Boardroom Cybersecurity

A Director's Guide to Mastering Cybersecurity Fundamentals

Dan Weis

Apress®

Boardroom Cybersecurity

A Director's Guide to Mastering Cybersecurity Fundamentals

Dan Weis

Apress®

Boardroom Cybersecurity: A Director's Guide to Mastering Cybersecurity Fundamentals

Dan Weis
Melbourne, VIC, Australia

ISBN-13 (pbk): 979-8-8688-0784-8 ISBN-13 (electronic): 979-8-8688-0785-5
https://doi.org/10.1007/979-8-8688-0785-5

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Project Manager: Jessica Vakili

Cover designed by eStudioCalamar

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 NY Plaza, New York, NY 10004. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on the Github repository: https://github.com/Apress/Boardroom Cybersecurity. For more detailed information, please visit https://www.apress.com/gp/services/source-code.

If disposing of this product, please recycle the paper

Table of Contents

About the Author and why this book

Dan Weis is the Penetration Testing Practice Lead at Nexon Asia Pacific. Dan has over 30 years' experience in IT, in a range of different industries, and was one of the first ten people in the world to become a Certified Ethical Hacker.

Dan also has over 18.5+ years of cybersecurity, management & consulting, penetration testing, and red team experience, with attributed zero-day vulnerabilities in SCADA/Control Systems software. Dan heads Up Nexon's team of cybersecurity experts, leading red and blue teams on offensive and defensive cyber operations to proactively assess company and government networks to increase their security posture and not become the next "headline."

Earning the nickname "The General" as a result of his multitude of industry qualifications, Daniel also holds an additional 22 industry certifications. In his spare time, Daniel undertakes research on the cybercrime underground, facilitates training sessions for budding ethical hackers, is a regular on the speaker circuit presenting on all things InfoSec and dark web, and has presented at over 80 conferences and events over the last five years.

Dan also has made appearances on television and radio and has a number of published resources, including books, magazine articles, newspaper appearances, online posts, and YouTube videos, and is an active participant in a variety of renowned security and industry programs. Dan has authored the book *Hack Proof Yourself! The essential guide for securing your digital world* and coauthored the book *Learn Social Engineering* that has received BookAuthority's Best Books of All Time award.

Preface

My name is **Dan Weis**, and thanks for picking up my book. I've been in the IT industry since 1994, and specifically in the Cybersecurity space for Over 18 years, performing penetration testing, vCISO services, security consulting, incident response, security auditing, and security training. I hold a multitude of certifications and have spent many years on the speaker circuit educating people and organizations on cybersecurity, cyber risk and resilience, the dark web, hacking and penetration testing, security awareness, as well as TV, radio, newspaper, and online resources. I breathe information security, and I love educating people and organizations to ensure that they don't become the next headline. We have enough issues to deal with in the world, without being hacked or beached as one of them.

I present to directors, boards, and organizations nearly every week on these topics, and the overwhelming feedback I get from most directors and boards is that they just don't understand cyber, cyber risks, pentests, audits, compliance, all these security areas where information is presented to them, and they need to try and decipher it to make decisions for the organization (and to obtain assurance) and also how this translates back to their obligations and requirements as directors. Because of this knowledge gap, all the information they receive is filtered because they don't understand the concepts, so the C-suite could be painting any picture for the organization and the directors would have no idea; by the same token

the IT manager, as an example, might be requesting a large amount of capital for certain cybersecurity technologies that may not even reduce the overall risk profile for the organization.

My goal with this book is to empower you with the knowledge that you need as directors and leaders to navigate the complex world of cybersecurity, to ask the right questions from both internal and external stakeholders, and to ensure your organization is as cyber-resilient as possible.

Introduction

The digital age has ignited a new era of opportunity and efficiency. However, this interconnected world has also created a rapidly evolving landscape of cyber threats. In 2023 alone, cybercrime caused an estimated $6 trillion in global damages, a staggering figure that showcases the immense financial risk organizations face today [1].

This book delves into the critical realm of cybersecurity, specifically focusing on the ever-present threats that can cripple any organization. We will dissect real-world attack methods and mitigation strategies, analyze industry and regulatory requirements as they impact your boardroom decisions, and expose the vulnerabilities that leave organizations susceptible to data breaches.

But why should cybersecurity be a top priority for CEOs, directors, and board members? A successful cyberattack can be catastrophic. Beyond financial losses, data breaches can erode customer trust, damage brand reputation, disrupt critical operations, and even lead to legal ramifications for the board and for directors, such as regulatory fines and lawsuits.

This book empowers you to make informed decisions for your organization regarding cyber risk. We will equip you to not only understand the evolving threat landscape and the potential impact of an attack but also to proactively reduce and mitigate those risks. This knowledge will ensure you fulfill your reporting obligations and demonstrate strong corporate governance in the face of ever-present cyber threats.

The digital age presents immense opportunities, but it also demands a heightened awareness of cybersecurity risks. This book is your road map to navigating this complex landscape, understanding your obligations as a director or board member, and ensuring your organization remains secure and thrives in this increasingly digital world.

How to Use This Book

This book is broken down into two parts.

Chapters	Part
1–5	Part 1 – Understanding the Cybersecurity Landscape: Threats, Roles, Governance, and Frameworks
6–9	Part 2 – Overseeing Cyber Risk: Requirements, Attack Vectors, and Mitigation Controls

Each chapter ends with a "Key Takeaways" section to reinforce understanding of important concepts as well as a set of key questions for stakeholders.

Appendix
At the end of the book, you will find an appendix listing AICD, ACSC, and other cyber risk resources that can be referenced to increase understanding.

Glossary
Security and technology glossaries are provided at the end of the book that can be leveraged to look up key terms and definitions.

Index
An index can be found at the end of this book.

References

[1] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

PART I

Understanding the Cyber Security Landscape: Threats, Roles, Governance and Frameworks

CHAPTER 1

The Evolving Threat Landscape: Understanding Cyber Threats in the Digital Age

The digital age has transformed how organizations operate, creating new opportunities for growth and efficiency. However, this interconnected world has also opened doors for malicious actors, leading to a constantly evolving landscape of cyber threats. In this chapter, we will explore the current and emerging threats that organizations face today, equipping you with the knowledge to protect your valuable assets and ensure business continuity.

D. Weis, *Boardroom Cybersecurity*, https://doi.org/10.1007/979-8-8688-0785-5_1

1.1 Traditional Threats with a Modern Twist

Although cybercrime tactics continue to evolve, some established threats remain a significant and ongoing concern for organizations; these include

Malware: Malicious software, including worms and ransomware, continues to plague organizations. Ransomware attacks, in particular, have become increasingly sophisticated over the years, encrypting critical data and demanding exorbitant ransoms for decryption.

Social Engineering Attacks: Social engineering attacks such as phishing and vishing aim to trick users into revealing sensitive information or taking an action, such as clicking malicious links or providing an access point into an organization. Phishing attacks continue to increase in sophistication daily along with business email compromise attacks (BEC) that target specific individuals within organizations.

The Human Element: The Insider Threat: Cyber threats don't always come from external sources. Disgruntled employees (malicious insiders), contractors, or even business partners can pose a significant risk. Typically, insider attacks are orchestrated by employees, often someone who feels they were mistreated, for example, they have been missed for that big promotion they had their heart set on, or someone who has been engaged by a competitor for competitive advantage. There are a number of cases where employees accept a role at another organization which is a competitor, and within their notice period, they exfiltrate data or sabotage the current employer to further enhance the competitor's position.

Typically, insider threats can involve stealing data, sabotaging systems, or inadvertently introducing malware through negligence.

Organizations need to implement robust access controls and security awareness training to mitigate insider threats.

Denial-of-Service (DoS) Attacks: These attacks overwhelm a website or server with traffic, rendering it inaccessible to legitimate users. DoS attacks can cripple online services and disrupt critical operations.

Traditional Network-Layer Attacks: Attacks exploiting vulnerabilities in systems or wired/wireless networks leveraging exploits.

Man-in-the-Middle (MitM) Attacks: MitM or interception attacks involving "sniffing" or sitting between two parties to intercept sensitive information.

Cryptojacking: This involves using a victim's computer to mine cryptocurrency without their knowledge or consent. Cryptojacking can significantly drain resources and impact system performance.

1.2 The Rise of New Threats

As technology advances, so do cybercriminals' techniques. The following are some emerging threats that organizations should be aware of:

Supply Chain Attacks: Although these attacks have been happening since as far back as 2007, they were few and far between and not widely publicized. With

the massive increases in supply chain attacks over the past two years, I would treat these attacks as a new threat and attack vector that all organizations now need to consider. Cybercriminals are increasingly targeting third-party vendors and suppliers to gain access to an organization's network. These vulnerable areas are usually linked to vendors with poor security practices, which makes it crucial to assess the cybersecurity posture of your entire supply chain. Recent examples include the SolarWinds Attack (2020), the Kaseya Supply Chain Attack (2021), the MOVEit Software Attack (2023), the Okta Supply Chain Attack, and many more [2][3][4].

Internet of Things (IoT) Vulnerabilities: The growing number of interconnected devices within the IoT world creates new attack surfaces. These devices are often poorly secured, making them prime targets for cybercriminals to gain access to a network.

The Weaponization of Artificial Intelligence (AI): AI has taken the world by storm and is creating challenges due to the pace and speed of change and adoption. While AI holds the potential to enhance security measures (e.g., it is currently being used by security operation centers (SOCs) to identify threats and breaches faster), it is also actively being used by malicious actors to launch more complex and targeted attacks. AI-powered tools can be used to automate attacks, personalize phishing attempts, and even bypass traditional security measures. Current AI attacks are also being used to generate sophisticated voice and video recordings, imitating individuals, and are used in social engineering attacks.

An example of this is deepfakes [5][6]. Attacks using deepfakes and AI increased by 700% between 2022 and 2023, according to the *Wall Street Journal*. When a *Wall Street Journal* reporter experimented with an AI-generated version of herself, she was able to trick Chase's system [7].

AI and deepfakes are also being used in other ways to influence world events, for example, in fake election videos, and were utilized during the war in Ukraine by Russia, to disseminate misinformation [8].
Current trends see these attacks targeting individuals within organizations to facilitate payments to attackers.

Cloud Security Risks: Businesses are increasingly relying on cloud-based storage and services. However, cloud environments can be vulnerable to cyberattacks if not properly secured. Organizations need to understand the shared responsibility model of cloud security.

Cyberwarfare and State-Sponsored Attacks: Exacerbated by current conflicts, cyberwarfare is a growing threat. Nation-state actors are deploying sophisticated attacks for espionage, misinformation, disruption, and critical infrastructure sabotage, raising the specter of widespread damage.

As you can see, cyber threats are constantly evolving with new tactics and vulnerabilities emerging all the time. Constant vigilance is key.

Understanding current and emerging cyber threats is crucial for organizations in today's digital age. By being aware of the risks and implementing robust security measures, you can significantly reduce your organization's vulnerability to cyberattacks and protect your assets and data.

1.3 Key Questions for Your Organization

- Do we understand the current cyber threats our organization faces, both traditional (e.g., malware, phishing, DoS, supply chain attacks, cloud security risks) and emerging (e.g., IoT vulnerabilities, AI-powered attacks)?
- Are we regularly updated on the evolving threat landscape and the potential impact of these threats on our organization?
- Do we have a process in place to assess and prioritize these threats based on their potential impact on our operations, finances, and reputation?
- Have we assessed our vulnerability and implemented robust security measures to protect against traditional threats like malware, phishing, and denial-of-service (DoS) attacks?
- Have we assessed our vulnerability to emerging threats like supply chain attacks, IoT vulnerabilities, and AI-powered attacks?
- Are we implementing appropriate security measures to address these emerging threats, such as supply chain security assessments, securing IoT devices and AI-powered threat detection tools?
- Are we regularly reviewing and updating these measures to keep pace with the evolving tactics used by attackers?

- Are we staying informed about the latest developments in the threat landscape and adjusting our security strategy accordingly?
- Have we considered the risk of insider threats and do we have a plan in place to address insider threats from disgruntled employees or negligent individuals? This could include access controls, monitoring, and behavioral analytics.
- Are we monitoring user activity and implementing security measures to detect and prevent unauthorized access or data exfiltration?
- Are we regularly assessing and updating our understanding of the evolving threat landscape through threat intelligence and security awareness training?
- Are we educating our employees about these threats and providing training on how to identify and avoid them?

1.4 Key Takeaways

- **Cyber Threats Are Constantly Evolving:** New tactics and vulnerabilities emerge all the time, requiring ongoing vigilance and consistent education and awareness.
- **Traditional Threats Remain Significant:** Malware, social engineering, DoS attacks, and network vulnerabilities are still major concerns.

- **New Threats Require Attention:** Supply chain attacks, IoT vulnerabilities, AI-powered attacks, cloud security risks, and cyberwarfare pose growing dangers.
- **The Human Element Is Critical:** Insider threats from disgruntled employees or negligent individuals can cause extensive damage. Lack of awareness and training can lead to increased risks via human-based attacks such as social engineering.
- **Understanding the Threat Landscape Is Crucial:** By being aware of the current and emerging risks, directors can ask effective questions and make informed decisions about cybersecurity measures.
- **Robust Security Measures Are Essential:** Organizations need to implement strong defenses to protect their assets and data.

Having explored the ever-present cyber threats in this chapter, Chapter 2 dives deeper into the malicious actors' arsenal. We'll dissect real-world attack methods, analyze how organizations can implement effective defenses, and equip you to build a robust cyber defense strategy. The subsequent chapters will delve deeper into specific threats, explore best practices, and explain compliance and board responsibilities, empowering you to navigate this complex landscape.

Empowered by an understanding of these threats, directors can fulfill their cybersecurity oversight duties and make informed decisions that safeguard the organization.

References

[2] https://en.wikipedia.org/wiki/Supply_chain_attack

[3] www.upguard.com/blog/supply-chain-attack

[4] https://cyberint.com/blog/research/recent-supply-chain-attacks-examined/

[5] www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

[6] www.fortinet.com/resources/cyberglossary/deepfake

[7] www.wsj.com/articles/i-cloned-myself-with-ai-she-fooled-my-bank-and-my-family-356bd1a3

[8] www.cnbc.com/2024/04/08/state-backed-cyberattacks-ai-deepfakes-top-uk-election-cyber-risks.html

CHAPTER 2

Understanding the Who and Why

It's important for directors and board members to understand the motives and threat actors behind cyberattacks. It's big business and the third-largest economy in the world. A 2023 report by Cybersecurity Magazine [9] estimated that cybercrime caused $6 trillion in global damages and is expected to cost $9.5 trillion by the end of 2024 [10]. A recent report from the World Economic Forum anticipates the costs to climb higher, exceeding $23.84 trillion by 2027 [11].

Cybercriminals launch attacks for a variety of reasons, often categorized by the desired outcome. The following is a breakdown of some common motives behind cyberattacks:

Financial Gain

This is the most prevalent motive. Cybercriminals aim to steal money directly from individuals or organizations through various techniques:

> **Financial Account Takeover:** Hacking into bank accounts or obtaining credit card information to steal funds (think AI and deepfakes)
>
> **Ransomware:** Encrypting critical data and demanding a ransom payment for decryption

D. Weis, *Boardroom Cybersecurity*, https://doi.org/10.1007/979-8-8688-0785-5_2

Extortion Attacks: Often used in conjunction with ransomware attacks, extortion attacks are leveraged against an organization once their data has been stolen (or exfiltrated) during a cyberattack. Some attacks are specifically designed to steal data for this reason; others are daisy-chained with other attacks such as data breaches and ransomware.

Data Theft and Espionage: Stealing sensitive information for various purposes such as

- **Identity Theft:** Using stolen personal information (e.g., tax file numbers and personally identifiable information (PII)) to commit fraud or open new accounts in the victim's name.
- **Corporate Espionage:** Stealing trade secrets, intellectual property, or confidential business information from competitors.
- **Extortion Attacks:** Same as financial gain above.
- **State-Sponsored Attacks:** Foreign governments may launch cyberattacks to steal classified information or disrupt critical infrastructure or to spread misinformation campaigns.

Disruption and Sabotage: Aiming to disrupt operations or damage a target organization's reputation, including

- **Denial-of-Service (DoS) Attacks:** Overwhelming a website or server with traffic, making it inaccessible to legitimate users.

- **Hacktivism:** Using cyberattacks to promote a political or social agenda. Hacktivists are individuals or groups who use cyberattacks to promote a particular social or political cause, which can damage an organization's reputation and disrupt operations.
- **Destructive Attacks:** Disrupting critical infrastructure or causing physical damage by manipulating control systems (rare but impactful).

Personal Vendetta: Carrying out cyberattacks out of spite or revenge against a specific person or organization. This could involve disgruntled employees, former business partners, or even competitors.

It's important to note that some attackers may have more sophisticated goals beyond these immediate disruptions. Advanced Persistent threats (APTs) are attackers who meticulously plan and execute intrusions to steal sensitive data over a long period, often remaining undetected for months or even years.

Thrill-Seeking and Notoriety: Some attackers are motivated by the challenge and excitement of breaking into computer systems and gaining unauthorized access. They may also seek notoriety by publicizing their actions online.

It's important to note that motives can overlap. For example, an attacker might launch a ransomware attack for financial gain but also steal data during the process to potentially sell it on the black market or extort the organization.

In addition, **the threat landscape is continually evolving:** Attackers are constantly developing new techniques to exploit vulnerabilities. This includes emerging technologies like artificial intelligence (AI) and Internet of Things (IoT) devices. Social engineering tactics also consistently become more sophisticated, preying on human emotions and trust. Adding to this complexity is the rise of supply chain attacks, where attackers target vulnerabilities in third-party vendors and suppliers to gain access to an organization's network.

Other considerations as to why an organization may be targeted include

Data They Are Holding: The more valuable the data, the more likely they are to be targeted.

Financial Interests and Assets: Larger companies can often pay ransoms as opposed to smaller organizations.

How Public Facing They Are: If an organization is often in the public domain and is high profile and well known, the more likely they would be to pay ransoms and extortions.

Political, Conflicts, Type of Organization, and Other Interests: For example, anti-abortion activists targeting a new abortion clinic, pro-Israel supporters targeting Hamas, etc.

Partner Organization Is Breached: An organization (outside of your control) is breached who held some data (even just emails) from your organization. Attackers then target your organization as part of the wider exposed data set.

Low-Hanging Fruit: Your organization may be classified as low-hanging fruit; that is, you may have a lower level of security maturity compared to other organizations. Attacks can often be opportunistic, and attackers are always after the path of least resistance. If you are running known insecure or legacy systems, the more risk-exposed the organization will be to cyberattacks.