC), "Yahoo! Inc.," Form 10-Q, 2016, https://www.sec.gov/Archives/edgar/data/1011006/000119312516764376/d244526d10q.htm; Charlie Nash, "Yahoo Admits It Knew About Security Breach in 2014," Breitbart, November 10, 2016, https://www.breitbart.com/tech/2016/11/10/yahoo-admits-it-knew-about-security-breach-in-2014/.

9. David Shepardson, "Verizon Says Yahoo Hack 'Material,' Could Affect Deal," *Reuters*, October 13, 2016, http://www.reuters.com/article/us-verizon-yahoo-cyber-idUSKCN12D2PW.

10. Reuters, "Yahoo Is Sued for Gross Negligence Over Huge Hacking," *Fortune*, September 23, 2016, http://fortune.com/2016/09/23/yahoo-is-sued-for-gross-negligence-over-huge-hacking.

11. "Important Security Information for Yahoo Users," *Business Wire*, December 14, 2016, http://www.businesswire.com/news/home/20161214006239/en/Important-Security-Information-Yahoo-Users.

years ago—and had not been reported until now." In the fall of 2017, nearly a year later, Yahoo expanded the scope to include all 3 billion user accounts.[12]

Senator Mark Warner of Virginia said, "If a breach occurs, consumers should not be first learning of it three years later. Prompt notification enables users to potentially limit the harm of a breach of this kind, particularly when it may have exposed authentication information such as security question answers they may have used on other sites."[13] This reflected a notable advancement in the public's demonstrated understanding of data breaches: By the end of 2016, many people finally recognized that the compromise of their account credentials from one vendor could enable attackers to gain access to other accounts, as well.

In the meantime, Yahoo's executives were oddly absent. There was no spokesperson who put a human face to the company; no public press conference or interviews. When CEO Marissa Mayer canceled Yahoo's quarterly analyst conference call in October, reporter Stuart Lauchlan wrote, "The more cynical among us might wonder whether it's . . . an expedient way to avoid any difficult questions . . . such as when did Mayer find out about the breach . . .?"[14]

Due to the timing of the Yahoo breach discovery, it is possible to quantify precisely how much the breach disclosure impacted the value of the company. This was a rare and eye-opening development that cemented the company's place in data breach history. The original purchase price announced by Verizon and Yahoo in July 2016 was $4.83 billion.[15] By October, Verizon indicated that the impact of the security breach was "material" and could trigger a renegotiation of the purchase price or cause Verizon to back out of the deal completely.[16]

Ultimately, the Verizon deal went through, but $350 million was sliced off Yahoo's price directly as a result of the data breach.[17] (For comparison, this is roughly equivalent to the total annual budget of Vatican City.) Mayer resigned upon the close of the sale.

The fact that the Yahoo data breaches had a material, quantifiable impact on the company's value—and even threatened to kill the sale—sent a strong message to corporate boards of directors and executive teams throughout the country. Cybersecurity subsequently became a much bigger factor in mergers and acquisitions. Potential acquirers realized they needed to step up their due diligence efforts to detect potential breaches early on and reduce the risk of unexpected liability down the road.[18]

---

12. Hayley Tsukayama, "It Took Three Years for Yahoo to Tell Us about Its Latest Breach. Why Does It Take So Long?" *Washington Post*, December 19, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/12/16/it-took-three-years-for-yahoo-to-tell-us-about-its-latest-breach-why-does-it-take-so-long.

13. Tsukayama, "It Took Three Years."

14. Stuart Lauchlan, "Missing Marissa Mayer Leaves Yahoo! Questions Conveniently Unanswered," *Diginomica*, October 19, 2016, http://diginomica.com/2016/10/19/missing-mayer-leaves-yahoo-questions-conveniently-unanswered.

15. Todd Spangler, "Verizon Announces $4.83 Billion Yahoo Acquisition," *Variety*, July 25, 2016, http://variety.com/2016/digital/news/verizon-yahoo-acquisition-announcement-1201821960.

16. Shepardson, "Verizon Says."

17. Vindu Goel, "Verizon Will Pay $350 Million Less for Yahoo," *New York Times*, February 21, 2017, https://www.nytimes.com/2017/02/21/technology/verizon-will-pay-350-million-less-for-yahoo.html.

18. Kim S. Nash and Ezequiel Minaya, "Due Diligence on Cybersecurity Becomes Bigger Factor in M&A," *Wall Street Journal*, March 5, 2018, https://www.wsj.com/articles/companies-sharpen-cyber-due-diligence-as-m-a-activity-revs-up-1520226061.

But the full costs of the Yahoo data breach were not borne by Yahoo or Verizon. They were borne by society as a whole: by the untold number of people whose passwords were stolen and used to access their accounts, by third-party businesses that were hacked using the Yahoo password database, and by the innumerable data subjects whose information was stolen.

Throughout the whole saga, Yahoo downplayed the potential risks to customer data. The company's breach announcements provided the minimum necessary information to meet many states' legal requirements for breach disclosure. For example, Yahoo's December 2016 announcement stated that "the stolen user account information may have included names, email addresses, telephone numbers, dates of birth, hashed passwords (using MD5) and, in some cases, encrypted or unencrypted security questions and answers. The investigation indicates that the stolen information did not include passwords in clear text, payment card data, or bank account information. Payment card data and bank account information are not stored in the system the company believes was affected."[19]

The elephant in the room was the vast treasure trove of data held in customer accounts on Yahoo's systems, which criminals may well have accessed. Of the 3 billion people whose accounts may have been compromised:

- How many were accountants, who email tax returns, Social Security Numbers (SSNs), and financial information to their clients?
- How many were doctors, who forward patient information from their hospital accounts to their personal email accounts so they can work from home?
- How many were real estate agents, who email their customers' bank account numbers to title companies upon closing of a sale?
- How many were small, online retailers, who receive emails with credit card information from customers?
- How many were attorneys, who regularly exchange all types of highly sensitive data with their business and personal clients, for family law cases, medical malpractice lawsuits, business negotiations, and more?

These are just a tiny fraction of the ways that medical information, SSNs, bank account numbers, credit card numbers, trade secrets, and more find their way into email accounts. The fact is, an email system with billions of accounts absolutely contains all of these types of information, exchanged by senders and recipients via email. All of this data is heavily sought after by criminals.

When Yahoo stated, "Payment card data and bank account information are not stored in the system the company believes was affected," this can only be described as willful ignorance. The company narrowly scoped the incident to include only data provided directly to Yahoo for customer accounts. It completely ignored the fact that 3 billion customers had entrusted Yahoo with *their* sensitive information. In much the same way that National CSS had waved off the risks to data stored within customer accounts (see Chapter 2, "Hazardous Material"), Yahoo ignored the issue, too. The public didn't call them on it.

19. "Important Security Information."

Yahoo recommended that users "review all of their online accounts for suspicious activity and . . . change their passwords and security questions and answers for any other accounts on which they use the same or similar information used for their Yahoo account." However, it provided no details about how a user would check for "suspicious activity." Yahoo also made no offer to assist with identification of suspicious activity, despite the fact that automated log analysis across their full data set would be far more efficient and effective than making every user check his or her own individual account.

One might be forgiven for wondering if Yahoo didn't really *want* users to find out if their accounts had been accessed by an unauthorized user. After all, what was the incentive for Yahoo to help users find out if their accounts had been accessed inappropriately? That would only have led to many other alarming questions and potentially much greater liability.

The Yahoo breach was only the beginning of what would become a global epidemic of cloud account compromises. Fueled by easy access to stolen passwords and weak authentication methods, criminals developed scalable, organized methods for breaking into cloud accounts and mining the valuable data they contained. Over the coming years, issues of visibility and control within the cloud environment came to a head.

Cloud breaches have introduced a host of new issues for response teams, from questions about cloud-based evidence to notification requirements. In this chapter, we will enumerate the different types of cloud data breaches and common response considerations. We will discuss issues of control and visibility, including access to evidence and ethical considerations. Finally, we will discuss the ways that cloud security has been undermined, how that has contributed to the epidemic of data breaches, and choices that we can make as a society to reduce risk for all.

13.1 Risks of the Cloud

Over the past decade, organizations of all kinds—from healthcare to government to finance—have shifted to the cloud, in order to take advantage of the many benefits, such as cutting-edge software, scalability, and lower cost of maintenance. According to McAfee, a whopping 97% of organizations use cloud services in some form or fashion, and 83% reported that they store "sensitive data" in the cloud. This includes personal customer information, payment card data, government identification data, healthcare records, intellectual property, and more.[20]

But the benefits of the cloud also come with significant risks. A quarter of organizations reported that they had suffered "data theft from the public cloud." The security of cloud providers and their customers is deeply intertwined. "Our breach is their breach, and their breach is our breach," quipped one CEO.[21]

Typically, data breaches in the cloud occur for one of the following reasons:

- Security Flaws
- Permissions Errors

20. "Navigating a Cloudy Sky," McAfee, April 2018, https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-security-report.html.

21. "Navigating a Cloudy Sky."

- Lack of Control
- Authentication Issues

In this section, we will discuss common reasons that cloud breaches occur, as well as challenges and best practices for responders.

13.1.1 Security Flaws

Cloud providers work hard to project an image of invincibility since customers naturally seek to host their data in a secure place. However, cloud providers suffer from vulnerabilities and data breaches, just like other organizations. These can occur because of bugs in software developed by the cloud provider, issues involving third-party applications, or staff errors.

For example, the Dropbox file sharing service, used by millions of people around the world, has suffered a string of highly publicized security issues that may have resulted in data breaches. In 2011, Dropbox pushed out a code update that accidentally removed authentication requirements for customer accounts—meaning anyone could access customers' sensitive data, even without a correct password. Customer data was exposed for nearly four hours before Dropbox implemented a fix.[22]

The following year, Dropbox customers sounded an alarm when they began receiving targeted spam messages to email addresses that, in some cases, they had created exclusively for use with Dropbox.[23] Dropbox investigated and announced that an employee's password had been stolen and used by attackers to access a document containing customer email addresses.

Reportedly, the Dropbox employee had reused a password on his or her LinkedIn account and work account. After LinkedIn was breached, criminals used the employee's stolen LinkedIn password to log in to the employee's work account, too—neatly illustrating how breaches can lead to more breaches.[24] The events triggered scrutiny of Dropbox's internal security and password management practices. In response, Dropbox announced that it was introducing two-factor authentication as an option for customers, in addition to other security measures.

Four years later, the other shoe dropped. In 2016, cybercriminals on the dark web were found peddling a database containing 68 million Dropbox user passwords. Dropbox sent an understated message to customers, explaining that "we learned about an old set of Dropbox user credentials (email addresses plus hashed and salted passwords) that we believe were obtained in 2012. Our analysis suggests that the credentials relate to an incident we disclosed around that time." Never mind that *four years* had gone by, and Dropbox had never previously indicated that any customer passwords could have been stolen. Now, Dropbox confidently declared that "[b]ased on our threat monitoring and the way we secure passwords, we don't

22. Ed Bott, "Why I Switched from Dropbox to Windows Live Mesh," ZDNet, July 4, 2011, https://www.zdnet.com/article/why-i-switched-from-dropbox-to-windows-live-mesh/; Arash Ferdowsi, "Yesterday's Authentication Bug," *Dropbox Blog*, June 20, 2011, https://web.archive.org/web/20110718041143/http://blog.dropbox.com/?p=821.

23. Ed Bott, "Dropbox Gets Hacked . . . Again," ZDNet, August 1, 2012, https://www.zdnet.com/article/dropbox-gets-hacked-again/; Emil Protalinski, "Dropbox Finds No Intrusions, Continues Spam Investigation," ZDNet, July 20, 2012, https://www.zdnet.com/article/dropbox-finds-no-intrusions-continues-spam-investigation/.

24. Samuel Gibbs, "Dropbox Hack Leads to Leaking of 68m User Passwords on the Internet," *Guardian*, August 31, 2016, https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach.

believe that any accounts have been improperly accessed"—although the company offered no evidence to support that claim.[25]

Third-party software can also lead to cloud data breaches. For example, in 2016, a WordPress plug-in known as Custom Content Type Manager began stealing admin credentials after an update installed a malicious backdoor. Similarly, in 2018, a popular website accessibility plug-in called Browsealoud was infected and used to install a cryptocurrency miner on thousands of U.S. and U.K. websites. The plug-in's developer, Texthelp, said it was the victim of a "cyber attack," illustrating how a single vulnerable product can lead to widespread, cascading compromises in the modern software ecosystem.[26]

Tip: Check Your Provider's Breach History

Before uploading any sensitive data to a cloud provider, research the provider's history of data breaches. While data breaches happen to many reputable organizations, a pattern of multiple data breaches should send up a red flag. More important, analyze how the cloud provider responded to each breach. Did the provider communicate openly, honestly, and in a timely manner? Did the cloud provider appear to have a strong monitoring program in place? Or, are there indications that the provider did not understand the full scope of the breach, or perhaps even deliberately minimized or hid important details? Make sure to select only cloud providers that you trust will notify you of a breach in a timely manner and provide the evidence you need to properly respond.

13.1.2 Permission Errors

When data is already up in the cloud, a checkbox can make the difference between proper security and a serious data breach. Too many unfortunate system administrators have experienced the sudden heart palpitations that come with the discovery that sensitive data was indexed on Google or found by an unusually inquisitive web visitor—often due to a simple permissions error.

For example, beginning in 2017, a series of data breaches involving Amazon S3 buckets (a type of data repository) was reported by security researcher Chris Vickery of UpGuard. Dow Jones exposed personal data of 2.2 million customers. An analytics firm working on behalf of the Republican National Committee exposed personal details relating to 198 million Americans. Booz Allen exposed more than 60,000 files containing highly sensitive data, including cleartext passwords used by contractors with Top Secret Facility clearances. The consulting firm Accenture exposed four buckets containing "highly sensitive data," including passwords relating to the cloud accounts of major customers. The list went on and on.

---

25. Joseph Cox, "Hackers Stole Account Details for Over 60 Million Dropbox Users," *Motherboard*, August 30, 2016, https://motherboard.vice.com/en_us/article/nz74qb/hackers-stole-over-60-million-dropbox-accounts.

26. Matt Burgess, "UK Government Websites Were Caught Cryptomining. But It Could Have Been a Lot Worse," *Wired*, February 12, 2018, https://www.wired.co.uk/article/browsealoud-ico-texthelp-cryptomining-how-cryptomining-work.

The breaches occurred because, in each case, someone had put sensitive data in an Amazon bucket that was accessible to the public—or, somewhere along the way, someone mistakenly unchecked the checkbox that limited access. The problem was rampant; security firm Skyhigh Networks estimated that 7% of all Amazon S3 buckets were publicly accessible.[27]

Breaches of this type are often discovered and reported by members of the public. It's easy to check to see whether an Amazon bucket is public simply by typing the name of the bucket into the address bar of your web browser, as part of a URL. In recent years, plenty of open-source tools have emerged to quickly enumerate public buckets and check their contents. Once reported, the first step is to remove the unauthorized access as quickly as possible. If access logs exist, investigators can analyze them to determine whether the data was actually accessed by an unauthorized party. Granular log data can enable investigators to rule out a breach. However, often access logs are not collected in the first place, or if they are, the logs go back for only a short period. Response teams need to collect and preserve cloud access logs as quickly as possible in these types of cases, in order to maximize the chances of ruling out a breach.

In many cases, third-party service providers are responsible for the error—but the contracting organization still bears the brunt of the reputational damage. For example, Scottrade Bank suffered an embarrassing data breach after a third-party vendor, Genpact, left 20,000 customer records in a public Amazon S3 bucket.[28] In a similar case, Verizon was shamed in a July 2017 breach announcement after one of its suppliers, NICE Systems, accidentally left 14 million customers' personal information sitting in a publicly accessible Amazon S3 bucket. The customer data included names, phone numbers, account details, and PINs.

For responders, the involvement of a third party can dramatically complicate breach response. For one thing, your organization may not have direct access to the misconfigured cloud account, leading to delays in containment. This can also cause delays in evidence preservation, which can result in lost evidence and make it harder to "rule out" a breach.

Tip: Exposure Is Not Always a Breach

Accidental cloud data exposure is very common—but it doesn't always result in a data breach. When data has been exposed by mistake due to a permissions error or similar issue, investigators should preserve and review any existing access logs and file metadata in order to determine whether unauthorized access actually occurred. In some cases, data may not have been accessed at all, or accesses can be traced back to authorized users, enabling the organization to avoid a costly breach declaration.

27. Catalin Cimpanu, "7% of All Amazon S3 Servers Are Exposed, Explaining Recent Surge of Data Leaks," *BleepingComputer*, September 25, 2017, https://www.bleepingcomputer.com/news/security/7-percent-of-all-amazon-s3-servers-are-exposed-explaining-recent-surge-of-data-leaks/.

28. Steve Ragan, "Scottrade Bank Data Breach Exposes 20,000 Customer Records," CSO, April 5, 2017, http://www.csoonline.com/article/3187480/security/scottrade-bank-data-breach-exposes-20000-customer-records.html (accessed February 19,2 019).

13.1.3 Lack of Control

One of the most common (and least-detected) forms of a data breach is when employees upload sensitive documents to their personal email or cloud accounts. Often, they do this for well-meaning purposes, in order to work remotely or share files with collaborators, not realizing that this can lead to serious security problems. Once the employee hits "send," the data is functionally outside the organization's control. It may be analyzed by third-party cloud providers, stolen by undetected hackers, stored on the employee's home computer, or improperly tossed away.

Simply uploading files to the wrong cloud provider may trigger a data breach, depending on the type of data and the legal framework that applies. This is because cloud providers may routinely access user data, sell or share data with third parties, or even create derivative data products. Meanwhile, unknowing users may blithely upload regulated data, expecting it to be private, without understanding the consequences.

For example, Oregon Health & Science University (OHSU) was hit with a record $2.7 million fine that was due in part to improper use of the cloud. In 2013, a faculty member discovered that physicians-in-training had uploaded a spreadsheet of patient data to Google, in order to "provide each other up-to-date information about who was admitted to the hospital under the care of their division."[29] Despite the residents' best intentions, the outcome wasn't good. The hospital launched an investigation that uncovered another, similar practice in a different department, and ultimately discovered that more than 3,000 patients' information had been uploaded to the cloud without authorization.

At the time, Google's general terms of service included the following statement:[30]

> When you upload or otherwise submit content to our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works . . . communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services.

OHSU's representatives attempted to confirm that Google would not use the data in the ways they described, but they were unsuccessful. Absent the ability to rule out unauthorized use, OHSU notified the public and the Department of Health and Human Services. Later, the Office for Civil Rights conducted an investigation and concluded that there was "significant risk of harm to 1,361 of these individuals due to the sensitive nature of their diagnoses."[31]

---

29. Oregon Health & Science University, "OHSU Notifies Patients of 'Cloud' Health Information Storage," July 28, 2013, https://www.ohsu.edu/xd/about/news_events/news/2013/07-28-ohsu-notifies-patients-o.cfm.

30. "Terms of Service," Google, March 1, 2012, https://www.google.com/intl/en_US/policies/terms/archive/20120301/.

31. U.S. Department of Health and Human Services, Office for Civil Rights, "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information," July 28, 2013, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf; U.S. Department of Health and Human Services, Office for Civil Rights, "Widespread HIPAA Vulnerabilities Result in $2.7 Million Settlement with Oregon Health & Science University," July 18, 2016, https://web.archive.org/web/20160813124846/https://www.hhs.gov/about/news/2016/07/18/widespread-hipaa-vulnerabilities-result-in-settlement-with-oregon-health-science-university.html.

Google, of course, is not alone in its approach to analyzing and leveraging user-uploaded data. Nor were the hospital physicians-in-training at all unusual: Many dedicated employees decide, independently, to upload work data to the cloud in order to facilitate collaboration with peers or work from home. Unfortunately, when it comes to the cloud, employees' good intentions can cause big problems.

Controlling cloud use is difficult, particularly in complex environments such as hospitals and academia. Users crave the convenience of the cloud. Absent strong technical controls or safe alternatives, employees may unwittingly perpetuate data breaches.

Tip: Proactively Control Cloud Use

It can be challenging to work with a cloud provider in the event of a breach. Communication and access to digital evidence can pose major roadblocks for an investigation. When your data is uploaded to a cloud provider that you don't even have a formal relationship with, these challenges can prove insurmountable.

The best defense is prevention. Make sure all of your staff receive regular training emphasizing the important of using *only* approved cloud providers. Whenever possible, implement technical measures to control the spread of data, such as data-loss prevention (DLP) tools that block data transfers to unapproved sites, or software that monitors for the use of cloud applications and allows only approved connections.

13.1.4 Authentication Issues

All too often, the easiest way for criminals to break into cloud accounts is right through the front door, leveraging stolen passwords or other authentication weaknesses. In recent years, password theft has become a widespread epidemic, leading to countless data breaches. In 2017, Verizon reported that fully 81% of hacking-related breaches leveraged weak or stolen passwords.[32] This isn't surprising, given the shocking number of passwords that have been exposed in previous breaches, and the sophistication of cybercriminals' password-stealing tools.

In a 2017 report, Google researchers revealed that they had found 1.4 *billion* unique username and password combinations available on the dark web in a one-year period. The vast majority of these credentials were exposed in a data breach of a cloud service, such as MySpace, LinkedIn, or Dropbox. The researchers also found that criminals collected, on average, 234,887 credentials every week using phishing toolkits, and 14,879 credentials per week using keystroke loggers.

While that may sound like a lot of stolen passwords, it was undoubtedly just a subset of the total. "We emphasize our dataset is strictly a sample of underground activity," the researchers wrote, "yet even our sample demonstrates the massive scale of credential theft occurring in

32. "Verizon's 2017 Data Breach Investigations Report," Verizon Enterprise, 2017, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf.

the wild."[33] By October 2017, Yahoo announced that 3 billion customer accounts had been affected by a data breach—a single provider whose exposed accounts dwarfed those reported in Google's study.[34]

Stolen passwords are bought and sold (or sometimes just given away!) by criminals on the dark web, who use them to compromise victims' accounts, often to commit financial fraud or steal more data. The damage caused by stolen passwords is vastly amplified because of the fact that many people reuse passwords (sometimes with minor variations) for multiple accounts. Cybercriminals now routinely conduct "credential stuffing" attacks, taking lists of exposed credentials and automatically trying them on other websites in order to break into more accounts.

Two-factor authentication (2FA) can dramatically reduce the risk of account breaches, by requiring a second method of identity verification so that passwords alone cannot give a criminal access to your account. However, only an estimated 28% of people used two-factor authentication by late 2017, accounting to Duo Labs' *State of the Auth* report.[35] Those that do use 2FA often rely on a weak second factor, such as a PIN sent through SMS (text message), which can be intercepted or captured. Users that input a code from an application or device as their second factor can also be tricked into entering it into a phishing site, allowing criminals to access the victim's account in real time.

Shared Responsibility

Typically, cloud providers do not take responsibility for data breaches attributed to permissions errors or misuse of authentication credentials. For example, Amazon espouses a "shared responsibility" model, where Amazon claims responsibility for "security of the cloud" (e.g., software, hardware, global infrastructure), and the customer is responsible for "security 'in' the cloud" (e.g., identity and access management, permissions, etc.).[36]

Despite this seemingly neat division of responsibility, it's important for customers to recognize that the risk of permission errors and account compromises (and therefore the risk of a data breach) is strongly influenced by the cloud software's design and capabilities, the availability of training resources, default options set by the provider, and ease of access to audit utilities.

While customers undoubtedly play a role in defending against data breaches, the tools they rely upon to fulfill their responsibilities are largely controlled by the cloud provider. This influences both the risk of a data breach and its outcome.

---

33. Kurt Thomas et al., *Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials* (research paper, Google, Mountain View, CA, 2017), https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46437.pdf.

34. Nicole Perlroth, "All 3 Billion Yahoo Accounts Were Affected by 2013 Attack," *New York Times*, October 3, 2017, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

35. Olabode Anise and Kyle Lady, *State of the Auth* (Duo Labs Report, 2017), 5, https://duo.com/assets/ebooks/state-of-the-auth.pdf.

36. "Shared Responsibility Model," Amazon, accessed February 19, 2019, https://aws.amazon.com/compliance/shared-responsibility-model/.

13.2 Visibility

"Poor visibility is one of the greatest challenges to a navigator," opens McAfee's 2018 report on the state of cloud usage. McAfee's researchers surveyed 1,400 IT decision makers around the world and found that organizations everywhere were moving full steam ahead to the cloud. A whopping 83% of organizations now store sensitive data in the cloud. Frighteningly, fully one in four report that they have experienced a data theft. This number is all the more surprising given that organizations have very limited ability to see what is going on; nearly a third of respondents said they had "difficulty getting a clear picture of what data is in their cloud applications."[37] Logically, in order to know that data has been stolen, you have to be aware that it exists in the first place.

As cloud data breaches proliferate, the issue of visibility has become critically important. Moving to the cloud has many benefits, but in the process, organizations lose direct access to extensive volumes of authentication logs, application logs, and network data that is necessary to detect and properly investigate cybersecurity incidents. Customers are limited by the capabilities and responsiveness of the cloud provider. All too often, customers request digital evidence from a cloud provider in order to resolve a cybersecurity issue, only to find that the evidence does not exist or that their request is ignored, delayed, or denied. When the evidence does exist in a useful format, exporting logs may be prohibitively expensive, hampering both intrusion detection and forensic analysis efforts.

In this section, we will discuss issues of visibility in the cloud and the impact on breach detection and response, using business email compromise as an example. Specifically, we will delve into thorny issues such as access to evidence, quality of forensic data, and ethical considerations.

13.2.1 Business Email Compromise (BEC)

Email account break-ins seem to happen as often as the common cold—and often, users shrug them off. Business emails contain valuable data, such as banking details, SSNs, passwords, credit card numbers, and other details that can be sold on the dark web or used for fraud. Criminals that hack into email accounts find a wealth of valuable data, ready to be harvested.

Over the years, it became easier and easier for criminals to break in to email accounts. With the emergence of Microsoft Office 365 and other high-quality, cloud-based enterprise platforms, businesses of all sizes shifted to cloud-based email services, enabling users (and criminals) to access their inboxes from anywhere in the world. Between the rampant theft of passwords and the success of targeted phishing attacks, cybercriminals groups found that email was an easy target.

Organized crime groups soon developed repeatable, scalable methods for breaking into email and committing financial fraud. "[S]cammers have been using sophisticated email campaigns to defraud businesses of all sizes through the use of fake invoices, wire transfers, and international payment requests," reported Duo Security in July 2018. "The scams often rely on compromised email accounts inside a target organization, and the operations are growing at a

37. "Navigating a Cloudy Sky," 5 and 15.

terrific rate, with losses in the United States alone of nearly $3 billion in the last 18 months."[38] Globally, more than $12 billion was lost due to email account compromises in the same time period.[39]

Office 365 accounts have been particularly targeted. This makes sense given the popularity of the cloud solution. By 2018, Office 365 was widely recognized as the leading cloud office software provider, when a global survey of 135,000 corporate domains showed that it had achieved 56.3% market share[40]—well above that of the second leading provider, G Suite. As a result, many criminals fine-tuned their scams to take advantage of Office 365 features, designing phishing landing pages that mimicked the service's login pages and modifying the configuration of compromised user accounts in order to better hide their tracks.

In one common scam, an attacker hacks into a victim's email account and searches for references to an upcoming transaction (such as invoices or wire transfer instructions). Then, the attacker creates a spoofed invoice or wire transfer notification and sends an email requesting that the funds be transferred to the new location. Typically, the attacker's email is very similar to a real party in the communication, and because it is sent in the context of an existing transaction, the recipient often does not detect the scam until the money is gone and it is too late. Sophisticated criminals add mail filtering rules that send the real recipient's messages to the system archives, further lengthening the time to discovery.

Once criminals break into an email account, they often make a point of targeting related accounts, such as coworkers, clients, or anyone listed as a contact. In many cases, criminals download entire accounts of correspondence in order to mine the data offline.

13.2.1.1 BEC Response

The first step in responding to a BEC case is to cut off the attacker's access, typically by changing the user's password. In cases where other accounts may have been compromised, it is generally considered prudent to reset passwords for all potentially affected accounts, even if a compromise is not confirmed. Many organizations implement two-factor authentication (2FA) in an emergency immediately following a BEC discovery. While this is not the ideal method for implementing 2FA, it can dramatically reduce the risk of further compromise.

Responders should also check affected accounts for mail forwarding rules. All too often, attackers set up a rule that forwards all emails to a third-party account, such as a Gmail or Yahoo account that they control.

Finally, it may be wise to immediately place a legal hold on affected mailboxes so that important messages involved in the case cannot be accidentally (or purposefully) deleted.

13.2.1.2 BEC Investigations

It used to be the case that when businesses were alerted to an unauthorized email access, they simply reset the user's password and moved on without investigating a potential data breach

38. Dennis Fisher, "The Rise and Rise of Business Email Compromise Scams," *Decipher*, Duo Security, July 16, 2018, https://duo.com/decipher/the-rise-and-rise-of-business-email-compromise-scams.

39. Federal Bureau of Investigation, "Public Service Announcement: Alert Number I-071218-PSA," July 12, 2018, https://www.ic3.gov/media/2018/180712.aspx.

40. Bitglass, "Cloud Adoption: 2018 War," p. 4, https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_Cloud_Adoption_2018.pdf

(as was undoubtedly the case for the vast majority of business accounts affected by the Yahoo breach). The concept that an email hack might be a data breach did not occur to most IT staff or executives. Moreover, a data breach could result in fines, reputational damage, or other negative consequences, which could be avoided by simply ignoring the risk and moving on.

This changed as the number of BEC cases rose and the availability of cyber insurance gave more businesses access to experienced data breach response teams who understood the risks involved in BEC. Instead of sweeping BEC incidents under the rug, businesses began notifying their insurers and investigating these cases as potential data breaches. This was especially true when the hack involved a financial loss (such as wire transfer fraud) or damage to third parties.

Today, BEC investigations generally involve the following activities:

- **Determine which accounts have been compromised.** This typically involves review of authentication logs, mail filtering rules, and in some cases, content. Often, a thorough investigation of an organization's email system reveals more compromised accounts than originally expected.
- **Identify sensitive information stored within the compromised accounts, such as protected health information (PHI) or personally identifiable information (PII).** Usually, this begins with an automated search of the mailbox for common terms or patterns, and may require a manual review for documents that cannot be programatically analyzed.
- **Determine whether the criminals accessed any of the sensitive information.** If logs for individual message reads are available, it may be possible to narrow the scope of compromised data by determining which messages the criminal actually accessed. Unfortunately, criminals often download the entire mailbox via IMAP, rendering all data compromised.

The costs of breach response for BEC cases can be astronomical because of the volume and sensitivity of data that many people store in their email accounts. "These attacks are expensive because, in order for the target company to understand the full impact and whether [PII] or [PHI] is at risk, they often require programmatic and manual searches of years' worth of emails for sensitive information," explained Beazley in its July 2018 report on BEC cases. "For larger scale email compromises, if the majority of users sent and received PII or PHI, the total cost of legal, forensics, data mining, manual review, notification, call center and credit monitoring can exceed $2 million. And even for the smaller scale email compromises, the costs can easily exceed $100,000."[41]

BEC cases are especially challenging and time-consuming when HIPAA-regulated PHI is involved. This is because the HIPAA Breach Notification Rule presumes that the data is breached unless the organization "*demonstrates that there is a low probability*" the data has been compromised. If an attacker gained access to a user's mailbox, then typically the data it contains is presumed compromised unless granular log data can conclusively show that specific messages or attachments were *not* accessed. Any data that has been compromised must be carefully analyzed so that all affected data subjects are enumerated and notified.

In cases that do not involve PHI, the process for resolving BEC cases may be different. In the United States, attorneys often take into consideration the attackers' intent. Some times, investigators can provide a record of the terms that the attackers searched for in the mailbox—

41. "Beazley Breach Insights - July 2018," Beazley, July 31, 2018, https://www.beazley.com/usa/beazley_breach_insights_july_2018.html.

such as "invoices" or "wire transfer." When the attackers' intent appears to be financial fraud, not theft of PII, the attorney may determine that the risk to data subjects is low and no notification is required.

13.2.2 Evidence Acquisition

Access to evidence is critical for BEC cases in order to rule out a data breach. Absent evidence, organizations face a tough choice; they can either:

1. **Notify a broad group**, which may result in overnotification and unnecessary financial, reputational, or legal damage, or
2. **Refrain from notification**, and risk costly fines and public outrage if the breach is later discovered and confirmed.

For BEC cases, useful evidence normally includes:

- Login events, including date, time, duration, IP address, and browser type
- Search events, logged by session ID and tied to user account accesses
- All email activity, including read events, duration of message views, cration, delivery, etc.
- Attachment view events

Unfortunately, cloud email providers rarely provide the same depth and variety of log data that is available from well-instrumented on-premises installations. In many cases, granular log data is not collected in the first place or, if it is, getting it from the cloud provider may require extensive conversations or legal action—and even then, the response team may not be successful.

Challenges for cloud-based evidence acquisition include:

- **Lack of logs** - The cloud provider simply may not be logging activities needed for resolving potential data breaches. Even when a cloud provider does have logs, it is typically just authentication or application logs, and not the full depth of activity logs that could be available from a local enterprise environment.
- **Limited or inconsistent export capabilities** - Cloud providers may cap or throttle the amount of log data that can be exported at a time, slowing investigations or causing errors.
- **High costs for log export** - There can be a cost to export data from the cloud, and log data is no exception. Unfortunately, the cost of exporting logs is typically not built into the budget (or even considered) when migrating to a cloud provider.
- **Changing log format** - Cloud providers can (and do) change the format of their logs at any time. This can create special challenges for investigators, who require a standard format to parse data in bulk.
- **Lack of documentation** - Investigators need to understand the meaning of important fields in logs, but all too often the format of log data is not well documented or existing documentation is outdated/incorrect.

Since Office 365 has been particularly targeted, many investigators find themselves gathering evidence from Microsoft's native cloud logging system or on the phone with Microsoft support teams. However, until early 2019, granular logging for mailbox activities was not enabled by default in Office 365. That meant that many organizations suffered a breach, only to discover that they did not have the evidence they needed to rule anything out. Even for organizations that wanted to implement logging, many did not realize that mailbox logs had to be enabled in two different places, and when it was turned on, the evidence produced was of limited value in BEC investigations.

In 2019, after the saga of the "Magic Unicorn Tool" played out in the public eye, Microsoft implemented default logging of mailbox activities for all new corporate accounts. More logs were available for higher-tiered customers, but a basic level of logging was stored for all corporate users, greatly facilitating investigations.

The Magic Unicorn Tool

"Do you have the secret Office 365 forensics tool?" a breach response manager for a major company asked our forensics team.

"What secret tool?" I replied. He explained that a few forensics firms they worked with possessed a secret tool that could pull extra activity details out of Office 365. These details were not accessible using the normal, published Office 365 query mechanisms. He said the tool was very secret and he wasn't at liberty to share more.

We waved it off, figuring it was a marketing ploy. Our team couldn't imagine that Microsoft would fail to disclose that such valuable data existed, especially when thousands of its customers were battling the spectre of a breach. Forensics folklore, we concluded.

But the rumors continued. Major insurers and law firms started to screen forensics firms based on whether they had "the secret tool." Only a handful did—the rest were shut out. Over and over, forensics professionals started to hear, "Sorry, we can't send you cases if you don't have the secret tool." And yet, there were no details, and no one with knowledge of the tool would even confirm its existence.

What was this secret tool? If it existed, we had to get it.

As luck would have it, two of our colleagues were at Microsoft headquarters for a meeting with Microsoft's security and IT team. While onsite, they pulled Microsoft staff aside. An internal security team member and an Office 365 developer both insisted, separately, that the secret tool could not possibly exist. We had it straight from the horse's mouth. The "Magic Unicorn Tool," as we dubbed it, was not real.

Emboldened, we called one of our attorney partners, who had been interested in using our forensics team on an Office 365 email compromise case. He flatly disagreed, stating that the tool existed. Then, he gave us a list of five major forensics firms that were (quietly) advertising that they possessed the secret tool. The attorney sent his case over to one of the firms that had the tool. Whether it worked as advertised, the Magic Unicorn Tool was a clear competitive advantage.

(*Continues*)

(*Continued*)

We needed help. I wrote a message to a forensics community mailing list: "Does this 'secret tool' actually exist?" A few people wrote privately to share vague rumors, but no one had specifics.

The next morning, a forensics community leader confirmed that the tool existed. "It's True. All of it. The Dark Side of o365. The Jedi who can perform this magic," he wrote. "It DOES in fact exist." But he himself could not share details.

We were stymied. How could such a tool exist but remain secret? It was as if Alexander Fleming had discovered penicillin but kept the details hidden in order to make more money. It just seemed wrong.

"We're going to run this to ground," I announced confidently to our team—but inside, I had the feeling you get when you're losing a hand of poker.

The tide turned on Friday, June 8, 2018. Out of the blue, an email popped onto the forensics community mailing list. It contained a single link, to a video. On the screen, a familiar white mask began to speak.

> Greetings . . . We are Anonymous. Today we come bearing gifts. . . . We are here to better humanity by uniting forensic examiners. For the good of citizens and public companies we demand there be no secrets.
>
> Stop this child's play. Over the years we have seen companies delay artifact disclosure. This is dangerous like 0-day vulnerability disclosure. Some places view this as competitive intelligence. They reap the benefits, make lots of money and live like a Saudi prince . . . ultimately, this is usually at the mercy of some companies having to overreport, notify and pay lots of money.
>
> Forensic artifacts should be shared, scrutinized, vetted and improved—not hidden. Not thwarted . . . The gold mine of data that allows you to determine various actions despite audit logging not being turned on does exist. The API you seek is called Activities. . . . There may be others but this is one of them. Now the community can do the rest and what is right.
>
> We are Anonymous. We do not forgive. We do not forget. Until next time.

Ten days later, CrowdStrike published a detailed blog post. "[W]e recently discovered a capability within Office 365 that allows for the retrieval of Outlook mailbox activity logs that far exceeds the granularity provided by existing, documented Office 365 log sources," they wrote. "This capability represents access to an always-on, mailbox activity recording system that is active by default for all users." They released a Python module to automate retrieval.

Our team's forensic analysts quickly created a wrapper script called the Magic Unicorn Tool, which produced human-readable reports that were useful for BEC cases. The new tool worked retroactively; even if a customer had not enabled logging, the tool was still able to retrieve detailed mailbox activity logs spanning six months in the past. In other words, Microsoft had been collecting the data the whole time—it was simply not made available to customers.

Days after its release, Microsoft cut off public access to the Activities API, killing the Magic Unicorn Tool. Customers that discovered data breaches after this point were out of luck, unless they were large enough to get special attention from Microsoft's support team.

In January 2019, Microsoft announced the upcoming release of new logging capabilities that included most (but not all) of the data. However, in March, the company announced that the feature would "no longer be available." For the latest status, visit the author's website, hackeralien.com.

13.2.3 Ethics

The saga of the Magic Unicorn Tool raises important ethical questions for breach responders, forensic analysts, and the broader cybersecurity community. Below are a few such questions.

- **What is the responsibility of cloud providers to support forensic investigations?**

Data breaches involving cloud accounts are inevitable, much like fires in a city. When a data breach happens, however, customers may not have access to the information they need to detect, contain, or investigate the crisis. Forensics evidence is critical for detecting and resolving data breaches. Yet all too often, cloud providers do not make it available to customers, or if they do, it comes with a hefty price tag that many cannot afford. Customers often do not realize that by moving to the cloud, they will lose easy access to critical log data that is readily accessible from on-premises software installations—until it is too late.

As a result, many organizations do not have the visibility to support early detection of data breaches in the cloud. When they get hacked, they end up over- or under-notifying since they do not have the detailed evidence to fully understand what occurred. This is an especially challenging issue for cash-strapped organizations, which cannot justify paying a premium for logs.

Like fires, data breaches don't just damage individuals. The impact extends to the wider community. For example, when an email account is hacked and thousands of people's stolen personal records are used to commit fraud, the impact can spread to financial institutions, merchants, insurers, and ultimately the customers they serve. When a million cloud account passwords are stolen, fraudsters use these as ammunition to break into innumerable other accounts, such as bank accounts, medical portals, e-commerce sites, and more, causing far-reaching consequences. Any individuals or other organizations with potentially compromised sensitive information may experience follow-on attacks, fraud, extortion, or other negative consequences as a direct result of a breach.

There are ways to reduce the risk of fire, to contain it, and to prevent it from spreading. Society has collectively invested in fire mitigation and developed prevention and response tactics using community resources. Healthy cities have effective fire prevention strategies built into building code, as well as fast alerting and response systems. Fire hydrants with standardized measurements are installed throughout the city to ensure that responders have access to the water they need, wherever they are. Building elevators are fitted with fire keys that are distributed to responders in advance of an emergency. All of these are measures that most individual organizations could never implement alone.

Similarly, there are ways that society can reduce the risks associated with data breaches. If an appropriate level of logs were readily available to customers of any cloud platform, then data breaches could be detected more quickly, and the investigations would be far more effective, reducing risk for all.

There are many reasons that cloud providers do *not* make log data available to customers. Collecting, maintaining, and delivering log data is a cost. There are the costs of configuring their systems to generate logs in the first place. There are costs associated with storage: hardware, software licensing, power, etc. There are the costs to develop an interface for customers to retrieve the data. There are the human resources costs involved in supporting the delivery of log data. Customers typically do not include logging as a top selection factor. In short, there is currenly little incentive for cloud providers to invest in forensic log data collection and

production because the increased costs, if passed along to the customer, would simply make them less competitive.

Once again, there are parallels in fire management. For example, fire suppression systems and other physical safety mechanisms are a cost for building owners. Imagine if landlords offered fire suppression systems only as an option (not a requirement) and charged tenants an extra fee to install and maintain them! Many of the poorest and most vulnerable tenants would choose to save the money and take the risk, leading to more fires and ultimately costing the larger community. This is essentially what is happening with cloud service log data today.

Today, Microsoft has finally enabled Office 365 logging by default, after extensive pressure from customers, insurers, attorneys, and others. Customers don't get *all* the logs for free; those that are willing to pay a premium get more data about their environment and a longer retention time. Still, Microsoft's decision to make a minimum set of logs available by default for all corporate customers is an enormous step forward, and one for which the tech giant should be commended.

Cloud breach detection and response is a team effort, which necessarily requires support from the cloud providers themselves. Like landlords, cloud providers are in the unique position of controlling the infrastructure. They can decide what type and quantity of evidence will be made available to customers. In order to reduce risk, all cloud providers need to make an appropriate amount of logging available to customers by default. If this became standard practice, it would increase early detection and improve the speed and accuracy of investigations for everyone.

The cloud provides an incredible opportunity to centralize and standardize logging and breach response tactics and trained personnel. To take advantage of this and reduce risk, cloud providers and their customers need to join together, develop standardized methods for accessing logs and other critical resources, and ensure that responders have the resources they need quickly and efficiently.

- **Should "unauthorized" sources of evidence be used to determine whether a data breach has occurred?**

By all accounts, the secret Activities API was not designed for forensic purposes. Even after the Magic Unicorn Tool was revealed, Microsoft's staff insisted that the data was "not a forensically sound data source" during conversations with customers and breach responders. "The info there is accurate," stated one Microsoft specialist, "but some records may be missing because they are back-end logs used for a different purpose."[42] If there is a possibility that some records are missing, investigators cannot reliably use the data as a method for ruling out unauthorized access to sensitive data. Yet forensics firms have long touted the secret Microsoft API as a reliable log source, attorneys have made decisions based on the output, and insurers paid for their work. In cases where cloud providers cannot or will not confirm that a source of data is accurate or complete, response teams should be extremely cautious about using the data as a basis for drawing conclusions.

- **What standards should forensics professionals hold themselves to for disclosure of "zero-day forensic artifacts"? What responsibility do attorneys, insurers, and other trusted providers have for circulating and disseminating critical information?**

42. Direct conversation between the author and representatives from the Microsoft's Global Incident Response and Recovery Team and the Diagnostics and Recovery Toolset (DaRT) group, February 2019.

In cybersecurity, a "zero-day vulnerability" is a vulnerability that defenders do not yet know about. "Zero-day" refers to the number of days that defenders (such as software manufacturers or enterprise security professionals) have had to mitigate the vulnerability. Publicly disclosing a zero-day vulnerability can place innocent organizations at great risk since attackers can immediately begin exploiting the vulnerability, while defenders have had no time to fix it. Over the years, there has been extensive debate about the ethics of vulnerability disclosure, and it is generally considered good ethical practice to notify software manufacturers and other defenders privately first, to give them time to fix the problem, prior to disclosing the issue to the world.

"Zero-day forensic artifacts" are a newer concept. The term refers to forensic artifacts that are not publicly known, such as Microsoft's Activities API. In some cases, the organization producing the evidence may not even be aware that it exists. Forensic artifacts are critical for investigating data breaches and other cases involving digital evidence. The more forensic artifacts exist and the more granular their data, the more likely it is that investigators will be able to reach correct and complete conclusions.

In the case of the Magic Unicorn Tool, only a handful of forensic analysts knew about the secret source of evidence. Its very existence was kept hidden by several respected forensics firms, as well as Microsoft itself, for well over a year by several accounts. (Many individual Microsoft employees appear to have been genuinely unaware of this data's existence.) Those that were in the know believed that they had greater ability to resolve data security breaches and could "rule out" access to data that others could not, therefore reducing or even eliminating the risk of overnotification for their clients. They were able to charge a premium for access to the secret API, greatly bolstering their revenue. Over the years, they engaged in a concerted effort to hide the existence of the secret API, in order to prevent other firms from similarly obtaining the data, and also out of fear that Microsoft might shut down direct access if it became publicly known (which Microsoft did).

While this was going on, countless organizations that did not have access to the information (and did not even know it existed) were forced to make decisions based on incomplete information, resulting in unnecessary risk not just for their own organizations but for the affected data subjects.

Clearly, withholding critical information from data breach victims and the forensics community was harmful. Many organizations over- or underreported due to lack of evidence, when the evidence may have actually existed—they just didn't know it. Since BEC cases were a huge epidemic, there were economic consequences as well. Forensics firms and attorneys that did not have access to the secret tool were inexplicably cut out of the market, hurting small firms in particular. In the meantime, the firms with access to the secret tool raised prices, in some cases gouging customers and insurers that had no other options.

After the fact, many questions remain about the completeness and accuracy of the secret data, particularly since Microsoft's team itself has repeatedly stated that it was not designed for forensics purposes. Secret sources of evidence cannot be vetted by the broader forensics community, raising the risk of omissions, misinterpretations, and errors in investigations.

There are clearly many benefits to encouraging transparency in forensics artifact disclosure, much like vulnerability disclosure. By sharing information about forensic artifacts, they can be vetted by the wider community and made available to all data breach victims that need

them. Transparency also creates a healthy, competitive market, ensuring that forensics firms and attorneys are hired based on the quality of their service, at reasonable, fair prices. Finally, transparency ensures that cloud providers themselves are in the loop and can speak to the quality of their own data sources.

13.3 Intercepted

Many cloud breaches don't have to happen. Technology exists to better secure data in the cloud; but for political and business reasons, it has not been widely deployed. In some cases, security technology has been deliberately allowed to atrophy or been actively undermined, leading to the epidemic of cloud breaches that we see today.

13.3.1 The Beauty of End-to-End Encryption

End-to-end encryption is a perfect example. True end-to-end encryption renders data inaccessible to anyone except the person who holds the key. This is a very powerful tool for cloud security. Theoretically, it is possible for users to upload data to the cloud, while ensuring that no one—not even the cloud provider—can read the data. To accomplish this, the decryption key would be stored on a device that is controlled by the user or the organization's IT team, and not the cloud provider. (For maximum security, it can even be stored on physical removable media such as a Yubikey.)

BEC cases, in particular, could be dramatically reduced if end-to-end email encryption were widely and correctly deployed. Imagine: Even if an attacker broke into an email account, only the message headers (such as sender, recipent, and subject line) would be legible. The contents would be inaccessible without the decryption key. (This is accomplished using public key cryptography, discussed in depth in Chapter 5, "Stolen Data.") There would be no need for responders to worry about which emails were read or comb the messages for spreadsheets containing PHI, tax returns, or SSNs. As long as the decryption key was stored separately, none of the message contents could be read by a third party.

If John Podesta had used end-to-end email encryption, the contents of his messages would have been unreadable, and the Clinton campaign megaleak would not have occurred. If the Oregon Health and Science residents had used end-to-end encryption to protect their spreadsheet prior to uploading it to Google, patient medical information would not have been exposed. If Booz Allen had used end-to-end encryption for data in its Amazon S3 buckets, it wouldn't have mattered so much that the permissions were set incorrectly—the contents would not be readable.

Phishing attacks, too, can be prevented using the same technology that supports end-to-end email encryption—public key cryptography. Using public keys, senders can digitally sign their messages, and recipients can verify the sender. Instead of relying on spelling errors and "out of character" language, users could simply check the message signature to determine whether an email was truly sent by the person they expected.

13.3.2 The Ugly Side of End-to-End Encryption

Although in theory, end-to-end encryption can solve many security problems, in practice there are many challenges to implementing it. Key management is particularly tricky. In order to read encrypted emails, users need to have their private key stored on any device they use or in a place accessible to all of their devices. In order to send an encrypted email, users first need a copy of the recipient's public key, which requires a distribution mechanism. These are just a couple of the issues that arise when implementing end-to-end encryption; there are many other logistical details to consider, such as key escrow and enterprise access for purposes of data-loss prevention and malware detection.

Compounding the inherent complexities is the fact that email and cloud-based storage products have advanced and matured over the past two decades—but end-to-end encryption was not integrated along the way. In fact, end-to-end encryption technology was largely left to atrophy. There are reasons for this: businesses and government organizations alike have a vested interest in analyzing user-generated content. Cloud providers actively mine communications and document repositories in order to generate ad revenue and to offer features such as search and spam filtering. Government agencies such as the National Security Agency (NSA) wanted the ability to read peoples' emails easily and engaged in a decades-long effort to undermine the implementation of encryption. While it is possible to deploy end-to-end encryption in such a way that authorized third parties can still access contents, this creates additional work and slows down analysis efforts. Absent strong pressure to deploy end-to-end encryption, it was easier for providers to just leave it out entirely.

The tide began to turn when HIPAA and other regulations emerged and gradually gained traction. These regulations incentivized organizations such as healthcare clinics to deploy encrypted email and file transfer solutions in order to protect sensitive personal information. However, by that time, enterprises, cloud providers, and government agencies were already reaping the rewards of their data-mining programs, and many important security tools such as spam filtering software relied upon access to unencrypted content.

Instead of implementing true end-to-end encryption solutions, it was easier to leverage existing solutions like secure web portals or encrypted PDFs. Organizations deployed "faux" email encryption, where recipients received a link to a "secure" message stored in a web portal or an encrypted PDF. Faux email encryption is clunky, annoying, and (ironically) not very secure. When it is implemented in a web portal, recipients typically choose weak or reused passwords, and when it is implemented as encrypted PDFs, the password is often weak or sent in a subsequent email message, rendering the encryption pointless. The technology worked well enough to meet compliance requirements, however, and so it remained.

The result was that end-to-end encryption products were not developed at scale and were never integrated with popular cloud services. The technology stagnated. While this enabled governments and businesses access to monitor email, it also left a gaping security hole. Attackers who broke into email and cloud accounts found reams of juicy, sensitive data, unprotected once the login interface was breached.

Integrating end-to-end encryption into popular services now is a much harder problem than it might have been at the dawn of the industry since it is more difficult to "bolt on" technical solutions after the fact, as opposed to building functionality into early prototypes. In certain environments, deploying end-to-end encryption today is feasible. For example, at the author's

consulting firm, all internal emails are GPG-encrypted automatically because the business has full control over the endpoints and a relatively small user population. However, in more complex environments such as hospitals, it remains a difficult challenge. In recent years, there has been a resurgence of interest in end-to-end encryption, for reasons that we will discuss in the coming sections.

13.3.3 Large-Scale Monitoring

Communications encryption experienced a renaissance when Edward Snowden, a mild-mannered Department of Defense contractor, breached the NSA. After vacuuming up an estimated 1.7 million documents, Snowden fled to Hong Kong and began contacting reporters, exposing the NSA's shockingly ubiquitous monitoring programs.[43]

Snowden's leaked documents showed that to gain access to communications, the NSA had broken or circumvented key Internet security technologies and installed monitoring systems that gave them immediate access to private data hosted by major cloud providers, including:

- AOL
- Apple
- Facebook
- Google
- Microsoft
- Skype
- Yahoo
- YouTube

According to one internal NSA presentation, accessible data included:

- Chat
- Email
- Photos
- Social networking details
- Stored files
- Video
- Voice conversations

43. Chris Strohm and Del Quentin Wilber, "Pentagon Says Snowden Took Most US Secrets Ever: Rogers," *Bloomberg*, January 10, 2014, https://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.

Any monitoring system increases access and therefore inherently increases the risk of a data breach. As discussed in Chapter 2, "Hazardous Material":

> The risk of a data breach increases with (a) the number of people who have access to the data, (b) the number of ways that the data can be accessed, and (c) the ease of obtaining access.

Security expert Bruce Schneier called attention to this point when analyzing the NSA's extensive communications monitoring capabilities. "The more we choose to eavesdrop on the Internet and other communications technologies, the less we are secure from eavesdropping by others," he said. "Our choice isn't between a digital world where the NSA can eavesdrop and one where the NSA is prevented from eavesdropping; it's between a digital world that is vulnerable to all attackers, and one that is secure for all users."[44]

Breach Notification Exceptions?

In addition to NSA documentation, Snowden stole more than 160,000 actual intercepted emails and instant message conversations, and 7,900 documents, captured from more than 11,000 online accounts. These conversations, stored in the NSA's searchable database, were easily accessible to any analyst in his position. The *Washington Post* combed through the leaked personal communications and found that many of the account holders belonged to American citizens. The leaked data included "medical records sent from one family member to another, résumés from job hunters and academic transcripts of schoolchildren."[45]

The *Post*'s analysis begs the question: Whose data was leaked? It's hard to argue that the disclosure of those 11,000 account holders' details was anything other than a data breach. And yet, there is no indication that any entity took responsibilty for identifying and notifying the subjects. The data contained medical records and schoolchildrens' data—information that might have been protected by federal law when it was sent across the Internet. There is no indication that any breach notifications were released after the data was leaked to the press.

13.3.4 Investment in Encryption

The revelation of the NSA's surveillance programs spurred developers and users around the world to invest in stronger cloud security programs.[46]

---

44. Glenn Greenwald, *No Place to Hide* (New York: MacMillan US, 2014), 205.

45. B. Gellman, J. Tate, and A. Soltani, "In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are," *Washington Post*, July 5, 2014, https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

46. Robert Hackett, "Snowden Leaks Advanced Encryption by 7 Years, US Spy Chief Says," *Fortune*, April 25, 2016, http://fortune.com/2016/04/25/snowden-encryption-james-clapper.

Google quickly launched an "End-to-End" encryption project, releasing a open-source browser plug-in that encrypts Gmail messages using PGP.[47] Although the project was highly touted in the wake of the Snowden leaks, Google eventually dropped the development, leading *Wired* to declare the project "vaporware."[48]

At the same time, a group of scientists from around the world founded "Protonmail," a webmail system that supported multiple levels of encryption—including the "Paranoid" option where only the end user has access to the encryption key.[49] Protonmail reportedly has no way of accessing user emails—or providing third parties with access—when they do not hold the decryption keys in the first place. "There are many companies and governments that would love to see us fail," say the Protonmail founders.

A plethora of new communications and cloud products have emerged since then that incorporate end-to-end encryption—including WhatsApp, Signal, and other popular tools. While end-to-end encryption still remains elusive for mainstream email and cloud file-sharing products, the epidemic of data breaches has sparked discussion and created new incentives for investing in strong encryption in the cloud and beyond.

13.4 Conclusion

The cloud is the emerging battlefront for data breaches. The same benefit that makes the cloud popular—easy access to data from anywhere in the world—also makes it especially vulnerable. After years of password breaches and phishing toolkit development, organized crime groups have perfected the art of breaking in through user login interfaces. Today, criminals have repeatable, scalable processes for hacking cloud accounts and monetizing access to data. Defenders are at a disadvantage since strong security technologies like end-to-end encryption have not been widely deployed in the cloud, due to business and government pressures.

Reducing cloud data breaches requires reducing one or all of the five data breach risk factors. Today, cloud providers and government agencies alike amass data at fantastic rates, fueling development of products and services that are now deeply ingrained in the fabric of our society. Controlling the epidemic of data breaches will require addressing issues of access, proliferation, and retention of cloud data—and there are tradeoffs. With investment, it is possible to reduce the risk of data breaches, but many of the underlying issues are systemic and must be addressed at a global scale.

The good news is that defenders can, in time, turn the cloud into an advantage. If cloud providers raise visibility for customers and implement standard log formats and export options, then it is possible for cloud-based monitoring and response to become highly scalable and efficient.

---

47. "FlowCrypt: Encrypt Gmail with PGP," Chrome Web Store, accessed June 5, 2019, https://chrome.google.com/webstore/detail/flowcrypt-encrypt-gmail-w/bnjglocicdkmhmoohhfkfkbbkejdhdgc

48. Andy Greenberg, "After 3 Years, Why Gmail's End-to-End Encryption Is Still Vaporware," February 28, 2017, https://www.wired.com/2017/02/3-years-gmails-end-end-encryption-still-vapor.

49. Hollie Slade, "The Only Email System the NSA Can't Access," *Forbes*, May 19, 2014, https://www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access.

This page intentionally left blank

Afterword

In little more than a decade, data breaches grew from a nameless problem to a pervasive, insidious epidemic. Today the number of breaches is overwhelming, especially considering that many breaches are never publicly reported. Data breaches affect our economy, drain resources, and damage reputations of otherwise highly functional organizations. Every organization on the planet is at risk of a data breach, and therefore it is critical that we develop effective, scalable tactics for managing them.

The purpose of this book is to establish a practical, lasting foundation for data breach management. Along the way, we studied real data breaches, identified critical decision points, and provided lessons learned.

Key takeaways from this book include:

- **Data = Risk** (Chapter 2, "Hazardous Material"): Storing, processing, or transmitting data creates risk for an organization. The most effective way to reduce your risk of a data breach is to minimize the data you collect and to carefully control what remains.
- **The Five Data Breach Risk Factors** (Chapter 2): These five general factors influence the risk of a data breach: retention, proliferation, access, liquidity, and value.
- **A Data Breach Is a Crisis** (Chapter 3, "Crisis Management"): Every crisis is an opportunity. It's important to recognize that data breaches are crises, which have the potential for both negative and positive consequences, depending on how you react.
- **Manage DRAMA** (Chapter 4, "Managing DRAMA"): In order to successfully navigate a data breach response, your organization must:
  - **Develop** your data breach response function.
  - **Realize** that a potential data breach exists by recognizing the signs and escalating, investigating, and scoping the problem.
  - **Act** quickly, ethically, openly, and empathetically to minimize the impact of a breach.
  - **Maintain** data breach response efforts throughout the chronic phase and potentially long term.
  - **Adapt** proactively and wisely in response to a potential data breach.
- **Breached Data Is Valuable** (Chapter 5, "Stolen Data"): When breached data is exploited, it is typically used for fraud, sale, intelligence, exposure, or extortion.
- **Strategies for Industry-Specific Breach Response** (Chapter 6, "Payment Card Breaches," Chapter 7, "Retailgeddon," and Chapter 9, "Healthcare Breaches"): Breaches involving payment card data or healthcare information are typically affected by industry-specific regulations and standards, such as PCI and HIPAA.

- **We Are All Connected** (Chapter 8, "Supply Chain Risks," and Chapter 13, "Cloud Data Breaches"): The risk of a data breach is transferred throughout our global society in a massive, complex web of suppliers, customers, and peers. As organizations increasingly move sensitive data to the cloud, the risks and rewards of a shared infrastructure become ever-more apparent.
- **Exposure and Extortion Tactics** (Chapter 10, "Exposure and Weaponization," and Chapter 11, "Extortion"): In the past few years, tactics involving data exposure and cyber extortion have matured. Today, professional groups around the world engage in data exposure and extortion operations, for a variety of purposes.
- **Transfer Risk** (Chapter 12, "Cyber Insurance"): Cyber insurance has given us new ways to transfer risk while fundamentally altering breach response practices.

There are many open issues to be resolved before data breach management stabilizes. For example:

- In the coming years, more regulations undoubtedly will emerge. Ideally, the confusing patchwork of state, national, and international regulations will merge into a more unified approach to data breaches, although the complexity may become worse before it gets better.
- Society needs to develop a comprehensive, unified definition for data breaches in order to establish standards for preventing, managing, and responding to them.
- Effective approaches for tracking and measuring data breaches need to be developed, beyond vendor reports and news stories.
- Standards for monitoring, logging, and controlling data in the cloud need to be defined and implemented in order to facilitate the growing issue of breach response in the cloud.

We are in the infancy of an industry. This is both a stressful time and one that is full of potential. Everyone involved in data breach management right now has a voice and an opportunity to initiate positive change. This book provides a strong foundation for understanding the current state of data breaches, with the goal of helping all of us work toward a better future.

Index

Photo by izusek/gettyimages

Register Your Product at informit.com/register

Access additional benefits and **save 35%** on your next purchase

- Automatically receive a coupon for 35% off your next purchase, valid for 30 days. Look for your code in your InformIT cart or the Manage Codes section of your account page.
- Download available product updates.
- Access bonus material if available.*
- Check the box to hear from us and receive exclusive offers on new editions and related products.

**Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.*

InformIT.com—The Trusted Technology Learning Source

InformIT is the online home of information technology brands at Pearson, the world's foremost education company. At InformIT.com, you can:

- Shop our books, eBooks, software, and video training
- Take advantage of our special offers and promotions (informit.com/promotions)
- Sign up for special offers and content newsletter (informit.com/newsletters)
- Access thousands of free chapters and video lessons

Connect with InformIT—Visit informit.com/community

informIT®
the trusted technology learning source

Addison-Wesley • Adobe Press • Cisco Press • Microsoft Press • Pearson IT Certification • Que • Sams • Peachpit Press

Pearson