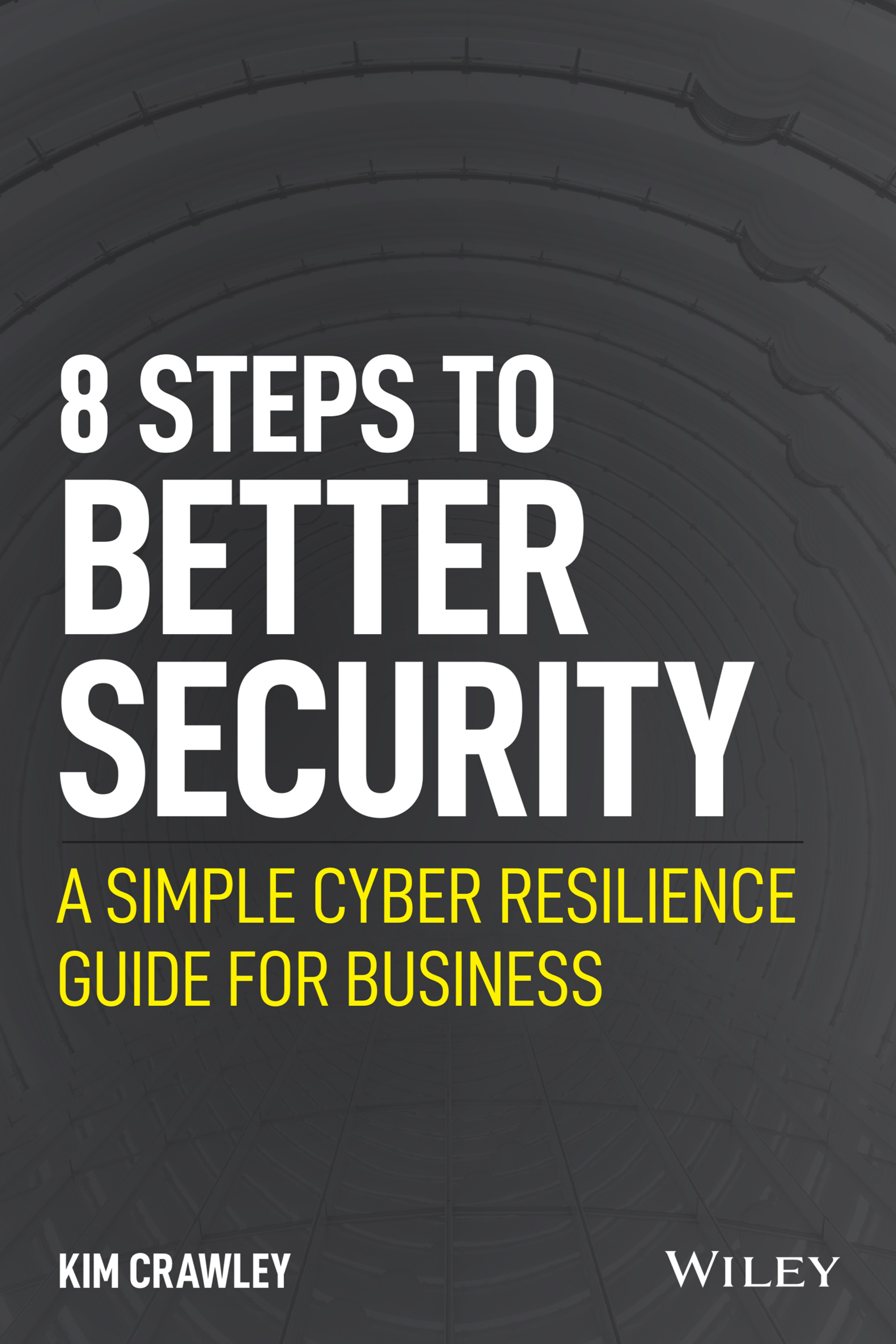

8 STEPS TO BETTER SECURITY

A SIMPLE CYBER RESILIENCE GUIDE FOR BUSINESS

KIM CRAWLEY

WILEY

8 Steps to Better Security

A Simple Cyber Resilience Guide for Business

Kim Crawley

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

978-1-119-81123-7
978-1-119-81125-1 (ebk.)
978-1-119-81124-4 (ebk.)

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at `www.wiley.com`.

Library of Congress Control Number: 2021942648

Cover image: © Zhenjin Li/Getty Images
Cover design: Wiley

To Jay for loving me.
To the Smith (Smith-Collins) clan for giving me a new family.
To Tori for upholding the responsibility of being the last Crawley in my life.
To Kate Brew, Joe Pettit, David Turner, Haris Pylarinos, Aris Zikopoulos, Daphne Deiktaki, Kate Bevan, and Phil Wylie for the professional opportunities you've granted me.

About the Author

Kim has been a prolific cybersecurity researcher and writer for well over a decade. Her years spent with BlackBerry Cylance, AT&T Cybersecurity, Venafi, and several other cybersecurity industry leaders gave her a thorough perspective on enterprise cybersecurity needs and trends. Years of friendships with CISOs, malware researchers, cyber threat intel specialists, and network administrators have provided her valuable insight to the scary ways the cyber threat landscape is evolving. Currently, Kim is focused on running Hack The Box's new blog, writing books about practical cybersecurity knowledge, and doing a little bit of dark web OSINT for a major Canadian bank on the side.

Acknowledgments

To my loving partner, Jay Smith, for all the times you've bragged about your "brilliant cybersecurity hacker girlfriend" to your family and your buddies. We're three years together, going strong! Let's make it three decades.

To my late father, Michael Crawley, for teaching me how to write for a living, from my toddler years to my twenties. It's a shame you didn't live long enough to witness my success.

To my publisher, Jim Minatel, for believing in my wacky ideas, and to my editor, Robyn Alvarez, for her patience with my eccentricities.

All the soft animals in my bed are also very much loved and appreciated.

Contents

Foreword

I first met Kim Crawley in person in October 2019, in Toronto at SecTor, Canada's version of DEFCON. We'd been acquainted for a long time via Twitter, and she was the one who originally turned me onto SecTor and inspired me to submit a talk, citing the merits of her hometown and the conference. She was right about both. In between the superb sessions there, amidst the fantastic energy of that conference and the international vibe of the city, we walked around and talked about information security, cyber resilience, and neurodiversity, topics woven deeply into the fabric of both our lives. Over lunch one afternoon, our conversation came around to how our industry can do a better job of helping small and midsize organizations better prepare for strategic response to cybercrime. We agreed that by helping smaller and more vulnerable organizations, the larger organizations and the collective industry as a whole would also benefit. We compared notes on tactics and strategies that don't have to cost a lot of time or money.

Shortly after our time and discussions at SecTor, Covid-19 hit. Kim didn't slow down. She founded DisInfoSec, a pop-up infosec conference showcasing infosec professionals who identify as neurodivergent (including ADD, AHDH, autism, Asperger's, dyslexia, and more). Inspired by Lesley Carhart's PancakesCon and other events, DisInfoSec was a first-of-its-kind event and took place on July 11, 2020. The con included a lot of great talks and raised funds for the Autistic Self Advocacy Network, the Autistic Women and Nonbinary Network, and the Council of Canadians with Disabilities. Kim's commitment to improving inclusion and nudging the world to a better place is showcased in her actions, and this new book is merely an extension of her productive mindset.

If you're new to Kim's work, her past and present articles on infosec and cyber for AT&T Cybersecurity, Cylance, and others are some of the most accessible to read, especially for anyone who is new to those topics. Kim writes with spirit and an intimate awareness of the diverse audiences who may be reading, which makes her style a stand-out. Her new book is no exception: *8 Steps to Better Security: A Simple Cyber Resilience Guide for Business* is an easy read for first-timers, seasoned veterans, and anyone else keen to learn more about infosec and cyber resilience using practical, quick-win steps you can take right away to better prepare your organization for a strategic response to unplanned events that would otherwise compromise your productivity, reputation, and bottom line. That's real peace of mind, and I don't know about you, but these days I'll take all of that I can get. Enjoy the book!

Chad Calease

Chief Information Security Officer

`https://resilience.sh`

Introduction

Pandora's box has been opened. Businesses in all industries run on computer data, and now there's no turning back.

When I was little, offices were still full of filing cabinets. Each customer, patient, client, vendor, and supplier had their own labeled manila folder in one of those cabinets. In fact, many offices have kept their filing cabinets well into the 21st century. Spilling your coffee on a few forms could damage lucrative business data. Unauthorized data access happened if someone found the secretary's physical key and unlocked cabinets they weren't entitled to. Some cabinets were designed to be fire resistant. But backing up all that data to a second location for the sake of business continuity in a disaster is always a good idea, one that was often not conducted because a clerk would have to put each page through the photo copier one by one, ever so tediously.

Now businesses keep their lucrative data on computers, whether that business is Smith's Convenience on the street corner or a multibillion-dollar military contractor. Some of these businesses still have filing cabinets, but they're working hard to digitize as much as possible.

The computer data that flows through businesses in all industries isn't just sensitive data on customers. It isn't all precious financial data, either. Some of it is security patches for our operating systems, applications, and firmware. Some of it is the email your employees are sending and receiving, whether on a company-owned PC or on their phone wherever they are. Some of it even keeps devices in the office running—your smart thermostats and your internet-connected heart monitors.

Keeping all the data that flows through your business secure is absolutely vital. Otherwise, a cybercriminal could steal your trade secrets or your clients' credit card data. Or they could perform a distributed denial-of-service attack on your production systems. Or they could infect your whole network with ransomware, both on the premises and on the cloud. Your company can be liable for any sensitive data that's stolen, especially if it results in your customers and vendors being harmed. And if your production systems face even a couple of hours of downtime, your business could lose millions in productivity. Chances are there are data privacy and security regulations that also apply to your business, and you could face hefty fines for security incidents and noncompliance. Often, fines can be in the millions under laws such as the European Union's General Data Protection Regulation.

A few hundred thousand dollars spent on improving your security will likely save your business millions of dollars in the long run. But simply spending money isn't enough. You need to spend it wisely, and you need to work on security every day. As cybersecurity expert Bruce Schneier says, "Security is a process, not a product."

I have spent the past several years researching and writing about cybersecurity for business on behalf of many major tech brands, such as AT&T Cybersecurity, Venafi, BlackBerry Cylance, Comodo, and Sophos. And every day I work, I have discussions with people who directly work on improving the security of businesses of all sizes and in a wide variety of industries.

I know it can be overwhelming when people are tasked with improving their company's cybersecurity. Where do you start? More importantly, how do you convince your executives that having a decent security budget and hiring security professionals is important? It's a struggle many people around the world face all the time.

I'm a regular computer security geek. But I've been adjacent to businesspeople my whole life. My (now retired) mother went from working in payroll to being a human resources director and vice president for Bayerische Landesbank back when they had a Toronto branch in the 1990s. I have friends who work as equity traders for companies like Manulife Financial. More importantly, I'm friends with many chief information security officers (CISOs).

So, I'm a geek and a "creative class" person according to Richard Florida. But although I don't fit in with the suits on Bay Street and Wall Street, I know how they think. I know what makes them tick: money, of course!

Ultimately, applying the advice in this book will cost you money, but it will save your business a lot more money over time. Spend $1 now to prevent losing $10 in the future. Think beyond next quarter's profits! Security-harden your business for the years ahead.

I'm going to be honest with you. Looking at the business bestsellers often makes me cringe. I distrust all books that say they're going to make me rich. I'm not an individualist-capitalist (I don't have any capital!); I believe in society, and I believe we're all interdependent. I think some of your success is in your hands, but a lot of your fate is in the hands of other people. I strongly believe that absolutely no one is "self-made."

I pride myself in sharing honest and useful information with the world, not tips on how to leverage market disruption for maximum capital gains, or whatever. I might as well tell you a 100 percent cabbage soup diet will make you permanently skinny and cure all disease on Earth. Honestly, my conscience doesn't feel good about that stuff. This book is for businesspeople, whether you wear a Brooks Brothers suit or a Lacoste polo shirt and khakis or a hard hat and overalls or jeans and a T-shirt. Cyber threats are bad now, and they'll only get worse. Make sure your business thrives in the ever-evolving cyber threat landscape with the eight steps in this book.

That's what I love to do: take useful information, share it in simple language, and break it down into manageable little bites. This book won't make your brain hurt. You can read one chapter at a time, or even just a few pages at a time, and glean useful insight that you can use in your everyday lives—as long as working in a business is part of your everyday life.

This book is based on the research I've done and knowledge I've acquired through years of work as a cybersecurity news and information scribe. And my knowledge is augmented with the insight of many of the world's top CISOs and other business leaders in security. It was a great pleasure for me to interview all these people and pick their brains a little bit for your benefit. This book is further enhanced with the findings of business security research studies and the aftermath of some of the most notable business security incidents. Mistakes become valuable when we make sure we learn from them!

Let's summarize the topics I cover in this book. Chapters 1 through 8 cover what this book is all about: *8 Steps to Better Security*. Each of those chapters is one of those steps. Chapter 9 will show you how to put it all together.

Chapter 1, "Step 1: Foster a Strong Security Culture": This is where everything starts—not with an audit or a security budget, but with how to make sure everyone in your organization takes security seriously, from your janitor to your CEO. Policy is vital, but it's useful only if it influences people's behavior. The best information security policies in the world become ineffective if people don't abide by them and enforce them. I'm fascinated by psychology and sociology, and these areas are a lot more important to cybersecurity than laypeople assume. This chapter will explain how you can begin to foster a strong security culture, whether you're a new startup or a 50-year-old company. If you do something more than three times, it'll become a habit. Making sure your habits and attitudes are good will set the foundation for everything your business does with regard to cybersecurity. Effective information security is paramount in the 21st century, regardless of your company's industry or size. So, let's get off to the best possible start. This chapter will show you how.

Chapter 2, "Step 2: Build a Security Team": If your company is medium-sized or larger, you'll benefit from having staff who work on cybersecurity as their full-time job. If your company is smaller, your one to five IT specialists will need to be tasked to manage your business's information security, even if your IT specialist is the nerd who comes into your little shop once a week to make sure your point-of-sale works properly. How your company builds a security team will vary according to your size and industry. The principles and advice in this chapter are designed to be useful for businesses of all kinds. The buck must stop somewhere. Make sure the buck stops with people who are ready to security-harden your company and rise to the challenge of any potential security incidents. This chapter includes tips on what sort of experience and credentials people should have in particular roles, so you can hire and delegate intelligently

Chapter 3, "Step 3: Regulatory Compliance": In business-speak, this is a major "pain point" for most companies. Pretty much all companies of all sizes and in all industries must comply with your region's general data privacy regulations. On top of that, if your company is in the medical field, there are usually regulations specific to healthcare data that must be complied with. If your company is in finance, there are usually financial-sector data privacy regulations as well. On top of that, if your company is in or deals with the public sector, there is often another whole set of regulations that are also crucial to abide by. Some audits are random and unpredictable, some may be scheduled, and some may occur in response to a data breach or similar incident. This chapter will help you take an inventory of which specific regulations apply to your business. From there, I offer tips to help you make sure you're set up for compliance so your business can continue to comply every day your business operates. Cybersecurity experts debate over how useful regulations are when it comes to preventing or mitigating security incidents. But we all agree that compliance is a must because the hefty fines for violations can really hurt your bottom line. The reputation damage can be immense too. Customers and clients need to feel that you take the security of their data seriously if they're going to be comfortable with spending money on your company's products and services.

Chapter 4, "Step 4: Frequent Security Testing": You absolutely cannot know how well secured your company's networks, computers, and applications are without frequent security testing. Having your assets security tested isn't simply a matter of emailing a third-party security firm and saying, "I need a security test." Cybersecurity testing comes in many different forms. The kind of testing you need will vary according to many different factors, including but not limited to the types of networks you have, how large they are, and which industry your business is in. So, knowing where to start when it comes to security testing will take this entire chapter, at the least. But don't be dismayed. This book is designed for businesspeople, not computer nerds. By the time you're done reading the chapter, you'll be ready to initiate the security testing your company needs in order to face the ever-evolving cyber threat landscape with confidence. The security testing your company needs can be a combination of internal red team specialists and third-party penetration testers. They may need to test once per year or every time your network changes in a significant way. Don't know what a red team or penetration testing is? Then this chapter is definitely for you!

Chapter 5, "Step 5: Security Framework Application": A cybersecurity framework is a set of standards that companies can base their security policies and procedures on. The most popular cybersecurity frameworks focus on how your business should prepare for and respond to cybersecurity incidents. Often companies can choose which framework is most useful for their organization. Unlike security regulation compliance, using a cybersecurity framework is optional, but highly recommended nonetheless. Also, unlike security regulation compliance, cybersecurity frameworks aren't usually tied to a particular state, province, or nation. The same frameworks are used by organizations around the world in many different countries and industries.

The NIST Cybersecurity Framework is the most widely implemented framework, and other frameworks have been inspired by it. Some of the other frameworks I cover in this chapter include ISO 27000 Cybersecurity Framework Series, CIS Cybersecurity Framework, and COBIT Cybersecurity Framework. I explain the basics of each of these frameworks and share what cybersecurity experts believe are their strengths and weaknesses. No matter what, though, your organization must have policies and procedures for preparing for and responding to security incidents. With proper preparation, cyber incidents will do much less harm to your organization, and you will save money in the long run.

Chapter 6, "Step 6: Control Your Data Assets": Every bit of your organization's data is stored on at least one computing device. Whether your network is on the premises, on the cloud, or on a hybrid network. Whether your company has a bring-your-own-device policy or not. Whether your workers work in the corporate office or from their homes. Your organization must first determine where all of your data resides, how it's transmitted, and which entities own the devices, and then design policies and procedures for securing all of those devices.

These data assets not only contain intellectual property and sensitive data (such as login credentials and financial information), but also keep your business running each and every day. A retail business needs a constantly operating point-of-sale system. An online service needs an always-working web application. A dental practice needs their radiography machines to always work, and so on. Computers with downtime result in lots of lost revenue and customers. Your organization needs to fully understand and control all of your data assets to protect them from cyber incidents.

Chapter 7, "Step 7: Understand the Human Factor": Many laypeople believe that successful cyberattacks require intense computer wizardry from cyberattackers, but the sad truth is that most cyber incidents, including the most destructive attacks, involve social engineering at one point or another. Fooling the people within your organization who have access to your computer systems is the most common way that cyber threat actors gain unlawful entry into your organization's networks. Phishing is a primary means of social engineering exploits. What is phishing? Phishing is when a threat actor uses a web page, text message, email, or social media post to imitate a trusted entity, such as a bank, a utility company, the government, or a well-known business. Even us cybersecurity professionals sometimes succumb to phishing attacks. We must never get overconfident. This chapter will cover how employees and contractors should be trained to prevent phishing attacks, as well as how to prevent other social engineering attacks, such as downloading Trojan malware. This chapter is also designed to consider how organizations have evolved during the Covid-19 pandemic to support many employees and contractors working from home for the first time.

Chapter 8, "Step 8: Build Redundancy and Resilience": Any cyber incident or technical glitch that causes network downtime hurts your business's productivity. That loss of productivity has an immediate impact on your bottom line. Here's how to design networks with redundant capacity through the power of the cloud, how to properly back up your data and applications from threats like ransomware, and how to design hot sites and cold sites for business continuity in the face of potential disasters. Your organization needs backed-up data and extra computers to survive the cyber threats that can impact any entity.

Once we cover all eight steps, we finish with Chapter 9, "Afterword." I have advice for implementing all eight of these steps. But my knowledge is augmented with tips from some of the world's top business cybersecurity professionals. So, as you prepare to improve the cybersecurity of your organization, you'll benefit from an amalgam of the best advice available.

Congratulations, you're ready to prepare your company for the evolving cyber threat landscape, no matter which country or industry you're in or the size of your business! Pat yourself on the back and then get to work. You can do it. I believe in you.

Chapter 1
Step 1: Foster a Strong Security Culture

People generally assume that cybersecurity is a technological area of study and take it for granted that cyber threat actors, called *hackers* by laypeople, must be computer geniuses. They have to have some mastery of computer programming code and an advanced understanding of how computer networks work. And if you take the Hollywood stereotype really seriously, then you probably believe that the most notorious cyberattackers work from an elaborate computer lab in their mom's basement, wearing a hoodie and typing at 400 words per minute. I imagine something like the movie *War Games*, but with a more 21st century–style presentation.

So, surely, if you're learning about cybersecurity, it's all about computer science stuff, right? You likely bought this book because you're a businessperson who wants to improve the security posture of your company. So, maybe you expect this book is about hiring the right supernerds for your IT department, and then you just let them do their technical wizardry. Why do you need eight steps for that? Step 1: hire computer experts. Step 2: don't think about cybersecurity ever again.