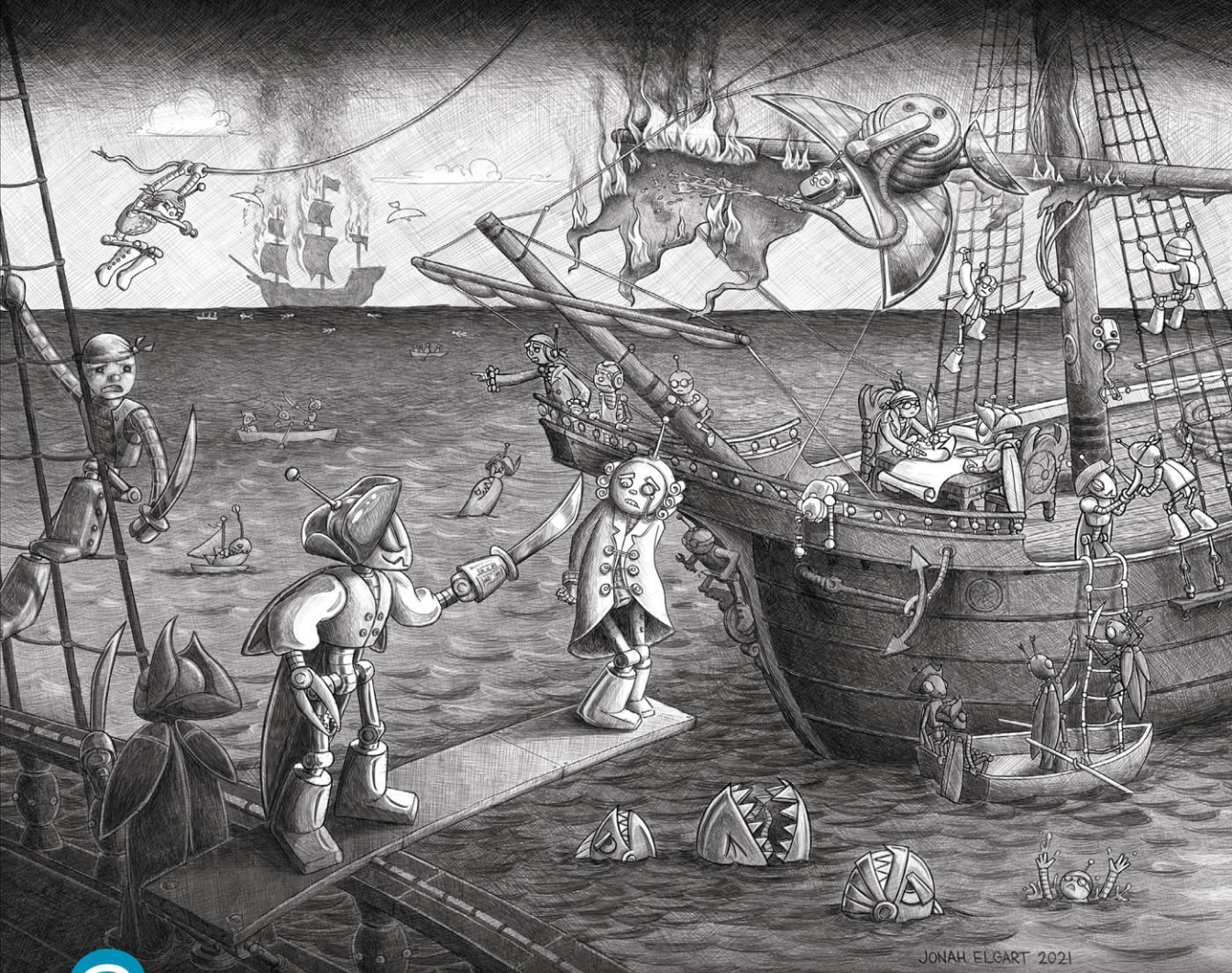
Ransomware & Cyber Extortion

RESPONSE AND PREVENTION



Sherri **DAVIDOFF** | Matt **DURRIN** | Karen **SPRENGER**

Praise for *Ransomware and Cyber Extortion*

"*Ransomware and Cyber Extortion* is a masterstroke that will lead both technical and non-technical readers alike on a journey through the complex and sometimes dark world of cyber extortion. The encore of practical advice and guidance on preventing ransomware can help organizations of all sizes."

—Russ Cohen, Head of Cyber Services US, Beazley Group

"Davidoff and team have built a magisterial and yet still approachable guide to ransomware. This just became the definitive and classic text. I've been writing about some of these attacks for years and still was blown away by how much more they taught me. I'll hand this to every infosec newcomer and senior consultant from now on."

—Tarah Wheeler, CEO, Red Queen Dynamics

"Ransomware attacks are no longer encrypt-and-export incidents; they have evolved into sophisticated, multipronged attacks that require a multidisciplinary response of forensic, technical, and compliance expertise and savvy cybercrime negotiation skills. Sherri Davidoff, Matt Durrin, and Karen Sprenger are that 'Dream Team' and concisely help the reader understand how to prepare for and respond to ransomware attacks. This book is a must-read for every member of an internal or external incident response team."

—Jody R. Westby, CEO, Global Cyber Risk LLC, Chair, ABA Privacy & Computer Crime Committee (Section of Science & Technology Law)

"A thoroughly delightful read, *Ransomware and Cyber Extortion* takes the topic everyone is talking about and deconstructs it with history and actionable guidance. A must-read before you next brief your board or peers on your own incident response plans."

—Andy Ellis, CSO Hall of Fame '21

This page intentionally left blank

Ransomware and Cyber Extortion

This page intentionally left blank

Ransomware and Cyber Extortion

Response and Prevention

Sherri Davidoff
Matt Durrin
Karen Sprenger

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

Cover illustration by Jonah Elgart, bolognasalad.com

Screenshots by LMG Security have been reprinted with permission.

Definition icon courtesy of Colorlife/Shutterstock
Head's Up icon courtesy of iDesign/Shutterstock
Tip icon courtesy of maya_parf/Shutterstock

Visit us on the Web: informit.com/aw

Library of Congress Control Number: 2022942883

ISBN-13: 978-0-13-745033-6
ISBN-10: 0-13-745033-8

ScoutAutomatedPrintCode

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

This page intentionally left blank

To my husband and best friend, Tom.
– Sherri

To my caring, loving, and PATIENT wife Karah.
– Matt

To my mom, my dad, and my sister, for love and support through all of my adventures.
– Karen

This page intentionally left blank

Contents

I want to devise a virus
To bring dire straits to your environment
Crush your corporations with a mild touch
Trash your whole computer system and revert you to papyrus
—Deltron 3030, "Virus," May 23, 2000

This page intentionally left blank

Preface

No one realized when the hip hop song "Virus," was released in 2000 that it would turn out to be prophetic. Featuring a protagonist (Deltron Zero) who wanted to "develop a super virus," the lyrics describe his plans to infect and destroy computers around the world: "Crush your corporations with a mild touch / Trash your whole computer system and revert you to papyrus."[1]

More than two decades later, ransomware has reached epidemic proportions, shutting down hospitals, schools, law firms, municipalities, manufacturers, and organizations in every sector. Victims around the globe are routinely infected and forced to revert to pen and paper (for those lucky enough to still maintain supplies).[2,3] Worse, cyber attackers have discovered that threatening to publish information can give them similar leverage, leading to enormous—and purposeful—data leaks.

Today, data is wielded as a weapon. By threatening the confidentiality, integrity, and availability of data, criminals reap profits and force victims to bend to their will. After years of escalating ransomware attacks, brazen data publication, and a daily barrage of new victims touted in the headlines, they have honed their strategies and developed a scalable, successful business model.

The impacts of cyber extortion are far-reaching. Business operations have been halted, both temporarily and in some cases permanently. Medical records have been destroyed and patients' lives put in jeopardy. Key intellectual property has been sold to competitors. Private emails and personal details are routinely dumped so that they become visible to the public eye.

Court cases resulting from ransomware and data leaks are multiplying, even as victims and insurers pour funds into victim compensation and corrective action. Law enforcement agencies around the world are working every day to dismantle cyber extortion rackets, even as the criminals themselves crow to the media that they are not afraid.

"Extortion fatigue" is real. The problem is so pervasive that people can't digest the full scope and impact. At the same time, cyber extortion is wildly underreported. After all, no victim purposefully calls the media when they find out they've been hacked. Cases are routinely negotiated quietly, in secret. As a result, the true extent of cyber extortion cannot be known but is undoubtedly far greater than any statistics indicate.

Response is crucial. The steps taken by a victim organization in the hours, days, and months after a cyber extortion attack can dramatically impact the outcome.

1. Deltron 3030, "Virus," *Deltron 3030*, May 23, 2000, https://genius.com/Deltron-3030-virus-lyrics.
2. www.beckershospitalreview.com/cybersecurity/georgia-health-system-reverts-to-paper-records-after-ransomware-attack-5-details.html.
3. www.forbes.com/sites/tommybeer/2020/09/28/report-big-us-hospital-system-struck-by-cyberattack-forcing-staff-to-resort-to-paper-and-pen/.

This book is a practical guide to responding to cyber extortion threats, including ransomware, exposure extortion, denial-of-service attacks, and more. Throughout the book, we'll draw heavily from real-world case studies, as well as the vast library of unpublished cases handled by the authors during their work as response professionals. Readers will emerge better prepared to handle a cyber extortion attack properly, which will help minimize damage and expedite recovery.

As highlighted throughout the book, cyber extortion is typically the last and most visible phase of an intrusion. Often, cybercriminals have access to a victim's environment or data for an extended period of time, siphoning off key information, researching the victim, and installing malware and other tools that will maximize their leverage.

By employing effective cybersecurity prevention measures throughout society, we can reduce the risk of cyber extortion and cybercrime more generally. In the last chapter of this book, we delve into the underlying causes of cyber extortion and provide recommendations for reducing this risk.

Since cyber extortion actors, tools, and tactics evolve constantly, throughout this book we emphasize response and prevention techniques that will stand the test of time.

Who Should Read This Book?

This book is intended to be a valuable resource for anyone involved in cyber extortion prevention, response, planning, or policy development. This includes

- Chief information officers (CIO) and chief information security officers (CISO) who are involved with planning, their organizations' cyber extortion response or developing prevention strategies
- Cybersecurity professionals, incident responders, forensics investigators, ransom negotiators, cryptocurrency payment processors, and anyone involved in ransomware and cyber extortion response
- Technology staff, including system administrators, network technicians, help desk workers, security teams, and other individuals responsible for responding to cyberattacks or securing their environments
- Executives who want a deeper understanding of the cyber extortion threat and effective response and prevention strategies
- Legislators, regulators, law enforcement agents, and anyone involved in establishing policy relating to cyber extortion
- Anyone interested in learning more about ransomware and cyber extortion attacks

How This Book Is Organized

This book is designed to be a practical guide for response and prevention of ransomware and cyber extortion threats. Here is a summary of our journey in this book:

- **Chapter 1, Impact:** Cyber extortionists threaten the confidentiality, integrity, and availability of information in an effort to gain leverage over a victim. The four types of cyber extortion are denial, modification, exposure, and faux extortion. Impacts of cyber extortion range from operational disruption to financial loss, reputational damage, lawsuits, and more. In addition to targeting victims directly, adversaries compromise technology suppliers such as managed services providers (MSPs), cloud providers, and software vendors.
- **Chapter 2, Evolution:** Ransomware and cyber extortion attacks have been around longer than most people realize and come in a variety of forms. In this chapter, we cover the history of ransomware and its impact on affected organizations, and then follow its evolution into the bustling criminal economy that drives it today.
- **Chapter 3, Anatomy of an Attack:** Extortion is the last phase of a cyber extortion attack. Adversaries first gain access to the victim's technology environment and then take steps to expand their access, assess the victim, and prepare prior to extortion. In this chapter, we step through the phases of a cyber extortion attack. Along the way, we identify indicators of compromise and provide response tips that can mitigate or even stop the attack in progress.
- **Chapter 4, The Crisis Begins:** The early stages of cyber extortion response significantly impact how quickly an organization recovers and is able to resume its normal operations. In this chapter, we provide insight on recognizing the common early indicators of a cyber extortion attack. We also walk through the concept of triage and explain how development of a clear and effective response strategy is critical early in the response process.
- **Chapter 5, Containment:** When a cyber extortionist strikes, quick action can reduce the damage and help speed recovery. In this chapter, we discuss techniques for halting data exfiltration and file encryption/deletion, resolving denial-of-service attacks, and locking the adversary out of the victim's environment. We end the chapter by talking about threat hunting, including methodology, sources of evidence, tools and techniques, staffing, and results.
- **Chapter 6, Investigation:** Taking the time to conduct an investigation is critical for both short- and long-term resolution of cyber extortion incidents. In this chapter, we discuss reasons for investigating, techniques for identifying the adversary, methods for scoping an attack and tracking down "patient zero," and the fundamentals of data breach investigations. We also cover evidence preservation, which has the potential to reduce the long-term damage of cyber extortion attacks.

- **Chapter 7, Negotiation:** How do you reach an agreement with criminals? This chapter is a practical guide to initiating, managing, and completing a ransom negotiation. You'll learn about haggling, proof of life, and closing the deal. We also discuss common mistakes made during cyber extortion negotiations and ways to avoid them.
- **Chapter 8, Payment:** Although paying a ransom may be undesirable or even unthinkable for some, in many cases it is the victim's chosen path forward. In this chapter, we discuss the pros and cons of paying a ransom, and then the practicalities of the payment process, including forms of payment, types of intermediaries, timing issues, and what to do after payment has been made. We also discuss payments prohibited due to sanctions and consider the due diligence that victims should conduct before any payment is made.
- **Chapter 9, Recovery:** The goal of every incident is to return to normal operations. In this chapter, we cover the process of recovery, as well as strategies for reducing the risk of data loss and reinfection, which can enable the victim to resume operations with confidence. Along the way, we also describe key improvements for your environment that can reduce future risk and increase defensive capabilities.
- **Chapter 10, Prevention:** Cyber extortion is typically the last phase of a cyberattack. Fundamentally, prevention is best accomplished by implementing a strong, holistic cybersecurity program. In this chapter, we highlight the keys to building such a cybersecurity program, and then delve into specific defensive steps that help to reduce the risk of cyber extortion attacks or mitigate their impact. We conclude by discussing broad-scale, macro changes that are needed to effectively combat the cyber extortion epidemic.

Other Chapter Elements

Throughout each chapter we have included other elements meant to highlight important information, concepts, or examples, some with graphical icons to easily identify each element:

- **Learning Objectives:** A bulleted list of the material covered in that chapter
- **Case Studies:** Real-world cyber extortion cases that demonstrate the concepts being discussed
- **Definition:** Explanations of terms that are specific to cyber extortion or cybersecurity
- **A Word About:** Discussion of a key term and how it is used in this book
- **Tip:** Actionable information for the reader
- **Heads Up!:** Useful background information for the reader

Discussion Questions

At the end of each chapter, we include a section called "Your Turn!" in which we provide the opportunity for you to create your own scenario. We then offer questions for you to consider and discuss with others. Our hope is that this section will provide you with countless opportunities to evaluate cyber extortion incidents from all angles and understand that there is no one right answer when responding to such attacks.

Checklists

At the end of this book, you will find a series of checklists meant to be used (and reused) to help you prevent, and if necessary respond to, cyber extortion. They compile information found in the book in a high-level, quick-and-easy reference format.

Stay Up to Date

For regular updates and commentary on the latest cyber extortion and ransomware developments, visit the authors' website: ransombook.com.

Adversary tactics are rapidly evolving, and best practices for response and prevention evolve with them. In this book, we present a foundation for responding to cyber extortion events and preventing these devastating attacks.

Visit the authors' website for the latest news, response tips, discussion topics, and more. As we all share information and experiences, it is our hope that our global community can work together to shine a light on cyber extortion and reduce the risk.

This page intentionally left blank

Acknowledgments

It takes a village to produce a book, and this one is no exception. We'd like to thank the many people who contributed, from concept to production and everything in between.

First and foremost, thanks to our editors Haze Humbert and James Manly, whose wealth of publishing experience and professional insights were invaluable. We especially appreciated your expert cat-herding skills, and how you patiently kept the process moving forward while giving us grace and time as we all navigated the uncharted waters of working together during the pandemic.

We are grateful to our colleagues Michael Ford and Ben Mayo, who took the time to review the book outline in the early phases to ensure we comprehensively addressed our audience's needs. Michael also provided deep and substantive feedback throughout the entire book, for which we cannot thank him enough. We'd also like to thank Pearson's excellent editing and production teams, including Julie Nahil, Menka Mehta, Aswini Kumar, and Jill Hobbs.

You *can* judge a book by its cover, and we feel so fortunate that artist Jonah Elgart lent his incredible skills to this work—researching actual pirate ship designs, sharing paintings and ideas, and even putting some "Easter eggs" into the illustration (see if you can find all three authors and the artist himself on the cover!). Thank you, Jonah, for gracing our written words with such a beautiful and thought-provoking work of art.

Cryptocurrency payment expert Marc Grens, co-founder of DigitalMint, kindly gave his time for an extensive interview and answered our many in-depth questions on the evolving cryptocurrency due-diligence and payment processes. His firsthand expertise in this area was invaluable, and we are grateful for the opportunity to bring this information to our readers.

Cyber insurance veterans Bob Wice and Frank Quinn took the time to give in-depth interviews that gave us a behind-the-scenes perspective on cyber insurance and risk management. Thank you for your trust and enabling us to share your wisdom with the readers of this book.

Ransomware and cyber extortion is a deep and quickly evolving topic. We've learned through experience by handling a variety of cases at LMG Security, with the support of our incredible team. Many thanks to all of our colleagues at LMG, particularly Derek Rowe, Madison Iler, and Dan Featherman. Thanks also to our longtime attorney (now judge) Shane Vannatta, for helping us to navigate the early days of ransomware and cyber extortion.

We are also grateful to our many colleagues who helped to shape our understanding of ransomware and cyber extortion over the years, including Scott Koller, Ryan Alter, Randy Gainer, David Sande, Marc Kronenberg, Bill Siegel, David Sherman, Katherine Keefe, Brett Anderson, Luke Green, Sue Yi, Mike Wright, Jody Westby, Sean Tassi, Peter Enko,

Dave Chatfield, Mark Greisinger, Vinny Sakore, Andrew Lipton, Michael Phillips, Marc Schein, and Michael Kleinman.

On a personal level, each of us would like to share our gratitude individually as well.

From Sherri: Many thanks to my dear little ones, Violet and Thunder, whose love and enthusiasm buoyed me every day. My husband, Tom Pohl, and my amazing friends, Annabelle Winne and Jeff Wilson, were there for me every day: cheering me on, listening, and providing wise advice. I couldn't have done this without you. I am grateful for my friends and family, especially my father, E. Martin Davidoff, my mother, Sheila Davidoff, my sister, Laura Davidoff Taylor, as well as Jessie Clark, Shannon O'Brien, Kaloni Taylor, Steve McArthur, Kevin Head, Samantha Boucher, Deviant Ollam, Kelley Sinclair, and so many others. Your constant support got me through the long journey of book writing once again. Above all, I feel so lucky to work with Karen Sprenger and Matt Durrin, my incredible co-authors! I have learned so much from you, both in the trenches while responding to extortion cases and during the process of crafting this book. No one could ask for a better team.

From Matt: I'd like to specifically thank my wife, Karah Durrin, and my daughter, Lauren Durrin, for being my quiet inspiration during the writing process. I could not have done this without your amazing and tireless support. I'd also like to thank all of the friends and family who helped me keep going throughout the journey. In addition to the people in my personal life, I'd like to extend a huge thank you to the LMG Security team for giving me the opportunity to make cybersecurity my career. It has been a wild ride, but I feel so blessed to be surrounded by such a wonderful and talented group of people. Finally, I'd like to thank my partners in crime (stopping), Sherri Davidoff and Karen Sprenger. I likely would have never discovered my passion for cybersecurity without both of you amazing women. Sherri believed in me enough to give me an opportunity to dive into the industry. Karen, in addition to being a fantastic security expert, was the person who first taught me how to properly capture a forensic hard drive image. I'm so grateful to have you both as friends and mentors. Thank you both and here's to continuing our shenanigans together!

From Karen: In addition to those listed above, I'd like to thank my mom, Genie Thorberg, my biggest champion and the person who taught me how to use a computer; my dad, Bob Sprenger, who gave equal parts love and life lessons; and my sister, Rhonda Johnson, the first and best of many strong women who led the way for me. To my partners in shenanigans, Sherri Davidoff and Matt Durrin, thank you for the love, laughter, and commitment throughout this project. Although you have not yet succeeded in turning me into a night owl, you have made a daunting task achievable and, dare I say, enjoyable. I'll look forward to swapping cybercrime news links for many years to come. I've had the great blessing of working for women-led companies at key points during my career. Thank you to Linda Wright and Desiree Caskey, who gave me my start many years ago—before I realized that women in technology were few and far between. And especially to Sherri, a particularly heartfelt thank you to you for taking a chance on me all those years ago and giving me a place to spread my wings in cybersecurity and business development. I've learned and grown so much working with you. Finally, thank you to my pack of poodles, Jasper and Gracie, who spent hours lying at my feet to keep me company throughout the whole process, and Sadie, who joined us near the end. I couldn't have done it without the three of you.

About the Authors

Sherri Davidoff (left), Matt Durrin (center), Karen Sprenger (right)

Sherri Davidoff is the CEO of LMG Security and the author of *Data Breaches: Crisis and Opportunity*. As a recognized expert in cybersecurity, she has been called a "security badass" by *The New York Times*. Sherri is a regular instructor at the renowned Black Hat trainings and a faculty member at the Pacific Coast Banking School. She is also the co-author of *Network Forensics: Tracking Hackers Through Cyberspace* (Addison-Wesley, 2012). Sherri is a GIAC-certified forensic analyst (GCFA) and penetration tester (GPEN) and received her degree in computer science and electrical engineering from the Massachusetts Institute of Technology (MIT).

Matt Durrin is the Director of Training and Research at LMG Security and a Senior Consultant with the organization. He is an instructor at the international Black Hat USA conference, where he has taught classes on ransomware and data breaches. Matt has conducted cybersecurity seminars, tabletop exercises, and classes for thousands of attendees in all sectors, including banking, retail, healthcare, government, and more.

A seasoned cybersecurity and IT professional, Matt specializes in ransomware response and research, as well as deployment of proactive cybersecurity solutions. Matt holds a bachelor's degree in computer science from the University of Montana, and his malware research has been featured on *NBC Nightly News*.

Karen Sprenger is the COO and chief ransomware negotiator at LMG Security. She has more than 25 years of experience in cybersecurity and information technology, and she is a noted cybersecurity industry expert, speaker, and trainer. Karen is a GIAC Certified Forensics Examiner (GCFE) and Certified Information Systems Security Professional (CISSP) and holds her bachelor's degree in music performance (yes, really). She speaks at many events, including those held by the *Wall Street Journal* Cyber Pro, Fortinet, the Internal Legal Tech Association, and the Volunteer Leadership Council. In her spare time, Karen considers "digital forensics" a perfectly acceptable answer to the question, "But what do you do for fun?" A lifelong Montanan, she lives in Missoula with oodles of poodles.

Chapter 1

Impact

Heck, what's a little extortion among friends?

—Bill Watterson

Learning Objectives

- Define cyber extortion and explain the four types (denial, exposure, modification, and "faux")
- Understand the impacts of cyber extortion on modern organizations
- Recognize that adversaries can leverage technology suppliers to compromise victims and conduct cyber extortion on a massive scale

Company X was a thriving accounting firm headquartered in a major U.S. city. Every day, its staff handled bookkeeping, financial oversight, tax preparation, and a myriad of other tasks for hundreds of clients.

Suddenly, one Monday morning, everything stopped. An early-rising staff member walked into the office and heard a frightening sound. Every computer was shouting a message: "Attention! What happened? All your files, documents, photos, databases, and other important data are safely encrypted with reliable algorithms. You cannot access the files right now. But do not worry. You have a chance!"

Scattered around the office were papers everywhere. All of the printers in the office had printed the ransom note, over and over, until the paper trays were empty. The point-of-sale systems that staff used to process credit cards had spit out the ransom notes on printed receipts, over and over, until the long reams spilled off the desks.

A chilling voicemail awaited one of the firm's partners: "Hello, Mr. [REDACTED]," stated an emotionless male voice with an Eastern European accent, "I'd like to notify you that we downloaded 500 gigabytes of data from your servers. If you're planning to just restore your data without paying for decryption, we'll sell your company's data on darknet.

"Unless you contact us ASAP, we'll notify all of your clients that we are in possession of their private data, like Social Security numbers and tax forms. We urge you to get in touch with us using the email from the text file we've placed on your desktop."

The voice paused for effect. "If we leak that data, your business will be as good as gone. We are looking forward to receiving your reply via email."

Click. With that, the voicemail ended.

The criminals demanded $1.2 million to restore access, and refrain from publishing the client data.

In the meantime, the firm was down. Databases containing client files were fully encrypted and unusable. Employees couldn't access shared folders, including client documents, firm payroll details, human resources (HR) data, and more. All of the clients that depended on them for daily bookkeeping or time-sensitive services were stuck.

Fortunately, the firm's cloud-based email was still available, too—and the criminals leveraged that. "Good morning," the criminals wrote in a follow-up email. "I think you still cannot understand what situation your company is in now. … First of all, we will sell the personal data of your employees and customers on the market. … [You] will be sued by both your employees and your clients." The criminals attached the partners' own personal tax returns to the email to illustrate the threat.

It quickly became clear that the criminals had hacked the firm's email accounts as well and were monitoring the victim's response. "We also saw the report that [antivirus vendor] provided you," the criminals wrote. "It contains many errors."

The criminals had a playbook. Day in and day out, they held organizations hostage using the Internet. First, they gained access to their victim's network. For Company X, the initial hack occurred in May, when an employee opened an attachment in a phishing email. The employee's computer was infected with malware—specifically, a remote access Trojan (known as a "RAT"), which gave the criminals remote access to the employee's computer.

Company X's antivirus software did not detect the infection. The criminals lurked for about three months. They occasionally logged in to the employee's computer remotely, presumably to check that their access still worked, but did little else. It is possible that during this time, these criminals simply peddled access to the hacked computer on the dark web. Hackers known as "initial access brokers" specialize in gaining access to computers. They then sell this access to other criminals, and in this way quickly turn their crime into profit. The purchasers—often organized crime groups—then take the next step of exploring the victim's network, stealing data and potentially holding them for ransom.

Suddenly, in August, criminals later identified as the Twisted Spider ransomware gang[1] remotely logged onto the employee's infected computer. Using common penetration testing tools, they stole passwords from the employee's computer, including the username and password of the managed service provider (MSP) that remotely administered the company's computers. Then, they used these credentials to take full control of Company X's network.

The Twisted Spider gang went straight for the heart: They copied all of the files from the firm's primary data repository. Then, they installed fast and effective ransomware software that encrypted all of the company's servers, including databases, application

1. Jon DiMaggio, *Ransom Mafia: Analysis of the World's First Ransomware Cartel* (Analyst1, April 7, 2021), https://analyst1.com/file-assets/RANSOM-MAFIA-ANALYSIS-OF-THE-WORLD%E2%80%99S-FIRST-RANSOMWARE-CARTEL.pdf.

servers, domain controllers, and more. They left workstations alone, not bothering to comb through individual accounts or computers. It was like a well-executed smash-and-grab.

The criminals knew their victims' pain points. They knew that the short-term business interruption was impactful, but even more devastating were the potential long-term consequences that could arise from angry clients who were upset that their data was stolen. The Twisted Spider hackers made sure to demonstrate that they had access to sensitive, regulated information, ranging from Social Security numbers to tax details. They explicitly reminded the victim's executives that they could be sued by employees and clients. They made it clear that they were prepared to publish the data and directly contact affected clients so as to damage the firm's reputation. This, in turn, could lead to loss of business, plus lawsuits, threatening the firm's very survival.

Company X paid the ransom—or rather, their cyber insurance firm paid the ransom, less a $25,000 deductible. The authors of this book were called to handle the negotiation and successfully obtained a hefty discount, settling the case for a little less than $600,000. Not surprisingly, Twisted Spider appeared to leverage inside information during the negotiations: Company X had an insurance policy with a ransomware sublimit of $600,000.

Once Twisted Spider verified that the money was received (in the form of cryptocurrency), the criminals provided preconfigured software to decrypt the encrypted files, and "confirmed" via chat that they had deleted the data. They even created a full list of all files that they claimed to have deleted, and shared this via email, presumably to provide the victim with documentation that could assuage client concerns or negate the need for notification. However, Company X's cyber lawyers determined that notification was required anyway, for both legal and ethical reasons.

1.1 A Cyber Epidemic

Company X was not alone in suffering such an attack. Thousands (if not millions) of organizations have been hit with cyber extortion over the past decade. What was once a novel crime has become mainstream—at great cost to society.

Cyber extortion attacks have shuttered hospitals, forced school closures, disrupted the food supply, and even caused large-scale fuel shortages. Today, ransomware attacks are also being pushed out to thousands of organizations simultaneously through the technology supply chain.

The cost of ransomware was estimated to hit $20 billion in 2021, and is predicted to balloon to $265 billion by 2031, according to research firm Cybersecurity Ventures.[2] In a global survey, 37% of organizations reported that they were hit by ransomware attacks in

2. David Braue, "Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031," *Cybercrime Magazine*, June 2, 2022, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

2020,[3] although the full scale of the problem is impossible to assess because many victims do not report the crime.[4]

Propelled by their success, cybercriminals have invested in increasingly sophisticated cyber extortion technology and business models. Cyber extortion has evolved from small, one-off attacks to a bustling criminal economy, with franchises, affiliates, specialized software, and user-friendly playbooks.

Defenders need to ramp up their efforts, too. It is possible to dramatically reduce the damage of a cyber extortion crisis, or even prevent one altogether, by acting quickly and strategically in response to prodromal signs of an attack. Given that cyber extortion tactics evolve quickly, defenders' tactics must constantly adapt as well.

In this chapter, we first build a foundation by evaluating the impacts of cyber extortion and understanding how this crime has evolved. Then, we discuss key technological advancements that have facilitated the expansion of ransomware specifically, as well as other forms of cyber extortion. Modern cyber extortion gangs have adopted scalable business models that often involve affiliates and industry specialists, and increasingly leverage threats of data exposure. We conclude by analyzing the next-generation cyber extortion business model, which will provide context for the response and prevention tactics introduced throughout this book.

1.2 What Is Cyber Extortion?

Definition: Cyber Extortion

Cyber extortion is an attack in which an adversary attempts to obtain something of value by threatening the confidentiality, integrity, and/or availability of information technology resources.

Extortion is a crime that has evolved along with humanity. It refers to the act of obtaining something of value "by force, intimidation, or undue or illegal power."[5] As the Internet evolved and organizations around the world came to depend upon computing resources to operate, cybercriminals adapted old tactics to this new digital world.

3. Sophos, *The State of Ransomware 2021*, 2021, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf.

4. Danny Palmer, "Ransomware Victims Aren't Reporting Attacks to Police. That's Causing a Big Problem," *ZDNet*, October 5, 2020, www.zdnet.com/article/ransomware-victims-arent-reporting-attacks-to-police-thats-causing-a-big-problem/.

5. "Extortion," Merriam-Webster, www.merriam-webster.com/dictionary/extortion.

1.2.1 CIA Triad

To create leverage, adversaries threaten one or more of the three security objectives for information and information systems, as defined by the Federal Information Security Management Act (FISMA) of 2002:

- Confidentiality
- Integrity
- Availability

Colloquially, these three objectives are known as the "CIA Triad," based on their acronym.[6] The CIA Triad was specifically designed for use by departments, vendors, and contractors of the federal government; however, it has been widely adopted by other organizations and the information security community itself. Although cyber extortion can violate any of the three CIA objectives, today's adversaries most commonly threaten confidentiality and availability.

1.2.2 Types of Cyber Extortion

Cyber extortion attacks fit into one of four categories—exposure, modification, denial, or faux:

- **Exposure:** Threatens the *confidentiality* of information resources. For example, an adversary may steal data from a victim, and threaten to either publish or sell it unless a ransom is paid.
- **Modification:** Threatens the *integrity* of information resources. An adversary can modify key elements of an organization's data, such as patient records or bank transactions, and demand a payment in exchange for restoring the original data or identifying the changes.[7] This type of attack is rare at the time of this writing, but adversaries may decide to leverage it in the future, particularly if scalable modification tools are developed.
- **Denial:** Threatens the *availability* of information resources. Ransomware attacks are the most common example of denial extortion. In these cases, an adversary encrypts a victim's files and refuses to release the decryption key unless a ransom is paid.

6. "Standards for Security Categorization of Federal Information and Information Systems," National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, February 2004, https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

7. "Enterprise Ransomware," CyberCube, 2022, https://insights.cybcube.com/enterprise-ransomware-report.

Distributed denial-of-service (DDoS) attacks have also been used by adversaries to create leverage for extortion.[8,9]

- **Faux:** An attack that appears to be cyber extortion, but in fact is not. For example, the destructive "NotPetya" malware masqueraded as ransomware, but was actually designed to destroy the victim's systems with no hope of recovery. (See Chapter 7 for more details on the NotPetya attacks.)

A Word About the "Adversary"

When we use the term "adversary" throughout this book, we are referring to the collection of actors involved in executing a cyber extortion attack, and not necessarily to a single actor.

Modern cyber extortion attacks often involve many different actors. For example, an "initial access broker" may gain the first entry into a victim's network, and then sell or rent access to other adversaries.[10] Sophisticated cyber extortion gangs may have employees or contractors with specialized skill sets that are employed at various stages of an attack. For simplicity, all of these actors are included when we refer to the "adversary" throughout this book.

1.2.3 Multicomponent Extortion

Increasingly, adversaries use multiple forms of extortion in combination, in an effort to increase their chances of scoring a big payday. Starting in late 2019, the Maze group pioneered the "double extortion" trend, combining both ransomware and data exposure threats. The term "double extortion" refers to the use of two cyber extortion tactics in tandem, such as denial and exposure threats. This creates greater leverage for the adversary and can result in a larger payment from the victim.

8. Lance Whitney, "How Ransomware Actors Are Adding DDoS Attacks to Their Arsenals," *TechRepublic*, June 2, 2021, www.techrepublic.com/article/how-ransomware-actors-are-adding-ddos-attacks-to-their-arsenals/.

9. Lawrence Abrams, "Ransomware Gangs Add DDoS Attacks to Their Extortion Arsenal," *Bleeping Computer*, October 1, 2020, www.bleepingcomputer.com/news/security/ransomware-gangs-add-ddos-attacks-to-their-extortion-arsenal/.

10. Victoria Kivilevich and Raveed Laeb, "The Secret Life of an Initial Access Broker," KELA, August 6, 2020, https://ke-la.com/the-secret-life-of-an-initial-access-broker/.

Other groups such as RagnarLocker, Avaddon, and SunCrypt have combined DDoS tactics with traditional ransomware or data exposure threats.[11,12] For example, in an October 2020 attack on a home appliances company, the SunCrypt gang launched a DDoS attack against the victim's network after initial ransomware negotiations stalled. According to a leaked transcript, the criminals wrote: "We were in the process on the negotiations and you didn't show up so further actions were taken."[13]

We will discuss the expansion of extortion tactics in more detail throughout Chapter 2.

1.3 Impacts of Modern Cyber Extortion

Cyber extortion attacks have the potential to cause severe damage to organizations. Their impacts may include operational disruption, financial loss, reputational damage, and litigation, as well as ripple effects for employees, customers, stakeholders, and the broader community.

In this section, we discuss common negative effects of cyber extortion attacks, setting the stage for discussions of response and mitigation throughout this book.

1.3.1 Operational Disruption

The short-term impacts of cyber extortion can include partial or complete disruption of normal operations. This is particularly the case when the adversary uses denial tactics, such as ransomware or DDoS attacks.

For example, Scripps Health, a California-based health system, was hit with a ransomware attack in April 2021 that disrupted access to electronic health records for nearly four weeks. During this time, many patients were diverted to other facilities, and non-urgent appointments were delayed.[14] Later that summer, hackers affiliated with the REvil ransomware gang detonated ransomware at 1,500 organizations around the world, leveraging vulnerabilities in the popular Kaseya remote management software.[15] As a result, the

11. Lawrence Abrams, "Another Ransomware Now Uses DDoS Attacks to Force Victims to Pay," *Bleeping Computer*, January 24, 2021, www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/.

12. Sean Newman, "How Ransomware Is Teaming up with DDoS," *Infosecurity Magazine*, June 18, 2021, www.infosecurity-magazine.com/opinions/ransomware-teaming-ddos/.

13. Newman, "How Ransomware Is Teaming up with DDoS."

14. "147,000 Patients Affected by Scripps Health Ransomware Attack," *HIPAA Journal*, June 3, 2021, www.hipaajournal.com/147000-patients-affected-by-scripps-health-ransomware-attack/.

15. Liam Tung, "Kaseya Ransomware Attack: 1,500 Companies Affected, Company Confirms," *ZDNet*, July 6, 2021, www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms/.

Swedish grocery chain, Coop, was forced to close hundreds of stores, causing food to spoil and leading to a significant revenue loss for the company.[16]

In a recent survey, more than one-fourth of the organizations surveyed reported that they had been forced to close their organization at least temporarily following a ransomware attack,[17] and 29% were forced to cut jobs, according to security company Cybereason.[18] Downtime statistics vary widely, but in the authors' experience, partial recovery typically comes within two to five days; resumption of normal operations takes two to four weeks.

The good news (if you could call it that) is that 96% of ransomware victims were able to get some of their data back, either by restoring it from backups, using an adversary-supplied decryptor, or through another means, according to a 2021 survey conducted by security vendor Sophos. However, an important caveat applies: Victims that paid the ransom were able to recover only 65% of their data, on average. Only a mere 8% of victims surveyed were able to restore all of their data.[19] Permanent data loss can lead to errors and cause extra work for many years in the future.

Definition: Decryptor

The term "decryptor" refers to software that is used to decrypt data that was encrypted during a ransomware incident. While this term is not yet in the dictionary (as of the time this book was written), it is commonly used by ransomware response professionals, and so we will use it throughout this book. Note that ransomware decryptors can be obtained from many different sources, including free decryptors from security vendors, experimental utilities created by government or law enforcement agencies, and as software purchased from the adversary in exchange for a ransom payment.

Ransomware attacks can even put businesses *out* of business. In 2019, U.S.-based healthcare provider Wood Ranch Medical closed its doors forever after a ransomware attack encrypted all their patient data. "Unfortunately, the damage to our computer system was such that we are unable to recover the data stored there and, with our backup system encrypted as well, we cannot rebuild our medical records," wrote the practice in its final statement to patients. "We will be closing our practice and ceasing operations…"[20]

16. Lawrence Abrams, "Coop Supermarket Closes 500 Stores After Kaseya Ransomware Attack," *Bleeping Computer*, July 3, 2021, www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/.

17. *Ransomware: The True Cost to Business* (Cybereason, 2021), p. 14, www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf.

18. *Ransomware: The True Cost to Business*, p. 12.

19. Sophos, *The State of Ransomware 2021*, p. 11.

20. Wood Ranch Medical, "Wood Ranch Medical Notifies Patients of Ransomware Attack," September 18, 2019, https://web.archive.org/web/20191229063121/https://www.woodranchmedical.com/.

A Word About "Ransomware"

The term "ransomware" originally referred to malicious software used to deny victims access to information resources, typically by encrypting files or devices. Over time, colloquial use of this term has broadened to include other types of cyber extortion, such as threats to publish data.

In this book, we will use the term "ransomware" specifically to refer to the malicious software used to deny access to information resources. In the broader sense, we will use the term "cyber extortion."

1.3.2 Financial Loss

Cyber extortion can have a devastating impact on a victim's financial state. Losses typically accrue because of short-term disruption to the victim's revenue generation process, expenses related to the investigation and remediation costs, and the ransom payment itself. For example, the global shipping company Maersk reported total losses between $250 million and $300 million after its IT infrastructure was suddenly wiped out in the destructive NotPetya faux ransomware attacks of 2017. The NotPetya malware destroyed the hard drives of infected computers. Although it appeared to offer a recovery option in exchange for a ransom payment, in fact the files were unrecoverable.[21]

In this section, we discuss three common causes of financial loss in cyber extortion attacks: revenue disruption, remediation costs, and ransom payments.

1.3.2.1 Revenue Disruption

Obviously, any operational interruptions can cause an immediate disruption in revenue generation. This is especially impactful for businesses that generate revenue daily (as opposed to nonprofit organizations, schools, and public entities that may be funded on an annual basis). Hospitals, retailers, professional services firms, transportation, and manufacturing companies are particularly hit hard by such disruptions. For example, Scripps Health reportedly lost $91.6 million of revenue as a result of its 2021 cyberattack, largely due to "volume reductions during May 2021 from emergency room diversions and postponement of elective surgeries."[22]

Business interruption insurance can soften the blow to a victim's wallet. Typically, this type of insurance kicks in after a waiting period (such as 24 hours), after which the insurer will cover lost revenue up to a set dollar amount. See Chapter 12 for more information on cyber insurance coverage.

---

21. Mike McQuade, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

22. Robert King, "May Cyberattack Cost Scripps Nearly $113M in Lost Revenue, More Costs," Fierce Healthcare, August 11, 2021, www.fiercehealthcare.com/hospitals/may-cyber-attack-cost-scripps-nearly-113m-lost-revenue-more-costs.