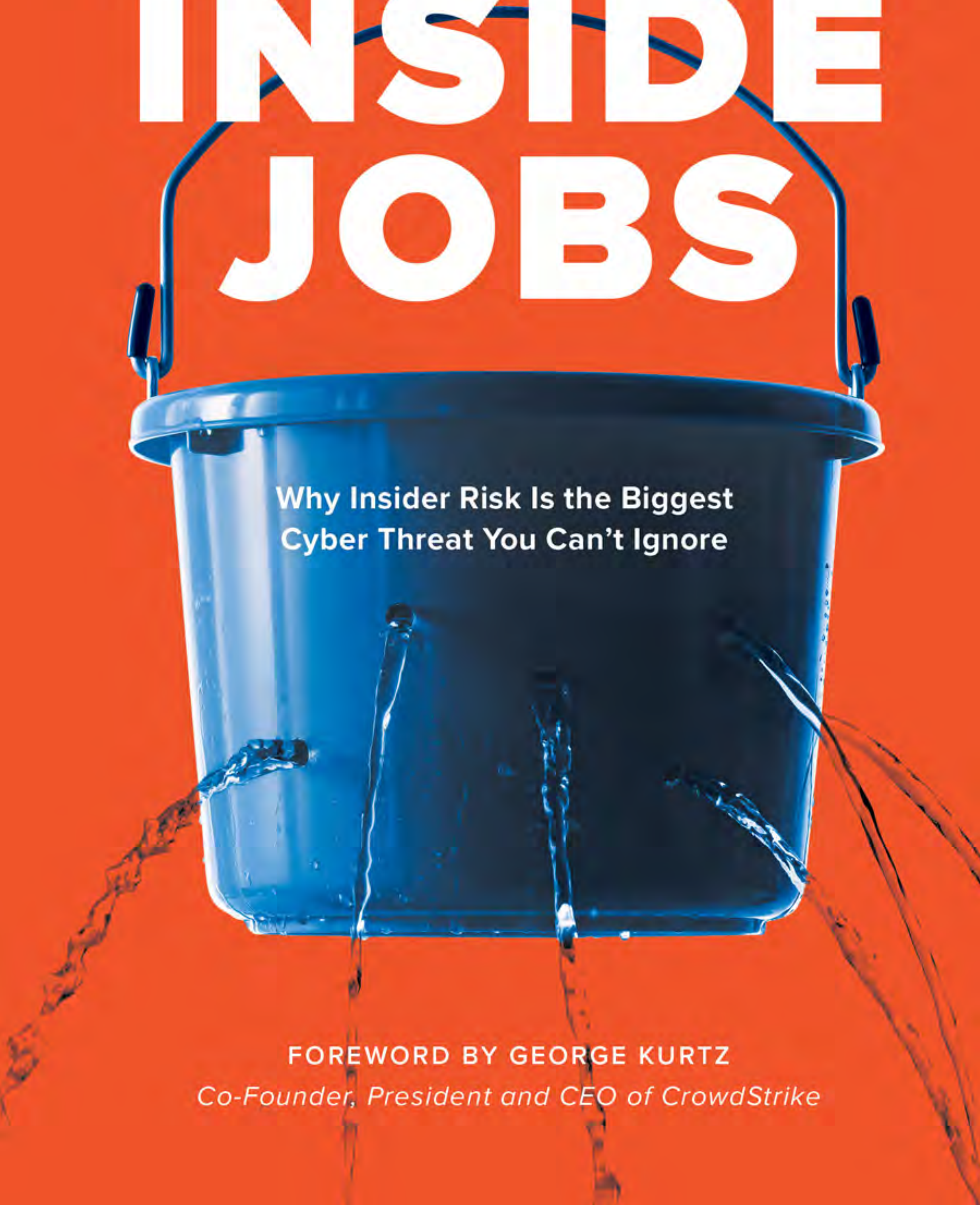
JOE PAYNE | JADEE HANSON | MARK WOJTASIAK

INSIDE JOBS



Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore

FOREWORD BY GEORGE KURTZ

Co-Founder, President and CEO of CrowdStrike

Praise for *Inside Jobs*

"In an era of sprawling cloud and consumerized IT, the challenge of security is not just to figure out who and what needs to be protected, but how to do so in the simplest way possible. This book drives this point home, and shows how to take friction out of security for users without putting data in jeopardy."

—**Dug Song**, cybersecurity expert, cofounder and CEO of
Duo Security, and cofounder of Arbor Networks

"This book addresses a problem that needs focus—insider threat is a very real issue that organizations need to grapple with and understand. It's one of the greatest underserved risks in cybersecurity today."

—**Amit Yoran**, CEO of Tenable, former president of
RSA, former national cybersecurity director at DHS,
and former director of US-CERT

"I never thought I'd read a book about cybersecurity insider threats that is actually—dare I say it—engaging. By illustrating technical points with compelling stories and examples, this book becomes a productive read not only for the CISO, but also for the CIO, the CHRO and the CEO."

—**Chip Heath**, author of best-sellers *Switch*, *Made to Stick*,
Decisive, and *The Power of Moments*

"Today, some of the most pressing problems in security revolve around insider threats and data security. Code42's new book provides new perspective on these problems and how much more important they have become in the increasingly remote and distributed workplace, suggesting major changes in how we approach data security."

—**Martin Roesch**, cybersecurity expert, creator of
Snort, and founder of Sourcefire

"I've seen too many organizations feel they have a cybersecurity program because they have a few cybersecurity products. This book really shows how the care of your data is fundamental to protecting it."

—**Ron Gula**, cyber industry pioneer; developer of Dragon,
one of the first commercial network intrusion detection systems;
cofounder of Tenable Network Security

"While many executives understand security threats from outside their company, most don't protect their business from insiders. Employees lose, steal, or misplace data more often than businesses realize, costing billions. *Inside Jobs* is packed with powerful examples and actionable advice every senior executive needs to know in a fast-paced book that can be finished in one plane ride."

—**David Meerman Scott**, marketing strategist,
entrepreneur, and best-selling author of eleven books,
including *Fanocracy* and *The New Rules of Marketing & PR*

"Data leaks are going to happen. Code42's approach to insider threat detection shows you exactly what you need to know when your confidential data is walking out the door and what to do about it."

—**Mike Wasserman,** security orchestration
engineer at The Pokémon Company International

Contents

Foreword

George Kurtz

Cyber threats come in many forms. CrowdStrike is best known for stopping threats coming from *outside* your organization: nation-state, eCrime, hacktivism, you name it.

Unlike the global bad actors we track—which our intelligence unit has personified with names like FANCY BEAR, GOTHIC PANDA, and MUMMY SPIDER—insider threats appear in much more benign forms. They can be the friendly network engineer, contract recruiter, or IT analyst whose office is just down the hall (at least it was before the pandemic). In many cases—maybe most—their unwanted actions are inadvertent, or they're simply unaware of doing anything wrong.

When it comes to protecting data, companies need to be vigilant and proactive. And they need systems and tools that let them take immediate action when required. With employees—and outside threat actors—able to work from anywhere, at any hour, with endless options to stash data on devices or in the cloud, every second counts: Incident detection and response needs to happen in real time and without limitations from time zones or geography.

This is precisely why CrowdStrike reinvented end-point and workload protection in the cloud. The effectiveness and rapid adoption of our revolutionary approach has exceeded everyone's expectations—even ours. The same thing has to happen with managing insider threats. Legacy approaches like data loss prevention (DLP) rely on "signatures"—just like the cumbersome antivirus and other end-point systems that CrowdStrike is replacing at enterprises across the globe. These outdated systems are just too complex and cumbersome and can't take advantage of the cloud's speed or scalability the way a cloud-native solution can.

Code42's book comes at an important inflection point for businesses and for the CISOs who keep those organizations safe from internal and external threats. Covid-19 forced companies to redeploy their workers and other resources on a massive global scale, practically overnight. They did it literally to preserve life and ensure business continuity under extreme conditions. Among the many unintended consequences, many organizations suddenly find themselves in a position to experience a huge leap forward in productivity and long-term business resilience, primarily because of moving key systems and processes to the cloud. In many cases, carefully planned business transformation strategies had to be accelerated, and accomplished in weeks instead of years. Some businesses are still reeling from these changes, but are now beginning to see the potential benefits from this forced transformation.

In security, and many other business-critical functions, moving from legacy premise-bound technologies to next-generation, cloud-native platforms has required a leap of faith from the early adopters. Once the benefits become widely known and accepted, truly disruptive cloud platforms like Salesforce, Workday, ServiceNow, CrowdStrike, and others will quickly become the rule, not the exception. As more organizations take that leap—whether from faith or simple necessity—the learning curve for transforming your business with the cloud flattens, and the adoption rate soars.

Today it's easier, faster, and more affordable than ever to provide true and meaningful protection against threats—from outsiders and insiders. This book will provide you with the knowledge and resources you need to make the leap. See you on the other side!

—George Kurtz, cofounder, president, and CEO of CrowdStrike

Introduction

The original title of this book was *The Aha Moment*. As we started working with organizations on the problem of Insider Risk, there were two distinct times in the process when a CISO would lean back in their chair and literally gasp. To be clear, "aha" was not actually the expletive they used, but you get the idea. These moments were visceral, and we started calling them "aha moments," because they became such a regular part of our process of working with new organizations.

The first aha moment happens when we outline the challenges faced when trying to protect an organization from Insider Risk while living in this new world of collaboration and the cloud. "Finally," they say, "someone is addressing this elephant-in-the-room problem." Or, "I knew that there had to be a better way." Or, "This seems so obvious in hindsight, but I haven't had time to consider all these cultural forces at work." What we have attempted to do in this book is to help you get to that first aha moment. It's ten chapters, but it may only take one or two chapters for you to have yours.

The second aha moment is not as pleasant. It's more of a "I can't believe this," or an "Are you kidding me?" moment. It happens when we put in place the technology to mitigate the new threats and the CISO is astounded at *how many* employees are exfiltrating data and *who* are actually doing it. Every CISO and security team knows it's happening. It's the depth and breadth of the problem that surprises most. Junior developers, salespeople, senior execs—they all take data that they shouldn't. If you want to experience the second aha moment, just reach out to us. Since you bought our book and are taking the time to read it to get your first aha moment, we won't charge you to try our product so that you can experience the second one for yourself. We've yet to meet someone who doesn't experience that aha moment.

Thanks again for reading. We hope you enjoy the book and find it helpful.

—Joe, Jadee, and Mark

CHAPTER 1

The Inside Is Your Blind Side

The potential for data to leak from your organization has never been greater, because taking it has never been easier.
—Joe Payne, President and CEO, Code42

"I'm calling the sheriff." That was how he started the call. It was a Saturday afternoon in May and I was in the middle of walking my golden retriever. On the phone was Rick Orloff, my chief security officer. Rick had been the CISO at eBay before he joined Code42, and before that he had been a senior executive at Apple. He was the guy who hunted down that lost iPhone that some engineer left in a bar—it was a big deal, especially to Steve Jobs. Rick had over twenty years of security experience and hung around with people who worked at three-letter agencies. He kept a grenade on the wall behind his desk so when you were on a Zoom call with him, it was always there over his shoulder. "I'm calling the sheriff," he said. "Marianne just downloaded the entire contents of her laptop hard drive onto an external hard drive." Marianne was an employee, but an employee who was leaving our company in five days. This looked like a textbook definition of insider threat.

Marianne didn't seem like someone you needed to worry about. She was in HR, had been with the company for over ten years, and was generally loved by everyone. But when she was successfully spear phished twice in four months, we had to let her go. Spear phishing occurs when a hacker sends an apparently legitimate email to a corporate insider, hoping to get that person to click on a link that installs malware on a corporate network. Because Marianne had been with us ten years, she got a nice severance package and her last day was scheduled for the next week. Everything seemed to be proceeding fine until I got the call from my chief security officer. "I'm calling the sheriff."

Well, as the story goes, we didn't call the sheriff. We called Marianne instead. "We know what you did and when you did it," we told her. "We know the brand and serial number of the external hard drive. Don't touch your laptop or that drive." Her response: "Okay, I just was trying to copy my contacts."

When she brought all the equipment back on Monday, we gave her her contacts. The laptop she had copied had all of our payroll data on it, including every Social Security number of every employee and every board member. It would have been a major breach—an embarrassing moment for a security company. And it was the day that I realized: insider threat is a huge problem. All of our information is portable. All of our employees have laptops. Every employee has some form of critical information. And modern workplace cultures like ours—where data sharing is encouraged—extend trust to employees every day. Calling the sheriff was not the answer. But what was? That's a long answer . . . and the reason this book was born. I hope it helps.

The New Work Reality

Marianne was one part of the collaboration culture that we've built at Code42. She had access to lots of data in the company so she could be efficient and do her job. I know that many of you operate in your businesses the same way. You understand that the success of that collaboration culture hinges on getting the right data to the right team at the right time. That means sharing critical information with all employees, contractors, and freelancers, just like Marianne. To get their jobs done, employees need to crunch, analyze, and organize this critical information in search of the key nuggets that might lead to the next breakthrough. All that data passes through their laptops, tablets, and phones. To collaborate effectively using that data, they need collaboration tools—Google Drive, Slack, Zoom, Dropbox, iCloud, Microsoft OneDrive, and many others.

And what does this collaboration actually look like? I'm thinking about what happens at Code42 in the course of a typical day—probably not that much different than what happens at your company. In the course of a few minutes, you might have Jennifer in legal working on a new customer contract in Google Docs while Andrew in sales shares a presentation with his team via Box. At the same time, Tom in marketing sends me our latest customer research via Slack, while Diane in security uploads a new version of the company security training to Google Drive for employees to access. These isolated moments capture a snapshot in time of the collaborative culture—moments put in motion by ongoing cooperation.

Even five years ago, this type of collaboration wasn't possible. But today it makes us all move faster. Is faster actually better? You bet! And we're not alone in that thinking. To achieve growth rates expected by investors, 80 percent of CEOs, CIOs, and CHROs want corporate cultures to work even more rapidly.[1] This allows us to serve our customers better and get innovation to the market ahead of our competitors. This is the great big upside to collaboration technology. But there is a downside. The downside is that these same technologies that make us more productive also make it much easier to exfiltrate data. The potential for data to leak from your organization has never been greater, because taking it has never been easier. Whether it's an employee like Marianne, who just wants to get some personal information off her work laptop, or a departing employee who wants to give himself a leg up in the job market, your people are exfiltrating critical company information at an alarming rate. According to recent market research, two-thirds of departing employees admitted that they took proprietary data with them when they left their company.[2] In 2018, that translated to 24 million quitters taking unauthorized data with them to their new employers. Of those insider threats, 73 percent went undetected.[3] This book is about how to mitigate that next great risk in security: insider threat.

What Is Insider Threat?

Insider threat is defined as the potential for an insider with authorized access to an organization to use that access either maliciously or unintentionally to act in a way that could negatively affect the organization. From the broadest perspective, insider threat includes any possible inside user action that might cause harm to an organization, such as:[4]

- Fraud
- Intellectual property theft
- Sabotage
- Espionage
- Workplace violence
- Social engineering
- Accidental disclosure
- Accidental loss of equipment or documents
- Disposal of equipment or documents

For the purposes of this book, we're focused on the data loss component of insider threat. Why? Because data loss represents a major blind side for organizations of all sizes. We reframe insider threat as Insider Risk, which surfaces when an employee, contractor, or freelancer moves data outside your organization's authorized collaboration tools, company network, and/or file-sharing platforms.

Data loss represents a major blind side for organizations of all sizes.

The techniques used are surprisingly simple. The most common? While "off-network"—at a coffee shop or at home—an employee uploads an attachment to her web-based Gmail or personal account and sends documents to herself. The second most common type of exfiltration: She uploads files to her personal Google Drive or Dropbox account. The third most common threat is what Marianne did: She downloads files to a thumb drive or an external hard drive. While some of these incidents are caused by frustration or ignorance, like what Marianne did, others stem from malice or a sense of entitlement. Nearly 75 percent of information security decision makers and 71 percent of business decision makers note a pervasive attitude of entitlement among the workforce at their organizations.[5] Many employees believe that if they created something (even if paid to do so), they somehow own it and have a right to keep it when they leave (and they don't). Many even believe that taking company data is essentially harmless.

Top data exfiltration methods

- **Personal email**
- **Personal cloud account**
- **USB thumb drive**

The case of Jawbone suggests otherwise. Jawbone produced Bluetooth fitness devices. When some Jawbone employees left the company for Fitbit, according to a suit filed by Jawbone against Fitbit, they took really important trade secrets with them.[6] In 2018, several former Jawbone employees were charged by federal prosecutors in Northern California with "allegedly absconding with confidential documents when they left the company for rival Fitbit," according to the *Washington Post*.[7] Long story short—Jawbone, valued at $3 billion with 450 employees in 2015, went bust in 2017.[8] That's despite Jawbone lawsuits against Fitbit over trade secrets, some of which Jawbone won.[9] [10] That $3 billion of value evaporated because of an insider threat that wasn't discovered and contained in a timely manner. Insider threat can be a true terminal risk to your organization and its survival.

A New Insider Threat Perspective

How are organizations reacting to this enormous, game-changing new risk posed by insider threat? Well, the data shows that most are not reacting at all. While 89 percent of security decision makers say that protecting sensitive company data is their biggest priority, the same percentage admit it is their biggest challenge.[11] In 2019, 69 percent of breaches involved insiders.[12] And yet, in that same year, only 10 percent of security budgets were focused on internal threats.[13] Sure, we need to protect ourselves from phishing, hackers, ransomware, and viruses. But we need to change the mindset of CISOs to recognize that insider threats are a bigger risk that needs attention. Again, most insider breaches—73 percent—go undetected for months.[14] That means that a Jawbone-like catastrophe could already be occurring in your organization—you just don't know about it yet.

In 2019, 69 percent of breaches involved insiders.

The case of SunPower, a US-based solar energy company, is a good example of the continuous nature of insider threat. In the last few years, SunPower has experienced three major breaches—all by insiders.[15] [16] [17] In these cases, SunPower IP was stolen by employees, managers, and executives through USB drive and email exfiltration. In one of these instances, SunPower sued more than twenty employees and a competitor for trade secret misappropriation, computer fraud, and breach of contract after 14,000 files containing market research, sales road maps, proprietary dealer information, and distribution channel strategies were removed and given to a competitor, according to *pv magazine*.[18] After each breach, SunPower turned to the courts to protect their proprietary technology from competitors, punish competitors and former executives, and win compensatory damages. But relying on the courts is an expensive and slow process. By the time a case gets heard it can be too late—significant damage to your intellectual property and competitive position has already occurred.

We know what you're thinking: "I've got security tools out the wazoo." It's not that your information security department doesn't want to protect your organization. They just need to adjust to the new reality of the collaboration culture. The vast majority of information security professionals rely on blocking access to information to contend with insider threats. Blocking is the literal antithesis of collaboration. Locking down data impedes collaboration and innovation, while actually increasing risk. When technology blocks an action (like sending a coworker a file via Slack) frustrated employees, contractors, and freelancers attempt to evade that blocking with unapproved apps and work-arounds. We see it all the time. The blocked employee simply uses his personal Gmail account or personal Dropbox folder to share the file . . . thus creating even more risk for the organization.

Trying to plug those leaks is a formidable task because they don't occur in isolation. They're infectious. Leaked data is a symptom of a much bigger problem than one frustrated, malicious, or ignorant employee or group of employees. That's because employees tend to share their off-network work-arounds. These work-arounds encourage even more individuals and groups of employees to go rogue in order to accomplish their objectives. Data leaks from rogue insiders put your intellectual property, product development, brand, and reputation at risk. When you fail to contain insider threat, as we saw with Jawbone, the results can be disastrous. What is needed is a change in mindset.

Trust, but Verify

In the early days of network security, we concentrated on building defined perimeters. Once you were on the "inside," we considered you safe and authenticated, and we gave you access to the things you asked for. Today, that approach is no longer considered effective. Organizations are simply too fluid, too distributed, too complex, and too porous. Just because you are inside the firewall does not mean we will give you free rein with corporate assets. We need a similar shift in thinking regarding data loss protection. It is not possible to define policies for all possible actions that may be harmful and then prevent those actions from happening. It is also not possible to classify data effectively across a complex, ever-changing organization.

We need a change in mindset. The new mindset requires us to watch *all* data activity across *all* users and vectors *all* the time. Whether it is source code, sales pipelines, HR data, marketing targets, customer lists, or financial information—it is all important. In today's fluid economy, we don't know which employee or contractor or executive is about to go work for our competitor. The new mindset requires us to trust first, then verify. Because collaboration and sharing are absolutely good for productivity, we trust and we allow sharing. But then we verify the sharing is not high-risk behavior.

The new security mindset requires us to trust first, then verify.

This mindset shift involves educating everyone in the organization on why security is important and how central it is to the success of the company. Without free access to necessary data, there's no ability to innovate and solve customer problems. But with free access comes the joint responsibility of securing that data. When everyone's responsible for security, an insider breach means that the entire corporate culture—and everyone who is a part of it—is victimized. This mindset turns insider threat into a breach of trust that affects all employees.

Secure the Collaboration Culture

Over the next nine chapters, we'll take you on a journey from the challenges created by the collaboration culture to the solutions that empower it. In the course of that journey, you'll meet our colleagues, customers, and industry leaders who will share their experiences balancing innovation and security.

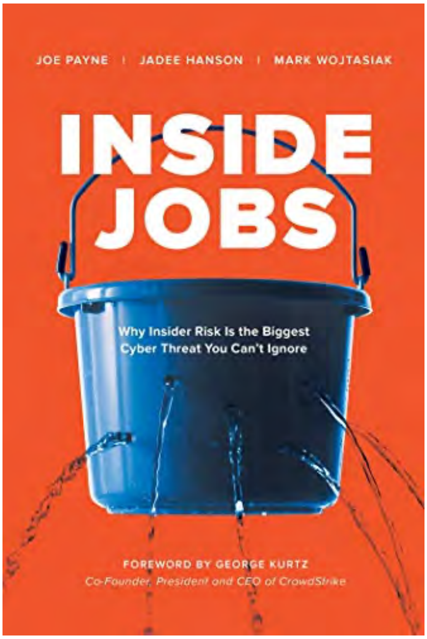
To that end, this book is divided into three parts:

- Part 1: A New Data Security Mindset
- Part 2: The Change Agents of the Collaboration Culture
- Part 3: How to Secure the Collaboration Culture

In Part 1, we explore the ways in which undeniable business forces, internal cyber risks, and data security dilemmas are pushing the boundaries of traditional security approaches. It's not that traditional security approaches are bad, per se. It's that they can't keep pace with the speed of change within modern enterprises. Massive transformations in workforce dynamics, technology catalysts, and the IP economy are driving the need for new security approaches, which we explore in Chapter 2. These changes place more critical data and information in the hands of insiders, who can put this data at risk all too easily. How? When they use unauthorized apps, work outside your VPN, and use personal cloud and email accounts. And that's just the beginning of the ways that insiders can imperil your proprietary data, as we present in Chapter 3. When you realize how the undeniable forces driving the collaborative culture produce the insider data risks that every organization faces every single day, you'll understand the heart of your data security dilemma. Your organization can't rely on the security approaches of the past, because they aren't equipped to deal with the corporate culture of today. In Chapter 4, we explore the root of that data security dilemma from three perspectives: blocking, the security approach of the past; people, who represent the security productivity challenge; and, finally, technology, which has failed to effectively secure the collaboration culture. We start in Chapter 5 with a view from the top—how CEOs, board members, and the line-of-business managers can facilitate innovation while responding appropriately to insider threat.

Part 2 of the book focuses on the change agents who design solutions for challenges we identify in the first half of the book. Chapter 6 puts the role of the chief information security officers (CISOs) and chief information officers (CIOs) in the spotlight, drawing an in-depth picture of the ways that progressive technology leadership benefits organizations. Chapters 7 and 8 investigate the role of legal departments and human resources in securing the collaborative culture. Then, in Part 3, we offer practical, hands-on frameworks and strategies for security teams that want to launch an insider threat program. Finally, in Chapter 10, we bring it all together and conclude with our best-practice recommendations and view on the future. If you only have time to read one chapter, go straight to Chapter 10.

We started with the story of Marianne, our HR employee who almost created a massive breach by taking all of our payroll data. But she didn't, because we saw the activity when it happened and we were able to get the data back before she left the company. When she was an employee, we never once slowed her down by blocking collaboration. Instead, she did her job in a trusted environment. By only acting when we needed to, we kept the business moving and kept her productive. We understand that this new approach is going to feel strange for security people. It is far easier to sit quietly in a corner and use technology to block possible threats than it is to engage in the messy world of people. Allowing the collaboration culture to thrive means letting people use technologies to share information broadly. It will also mean new engagement policies as we track down those who take data that they should not. We don't recommend calling the sheriff. But you will need to call the employee, and sometimes you will need to call HR and legal, too. We've written this book to help you navigate these new realities in these unusual times. We hope it helps. And we hope you enjoy it.


JOE PAYNE | JADEE HANSON | MARK WOJTASIAK
INSIDE JOBS
Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore
FOREWORD BY GEORGE KURTZ
Co-Founder, President and CEO of CrowdStrike

amazon.com

BARNES&NOBLE

INDIEBOUND

Google Play Books

iBooks