INTERNAL AUDIT AND IT AUDIT SERIES

CyRM℠

Mastering the Management of Cybersecurity

David X Martin

CRC Press
Taylor & Francis Group

CyRM℠

Mastering the Management of Cybersecurity

CyRM℠

Mastering the Management of Cybersecurity

David X Martin

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

First Edition published 2021
by CRC Press
6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL 33487-2742

and by CRC Press
2 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 978-0-367-56531-2 (hbk)
ISBN: 978-0-367-75785-4 (pbk)
ISBN: 978-1-003-09823-2 (ebk)

Typeset in Caslon
by SPi Global, India

For my family,
who gives life to the world around me.

Contents

Prong 2: CyberWellness℠

Prong 3: Cybersecurity as a Business Strategy

Introduction

Back in the 1990s—seems like eons ago, doesn't it?—General Electric CEO Jack Welch told business leaders, "If you're not confused, you don't know what's going on." I've always liked that admonition, because thinking you've got a handle on things can lead to arrogance and complacency; confusion keeps you humble. And if you're humble, you're teachable. And being teachable—being aware that there are many things you don't know (and even more things you don't *know* that you don't know)—keeps you seeking new information and remaining open to opportunities, all while staying alert to new threats.

At that time, I was the enterprise risk manager for Citicorp, the largest financial institution in the world, and I understood that financial institutions were mirrors of their environment. If the economy in which we're doing business is doing well, our customers do well, and we do well. The opposite is also true—even if you have the best risk professionals in the business. So back then, my approach was to thoroughly understand the environments we were operating in and to keep a keen eye on inflection points—leading indicators to know where those environments were going. For example, when our private clients in our emerging markets business started to move their private wealth offshore, I saw this as a leading indicator that their local economy was headed in the wrong direction.

Back then, the rate of technological innovation was a leading indicator, so I hired MIT professor Tsutomu Shimomura to "ethically hack" the bank. A few days later he came to me and said, "You guys are an easy target. All someone has to do is bombard your call center. No customer will be able to call in, and you'll be out of business in no time." I was startled. I quickly realized that cybersecurity—just like every other risk—needs to be managed.

Fast-forward to today: public scrutiny (and in some cases outrage) after cyberattacks, together with actions by regulatory authorities, have made cybersecurity a key leadership responsibility. When things go wrong, whether in a major or minor way, the ability to quickly identify and respond to a problem will determine the company's

ultimate recovery. Another major breach of cybersecurity will soon be in the news. The only question is how dramatic and costly that breach will be, and whether the full extent of the damage will ever be made public. Worse still, should hackers gain access to the financial records of a major national bank or important defense contractor, we'll quickly forget about the relatively insignificant attacks at retailers like Target and Home Depot.

What accounts for the increase in cybercrime? Three broad new security challenges have emerged.

First, there has been a previously unimaginable explosion in the amount of data, connections, transactions, and communications that has overloaded traditional data systems.

Second, institutions have lost the ability to effectively identify problems. Faster innovation cycles and a dizzying array of new products mean that most businesses find themselves unable to quickly recognize security breaches. Social networking systems, big data, cloud computing, mobile internet, and Internet of Things technologies are generating personal data streams that have made authorization and message filtration extraordinarily difficult.

Third, there's a lack of formal control mechanisms. In an environment where cybersecurity disruptions are becoming more pervasive and sophisticated, there are still no recognized standards for detection, response, remediation, and enterprise-wide communication. The management of these critical functions is often left to the IT department, which is usually directed to pursue outdated, hardened-shell strategies designed only to discourage penetration.

Armed with decades of experience as a leader in risk management, I examined this landscape, and it became clear to me that we need an information security model that continually assesses the validity, reliability, and value of the information it gathers. I developed and honed that security model into a process that I know can help companies avoid the worst pitfalls of a cyberattack. It's called cyber risk management, or CyRM℠.

CyRM℠ is a new paradigm that approaches security as a business problem and aligns it with business needs. So, instead of viewing security as a technical problem handled by technical people, it uses an outcome-driven approach that balances investment and risk. Even further, instead of throwing money at the problem at the expense of

executive engagement, it connects cybersecurity with business decision-making to impact business outcomes.

To effectively impact business outcomes, CyRM℠ needs to consist of three prongs:

1. **Risk Management:** It needs to apply the tenets of risk management to cybersecurity in order to take a broad view of risks across an organization to inform resource allocation, better manage risks, and enable accountability.

2. **CyberWellness℠:** It needs to encompass not only the firm as a whole, but also every employee who needs to be responsible for the risks they undertake. This requires an active process with cybersecurity—just like physical wellness programs in which the company takes an active approach to promoting employees' good health.
3. **Cybersecurity as a Business Strategy:** Cybersecurity needs to be repositioned for what it really is—a growth enabler, and not just designed to reduce operational risks by eliminating the dangers posed by viruses and hackers. It also needs to enhance product integrity, customer experience, operations regulatory compliance, brand reputation, and investor confidence.

This book lays out my approach to CyRM℠ and shows you—business leaders and IT managers alike—how to work together and succeed. Each chapter of this book tells you what you need to know about managing the current cybersecurity landscape. And each chapter ends with CyRM℠ Action Points—proactive steps you can take to prepare yourself and your company to survive and succeed. I'm looking forward to being your educator and guide as we delve into CyRM℠.

1

The Current Landscape

On September 7, 2017, one of the nation's largest credit monitoring agencies, Equifax, announced that more than 143 million customer accounts had been breached in what may be the most significant cyberattack to impact US consumers to date. The number of affected individuals has since risen to an estimated 147 million people[1]—all of whom likely had their names, Social Security numbers, birth dates, addresses, and driver's license numbers compromised in the attack.

Amid the Equifax controversy, the US Securities and Exchange Commission (SEC) made some striking disclosures of its own. Newly arrived SEC Chair Jay Clayton announced on September 20, 2017, that the SEC's own EDGAR filing system had been penetrated by cybercriminals months previously. This led to questions about the safety of such systems, as well as the risk of insider trading by individuals with advance knowledge of sensitive and nonpublic company information.

Since then, other recent high-profile cyberattacks have abounded. Much to the chagrin of fans of the popular television show *Game of Thrones*, the HBO television network was breached by a group that pilfered more than 1.5 terabytes of information, including show scripts and full episodes of several prominent shows. The *Guardian* revealed that Deloitte LLP, one of the "Big Four" accounting firms—whose advisory clients include large companies and government departments—had been the victim of a breach and had its internal email system compromised. Deloitte has since notified six of its clients whose information may have been "impacted" by the breach, and it has completed an internal investigation into the incident. It took Uber more than a year to admit it had been hacked. The rideshare company purportedly paid a "ransom" in exchange for a promise by the hackers to delete purloined data and keep the cyber incident quiet.

Large-scale data breaches continue to happen every year. In 2019, a few of the notable larger ones included those that happened at Capital One, Facebook, Quest Diagnostics, and First American. At Capital One, a single hacker gained access to more than 100 million customer accounts and credit card applications. Quest Diagnostics revealed that a user gained access to medical information of more than twelve million patients through a third-party vendor.

Approximately one year after the Cambridge Analytica scandal, Facebook admitted to unintentionally making public more than one million user emails. In an even larger breach, First American, a US real-estate title company, revealed that nearly 900 million records were compromised! In terms of ransomware attacks, 2019 was also a banner year.

In 2020, the Citizen Lab (associated with the University of Toronto) exposed a group of mercenary hackers dubbed "Dark Basin," based in New Delhi. These for-hire hackers went after Exxon and a German company called Wirecard. Hackers for hire provide services to clients looking to cause trouble from a distance—in a different jurisdiction with minimal friction and not much chance of getting caught.

In 2020 hackers broke into Lockheed Martin, one of the largest US defense contractors, by targeting remote workers. All hackers need to gain access to a company is one vulnerable point; once they find that, they can seize control of a whole network. Once they're in, they can steal data and secrets and even lock authorized users out of the network.

One of the biggest exposures for any company lies in the cloud. As supply chains become ever more complex, financial institutions rely on third parties to provide scale and agility. Third-party provides are often the vector that cyber intruders exploit to reach their intended target. This dramatically increases the attack surface—the constellation of opportunities available to hackers—that companies have to worry about. Trusting that third parties will attend to your security needs in the same manner you would isn't a prudent strategy. If you rely on a weak set of interfaces to interact with cloud services, security issues can arise concerning confidentiality, integrity, availability, and accountability.

Here are a few examples of problems that may arise with cloud technology. Attackers now have the ability to use your (or your