THE CYBER SAVVY BOARDROOM

Essentials Explained

HOMAIRA AKBARI
SHAMLA NAIDOO

netskope

THE CYBER SAVVY BOARDROOM

Essentials Explained

By HOMAIRA AKBARI and SHAMLA NAIDOO

Published by Netskope and Early Adopter Research
2585 Broadway, Box 111, NY, NY 10025

First Edition: September 2023

ISBN: 979-8-35092-080-2

Table of Contents

CHAPTER 1. BUILDING A CYBERSECURITY KNOWLEDGE BASE 15
Businesses Are More Connected Than Ever 16
The Need for Cybersecurity to Keep Up 17
The Stakes Are Now Higher 20
The Anatomy of the Digital Landscape 21

CHAPTER 2. UNDERSTANDING THREATS AND ATTACKERS, AND HOW THEY CREATE RISKS 25
Attacker Motivations 26
Attack Targets 28
Attack Vectors 33
Threat Intelligence: Tracking the Attackers 37
Assessing the Quality of Threat Intelligence 38
Making Use of Threat Intelligence 39
The Standard Playbook for Mounting Attacks 40
Key Questions for Decoding an Attack 40

CHAPTER 3. IDENTIFYING AND ADDRESSING CYBERSECURITY RISK 43
Understanding Cyber Materiality 45
Assessing Risks of New Technologies 46
AI-specific Cyber Risks 47
The Role of Cyber Insurance 49

CHAPTER 3 APPENDIX. REAL-WORLD EXAMPLES OF THE SEVEN RISK CATEGORIES 51

CHAPTER 4. THE DEFENSE ECOSYSTEM: PROTECTION 59
Key Elements of Cyber Protection 61
Infrastructure & Cloud Protection 61
Reducing Infrastructure Complexity 63
Endpoint (User-controlled Devices) Protection 64
New Technologies Protection 65
Enterprise Application Protection 65
Data Protection 67
People Protection 68
Suppliers Oversight 68

Supporting Security Capabilities **70**
Identity and Access Management Capabilities 70
Other Supporting Capabilities 70
Containment Strategy **71**
Key Categories for Containment Planning 71

CHAPTER 5. THE DEFENSE ECOSYSTEM: DETECTION, RESPONSE, AND RECOVERY **73**
Detection **73**
Incident Management **74**
Response **75**
Recovery and Resilience **75**

CHAPTER 6. OPTIMIZING A CYBERSECURITY PORTFOLIO **77**
Technology Architecture **77**
Vendors **78**
Portfolio Management **78**
Testing Strategy to Validate the Cybersecurity Posture **81**

CHAPTER 7. MEASURING EFFICACY AND MATURITY **85**
Operational-level Metrics **86**
Consolidate and Correlate Metrics to Amplify Value 88
Board-level Metrics **88**
Assessment of Cybersecurity Culture 89
Assessment of Cybersecurity Program Efficacy and Regulatory Compliance 91
Assessment of Cybersecurity Threat and Enterprise Risk Profile 91
Assessment of Investment Levels and Insurance Coverage 91
Assessment of Organization's Readiness to Manage Cyber Breach Impact 92

CHAPTER 8. CLOSING THOUGHTS AND REFLECTIONS **95**

GLOSSARY **101**

Acknowledgements

We wish to thank the following individuals for their contributions to this book.

Daniel Barriuso — Global CISO, Banco Santander

Hollis W Hart — Former President, International Franchise Management, Citi; Trustee Committee for Economic Development; Senior Fellow, The Conference Board

Stephane Lenco — VP, Global CISO, Thales Group

Maria Lewis Kussmaul — Founding Partner; Leader in Investment Banking and Head of Cyber Security, AGC Partners

David X Martin — CEO, David X Martin, LLC

David Platt — SVP & CSO, Moody's Corporation

Beth Stewart — Founder and CEO, Trewstar Corporate Board Services

Steve Weber — Partner, Breakwater Strategy

We also wish to extend special thanks to Netskope for sponsoring the cost of publishing this book and to the Netskope team for their invaluable insights.

About the Authors

Homaira Akbari is an award-winning business leader with a focus on cybersecurity, IoT, and AI. She has spent 12+ years of her career managing P&L and 12+ years in strategic and M&A advisory roles to corporations and private equity. She was President and CEO of SkyBitz Inc., COO of Liberty Media — TruePosition, Head of EMEA partner specialist sales of Microsoft, and held senior management roles at Thales. She was Associate Scientist at European Center for Nuclear Research (CERN). She is currently CEO of AKnowledge Partners and serves on several large publicly traded corporate boards. She holds a Ph.D. in particle physics from Tufts University and an MBA from Carnegie Mellon Tepper School of Business. She is a faculty member of cybersecurity at DCRO Risk Governance Institute.

Shamla Naidoo is a technologist, innovator, economist, law professor, and business leader with decades of experience in cybersecurity. She currently serves as a non-executive director for multiple domestic and international companies, Head of Cloud Strategy for Netskope, and an adjunct professor of law at the University of Illinois, Chicago. Previously she was global CISO and Head of Information Technology Risk at IBM. Applying her experience in the healthcare, finance, hospitality, energy, and manufacturing sectors, Shamla advises governments and industry on how to embrace innovation while managing risk. She has led cybersecurity programs for some of the most targeted companies in the world and has worked effectively with boards in many industries.

This book is dedicated to security and network leaders who collaborate every day to protect their companies and people.

Why We Wrote This Book

As the significance of cybersecurity has become more widely recognized, we have had the opportunity to serve on various corporate boards. In these roles, we assist companies in overseeing their digital agendas, focusing on cybersecurity capabilities, risk management, and performance.

We wrote this book because over and over in board of directors' meetings around the world, we saw board members and CEOs struggle to have meaningful conversations about cybersecurity. Basic terms and concepts were not well understood or had variable interpretations.

The importance of getting cybersecurity right cannot be overstated, as the consequences of failure can range from large-scale disasters to minor nuisances. A large-scale example is the 2017 massive data breach of a major credit reporting agency, affecting approximately 147 million people. The breach exposed sensitive personal information, including Social Security numbers, birth dates, addresses, and driver's license numbers. The incident was attributed primarily to a failure in patch management and inadequate security controls. This breach led to legal repercussions and severe financial and reputational damage for the company, as well as identity theft risks for millions of affected individuals.

Businesses may also experience smaller-scale nuisances like ransomware attacks or phishing scams. While these incidents may be recoverable, they can still disrupt operations, consume valuable resources, and damage a company's reputation. For instance, a small business may be locked out of its systems temporarily due to a ransomware attack, resulting in lost revenue, frustrated customers, and expensive remediation.

To fully leverage digital transformation and its potential for business growth, leaders in boardrooms must possess a practical, foundational understanding of cybersecurity. Such knowledge is crucial for all business owners, including small businesses that often lack the resources to

implement robust security programs or withstand cyberattacks. Providing board members with the necessary cybersecurity knowledge will enhance businesses' capacity to embark on successful digital journeys. We recognized the potential for bringing greater clarity to our industry by outlining a clear explanation of the cybersecurity landscape that effectively organizes the topic, provides a coherent structure, and lays the groundwork for future learning.

For us, this book is an act of giving back to worldwide communities of professionals who care to make the world more secure and equitable for everyone. We are not receiving any compensation for writing this book; instead, we aim to make a positive impact on the community, fostering a safer digital world for all.

While we wrote this book primarily for board members and corporate executives, we believe that other audiences, such as small businesses, family offices, not-for-profit organizations, and public sector leaders can also benefit from it.

We hope that you find our book useful.

— Homaira Akbari and Shamla Naidoo

Chapter 1. **Building a Cybersecurity Knowledge Base**

Cybersecurity encompasses the comprehensive defense of an organization, its people and assets, from cyber threats. With the exponential growth of digital assets, cyber threats have escalated to become one of the significant areas of business risk. Consequently, this topic has become an imperative at both the C level and board-of-director level, where the fiduciary duty of care now involves oversight of an increasingly vast digital asset portfolio. The duty of loyalty requires the board of directors to prioritize the company's interests above all else, including personal interests. This requires managing resources effectively to ensure that investments promote growth and success of the business. Every dollar spent on recovering from a cyberattack detracts from potential growth; therefore, the board of directors must strategically invest to minimize the likelihood and impact of such threats. However, cybersecurity should not be considered purely as a cost center for the business, but instead as an enabler that creates customers' trust in the organization and drives customer loyalty.

Today's cybersecurity concepts can be daunting for board members who are more versed in traditional disciplines such as finance, sales, and human capital management. The varying degrees of cybersecurity knowledge among board members can often lead to frustrating discussions. Every board member recognizes the need for greater cybersecurity understanding, particularly in light of developments such as the U.S. Securities and Exchange Commission's (SEC) new cybersecurity disclosure rules. But the technicality and ever-evolving nature of the subject, with its rapidly changing concepts, can breed complexity and confusion. Detailed yet overly technical explanations from CISOs and CIOs may not effectively aid the board of directors in their critical governance role: ensuring organizational safety and effective risk oversight.

Much board-level education today fails to provide a good foundation in the essentials of cybersecurity. While many publications offer basic best practices and "lists of questions to ask your CISO," they lack structured guidance on interpreting answers and facilitating discussion beyond

recent accomplishments or status reports. Board members need to know what good governance looks like across every dimension from cyber risk to threat prevention. Our book aims to bridge the gap between cybersecurity and board of directors' governance, providing board members and other stakeholders with a model of what cybersecurity operators do, why they do it, and how they accomplish their objectives for mitigating risk.

We have deliberately chosen not to mention any specific cybersecurity vendors by name because our intent is to maintain neutrality. It is our opinion that CISOs are best positioned to evaluate and implement the technologies and practices that will most effectively address their company's specific risk profile and objectives. Furthermore, while we offer guidance and best practices for board members, as well as examples of effective cybersecurity measures and metrics, we do not delve into the details of technology stacks or prescribe a one-size-fits-all approach for a best-in-class cyber program. By focusing on principles and strategies rather than specific products or vendors, our goal is to provide a comprehensive and adaptable framework and foundational knowledge for robust cybersecurity governance across diverse industries and organizations. We believe that this book, combined with board members' professional and life experiences, will equip them to better supervise cybersecurity risk and discharge their fiduciary responsibilities.

Businesses Are More Connected Than Ever

There is no going back to the world before digital connections; connectivity is now intrinsic to business operations and automation. Businesses have embraced digital transactions and infrastructure to increase speed, scale, and capabilities to remain competitive and foster innovation. They have reached a state of hyperconnectivity where traditional network and security perimeters have disappeared, and the branch office has been replaced by a distributed environment where people access data and company resources from anywhere, using any hyper-connected device.

The Need for Cybersecurity to Keep Up

Board members must understand that it is impossible to create fully secure software and infrastructure. The expanding digital footprint, coupled with emerging technologies such as generative AI and quantum computing, only amplify the challenge. Cybersecurity attacks are an inevitable risk.

EVOLUTION OF BUSINESS ENVIRONMENT

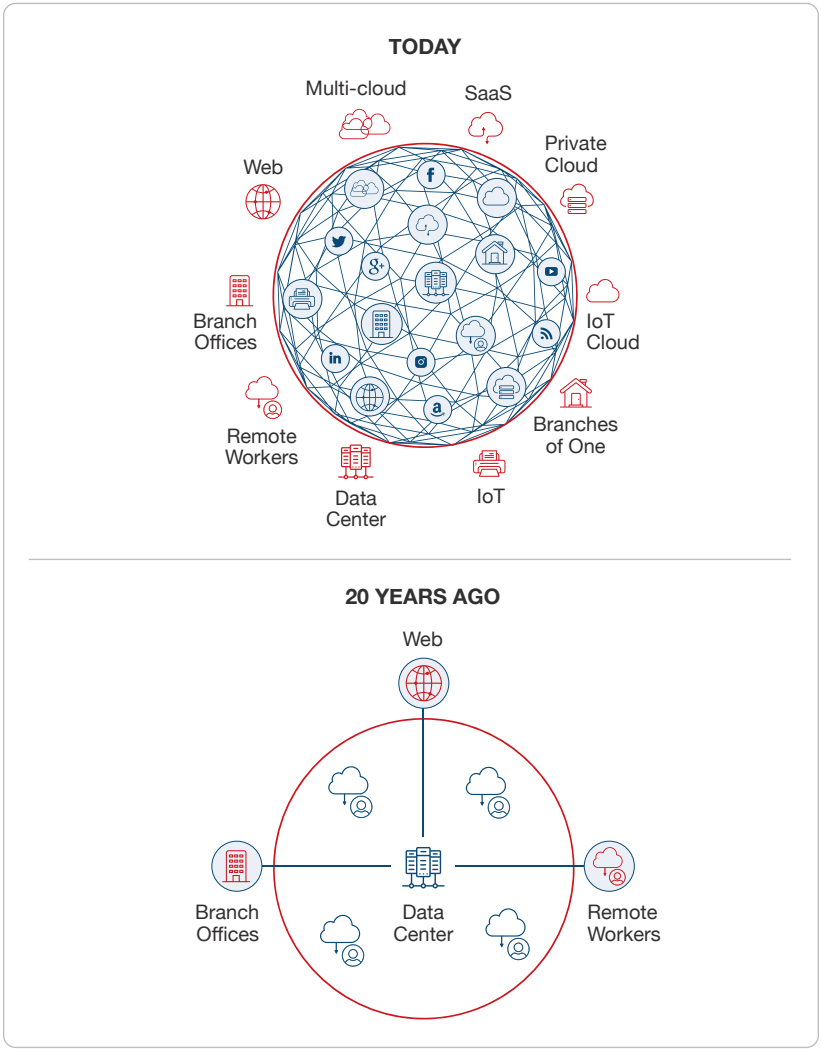


Figure 1. Evolution of Business Environment to a Hyper-connected and Complex Architecture

Attackers need to find only one vulnerability to successfully breach an organization. Vulnerabilities often originate in software, hardware, and people. The number one cause of cyber breaches is the compromise of a user's credentials. The techniques are so advanced that even the most knowledgeable people may be scammed. It is more important than ever for organizations to foster a strong cyber-aware culture.

As companies pursue their digital agendas, they create large footprints of technology assets that naturally increase the risk of cyberattacks against those assets. This, in technology terms, is often referred to as the growing attack surface. What is different about digital and cyber exposure is that the damage can be universal, and the speed and scale of a cyberattack can be exponential. While, previously, in a physical world, an attack was localized and the damage was contained. Companies must ensure that they continuously improve their cybersecurity defense including protection, detection, and mitigation capabilities and evolve to cover new and growing portions of the attack surface. Cybersecurity and technology resilience are essential to reap the benefits of digitization fully and safely.

As companies pursue their digital agendas, they create large footprints of technology assets that naturally increase the risk of cyberattacks against those assets.

In the past, cybersecurity architectures were modeled after traditional business and information technology (IT) environments. They were comprised of siloed organizations, processes, infrastructure, data, and IT systems, primarily housed on-premises or in company-controlled data centers. Crown jewels — a term used to describe the company's most important assets such as intellectual property, valuable data, or critical infrastructure — were protected by digital and physical perimeters, with access restricted to only a select group of privileged individuals whose actions were not subject to further verification.

Modern cybersecurity operates on the fundamental principle that no system element can be considered inherently trustworthy. This concept, commonly called Zero Trust, is increasingly important as cybersecurity

threats continue to evolve. While not all companies have implemented a Zero Trust architecture, it is essential to consider this concept when designing a modern architecture that is capable of authenticating each asset, including users, devices, networks, applications, and workloads. Even after initial authentication, access is continually monitored and verified, based on changing context, location, network, and other factors.

In the face of rapid technological progress such as application programming interfaces (APIs), Internet of Things (IoT), Artificial Intelligence (AI), container technologies, and quantum computing, companies must adapt quickly to remain competitive in today's complex and interconnected business environment. Implementing a Zero Trust security approach can help organizations secure the use of these technological innovations.

There is no better recent example of the rapid and sweeping impact of emerging technologies on businesses and governments than generative AI, which burst onto the scene with OpenAI's launch of ChatGPT in November 2022. Within just two short months, ChatGPT took the world by storm, with organizations and government entities alike rapidly adopting it as groundbreaking technology and laypersons getting access and a firsthand look at what generative AI can do. In Chapter 3, we will discuss the cyber risks that accompany the introduction of new technologies, using AI as a prime example.

A challenge with each new technology is how it brings unique cybersecurity vulnerabilities that companies must mitigate to safeguard their business assets. Companies require the products and services of multiple cybersecurity vendors — dozens or in some cases more than a hundred — each with expertise in different cybersecurity domains or technologies, to ensure proper security measures are in place. For example, a typical tier one bank spends between $500 million to $1 billion annually on its cybersecurity program and may have 80-150 cybersecurity vendors. While this can increase the complexity of the cybersecurity landscape, it's currently an essential strategy to proactively combat emerging threats and maintain uninterrupted business operations.

Today's large enterprises allocate an average of 5–10 percent of their information technology budget to cybersecurity. Smaller companies may have to spend even larger percentages. Regardless of a business's size, cybersecurity must be viewed as a critical investment. Continuous improvement and evolution of business asset protection are necessary.

BUT WHEN IT COMES TO CYBERSECURITY, WHAT DOES IT MEAN TO TRULY BE SECURE?

In cybersecurity, it is essential to acknowledge that there is no such thing as 100 percent effective security. Despite the best efforts and investments, no organization can ever be completely immune to cyber threats. This stems mainly from the ever-shifting threat landscape, where new vulnerabilities emerge, and threat actors devise increasingly sophisticated techniques to exploit those vulnerabilities. Recognizing this reality is the first step toward developing a robust and proactive cybersecurity strategy that prevents attacks it can and defends against attacks it cannot prevent.

At the same time, it is important to invest wisely and not overspend. A sustainable cybersecurity investment approach can help prepare a company for a rapidly changing digital future. In Chapters 4, 5, and 6, covering the Defense Ecosystem and portfolio optimization, we will discuss the cybersecurity technology portfolio and the benefits provided.

The Stakes Are Now Higher

The financial impact of cybersecurity breaches has risen, and board members have a fiduciary responsibility to ensure that their companies effectively defend against and manage the risks and consequences of cyber threats.

The cybersecurity industry is also adapting to meet the challenges. It is now possible to create a comprehensive portfolio of products and establish frameworks, policies, processes, security teams, and training programs to safeguard a company's assets, including its most precious

assets, i.e., its crown jewels. Cyber insurance is an additional valuable tool for companies that offer risk coverage in the event of a breach.

If an organization chooses to invest in cybersecurity and remains vigilant, it significantly reduces the probability of suffering a successful cyberattack. Conversely, if an organization neglects cybersecurity, it is almost inevitable that they will eventually fall victim to a cyber incident with potentially devastating consequences. It is crucial for organizations to adopt a proactive risk-based approach to cybersecurity, accepting that perfect security is unattainable but striving to minimize the likelihood and impact of cyber threats.

How then can board members determine whether their company is taking the necessary measures to protect itself? To us, at the core of this question is the responsibility of every board member to set an appropriate level of risk appetite for managing risks within the company's control. Evaluating whether the company is making the right level of investments, both financial and non-financial, in protecting and defending itself is a key component of this responsibility. Although perfect security outcomes are not guaranteed, nor are all security threats preventable, striving to minimize cybersecurity risks is crucial to building confidence in a digital world.

The Anatomy of the Digital Landscape

The technology landscape at even moderate-sized companies is complex. Board members need not be experts in every technology but should have a basic understanding to inform their risk perspective. To begin addressing cybersecurity, board members must first understand the assets that are targets of cyberattacks and need to be protected, as illustrated in Figure 2.

Figure 2 is more than just a visual representation of business asset groups — it lays out a taxonomy for assets that are targets of cybersecurity attacks. We will expand on this framework in later chapters to help board members build a meaningful understanding of cyberattacks' targets, type of attacks on each, ways to defend each separately and collectively, and the metrics that can be used to measure the effectiveness of the cybersecurity program. Our aim is to provide a visual representation of how to understand and examine

this body of cybersecurity knowledge and have more-informed conversations with security teams using this knowledge.

The most practical approach for board members to examine cybersecurity and its essential elements is to adopt a risk-based approach. Figure 3 presents different elements of a cybersecurity cycle, which involves identifying potential threats to an organization's

BUSINESS ASSET GROUPS

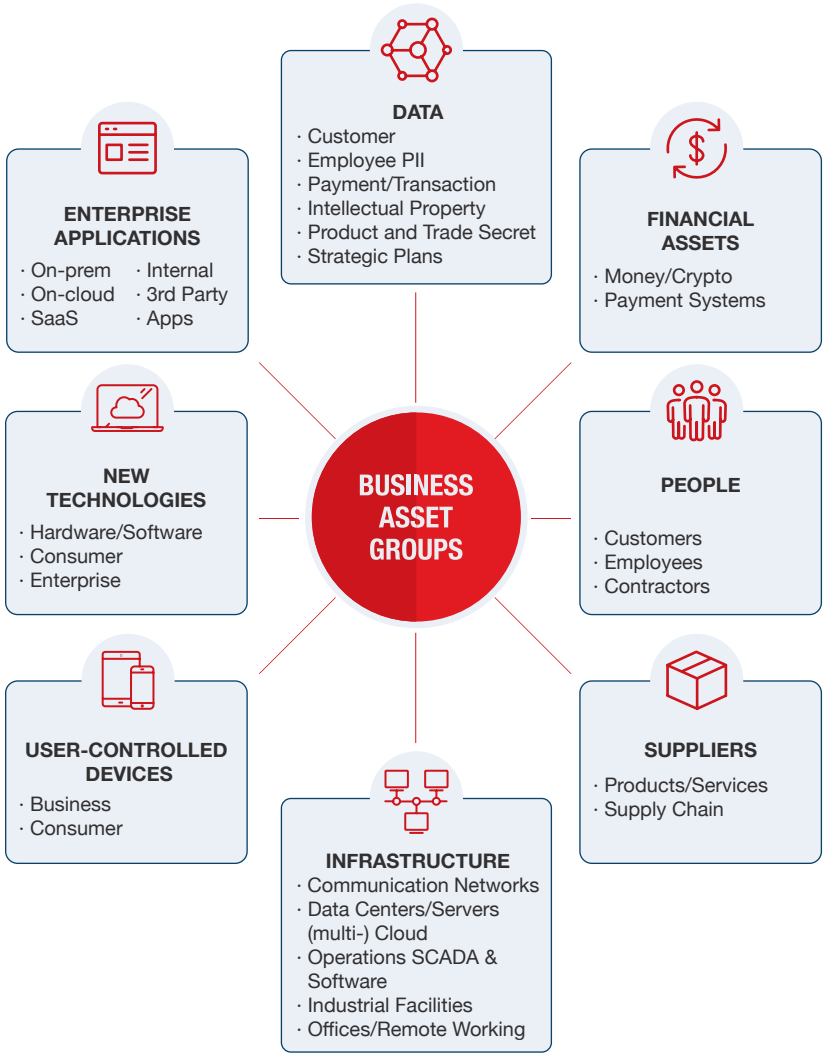


Figure 2. Map 1 – Business Asset Groups

key assets, assessing the risks of successful attacks, and determining strategies and the appropriate level of investment to protect, detect, and respond to these threats, and lastly having a plan to recover from the damages caused. This cycle is a valuable resource for board members to bear in mind as they navigate their organizations through these challenges.

Another question that often comes up is whether the organization should play offense as part of its defense. Some people believe that organizations should practice offensive security but typically corporations don't engage in the attack-first strategy. We don't cover any offensive security techniques in this book. However, they can be very effective in some circumstances, for example, when utilized for national security.

Figure 3 can be used as a reference for understanding the underlying cybersecurity structure, and the methods to manage threats and attacks.

CYBERSECURITY CYCLE

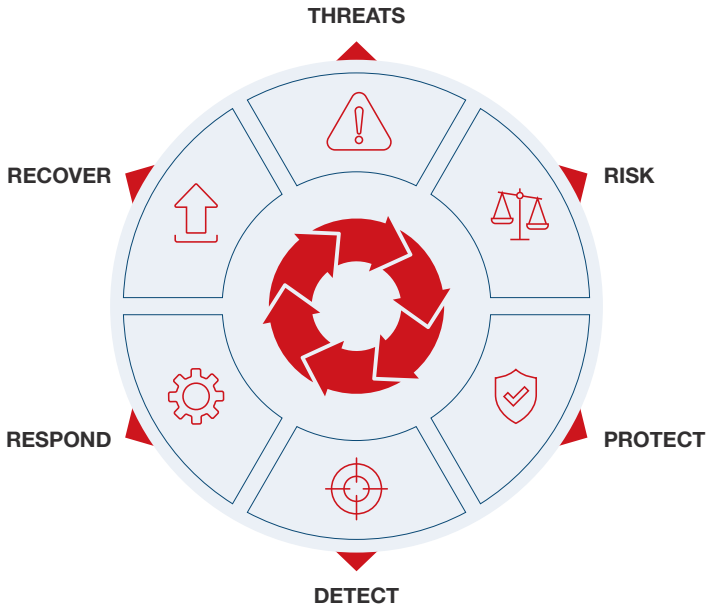


Figure 3. Cybersecurity Cycle

Chapter 2. **Understanding Threats and Attackers, and How They Create Risks**

A comprehensive understanding of the cybersecurity landscape includes knowledge of attackers' motivations, the types of attackers, and their methods of attack. In this chapter, we will explain threats and attackers, and explore ways to anticipate and manage potential threats posed by attackers. In the context of cybersecurity risk management, there are three lines of defense, each being a foundational element to the cyber risk management model.

- **First line of defense:** The risk identification and building the appropriate controls
- **Second line of defense:** The oversight of the risk management and control processes, including risk assessment and compliance procedures that are built into the technology and operations
- **Third line of defense:** The independent assurance that the risk is monitored and properly managed within enterprise risk appetite

There are no standard cybersecurity organization structures or definite ways to distribute the responsibilities within these three lines of defense to security teams. Security teams and CISOs typically provide the first line of defense and participate in the second line of defense. It is wise for boards of directors to understand how the traditional three-lines-of-defense model applies to security and define the most effective place to leverage the security team. For example, if an organization has constant outages with high system downtime, the company may want its security team to be the operational owner of the systems in the first line, whereas a company with numerous regulatory compliance failures may want the security team to participate in being a member of the second line of defense to ensure the controls are built properly.

In the context of cybersecurity risk management, there are three lines of defense, each being a foundational element to the cyber risk management model.

Attacker Motivations

The most significant change in threat actors over the past decade is how organized and structured many have become. Despite the efforts of governments, private sector vendors, and law enforcement to stop them, these groups continue to operate, and even to flourish. Many hacker groups today operate like corporations, with hierarchies, decision-making structures, and partnerships. They have forums for sharing knowledge, conferences, special interest groups, publishing research, and support groups.

While the potential for financial gain is a significant motivator for skilled engineers and computer scientists, it is not the only factor that drives individuals to become hackers. Examples of such non-financial factors are:

- Hacking provides an intellectually stimulating challenge with fame and recognition.
- Prosecution is difficult, laws are complex and varied, the burden of proof is high, and cross-country prosecution is limited and often impossible.
- Cyber warfare offers a new way to gain political, economic, and tactical advantages in a digital-first world.

The motivations that drive hackers to attack businesses and governments fall into five major categories:

- Financial gain
- Competitive gain
- Reputation damage
- Ideological promotion
- National security compromise

The ecosystem of hackers includes white-hat hackers, who are ethical hackers working to identify vulnerabilities in systems and networks; black-hat hackers, who use their skills for malicious purposes to gain unauthorized access and cause harm; and grey-hat hackers, who operate in a grey area between the two, using their skills to expose vulnerabilities without malicious intent. It's important to note that any individual attacker may have a mix of motivations, and the boundaries among the different types of hackers can be fuzzy at times. Nevertheless, understanding the motivations behind cyberattacks can

ATTACKERS, THEIR MOTIVATIONS, AND ATTACK METHODS

WHY ➡ • **Financial gain**

WHO ➡ • Hackers • Organized criminal groups • Malicious insiders

HOW ➡
- Stealing money through unauthorized access to financial accounts and/or money transfers.
- Leaking sensitive personal credentials to commit acts such as credit card fraud and/or sellingthem on the dark web.
- Demanding ransom payment by encrypting or locking an organization's access to data assets.

WHY ➡ • **Competitive gain**

WHO ➡
- Black-hat hackers (operating on behalf of corporate competitors)
- Malicious insiders • Nation-states

HOW ➡
- Stealing proprietary information such as product trade secrets to gain a competitive advantage, personal financial gain, or national advantage.
- Disrupting a competitor's operations to cause financial and reputation damage.

WHY ➡ • **Reputation damage**

WHO ➡ • Grey-hat hackers • Black-hat hackers

HOW ➡
- Exposing and publishing vulnerabilities about a company's systems to damage its reputation.
- Sometimes operating within legal limits but generally not with a positive intent.

WHY ➡ • **Ideological promotion**

WHO ➡ • Hacktivists

HOW ➡
- Attacking a company's public-facing assets such as websites, through defacement or attacks that make the website unavailable, to promote a specific message related to social, ideological, religious, or political causes.

WHY ➡ • **National security compromise**

WHO ➡ • Nation-states (directly or through sponsorship of criminal groups)

HOW ➡
- Compromising critical infrastructure such as electric grids to affect the economy, halt the operations of companies and state(s).
- Espionage such as breaking into sensitive government databases or foreign election interference by spreading disinformation.
- Similar to the tactics used by nation-state intelligence agencies and cyber warfare operatives.

Figure 4. Attackers, Their Motivations, and Attack Methods

help organizations better prepare for and prevent potential breaches. In Figure 4, we have illustrated who are the hackers behind each type of motivation and typical examples of how they achieve their goals.

Who the attackers are and what motivates them is a critical dimension of cybersecurity. Every company will have a different mix of attackers and motivations. By understanding the mindset and tactics of attackers, board members can better understand the specific exposures their company is facing, and the measures that the company is taking to mitigate these exposures.

Attack Targets

Hackers generally target an organization's crown jewels, which are its most valuable assets. To get to these crown jewels, hackers often exploit a perceived weak link in a company's defenses. Any device, system, or person can be the conduit to access or create the conditions to gain control of the company's infrastructure or systems. For example, people, including senior leaders, are targets because hackers can trick them into providing their credentials that lead to accessing the company's systems and in turn its crown jewels. Credentials are a key target because, once gained, they can be leveraged to mount successful attacks on other targets. Data is a target because its value can be monetized, and news of data exfiltration can cause immediate damage to business reputation. Critical systems are a target because, once breached, they can result in operational and business disruption.

The crown jewels of an organization typically consist of three categories of assets as illustrated in Figure 5:

- High-value data
- High-value business systems
- Other high-value assets

Having a good grasp of what comprises a company's crown jewels is essential for making informed decisions about cybersecurity priorities and budget allocations. Understanding how cyberattacks are executed can help board members appreciate the role of specific products and services as part of a broader cybersecurity program. In Chapters 4 and 5, covering the Defense Ecosystem, we will expand on how to defend against these attacks.

CROWN JEWELS OF A COMPANY

HIGH-VALUE DATA

PEOPLE DATA	• Personal and biometric information • Protected health information (PHI) • Personally identifable information (PII) • Social Security numbers (SSN)
TRANSACTION DATA	• Credit/debit card information • Online banking credentials • Loyalty points (hotel points, airline points, retail points)
INTELLECTUAL PROPERTY DATA	• Trade secrets and proprietary information • Products, inventions, and strategic plans

HIGH-VALUE BUSINESS SYSTEMS

PHYSICAL INFRASTRUCTURE	• Critical infrastructure: water, energy, etc. • Manufacturing sites • Communication network
APPLICATIONS	• Critical business applications and services • Customer relationship applications • Profitable business lines

OTHER HIGH-VALUE ASSETS

FINANCIAL ASSETS	• Critical financial infrastructure such as banks, SWIFT • Banking or other financial accounts • Actual money and cryptocurrency
INTANGIBLE ASSETS	• Reputation and public faith • Brand equity

Figure 5. Typical Crown Jewels within a Company

Key Definition: Vulnerabilities. Vulnerabilities are weaknesses in a company's technology environment that attackers can exploit. The weaknesses are generally introduced by one or more of the following:

- Leaving gaps in how technology and infrastructure are configured
- Service providers and partner weaknesses
- Known or unknown commercial software and hardware vulnerabilities
- Free and open-source software vulnerabilities
- How people use the systems and processes, leaving open doors behind

Vulnerabilities in commercial products such as software, servers, or firewalls may be known or unknown. A known vulnerability is an exploitable weakness in a system, application, or device that has been identified and made publicly available. Examples are servers that are obsolete and should have been replaced or flawed website software code that enables unauthorized access to usernames, passwords, and encryption keys. Code written to fix such vulnerabilities is referred to as a patch.

A known vulnerability is an exploitable weakness in a system, application, or device that has been identified and made publicly available.

Unknown vulnerabilities, also called zero-day vulnerabilities, are particularly dangerous and difficult to defend against because they are unknown to the software vendor and security community at large. Such vulnerabilities are often used by sophisticated attackers, such as nation-states, who may stockpile these zero-day vulnerabilities and save them for the moment at which they can be deployed to the greatest advantage. These vulnerabilities can remain undetected for years, making them a particularly insidious threat to organizations.

Hackers are often incentivized to find vulnerabilities more quickly due to their resale value on the black market, which can reach hundreds of thousands of dollars for a single vulnerability. Conversely, there are no

standards for developing vulnerability-free software, and the penalties for releasing software with vulnerabilities are unclear or nonexistent at this time. For example, a white-hat hacker may receive hundreds of dollars for submitting a well-documented and proven vulnerability to a software developer's bug bounty program, while the same vulnerability may sell for hundreds of thousands of dollars to criminal organizations or hostile nation-states.

Another example of the vulnerability management challenge involves technology giants such as Amazon, Google, and Apple. These companies provide indispensable software solutions for user-controlled devices and cloud environments that we rely on for daily productivity. Businesses (and consumers alike) must trust these providers to maintain robust security measures to safeguard their sensitive data since access to the underlying code is restricted to the providers themselves. While having the flexibility of these services offers some advantages, the lack of code ownership or even visibility can create difficulties for businesses that need to promptly identify vulnerabilities that could potentially compromise their data security. They can rely on the technology giants to secure against threats, or companies can choose to add a layer of security outside of the environment of these service providers.

Key Definition: The Dark Web. The dark web refers to a collection of websites and online services that are not indexed by search engines and are not accessible through normal web browsers. These sites are hidden behind layers of encryption and are often used for illegal activities such as drug trafficking, weapons sales, and other criminal activities.

The dark web is accessed using specialized software, such as Tor, which allows users to remain anonymous and untraceable. This anonymity makes it a popular destination for those seeking to engage in illegal activities, as they can conduct transactions without fear of being caught.

In a data breach, the stolen information is likely to be put up for sale on the dark web. To identify potential data breaches and other security threats, law enforcement agencies and companies often conduct scans of the dark web to detect whether any sensitive information has been

compromised and made available for sale. However, for these scans to be effective, they must be performed continuously. Inadequate cybersecurity policies and procedures can limit the effectiveness of such scans and result in some threats being missed or not acted upon.

Key Definition: Ransomware. Ransomware is one of the most prevalent examples of malicious software (malware). Regardless of industry focus or size, no company or federal, state, or local government agency is immune to ransomware attacks. Hackers execute ransomware attacks to gain control of and deny access to valuable data. They typically encrypt an organization's data using an unbreakable code, known only to the hacker. As a result, critical information becomes unavailable and business operations are disrupted.

While governments discourage companies and government agencies from paying a ransom, it is often the quickest way to regain access to the data. However, paying a ransom does not always guarantee the recovery of assets, as demonstrated in the Colonial Pipeline attack that occurred in May 2021. The company reportedly paid a ransom of $4.4 million to the cybercriminals. Despite the payment, it was reported that the decryption process was slow and difficult, and the company had to rely on its own backups to restore some of the data. In this instance, recovery was actually faster through backups than decryption, making payment unnecessary. In other instances, nation-states and hacktivists design their ransomware to never allow for recovery even after payment is made.

TECHNOLOGY IS AN ESSENTIAL COMPONENT OF CYBERSECURITY, but it's important not to overlook the role of people and culture.

Even with the most sophisticated cyber defense, a lack of awareness, carelessness, or intentional malfeasance by people leads to vulnerabilities that attackers can exploit. Board members should ensure that their organization has a strong cybersecurity culture that prioritizes awareness, education, and ongoing training for all employees, including contractors and third-party vendors.

Attack Vectors

Hackers use many attack vectors — an industry term for the methods by which an attack occurs — to gain entry and control over an organization's infrastructure and systems in order to steal valuable business assets. The emergence of new infrastructure or new enterprise application models, such as cloud or SaaS applications, introduces new attack vectors that hackers can exploit. As cybersecurity systems evolve to address these emerging attack vectors, malicious actors shift their focus to less defended attack vectors that permit them to bypass countermeasures. Awareness of existing and emerging attack vectors is essential, as is continuously updating cybersecurity measures to defend against them.

In the upcoming sections, we will demonstrate how companies are attacked, describing the most common attack vectors, vulnerabilities, and the reasons why vulnerabilities occur. In Figure 6, we list the common attack vectors targeting each business asset group.

Attackers often succeed because of vulnerabilities in existing software or mistakes in configuration. Common vulnerabilities that hackers target in any organization are:

- **Network vulnerabilities** such as allowing broad east/west access, which refers to the ability for traffic to move laterally within a network from one system or application to another, can enable attackers to move freely within a network, accessing and exfiltrating sensitive data.
- **Weak identity and access management** such as granting excessive privileges and not having disciplined sunset provisions to disable/revoke access privileges.
- **Defects in software and platforms** such as Microsoft Office 365, Salesforce.com, or Google Workspace that can be exploited by attackers.
- **End-of-life/obsolete hardware and software** that are no longer supported and can no longer be patched.
- **Idiosyncratic vulnerabilities** stemming from a company's unique infrastructures such as a custom application or an unusual branch office configuration that can be exploited by attackers.
- **Third-party vendors** often have access to sensitive data and systems, but may have weaker cybersecurity defenses than the organization itself.

COMMON ATTACK VECTORS TARGETING BUSINESS ASSET GROUPS

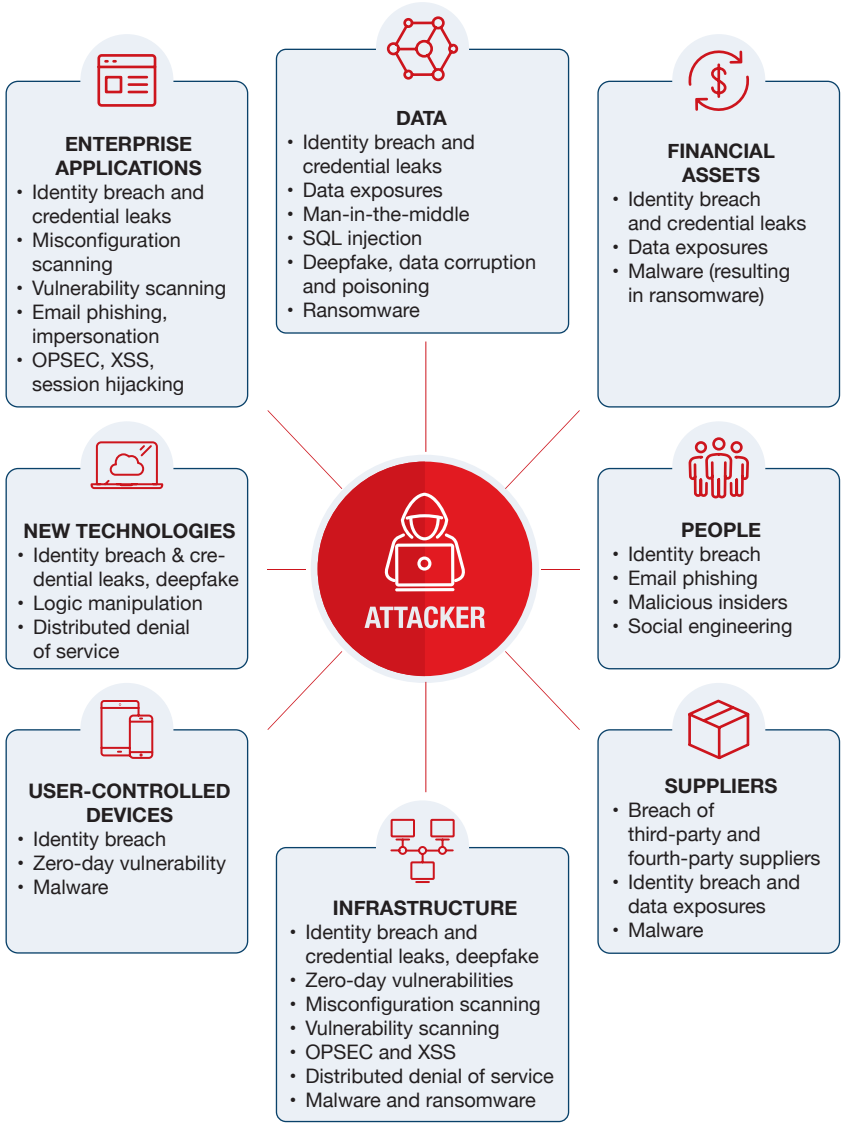


Figure 6. Map 2 — Common Attack Vectors Targeting Business Asset Groups

These vulnerabilities occur because of a number of inadequacies in the company's processes, policies, and systems. The most common examples are:

- **Inadequate IT administration:** Lack of knowledge, resources, expertise, and time to secure systems.
- **Inadequate cybersecurity controls:** Lack of good controls such as insufficient access control, lack of software updates and patches, lack of security penetration testing.
- **Poor design:** Lack of collaboration among development, operations, and security teams resulting in poor software design that has vulnerabilities.
- **Weaknesses in third-party technology:** Vulnerabilities outside of an organization's control, such as third-party software, cloud services, or internet-connected devices unsanctioned by the corporate security team.
- **Lack of employee training and awareness:** Employees are unaware of potential threats or lack training on security best practices.
- **Changing business environment:** Security teams may not anticipate changes in the technology environment, leaving them unprepared to protect and adapt to rapid and sudden changes.
- **Insufficient asset inventory:** Without a comprehensive Bill of Materials (BoM) or Software Bill of Materials (S-BoM), organizations may not be aware of all the software and firmware components in their environment that need to be secured or updated.
- **Accumulated tech debt:** Outdated technology and systems with embedded security flaws that have not been upgraded for a long time and that are no longer supported by the vendors, and therefore no longer upgradable.

We frequently hear from board members who have difficulty believing there is no comprehensive cyber defense solution. The primary reason for the lack of such a solution is that most businesses have, over many years, built their embedded technology infrastructure without sufficient consideration for cybersecurity. This oversight has led to a long list of inherent vulnerabilities that can differ significantly from one company to another, even among companies with similar technology architecture.

Despite having common vendors or infrastructure, every technology environment is ultimately bespoke, with strengths and weaknesses specific to that environment. Much attention and investment may go into retrofitting security practices, but gaps and weaknesses often remain undetected and unaddressed, leaving entry points into the entire digital environment from which an attacker can spread their nefarious activity. The criticism, "If the bad guys can find and exploit vulnerabilities, corporations should be able to as well" may be common among board members, but it ignores the complex reality we described above.

Key Definition: Detection and Mitigation. Given the complexity of the modern business landscape, no portfolio of cybersecurity technology can prevent all cyberattacks. Attackers need only one weak link to successfully breach an organization. Board members must be aware that some attacks will succeed and that cybersecurity defenses can never provide 100 percent protection, a fact that cybersecurity experts may be hesitant to convey. This is why it is important to have transparent communication among both private and public sectors with the acknowledgement of gaps and weaknesses.

Therefore, a comprehensive cybersecurity strategy must include not only protective and preventive measures but also mechanisms to detect and respond to successful attacks, as well as measures to minimize the damage caused by attacks. For instance, companies can implement additional security measures for high-value targets such as a superuser account and establish advanced backup and business continuity plans to protect against ransomware attacks. We will delve deeper into these topics in the Defense Ecosystem chapter, providing guidance as to what organizations should do to have an adequate cybersecurity defense.

A comprehensive cybersecurity strategy must include not only protective and preventive measures but also mechanisms to detect and respond to successful attacks, as well as measures to minimize the damage caused by attacks.

Threat Intelligence: Tracking the Attackers

Threat intelligence is the process of gathering information to help companies understand attackers and their techniques. An effective threat intelligence program provides insights on past, current, and future attacks, and will help to anticipate and prepare for potential threats.

By utilizing threat intelligence, a company can prioritize its cybersecurity program roadmap and focus on the most at-risk areas, which include:

- Protecting the crown jewels of the company
- Identifying and resolving known and prioritized vulnerabilities
- Prioritizing security improvements for assets most at risk
- Highlighting areas where the company is least prepared for potential threats
- Adopting new cybersecurity technologies to prepare for new threats that could be most damaging to a company's operations

Automated threat intelligence, detection, containment, response, and remediation functions are core components of an organization's cyber defense. These functions anticipate and prepare for potential threats by identifying vulnerabilities, quickly detecting and isolating ongoing attacks, mitigating the attacks, and restoring normal operations. Threat intelligence helps the entire organization, including board members, be proactive. In the best-case scenario, companies can prevent attacks that would otherwise have succeeded. In the next sections, we will provide insights into how organizations optimize their use of threat intelligence to enhance their cybersecurity posture.

Assessing the Quality of Threat Intelligence

Threat intelligence is only as good as the information that is collected and how that information is used. Threat intelligence is typically constructed from various sources of analysis and data, such as internal analysis, third-party data feeds, analyst reports, and other sources shown in Figure 7.

SOURCES OF AN EFFECTIVE THREAT INTELLIGENCE FUNCTION

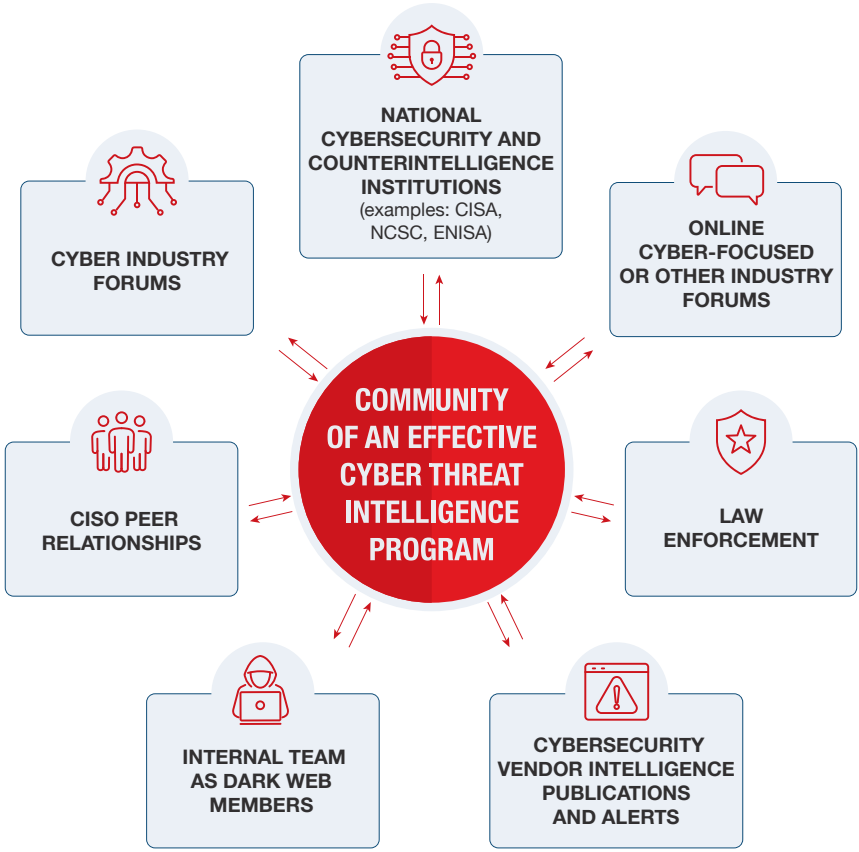


Figure 7. Sources of an Effective Threat Intelligence Function

A good sign that a company is actively using threat intelligence is when a company has an emergency protocol for taking quick action. Often called a big red button, invoking such a protocol leads to action being taken immediately and urgently upon discovering important new threat

intelligence insights. If no urgent insights have been found and acted upon, especially while others in the industry are taking action, that may indicate the company's threat intelligence is not effective.

THREAT INTELLIGENCE PAST, PRESENT, AND FUTURE

THREAT INTELLIGENCE ABOUT THE PAST AND PRESENT

A strong threat intelligence program provides board members with a review of the past performance of the cybersecurity function and the current operational status:

- Threats faced in the recent past, including changes to those threats, new threats that have appeared, threats that have dropped or diminished, and explanations of trends.
- Active threats facing the business, including a list of the most active attack vectors and their likely targets.
- The identity of hackers behind the attacks and insights into the motivations of the attackers.

By examining the data from past and present, companies can deploy better cybersecurity controls and tools, and have an enhanced readiness capability.

THREAT INTELLIGENCE ABOUT THE FUTURE

It can be difficult to predict or forecast accurately where adversaries will attack next. But companies must do scenario planning because such analysis often exposes weaknesses. This type of discovery process is one of the most critical roles of threat intelligence. Forward-looking threat intelligence and scenario planning are usually a combination of internal data and third-party analysis that provide insights about the future, such as:

- Threats that may emerge in the next 12 months.
- The potential for increased activity by certain known attackers or attacker groups.
- New motivations for hackers that may lead them to focus on certain targets.

By understanding these factors, companies can better prepare for upcoming attacks and protect themselves against potential harm.

Figure 8. Threat Intelligence Past, Present, and Future

Making Use of Threat Intelligence

A strong program of threat intelligence will likely lead the CISO to take many of the following actions that enhance a cybersecurity program:

- Hardening or temporarily disabling external entry points, such as websites that may be vulnerable to hacking attempts (For example, some banks took the precautionary measure of shutting down all their websites in Russia, Ukraine, and other relevant countries at the outbreak of the Ukraine war in 2022.)

- Segregating parts of the system under attack based on geography or by system category (For example, when an attacker targets IoT sensors to cause massive random web traffic bombarding a company's website, making the site unavailable to users, a company may choose to temporarily disconnect part or all of their IoT system.)
- Enhancing encryption and backup of data to protect against ransomware attacks
- Performing regular security assessments to identify potential vulnerabilities and risks and applying software patches to vulnerabilities immediately upon discovery
- Implementing threat hunting to proactively detect and investigate potential threats and vulnerabilities within an organization's network and systems
- Updating an incident response and crisis plan to handle new cyberattacks effectively

The Standard Playbook for Mounting Attacks

Several notable publications such as Lockheed Martin's well-known Cyber Kill Chain examines how attackers typically mount attacks. The Cyber Kill Chain describes the stages of a cyberattack, from initial surveillance to the final goal of the attacker. It is intended to help organizations understand and respond to cyber threats by breaking down the different phases of an attack and identifying potential opportunities for detection and prevention.

Many CISOs use this method to communicate attack-related updates to the board of directors. It is useful for board members to know about the Cyber Kill Chain, shown in Figure 9, because it explains an attack in sequence. Board members can ask how an attack proceeded through each of the steps in this chain to better understand an attack and how well defenses worked. The Cyber Kill Chain lists the general steps on how attacks are structured and may be reported differently at different companies.

Key Questions for Decoding an Attack

Cybersecurity attacks can be complex and may occur in a long series of stages that involve many attack vectors and target numerous crown jewels over a period of months or years. To adequately inform board members, CISOs should present answers to the following four

THE CYBER KILL CHAIN

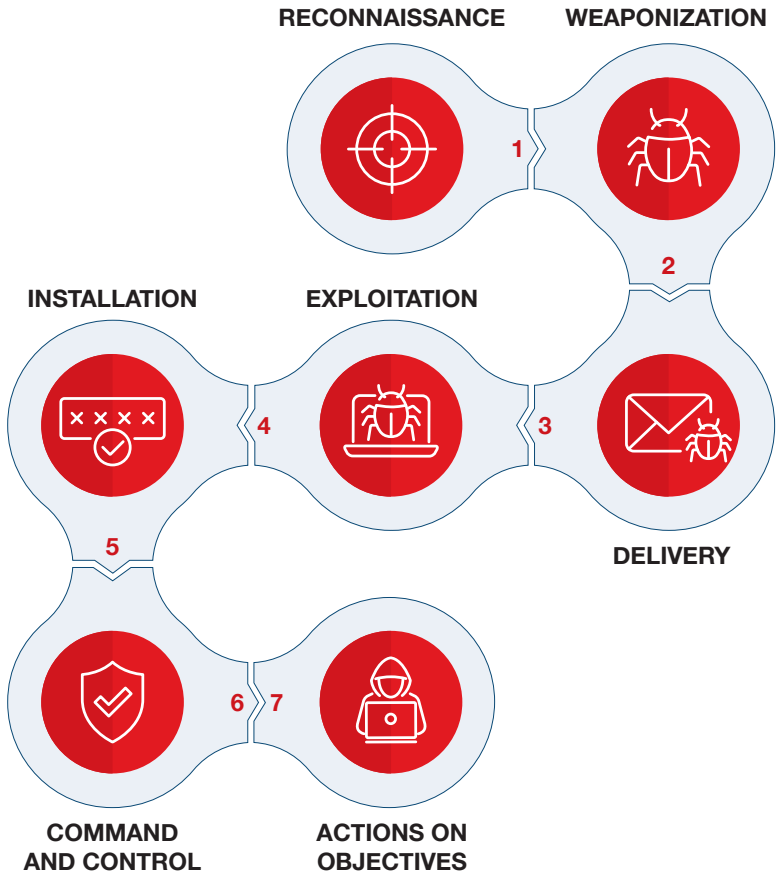


Figure 9. The Cyber Kill Chain

questions shown in Figure 10. In Chapter 3 Appendix, Real-World Examples of the Seven Risk Categories, we will show example answers for these four questions for several real-world breaches.

Explaining and analyzing complex attacks and presenting the key information enables the board of directors to engage with the company's cybersecurity roadmap both in terms of the defense ecosystem and regarding adoption of advanced tools in mitigating threats and preventing future attacks. CISOs must maintain transparency and honesty with the board of directors regarding the organization's cybersecurity posture. They should be candid about the

current state of security and be willing to admit gaps in knowledge when appropriate, using phrases like “we don’t know” or “we don’t know yet.” This open communication fosters a realistic understanding of the organization’s level of preparedness and encourages a collaborative approach to improve security measures.

FOUR KEY QUESTIONS FOR UNDERSTANDING A CYBERSECURITY ATTACK

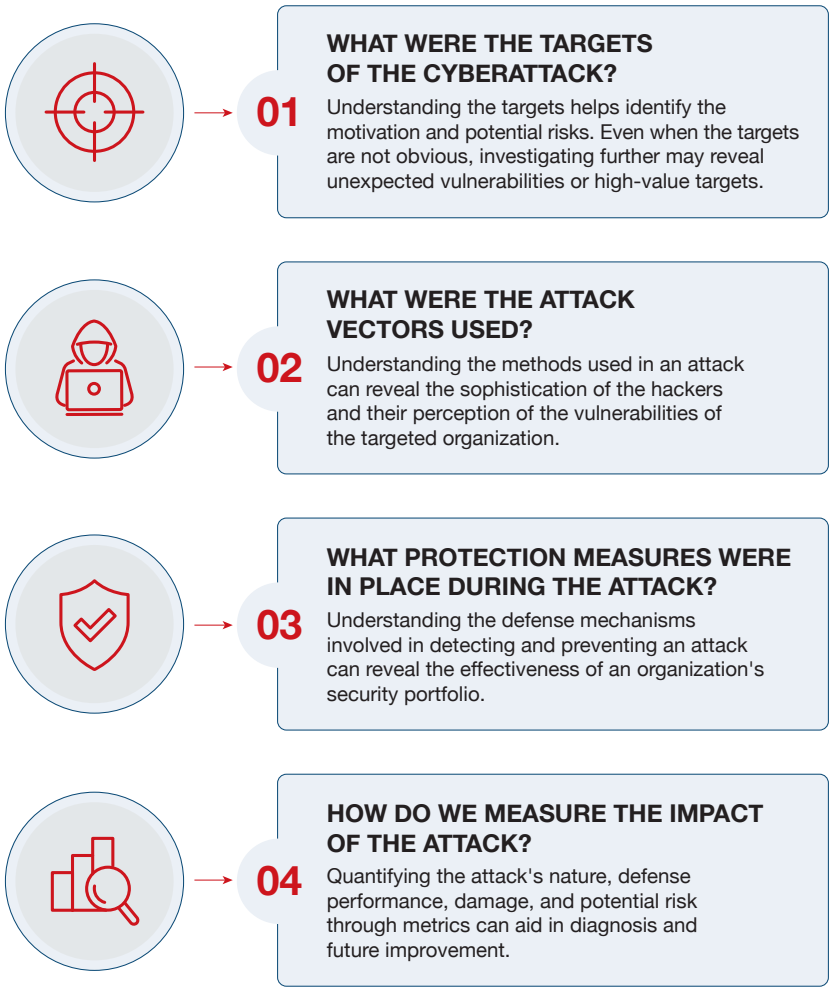


Figure 10. Four Key Questions CISO Should Answer for Board of Directors

Chapter 3. **Identifying and Addressing Cybersecurity Risk**

Cybersecurity risk is a critical component of enterprise risk management, and board members should be as familiar with assessing and managing cyber risks as they are with other forms of enterprise risk. Here, we group cybersecurity risks into seven commonly encountered categories and provide a definition for each. In Chapter 3 Appendix, we will give real-world examples for each of these risk categories.

- **Business Continuity Risk:** Disruption to an organization's operations can be caused by malicious actors who compromise hardware or software, resulting in downtime and lost productivity.
- **Data Risk:** Data can be corrupted, stolen, or misused by malicious actors or unauthorized actors. Data loss, corruption, misuse, or theft may occur because of hardware or software failure, human error, and malicious software.
- **Financial Risk:** An organization experiences a cyberattack event that results in a loss of income and value for shareholders. This may be due to cybersecurity under-investment or mismanagement.
- **Regulatory and Compliance Risk:** Non-compliance with current laws, regulations, and policies related to data privacy or cybersecurity can result in fines, penalties, and negative publicity. This type of risk can arise from under-investment in cybersecurity defense tools or inadequate policies and controls.
- **Supply-chain Risk:** When a legitimate party in the supply chain is the conduit through which a malicious actor gains access to conduct attacks on the company. This can be through building back doors into the supplier software and reporting back, or just being the weak link.
- **Brand and Reputation Risk:** This risk attaches to an organization's brand and goodwill. This includes damage to a company's reputation through public perception of its security and privacy practices and harm to customers and employees.
- **Strategic Risk:** When cybersecurity breaches result in undermining a company's strategy or loss of key intellectual property gives an advantage to the competitor.

Each of these risk categories can significantly impact the organization's financial results, competitive differentiation, employee morale, and business continuity. With an understanding of these risk categories, board members can become more effective in supervising cybersecurity risks.

In the enterprise risk function, prioritization of risks is visualized through a risk heatmap that maps the financial loss impact against the probability of a risk occurring. Cybersecurity is one of many enterprise risks that are tracked through the heatmap; companies use a range of tools to quantify the financial loss of a risk, from very sophisticated risk models to simple estimations.

To mitigate or reduce cyber risk, companies must first prioritize risks that can cause the most damage. We believe the most significant damage is done when a breach results in business continuity risk and causes partial or complete disruption to a company's ability to conduct business. This can have a major impact on a company's top and bottom lines and lead to customer losses.

We believe the most significant damage is done when a breach results in business continuity risk and causes partial or complete disruption to a company's ability to conduct business.

Data risk is another high risk for corporations. Data risk can cause financial loss, customer dissatisfaction, and significant regulatory penalties. Other high-impact risks are supply chain and regulatory and compliance risks. Interestingly, up to now brand and reputation risk have not caused substantial, long-term damage. While we acknowledge that breaches can damage a company's brand and reputation initially, the damage is typically healed quickly, as the public and companies alike have realized that breaches are a common occurrence in today's digital landscape. However, this may change over time.

Understanding Cyber Materiality

Board members are responsible for ensuring that the company makes sound decisions and trade-offs between different risks and related rewards. Understanding materiality and which risks create material impact can provide invaluable guidance to the cybersecurity team about where to focus their efforts.

Technology continuously forces traditional definitions of materiality to evolve. As we write this book, for example, the SEC adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. It's important for organizations to be prepared for such new regulations and to recognize that reporting incidents will become mandatory. The consequences of not reporting or being ill-prepared for these regulations can be severe, including increased liability, negative attention from proxy advisors and investors, and damage to the organization's reputation. As a result, organizations must ensure they are knowledgeable and proactive in their approach to cybersecurity, recognizing these are part of the practical and fiduciary duty to protect the company's assets and interests.

While not in its final ruling, the SEC offered example definitions of materiality in its proposed ruling which include incidents such as:

- Compromising the confidentiality, integrity, or availability of an information asset, or violating security policies and procedures resulting from accidental exposure or deliberate attacks to steal or alter data
- Causing degradation, interruption, loss of control, damage to, or loss of operational technology systems
- Unauthorized access or exceeding authorized access that has altered or stolen sensitive business information, PII, or IP resulting or potentially resulting in loss/liability for the company
- A malicious actor offering to sell or threatening to disclose sensitive company data publicly
- A malicious actor demanding payment to restore stolen/altered company data

While the SEC guidelines provide a useful framework, companies must prioritize the identification and management of material cyber risks that are specific to their unique situation. Adopting standardized definitions can be helpful, but companies should not rely solely on them. Instead, they should establish a documented process with clear parameters for determining material risk, ensuring that all relevant factors are considered. This approach will enable companies to set consistent standards and implement more comprehensive protection measures that will evolve over time.

When boards of directors provide clear thresholds and materiality triggers, it helps the CISO and other risk managers to provide appropriate and timely information and actionable insights needed for good board governance.

When boards of directors provide clear thresholds and materiality triggers, it helps the CISO and other risk managers to provide appropriate and timely information and actionable insights needed for good board governance.

This includes:

- The process and procedure for deciding which cyber risks are material, as well as the data used to make this decision
- Investments needed to mitigate material risk, and the trade-off between these investments and accepting a certain level of risk
- The cybersecurity investment roadmap based on the company's cyber risk profile and future threats determined through its threat intelligence program

Assessing Risks of New Technologies

Even if the current risks facing a company are well understood, adopting new technologies to support the business will keep expanding the number and types of risks a company faces. A company's cyber risk plan should accommodate a regular review of the latest technologies, what new risks they might present, and existing risks to which they may contribute.

Organizations must weigh the business value of the latest technology against potential data and business continuity risks, among other factors. These trade-offs have been made successfully in other

business categories for decades, and cyber risk trade-offs are no different.

We won't cover specific cyber threats associated with each new technology here. Many emerging technologies introduce cyber risks similar to the risks categories described earlier in this chapter. We recommend that board members ensure risk leaders conduct and document risk assessments for new technologies using established frameworks such as ISO 27005 or EBIOS RM. CISOs should include these risk assessment results in their reports on emerging potential risks.

CISOs also will use new technologies to deliver on the cybersecurity mission to protect the technology, data, and other digital assets. But while these innovative technologies provide great opportunities for security teams to automate or advance their systems, they often introduce new risks as well. One broad area in particular — artificial intelligence and machine learning (ML) — is something that board members should dig into in order to understand their inherent risks.

AI-specific Cyber Risks

AI and ML are potent tools that can perform complex tasks with automation and precision. Cybersecurity vendors use these technologies to analyze the behavior of systems and millions of events to detect and prevent attacks. However, hackers also use the power of AI and ML to their advantage.

AI can be categorized into various forms based on its capabilities, level of autonomy, and learning approaches. One of the most common forms of AI is known as Narrow or Weak AI, which is designed to perform specific tasks or solve well-defined problems. Narrow AI systems excel in their designated tasks but cannot generalize their abilities to other domains. For example, generative AI (i.e., ChatGPT, as impressive as it is) belongs to the Narrow AI category. While it is highly capable of performing specific tasks, such as generating realistic images, text, or music, it is limited to those particular domains. It does not possess the generalized intelligence or capabilities of Strong AI or Artificial General Intelligence, which refers to hypothetical AI systems that have human-level intelligence and can perform any cognitive task that a human

can do. These systems would be able to learn, understand, and apply knowledge across different domains. General AI has yet to be achieved, and it remains a subject of ongoing research and debate.

One of AI's main vulnerabilities is that it learns from data it ingests. If misleading or incorrect data becomes embedded in the AI's models, this can lead to inaccurate and deceiving outputs. This is why the top security threats for AI applications involve manipulating either the data itself or the machine learning and data models used by AI. Examples of these kinds of threats include:

- Data corruption and poisoning attacks: These occur when hackers inject bad data into ML models, leading the models to do something they should not. These attacks can have a significant impact, particularly when targeting widely used, pre-trained models which are, in turn, used by many AI developers. In this case, they are referred to as a transfer learning attack.
- Data manipulation attacks: These occur when attackers alter data from the training set or manipulate data labels or inputs, including visual and conversational data and interfaces, to create outcomes such as deepfakes, which then replace an individual's likeness in recorded videos, with potentially significant consequences.
- Logic manipulation attacks: These occur when the attacker alters the algorithm and how the model learns. The attacker can embed any logic within the AI system and then manipulate the system's decision-making process.
- Generative AI-specific attacks: While the attacks above all apply to generative AI, it is worth mentioning that ChatGPT itself has accelerated hackers' usage of AI. One of the immediate threats from ChatGPT is its formidable ability to be used to create phishing scams by conversing seamlessly with users via emails, texts, chat-boxes, or phone calls, all without the grammatical or spelling mistakes that have made earlier scams identifiable.

Board members' regular review of new technologies with the security and risk management teams should include specific sections on AI-based risks and how the company is using AI and ML models. In general, board members should not shy away from requiring in-depth examinations of the risks that may arise from new technologies, both now and in the future.

The Role of Cyber Insurance

Cyber liability insurance offers a means of transferring some of the risk and cost of cyberattacks to another party. Although cyber insurance cannot prevent cyberattacks, it can provide businesses with peace of mind and financial protection, assuming policies favor the company, are well understood, and the insurer and reinsurer are financially stable.

While it can be costly, a well-designed cyber insurance policy can cover various risks, such as data breaches, network failures, and cyber extortion. In the aftermath of a cyberattack, insurance can help cover response costs, including legal fees, notification expenses, and credit monitoring for affected individuals. It can also compensate for lost income and the costs of restoring or replacing damaged systems and data. A secondary benefit is that the insurance company is an independent party assessing how much risk a company is exposed to and whether or not they want to underwrite the company's risk.

Preparation is key to mitigating potential cyber-related events. Insurers often offer policyholders tools and resources to manage and mitigate cyber risks. Some insurers offer risk assessment tools, one-on-one consultation with a cybersecurity expert, training tools and videos to educate teams, a helpline, and access to consulting services that can help keep businesses protected. To ensure adequate coverage, organizations must carefully consider their policy options and collaborate with their risk management team. Additionally, every business must be prepared to fund activities such as:

- Forensic investigations
- Litigation expenses
- Regulatory fines
- Crisis management expenses
- Business interruption
- Cyber extortion and ransomware payments

Given the interconnected nature of businesses, companies should not overlook buying third-party coverage. It is not uncommon for a vulnerability in one system to be the point of entry into someone else's system and cause damage. Board members must understand the level of risk the company is exposed to and approve the investments

to purchase enough coverage for first-party claims and to buy additional coverage for third-party claims. Policy terms must be carefully developed and well understood. Without proper due diligence, companies may find themselves paying for coverage they thought they had, only to realize they are essentially self-insured for certain types of cyber incidents. It is important to work closely with a knowledgeable insurance broker and legal counsel to ensure the policy is comprehensive and covers the company's specific risks.

Cyber insurance is becoming more expensive as insurers adjust premiums and selectivity of coverage based on claim trends. To ensure that cyber insurance doesn't divert significant funds away from business growth and innovation, the company should develop a comprehensive budget that accounts for all cybersecurity-related expenses, including insurance premiums. By understanding the total cost of cybersecurity and evaluating the value of cyber insurance, the board of directors can make informed decisions about balancing risk and investment to protect the company's assets and promote growth.

Chapter 3 Appendix. **Real-world Examples of the Seven Risk Categories**

RISK CATEGORY: Business continuity risk	
DEFINITION:	Disruption to an organization's operations can be caused by malicious actors who compromise hardware or software, resulting in downtime and lost productivity.
REAL-WORLD EXAMPLE:	June 2017: A Dutch logistics and shipping company was the victim of highly destructive malware (malicious software).
Attack Target:	Company's IT systems.
Attacker:	Attributed to Sandworm cyber-espionage group with suspected links to Russia's military intelligence group.
Attacker Motivation:	Geopolitical targeting Ukraine with collateral damage bringing widespread chaos and financial harm.
Attack Vector:	The initial infection vector was a compromised update to M.E.Doc, a widely used Ukrainian tax accounting software. The malware then used a combination of the EternalBlue and EternalRomance exploits, which leveraged vulnerabilities in Microsoft's SMB protocol, to propagate laterally within networks. The malware also used credential-stealing techniques to gain further access to systems.
Protection Mechanism:	Unclear, however, the scale of the impact suggests that the attacked company's defenses were insufficient to prevent or mitigate the spread of the malware.
Attack Impact:	An estimated $300 million in damages. The company's shipping operations were severely disrupted, with numerous ships unable to load or unload cargo. Its port terminals and logistics services were also affected, leading to delays. Unclear if any of the damages were covered by the company's insurance since many sources classified this malware attack as an act of war.
Lessons Learned:	The company took significant steps to improve its cyber defenses and resilience. It also called for more clarity in cyber insurance coverage terms and a better understanding of the scope of protection.

RISK CATEGORY: Data risk	
DEFINITION:	Data can be corrupted, stolen, or misused by malicious actors or unauthorized actors. Data loss, corruption, misuse, or theft may occur because of hardware or software failure, human error, and malicious software.
REAL-WORLD EXAMPLE:	September 2017: A major credit reporting agency was the victim of a massive data breach that exposed the personal information of 147 million people.
Attack Target:	People's personal information, including Social Security numbers, birth dates, addresses, and in some cases, driver's license numbers.
Attacker:	A group of hackers, believed to be state sponsored, although the exact identity was not officially disclosed.
Attacker Motivation:	A combination of financial gain and espionage.
Attack Vector:	A vulnerability in the Apache Struts web application framework, which was exploited to gain unauthorized access to the company's systems and extract sensitive data.
Protection Mechanism:	Specific details about the protection mechanisms are not available; reportedly, the company failed to patch a known vulnerability in a timely manner. The company had cybersecurity insurance coverage.
Attack Impact:	The company paid $575 million (and potentially up to $700 million) as part of a global settlement with several federal agencies and 50 U.S. states and territories. As part of this settlement, the company made available up to $425 million to address potential threats and incidents of identity theft for the 147 million affected consumers.
Lessons Learned:	This breach was a wake-up call for organizations, governments, and individuals regarding the importance of data protection, and specifically proactive security measures, timely response, and ongoing vigilance to protect sensitive data.

RISK CATEGORY: Financial risk	
DEFINITION:	An organization experiences a cyberattack event that results in a loss of income and value for shareholders. This may be due to cybersecurity under-investment or mismanagement.
REAL-WORLD EXAMPLE:	May 2021: A major fuel pipeline system in the U.S. experienced a ransomware attack.
Attack Target:	Company's IT system.
Attacker:	A Ransomware-as-a-Service group, DarkSide, known for targeting organizations for financial gain.
Attacker Motivation:	Financial gain.
Attack Vector:	Not reported publicly, but most likely attackers gained access to the company's systems through a compromised virtual private network (VPN) account.
Protection Mechanism:	Public reporting is incomplete; however, the company had implemented cybersecurity measures to safeguard their systems.
Attack Impact:	Significant impact on the operations; the company proactively shut down the pipeline, causing fuel shortages, price spikes, and disruptions in the transportation and logistics sector in several states along the East Coast of the U.S. The company reportedly paid nearly $5 million in ransom, and it had cyber insurance coverage.
Lessons Learned:	It highlighted the risks that came with doing so little for so long to secure critical infrastructure, and that standard procedures for decommissioning and shutting down access points and obsolete equipment and networks would have reduced the organization's attack surface and risk of data breach in the first place.

RISK CATEGORY: Regulatory and compliance risk	
DEFINITION:	Non-compliance with current laws, regulations, and policies related to data privacy or cybersecurity can result in fines, penalties, and negative publicity. This type of risk can arise from under-investment in cybersecurity defense tools or inadequate policies and controls.
REAL-WORLD EXAMPLE:	October 2020: A European airline experienced a significant data breach.
Attack Target:	Company's customer data and payment information.
Attacker:	Magecart, a cybercriminal group.
Attacker Motivation:	Financial gain.
Attack Vector:	Injecting malicious code into the company's website and mobile app allowed the attackers to intercept and extract customers' payment information.
Protection Mechanism:	Not reported publicly; however, the company took immediate steps to mitigate the issue and secure customer data.
Attack Impact:	Exposure of the personal and payment information of approximately 380,000 customers, putting them at risk of fraud and identity theft. The company faced significant reputational damage and was fined £20 million by the U.K.'s Information Commissioner's Office (ICO) for violations of the General Data Protection Regulation (GDPR).
Lessons Learned:	Organizations must implement strong access controls and encryption to protect sensitive customer data, and have a comprehensive incident response plan in place, including clear communication with affected customers and regulatory authorities.

RISK CATEGORY: Supply-chain risk	
DEFINITION:	When a legitimate party in the supply chain is the conduit through which a malicious actor gains access to conduct attacks on the company. This can be through building back doors into the supplier software and reporting back, or just being the weak link.
REAL-WORLD EXAMPLE:	December 2020: A major U.S.-based software supplier was breached and used to distribute malware to private and public sector organizations worldwide.
Attack Target:	Sensitive information and intellectual property.
Attacker:	APT29 or Cozy Bear, reportedly a Russian state-sponsored hacking group.
Attacker Motivation:	Nation-state espionage and data theft.
Attack Vector:	A sophisticated attack method that involved compromising the company's software update system, allowing hackers to distribute malware to the company's customers.
Protection Mechanism:	The company had reportedly implemented several protection mechanisms; however, these defenses were not enough to prevent the attack.
Attack Impact:	The attack compromised data and systems of thousands of commercial and governmental organizations worldwide that had deployed the company's software. It is believed that the attack went undetected for several months. Financial losses were not disclosed but are estimated to be significant, as much as $90 million. In the immediate aftermath of the breach, the company's stock price fell by more than 25%, and the company faced several class-action lawsuits from investors who claimed that the company had failed to disclose the vulnerabilities that led to the breach. It is unclear what the company's insurance coverage was.
Lessons Learned:	The attack highlighted the importance of supply-chain security and the need for increased vigilance when it comes to third-party software and service providers, international cooperation in combating cyber threats, and the need for improved information sharing and collaboration among government agencies and private sector organizations.

RISK CATEGORY: Brand and reputation risk	
DEFINITION:	This risk attaches to an organization's brand and goodwill. This includes damage to a company's reputation through public erception of its security and privacy practices and harm to customers and employees.
REAL-WORLD EXAMPLE:	September 2022: A global U.K.-based hotel chain saw hackers irreversibly destroy their data, documents, and files, disrupting business at franchisees worldwide for several days.
Attack Target:	Sensitive data, documents, and files.
Attacker:	Hacker team of two by the name of TeaPea.
Attacker Motivation:	Originally ransomware but after attackers' attempts for ransomware failed, the hackers wiped out the company's data, just for fun.
Attack Vector:	Accessed the company's database through an easily bypassed weak password. Also, tricked an employee into downloading software through a malicious email attachment to gain access to the company's internal IT network.
Protection Mechanism:	The company had a strong infrastructure protection mechanism to prevent ransomware deployment, but it did not have strong identity and access management, or people protection mechanisms.
Attack Impact:	The company suffered from brand and reputation damage. Its booking system and mobile apps for certain locations were unavailable to franchisees and customers for extended periods. The financial loss is unknown currently but is estimated to be significant; certain franchisees have filed a class action lawsuit against the company.
Lessons Learned:	Resilience should always be the priority, i.e., stopping attackers getting into systems, because once they are in, organizations have very little control over what happens next. Additionally, account monitoring should be in place to identify compromised accounts.

RISK CATEGORY: Strategic risk	
DEFINITION:	When cybersecurity breaches result in undermining a company's strategy or loss of key intellectual property gives an advantage to the competitor.
REAL-WORLD EXAMPLE:	November 2014: The American entertainment subsidiary of a global corporation experienced a significant cyberattack.
Attack Target:	Sensitive information and key intellectual property – including executive emails, confidential business information, and unreleased films.
Attacker:	Reportedly a group linked to North Korea.
Attacker Motivation:	Politically driven by the release of a film about a fictional plot to assassinate North Korean leader Kim Jong-un.
Attack Vector:	A destructive malware "Wiper" erased data from the company's computer systems; also stolen credentials were used to gain access to the company's network. The exact method is not known but it is believed employees clicked on emails that appeared to be from trusted sources and opened the attachments or clicked on links that appeared directed to legitimate websites, inadvertently downloading the malware onto their computers.
Protection Mechanism:	The company reportedly had good defense mechanisms in place, but no details were made public.
Attack Impact:	Reputation damage and financial losses estimated from $100 million to $1 billion due to lost revenue and by creating an advantage to competing studios. The company also incurred the costs of investigating and responding to the breach, data restoration and recovery expenses, legal fees, and regulatory fines. The company had cyber insurance coverage, which reportedly helped to offset some of the financial losses resulting from the attack.
Lessons Learned:	Companies must have a robust incident response plan in place, including the need to involve law enforcement agencies and other external partners and for effective crisis communication and public relations strategies. Additionally, companies need to use multi-factor authentication and strong passwords.

Chapter 4. **The Defense Ecosystem: Protection**

Cybersecurity technologies exist to protect both digital assets, such as systems and data, and physical assets from cyberattacks. While there may be nuance and complexity regarding the role of a specific cybersecurity technology, in general they focus on one or more of the following key capabilities:

- **Protect:** measures that help to proactively prevent attacks and assure safe usage of business systems
- **Detect:** measures that identify vulnerabilities and discover attacks in progress
- **Respond:** measures that enable cybersecurity professionals or users to take actions to contain and manage an incident, and remediate the damage from attacks, during or after they have occurred
- **Recover:** measures that remediate impacted systems and place them back into service

The protection function usually includes numerous special-purpose technologies that work along with common security capabilities such as identity and access management. Protection is also provided by implementing various measures for containment – ways to limit the effects of any attacks that succeed.

Detection and response are the practices of making sure any attacks that slip by the protection mechanisms are identified as soon as possible. Incident management is all about figuring out which events become alerts and which alerts are attacks. The process should identify false alarms from actual attacks that can be escalated to incident response functions. Recovery and resilience management are post attack and crisis activities for enabling a business to resume operations. This step is often included in the response plan, so we have discussed it as such in this book.

Chapter 4 will expand a board member's knowledge of cybersecurity by explaining the essentials of protection technologies and practices. We will cover detection, response, and recovery in Chapter 5.

CYBERSECURITY PROTECTION MECHANISMS

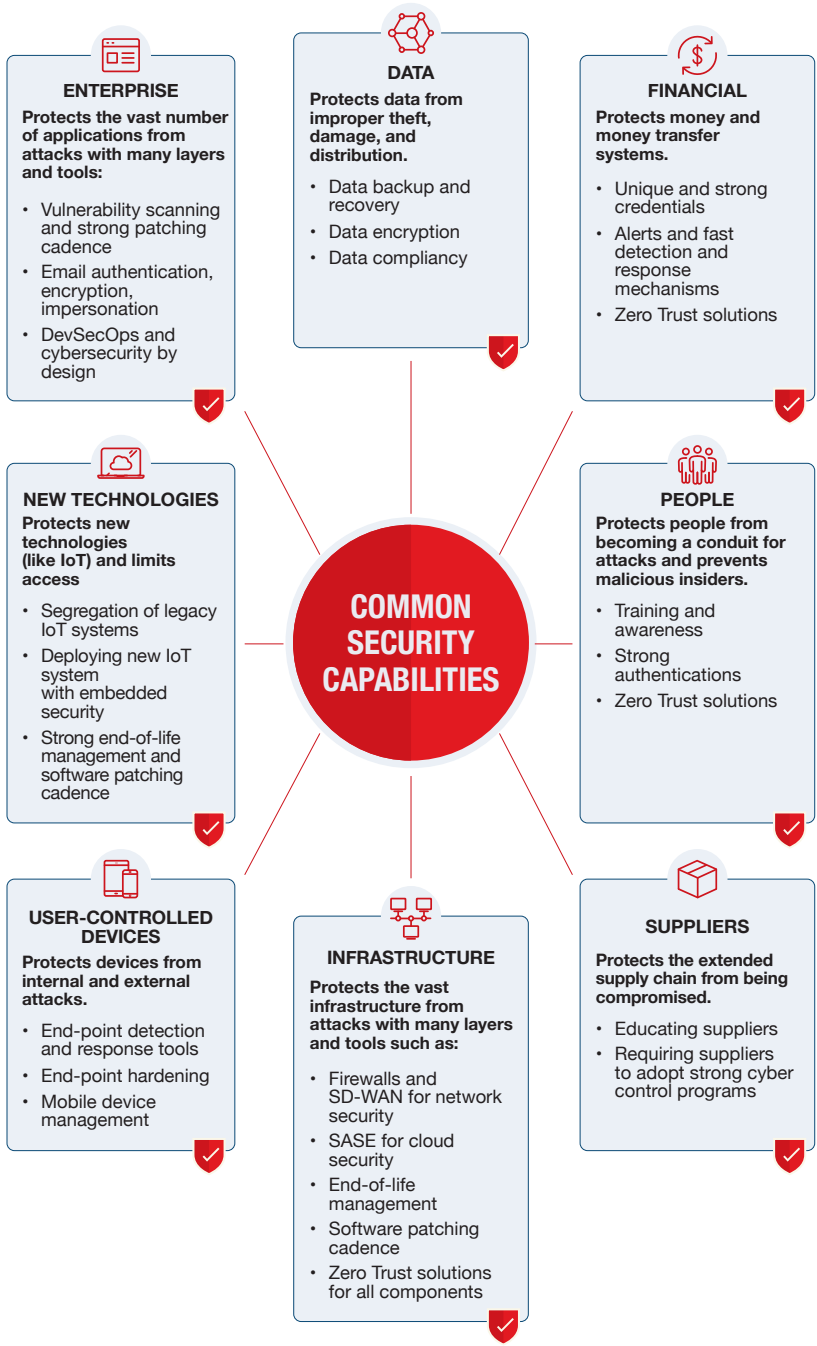


Figure 11. Map 3 — Example Protection Mechanisms by Business Asset Group

Key Elements of Cyber Protection

What does cyber protection ideally look like? The diagrams in Chapters 1 and 2 provide an illustrative protection ecosystem design that maps to business asset groups and attack vectors. Although a comprehensive cybersecurity protection program may take months or years to build and will vary from one company to another, many of the fundamental components will remain conceptually similar. Figure 11 gives a snapshot view of the protection ecosystem complexity and explains its important elements.

Infrastructure & Cloud Protection

Infrastructure defense mechanisms consist of multiple specialized security controls deployed to protect specific components of a network from threats. In the past, infrastructure and network services were more centralized, and these defense mechanisms were deployed in overlapping layers, like the layers of an onion. This approach was described as defense-in-depth. Layers included communication networks, data center and data storage, physical premises (including remote workers), operating systems, and operational and IT systems. Some of the essential components of this approach, such as a firewalls, have existed for decades, but the sophistication of security controls has grown as the infrastructure they protect has increased in size and complexity.

Today, infrastructure defense mechanisms do more than secure a corporation's physical and logical perimeter. They also enable secure access to company assets by authorized employees, partners, and customers, anywhere, anytime, and from any device. We refer to these ubiquitous services as cloud-based services. Cloud services are built and owned by specialists (cloud providers) to provide ready-to-use, on-demand technology and infrastructure solutions to customers.

> Cloud security is the set of processes, practices, solutions, and technology with which a company can secure its cloud environment.

The common models are:

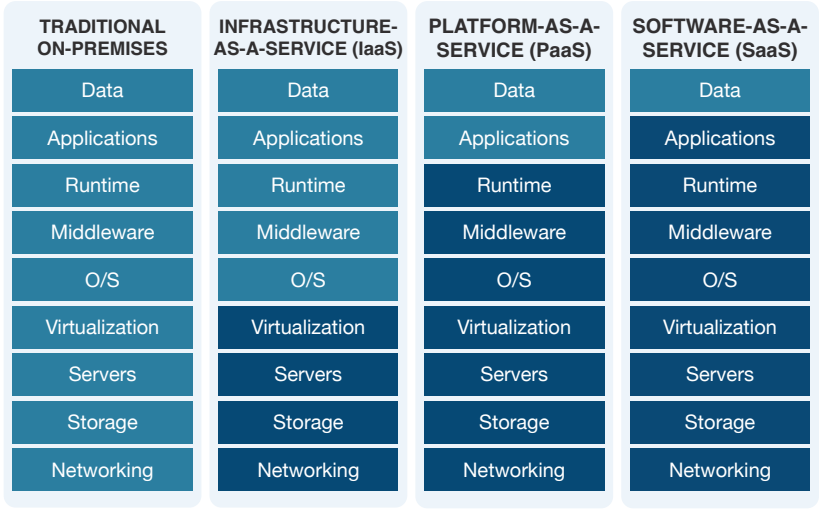
- **Infrastructure-as-a-Service (IaaS)** — backend servers, networking, and storage for running workloads (e.g., Google Cloud, Microsoft Azure, Amazon AWS)
- **Platform-as-a-Service (PaaS)** — platform solutions for developing, running, and managing applications (virtual Windows or Linux servers)
- **Software-as-a-Service (SaaS)** — application software (Salesforce or Workday)

Cloud services built to provide elastic capacity, allowing usage to expand and contract as needed, are making it possible to scale up quickly. However, the enabling hardware and technology are no longer on-premises, nor in the company's physical control. Digital assets stored or processed in these environments need to be secured through cloud-specific technologies, i.e., cloud security.

Cloud security is the set of processes, practices, solutions, and technology with which a company can secure its cloud environment. They offer companies visibility over networks they didn't build, applications they didn't write, and devices they don't own, along with controls they can implement to protect their data and services. Because of the relative newness of the cloud, many organizations are unaware of how their sensitive information can be accessed via the cloud or where their data is stored, or how their applications are managed and configured in the cloud. Cloud security controls can help answer these questions.

It should be emphasized that securing cloud resources is a shared responsibility between the cloud provider and the company (tenant), as shown in Figure 12. Clearly defining the security roles is crucial, as it helps define each party's responsibilities. Companies should understand the security posture provided by the cloud provider, and augment that with specific security controls to meet their own needs. This minimizes gaps in coverage that could allow attackers to infiltrate the system without detection.

TYPICAL CLOUD RESPONSIBILITY MODEL



- Light blue background: Company/tenant responsibility
- Navy background: Provider/landlord responsibility

Source: IBM Institute for Business Value's "The New Era of Cloud Security" (2021) (https://www.ibm.com/downloads/cas/J6N8WRGG)

Figure 12. Typical Cloud Responsibility Model

Reducing Infrastructure Complexity

Historically, addressing infrastructure challenges involved employing distinct solutions, leading to a proliferation of tools and a complex infrastructure. This complexity inadvertently created opportunities for errors and security gaps. The integration of cloud services further compounds the intricacy, significantly amplifying the likelihood of important security actions slipping through the cracks. Therefore, new architectures, deployment methods, and tools are necessary to implement and manage security.

Some important new architecture concepts include Security Service Edge (SSE), which aims to simplify the management of security, by consolidating security capabilities required to secure access to the web, cloud services, and private applications into a single platform. SSE capabilities may include access control, threat protection, data security, security monitoring, and acceptable use controls. Consolidating these technologies and providing security leaders with a unified point of visibility enables faster, more informed business and security decisions.

Critical cloud application security functions include identity and access management, data encryption, and cloud posture management. These security functions can be further combined and delivered as an integrated package with network functions. The combined concept is called Secure Access Service Edge, or SASE, which is a cloud architecture enabling formerly separate services to be delivered as a single, rapidly deployed, highly integrated, cloud-delivered service. SASE enables workers to access corporate resources within the office or remotely with a consistent set of network and security controls. This increases efficiency of workers and reduces the opportunity for mistakes and misconfigurations.

Endpoint (User-controlled Devices) Protection

Endpoint defense is the set of measures used to protect devices used by individuals, such as desktops, laptops, and smartphones – both corporate owned and personal – from cyber threats. These defenses are necessary because endpoint devices are frequently, if not exclusively, used outside of corporate-managed environments, and thus are not protected by corporate-managed physical security and other security controls. At the same time, these devices frequently have access to sensitive corporate information, whether through email, corporate intranet, internal messaging systems like Slack, or corporate data repositories. While the connection to these resources may be protected through a virtual private network, once the data is on the endpoint device, it requires equivalent protection to data stored within corporate systems.

Typical endpoint defense mechanisms include:

- A combination of automatic endpoint detection and response software (EDR), managed detection and response services (MDR), and extended detection and response technology (XDR)
- Antivirus/anti-malware software and personal firewalls
- Access controls such as login and password, biometric security, and token-based authentication
- On-device data encryption, patch management, application control, and web security controls

New Technologies Protection

In the Threat chapter, we explored emerging technologies' threats and specifically discussed AI and its cyber pitfalls. As companies use new technologies, they have to implement updated cyber defenses. One increasingly prominent example of such a new technology ecosystem is IoT.

IoT refers to the vast network of devices and sensors that connect physical objects or groups of such objects to one another and central command and control centers via communications networks and the internet. IoT is used both for consumer use cases and in the enterprise environment. IoT aims to enhance efficiency, convenience, and safety of physical objects by improving and automating processes. A well-known consumer IoT use case is Nest thermostats that are connected to the internet through house or office Wi-Fi and can be controlled remotely by the user through their mobile phone or a computer.

IoT vulnerabilities are similar to the vulnerabilities in any other IT environment. However, IoT is unique in its scale and its default lack of security, which attackers can use to weaponize IoT systems. Many current IoT deployments have outdated devices, equipment and software with weak security controls such as hard-coded credentials, and lack of encryption. IoT devices frequently cannot receive automated patches, leaving them vulnerable to cybersecurity threats. A robust IoT defense requires a comprehensive approach that includes but is not limited to:

- Segregation of legacy IoT systems and implementation of strong access controls
- Strong end-of-life management and software patching cadence
- Deploying newer IoT systems with embedded security to replace older, undefended systems

Enterprise Application Protection

Enterprise application protection involves the measures and practices used to protect software applications from unauthorized access, modification, and destruction. Enterprise applications range from enterprise tools (such as email or Slack) to critical business functions such as financial transactions, customer relationship management, supply-chain management, and human resources management.

Software security is a wide area and has many dimensions, but below, we discuss two topics as examples of what cybersecurity practitioners are concerned with.

- **Software security:** Legacy software codes were not written with security in mind and therefore they don't have security built into their design. President Biden's National Cybersecurity Strategy, published March 1, 2023, calls for shifting liability to software vendors for delivering insecure software products and services to incentivize vendors to follow secure-by-design principles and perform pre-release testing. The strategy specifically gives examples of Russia's compromise of the SolarWinds Orion platform and China's compromise of servers running Microsoft Exchange. Organizations must be mindful that all legacy and current software (on-premises or SaaS) have vulnerabilities and should hold software vendors responsible for continuously making efforts to uncover these vulnerabilities and releasing appropriate and speedy patches to address them. Customers can take several steps to encourage vendors to prioritize security, including negotiating contractual terms that hold vendors accountable for security issues and conducting security assessments and audits before making purchasing decisions. Organizations, in turn, must be held responsible for implementing the patches as soon as they are available. While this seems logical and simple, organizations often ignore these patches or don't perform them in an expedited manner. Boards of directors should require the management to present and monitor relevant operational-level KPIs such as the number of patches outstanding and the number of obsolete hardware/servers.

- **Email security:** Email continues to be an important inter- and intra-communication tool for companies. It also remains one of the most successful ways that attackers infiltrate an organization's infrastructure. While email phishing has existed for a long time, recent advanced threats such as carefully tailored malicious links, malware attachments, impersonation, and social engineering have made incoming email monitoring and auditing as well as monitoring outbound email traffic an indispensable protection. Like many other areas, the best email security relies on multiple defenses including but not limited to email authentication, email encryption, email filtering, antivirus and anti-malware software, and backup and recovery.

Data Protection

As we discussed in the Threat chapter, data is invariably one of the most valued crown jewels of a company. As a result, data theft is becoming more common and a greater risk. In March 2023, the CEO of ASML, Europe's largest chip toolmaker, said in a Financial Times article that he "was guarding against intellectual theft more fiercely than ever before, as a geopolitical tussle forces China to bolster its homegrown semiconductor industry." It is worth noting that reports of cyber-espionage activities by state-sponsored groups, including those allegedly originating from China, have been widely covered in the media and cybersecurity community. These reports have highlighted instances of intellectual property theft, data breaches, and other cyber intrusions targeting Western firms and governments.

Much of the cybersecurity defense ecosystem is dedicated to protecting company's data and preventing its loss. Outside of the many defense mechanisms discussed in other parts of this chapter, there are several data protection-specific mechanisms we want to highlight:

- **Data backup and recovery:** Regularly backing up critical data and systems and testing the recovery processes to ensure that data can be quickly restored in the event of a cyberattack.
- **Data encryption:** Using encryption to protect data both in transit and at rest by transforming data into a coded language that can be deciphered only by someone who has the appropriate decryption key. Over time, quantum computing will change what we think of as traditional encryption methods, and organizations will need to adapt.
- **Data residency and compliance:** The European Union's General Data Protection Regulation (GDPR) is one example of many laws in effect or under review that impact companies based on the location where they store data, or the location of their staff, customers, or markets. The effect of these regulations on business strategy should be reviewed with the corporate privacy officer, in-house legal counsel, or external resources like the International Association of Privacy Professionals (IAPP) (http://iapp.org).
- **Data loss prevention (DLP):** Software that detects exfiltration of data/categories of data and blocks and/or alerts so security teams can react appropriately to contain the loss and to prevent recurrence.

People Protection

One of the most important defenses against cyberattacks is for the community of a company to be informed and aware of the ways that attackers target them as individuals. Earlier, in the Enterprise Application Defense section, we discussed email security. Clicking on a link or downloading a file contained in a phishing email can set off a chain of events leading to a significant security breach. Users can also be lured to give up their passwords and other confidential information to hackers. In fall 2022, hackers started an attack with a social engineering campaign on an employee at a major U.S.-based ride-sharing company to approve the multi-factor authentication notifications sent to the employee's phone. When the employee provided this authentication, attackers got access to a VPN, in turn granting access to the company's internal network from which the attacker found further vulnerabilities and was ultimately able to take over multiple services and internal tools.

There are several defense mechanisms that ensure staff and others with access to sensitive data do not make decisions that open a company to cybersecurity risks:

- Continuous training, with real-time testing of stakeholders, and communication of new attack vectors to the company's community of users
- Strong authentication policies as described in the Identity and Access Management section
- Segregation of duties to minimize the risk of a single individual having excessive control over critical processes, systems, or data
- Security solutions focusing on people behavior patterns, flagging anomalies, and providing alerts for high-risk activities of insiders
- Zero Trust solutions as described in Chapter 1

Suppliers Oversight

The increased reliance on third-party suppliers has amplified the cybersecurity risk they pose to companies that work with them. As monitoring, managing, and auditing these suppliers presents significant challenges, addressing their risk has become a top priority for both regulators and companies alike.

The increased reliance on third-party suppliers has amplified the cybersecurity risk they pose to companies that work with them.

Supply-chain defense protects organizations from attacks by and through their suppliers and vendors. This may be via the application of multiple defenses between the organization and the third parties such as the sanitization of data and processes connecting the organizations and restrictive application controls.

Supply-chain defenses became a key focus area for industry and regulators after Target's massive data breach in 2013, when attackers gained access to Target's network through a small third-party HVAC vendor whose credentials were stolen. The hackers were able to use a malware program to infiltrate Target's point-of-sale system. The hack resulted in significant financial losses for Target, as well as damage to the company's reputation. The company settled a class-action lawsuit brought by affected customers for $10 million.

Common supplier defense mechanisms include:

- Maintaining an inventory of suppliers categorized by cybersecurity risk
- Educating suppliers about cybersecurity defense
- Obligating suppliers to adopt strong cyber control programs as part of their contracts
- Requiring suppliers to provide a detailed outline of their cyber risk reviews including identification of sub-contracting
- Reviewing a bill of materials for all component parts from the software and hardware manufacturing processes
- Using assessment tools that evaluate supplier security health, which should be independent and include automated testing tools, sample audit testing, and live penetration testing

While suppliers can introduce vulnerabilities into a company's technology ecosystem, their widespread reliance by most organizations cannot be underestimated. Striking a balance between the value of services provided and the risks introduced requires thorough oversight and robust partnerships. To effectively harness the business and technological benefits while mitigating risk, forward-thinking teams equipped with modern tools and automated monitoring practices may be necessary.

Supporting Security Capabilities

Various common security capabilities are required to support the protection mechanisms described earlier. For instance, these capabilities must identify the user, the device they're using, and the system they're accessing in order to provide the right level of protection. Other supporting functions are also essential, and recognizing the types of technologies that play these supporting roles is crucial to building a robust defense ecosystem.

Identity and Access Management Capabilities

The identity and access management defense layer includes authentication, authorization, and access control processes to ensure only authorized users can access technology resources. This capability is essential to all asset groups in the business environment. It is comparable to door locks, keys, and biometrics used to secure physical environments. Credentials have been used as a defense mechanism for decades and are usually a hacker's most useful entry into a target. Much of access management was conducted by humans in the past; now, most is automated. This form of defense has become more complicated as identity must be managed across numerous entities and infrastructures, from on-premises systems to multiple clouds, along with myriad enterprise applications and communications platforms. Today multi-factor authentication, Zero Trust access control, identity orchestration, adaptive trust, and credential management are best-in-class defense mechanisms that all businesses should use.

Other Supporting Capabilities

Every protective cybersecurity system is both a consumer and producer of information. Each also has complex configuration settings, as well as passwords to protect their own administrative interfaces. The operations of each system and the entire portfolio must be monitored. A subset of other supporting capabilities is:

- Security Information and Event Management (SIEM) is a capability that collects, collates, and analyzes data to detect anomalies and identify indicators of compromise.
- Cloud Security Posture Management (CSPM) and SaaS Security Posture Management (SSPM) are two capabilities to monitor the configuration of cloud and SaaS assets to make sure the configurations are correct.

- Administrative Password Vault is a system for managing and controlling access to administrative passwords used to gain superuser privileges.
- Security Operations Center (SOC) is a centralized function that monitors events, analyzes alerts, and identifies incidents.
- Executive protection refers to measures designed to safeguard high-profile individuals from targeted attacks.

Containment Strategy

An aspect of cybersecurity defense strategy is using network design and segmentation to support containment. The idea is that if attackers successfully intrude into the company's infrastructure or its business environment, they will have limited opportunities to expand their attack further and gain additional control.

In this regard, it is essential to design and create an infrastructure that limits the movement of any entity within the system so that when attacks do occur, the reach of the threat is minimal.

Companies should design their infrastructure, business environment, and cyber defense ecosystem to reduce the intrusion radius of any attack. In this regard, it is essential to design and create an infrastructure that limits the movement of any entity within the system so that when attacks do occur, the reach of the threat is minimal. When reviewing an organization's cyber program, it would be appropriate for board members to inquire what the CISO's containment strategy is. Containment strategy enhances the overall effectiveness of cybersecurity measures.

Key Categories for Containment Planning

The following are examples to implement containment strategies across a cybersecurity portfolio.

Containment with Zero Trust: Zero Trust is an approach for cybersecurity that assumes no entity is trusted. An entity can be a person, a device, a system, an application, and anything else that requests access to digital resources. Even after an entity is fully authenticated at the point of entry, trust is not continuous, and the entity's identity and access privileges must be periodically and/

or constantly re-verified. Networks based on Zero Trust can be segmented to limit access to only parts of the network or data required explicitly for specific workloads. A Zero Trust approach will also include monitoring of an entity's behavior to identify any anomaly across the network traffic. By limiting the scope of access, verifying trust, and monitoring behavior, Zero Trust principles help companies reduce their exposure to threats and ongoing damage from successful attacks.

Containment with Least Privilege: Companies often grant more access than is needed to complete a task because it can be difficult to determine exactly what privileges are required. With least privilege design, an entity's access to the network, data, applications, or other assets is limited to only those specific resources needed to complete a task or do a job. The effectiveness of the least privilege principle relies on regular access reviews to ensure that granted permissions align with the minimum required for a user's role and prompt revocation of permissions when they are no longer needed or appropriate. For instance, when an employee changes roles, it is essential to remove their previous access instead of merely adding the new role's permissions. Attackers exploit any available access, so it is crucial for companies to minimize opportunities by diligently managing access rights.

Containment with Network Segmentation: Network segmentation requires building smart networks containing subnetworks or networks with groups of related/dependent technology. If an attacker penetrates one segment of the network, effective network segmentation limits the attacker's ability to penetrate another segment and cause a broader impact such as infecting the entire system.

Chapter 5. **The Defense Ecosystem: Detection, Response, and Recovery**

Even after implementing a robust cybersecurity protection suite, breaches will still occur. While a modern cybersecurity technology portfolio can prevent a majority of attacks, a comprehensive security portfolio must also include detection and response tools for managing cyber specific incidents. The concepts of detection and response reflect the notion that it is not feasible to develop a defense system that can prevent all attacks.

Detection

To accurately detect attacks, companies first must establish a baseline of normal behavior. Companies must then monitor their environments around the clock and rapidly identify abnormal activity in the system. Detection technologies can pinpoint activities that deviate from the established baseline, such as users accessing files they don't need for carrying out their responsibilities or a sudden uptick in usage of a particular application. The technology should automate the process of attack detection and be able to provide information in near-real time in the form of intelligent, positive alerts. Organizations must also be cautious to avoid implementing overly sensitive anomaly detection mechanisms that generate excessive false positives. This can lead to alert fatigue and make it difficult to identify genuine threats amidst the noise. Striking the right balance between sensitivity and specificity in anomaly detection is crucial for an effective cybersecurity strategy.

As part of designing systems, it's essential for management to know how to turn off and block an infected area, including what is impacted, and how long it will take. It's important to decide in advance who can approve and/or know how to segment an infected area. Companies may also have other specialized monitoring tools and controls focused on their crown jewels. These tools and controls could include monitoring for attacks like reviewing alerts when a super-user account was activated, or an unauthorized individual accessed a high-value file.

Detection does not always have to be passive. A mature cybersecurity team will frequently deploy proactive, deceptive systems that deliberately try to draw out attackers. An example of this type of cybersecurity tactic is the use of honeypots. This tactic involves setting up intentional environments to lure attackers so they can be watched to gather intelligence and enabling the organization to detect, deflect, and defend against them. However, honeypots, while effective for short periods, require continuous monitoring, evaluation, and regular updates to stay effective – making them economically challenging to maintain over time.

Incident Management

Once an attack, or potential attack, has been detected, companies need a process to orchestrate and manage the response, the recovery from it, and investigations that help to determine how and why the attack occurred. The latter is crucial for remediation purposes and for identifying and removing vulnerabilities within a company's environment.

To perform incident management successfully, organizations should have a set of processes, policies, and systems in place that can provide the following capabilities:

- Forensic analysis to determine what happened before, during, and after an attack.
- Assessment of any damage, theft, or compromising of the integrity of systems, networks, data, or other assets.
- Performance analysis of the defense ecosystem to identify weaknesses in the portfolio or remediation tactics.
- Analysis that identifies the perpetrators of the attack, as well as their motivations. This should also determine if any third parties, such as law enforcement, should be engaged.
- Post-incident analysis to identify areas for improvement and update the Incident Response Plan accordingly. The analysis should include a review of the incident response process and an assessment of the effectiveness of the company's security controls.
- Detailed communication protocols for identifying who should be notified internally and externally, including key internal stakeholders, regulatory partners, compliance teams, outside auditors, customers, and investor management, with a clear decision-making process for when the board of directors should be informed.

Response

Response comes into play after a successful attack has been detected. At this point the Security Operations Center activates the various incident management processes, which take advantage of the containment planning. But if damage has been done, remediation is needed.

Remediation is about ensuring the company can recover operations as fast as possible from attacks and breaches, whether a data breach or any system compromise. Through remediation, companies contain an attack and restore operations from a catastrophic condition. For the highest-risk operational areas and the crown jewel assets, companies should have a plan to repair damage after a successful attack. This may involve isolating affected systems or networks, disabling compromised accounts, or limiting the attacker's ability to move laterally within the environment. Once contained, the company should be able to remediate the issue and restore affected systems to a secure state.

For example, having a well-tested, comprehensive, state-of-the-art backup system could allow a business to recover data compromised by an attack. Redundancy is an effective way to mitigate and protect against attacks. Redundancy means systems can run from multiple locations. It also means having backup systems within each individual location. Cloud systems are often easiest to mitigate since they usually have redundancy built in, are designed for resilience, and can be accessed remotely. Even when organizations can recover data, teams may need to use older backups to fully recover if the compromise has been ongoing for an extended period.

Most companies know they need a remediation plan. Still, many fail to invest adequately in a remediation plan before it is required.

Recovery and Resilience

Recovery and resilience are essential to any organization's remediation plan, especially in the face of a severe disruption such as a major cyberattack. Proper training allows companies to quickly respond when they notice a threat, which is crucial as any delay in formulating an appropriate response can lead to significantly higher damage. Organizations should establish ongoing relationships with law enforcement agencies specializing in cyberattacks. Other specialized

third-party auditors, legal, and regulatory experts can also help prepare for facing an incident and recovering from it. Developing these relationships before they are needed will make incident management, recovery, and crisis management in an emergency markedly easier and more effective.

Organizations should develop a Rapid Response Playbook to guide them on handling the situation should an attack reach a materiality level that requires public reporting.

Organizations should develop a Rapid Response Playbook to guide them on handling the situation should an attack reach a materiality level that requires public reporting. A Rapid Response Playbook is essential for proper crisis management, as breaches can advance at high speeds, and the scale of a breach can be enterprise-wide and devastating. This document should exist in both digital and paper form (in case the hackers have locked access to the digital version). At minimum, the playbook should include instructions on how to:

- Enable containment measures
- Restore normal operations
- Address data integrity problems
- Execute communications protocols
- Perform customer outreach
- Manage media and other third-party influencer queries
- Engage with regulators
- Protect against related extortion attacks

All teams involved in crisis management should practice this periodically, at a minimum yearly, through what are called tabletop exercises with the objective of strengthening the overall response and recovery plan. They should also review associated response procedures through guided discussion of one or more emergency scenarios. A well-planned Rapid Response Playbook can minimize the impact of a cyberattack and help ensure that businesses recover quickly and continue running successfully despite any incident.

Chapter 6. **Optimizing a Cybersecurity Portfolio**

The digital era and widespread use of cloud applications to support hybrid work environments in global ecosystems means there are always new assets and new data for companies to protect, potentially needing new cybersecurity technologies.

While there will always be new cyber defense products, a company's portfolio does not need to include stacks of tools from the hundreds of cybersecurity vendors. The goal is to have an integrated, well-designed portfolio that enables the organization to perform the essential cybersecurity functions of protect, detect, respond, and having crisis management procedures to recover from catastrophic or disruptive attacks quickly.

There are four key elements in creating and managing an effective cybersecurity defense portfolio: the technology architecture, the vendors, the portfolio management, and the testing strategy to validate the cybersecurity posture.

Technology Architecture

Companies can use several credible reference architectures to guide their cybersecurity portfolio buildup. Teams should look for portfolio designs that follow common and trustworthy industry frameworks, such as NIST (National Institute of Standards and Technology), COBIT (Control Objectives for Information and Related Technologies), COSO (Committee of Sponsoring Organizations of the Treadway Commission), ISO (International Organization for Standardization), and CISA (Cybersecurity and Infrastructure Security Agency) critical infrastructure frameworks. These frameworks offer structured ways to identify risks, select controls, and implement management tools. Following an established approach ensures company leaders can track progress against credible best practices. These frameworks are not one-size-fits-all, so organizations should still customize their portfolio to fit their unique strategies and assets. The business asset groups map (Figure 2. Map 1 - Business Asset Groups) can assist companies in identifying their crown jewel assets and ensuring that they have an effective set of cyber tools and controls for their security needs.

Vendors

Given the size, depth, and risk inherent in the cybersecurity sector, there is no shortage of solutions and tools. Having an abundance of standalone solutions can contribute to a complicated technological landscape, resulting in a suboptimal experience for end users and cybersecurity practitioners. When evaluating cybersecurity vendors, it's important to consider several factors. These include the vendors' ability to innovate and scale over time, the comprehensiveness of their product offerings, and how easily their solutions can be deployed and integrated into the company's existing and future IT environments. Other considerations include whether vendors' products offer protection for current and future workloads, whether their solutions replace existing solutions or protect only new types of business assets, and the expected return on investment. When dealing with cloud-delivered software, it is critical to carefully construct and execute vendor contracts to ensure companies receive precisely what they require with a high degree of reliability and precision, along with favorable Service Level Agreements (SLAs).

Because there is no single, catch-all cybersecurity solution, there will continue to be a need for multiple vendor solutions. It is vital that companies carefully assess the number of vendors they work with, necessary cybersecurity controls, and how well the tools from different vendors work together. Too often, portfolios become needlessly and overwhelmingly complex. To the extent possible, businesses should strive to simplify their portfolio by being selective about the vendors they partner with. Selecting the most complete and integrated suite of capabilities from a single source, instead of best-in-class from many vendors with limited integration, will enable teams to build upon the organization's security capability at scale.

Portfolio Management

The responsibility for assembling the cybersecurity technology portfolio typically belongs to the CISO at large companies and to the Vice President of Security at smaller companies. Regardless of whether they report to the CIO, legal, finance, or risk departments, the CISO must develop a comprehensive cybersecurity strategy and program roadmap. This involves overseeing, pruning, and refactoring the portfolio as needed. The CEO, COO, Chief Risk Officer, and Chief Internal Audit Officer should assist in evaluating the portfolio's

effectiveness. Board members, either directly or through a board of directors' committee, provide oversight. The higher the CISO's position within the C-suite, the greater their influence and autonomy, and the more their importance is communicated to the organization. Irrespective of their reporting lines, CISOs should have their own dedicated budget, have autonomy to set and implement cybersecurity strategy, and present directly to the board of directors.

Irrespective of their reporting lines, CISOs should have their own dedicated budget, have autonomy to set and implement cybersecurity strategy, and present directly to the board of directors.

At least on a biannual basis, the board of directors should hear about the effectiveness of the cybersecurity program, any planned changes to the approach, and major changes to the program or roadmap as the company adapts to changing trends. It is a good idea to hear directly from the CISO on these topics, but updates should be reviewed by other risk leaders in the company from second and third lines of defense, such as the enterprise risk, compliance, legal, and audit (internal and external) functions. This reporting is a critical area for the board of directors to ensure the organization has a continuing focus on cybersecurity controls. In Chapter 7 we offer some specific metrics to help the board of directors perform this important governance role.

The CISO's biannual report must provide a holistic, enterprise-wide view of cybersecurity including both operational and strategic perspectives. At a minimum, this report should include:

- Industry trends
- The effectiveness of the program and its achievements using operational-level and board-level metrics as discussed in Chapter 7
- Key threats and vulnerabilities that will impact the corporate strategy, material incidents, and management's response
- Regulatory compliance attestation and gaps
- Proactive adjustments to the program

The board of directors can evaluate the maturity and cohesiveness of the cyber program from these types of reports. For example, a less mature organization may include cloud security capability on

its roadmap to protect data in the cloud or even secure-by-design application development methods. A mature organization may include new architecture approaches such as using a Secure Access Service Edge (SASE) solution for cloud security or tools to secure emerging technologies like blockchain or quantum computing.

For mid-size or large entities, there should be a focus on simplification and standardization. Centralization of essential cybersecurity functions that do best with a holistic view, such as attack detection or response, must also be considered. In general, the board members should be able to recognize where approaches are fractured, which could weaken defenses and hamper quick actions. Examples are different tools being used in different geographies, and different business units with their own tools delivering disparate security results. Discussions around these topics can draw out themes such as a lack of resources, people or money, limited automation, turf wars, and culture inconsistencies.

WHY ARE THERE SO MANY SECURITY TECHNOLOGIES?

The constant efforts by attackers seeking new vulnerabilities help drive the abundance of security tools and vendors employed by organizations. However, it would be shortsighted to assign too much credit to attackers alone. Instead, two additional reasons contribute to this sprawl.

1. Many companies rely on outdated technologies and IT systems that were not designed with security in mind, creating vulnerabilities that attackers can exploit.
2. New technology innovations and unintended uses of those innovations are constantly expanding the attack surface, even when the emerging technology has some built-in security.

Organizations often purchase new tools to address the new vulnerabilities. Those individual purchases add up to become a sprawl of tools that often don't work together or don't address more than one use case.

Ultimately, the CISO must showcase prudent decision-making and business trade-off awareness in budget and investment discussions while conveying this within a coherent, risk-focused framework. Similar to other business units, CISOs should be asked to minimize costs while adhering to the company's cyber risk tolerance.

Testing Strategy to Validate the Cybersecurity Posture

Board members often grapple with how to fulfill their duty of care and effectively govern cybersecurity in this complex environment. They are faced with questions, such as whether the company is investing adequately in cybersecurity, what the company's security posture entails, and how they can validate and assess the associated risks and security updates. While external independent audits can provide relevant assessments, one of the most effective practices for evaluating the functionality of cybersecurity defenses is the implementation of a comprehensive testing strategy. This approach can help answer these questions and provide valuable insights into the organization's landscape.

While external independent audits can provide relevant assessments, one of the most effective practices for evaluating the functionality of cybersecurity defenses is the implementation of a comprehensive testing strategy.

Even when companies are proactive in implementing robust cyber defenses, the true effectiveness of these measures can be determined only through rigorous security testing. A variety of techniques and tools exist to scan the environment for vulnerabilities, weaknesses, and gaps, as well as both manual and automated methods to simulate attacks and assess the resilience of defense tools and mechanisms. Evaluating how well these defenses withstand simulated attacks allows the board members to gain a good understanding of operational risks and identify areas where such risks may accumulate, potentially evolving into material or strategic risks that require immediate attention. In this section, we have outlined a few essential concepts.

Vulnerability scanning, although distinct from testing, provides testers with potential targets and enables them to approach their work strategically rather than randomly. It serves as a reconnaissance step without being intrusive or disruptive. It can span all asset groups; however, it is vital to consider the tester's entry point into the environment. In some cases, testers may be provided with credentials or deliberately allowed to bypass regular controls, particularly when the objective is to assess the exposure of high-risk assets or evaluate vulnerability to insider threats. Understanding the context and purpose of vulnerability scanning enhances the effectiveness and relevance of the testing process.

Penetration testing involves conducting authorized cyberattacks that emulate the actions of a hacker, but with the explicit authorization of the asset owner and without the intention to cause harm. Testers launch cyberattacks against an asset or asset groups to assess the extent of their access and determine the effectiveness of existing security measures in detecting or stopping the attack. Penetration tests are typically performed manually to allow ethical hackers to adapt their methods when they are detected, blocked, or prevented from advancing further. Importantly, ethical hackers usually refrain from causing actual damage and instead provide detailed reports on their findings, whether successful or unsuccessful, enabling the asset owner to implement necessary remedial measures.

Application testing aims to identify vulnerabilities within a company's internally developed software that, if exploited, could potentially lead to exposure, compromise, or destruction of the company's assets. Applications can be tested by active attack, in which attackers look for common exploitable weaknesses. Alternatively, static application security testing involves scanning the software's source code for typical errors while dynamic testing assesses the executable code. Numerous software packages are available to automate scanning and testing processes, especially for applications under the control of the asset owner. Additionally, there are service providers who specialize in application testing.

An effective testing program should encompass all components of the defense ecosystem, including the people factor. It is crucial to incorporate various types of testing, utilizing different methods, while ensuring as much comprehensive coverage and repetition within the constraints of affordability. Testers may collaborate in groups, commonly referred to as red teams or blue teams denoting offensive (red) and defensive (blue) methods. For example, red team exercises involve simulating real-world attack scenarios to assess an organization's security defenses and incident response capabilities. Coupled with internal cyber audits and external SOX (the Sarbanes-Oxley Act) cyber audits, a proactive testing program is a powerful governance tool.

Chapter 7. **Measuring Efficacy and Maturity**

For board members, measuring the efficacy and maturity of a company's cyber program in its ability to protect against threats, detect attacks, and mitigate risks is essential. However, determining which cybersecurity metrics to use and how to collect data can be challenging due to variability in product quality and capabilities across cyber vendors and no standardization across companies and industries.

Frameworks such as NIST attempt to provide standardized metrics for benchmarking cybersecurity efficacy, but the need for standardization for risk-based metrics remains an issue. This highlights the importance of standardization efforts for cybersecurity metrics, which can benefit companies and the industry as a whole.

As cybersecurity breaches continue to make headlines, it is crucial to consider how cybersecurity metrics may integrate with executive compensation metrics in the future.

As cybersecurity breaches continue to make headlines, it is crucial to consider how cybersecurity metrics may integrate with executive compensation metrics in the future. Although the maturity of cyber programs does not yet permit this, recent events, such as publications of the Biden National Cybersecurity Strategy, and SEC and DOJ regulations on clawbacks, suggest that organizations should expect material cyber breaches to become subject to compensation clawbacks for executives.

To ensure that board members have the right set of metrics to assess a company's cybersecurity capability, it is helpful to categorize metrics into two groups:

- **Operational-level metrics** for understanding the efficacy of the cybersecurity program
- **Board-level metrics** for understanding the maturity level of the cybersecurity program as a whole

Cybersecurity practitioners are generally familiar with operational-level metrics. But when it comes to board-level dashboards, many companies need to create their own, as these metrics are less standardized. We present both types of metrics below. While we offer a range of typical operational-level metrics and identify those suitable for highly mature cyber programs, we don't provide specific numbers or ranges for these metrics since they vary from one company to another and depend on where a company is on its cybersecurity maturity roadmap. Similarly, we don't provide a typical board-level metrics dashboard because we believe that each CISO should be free to design one appropriate for their organization.

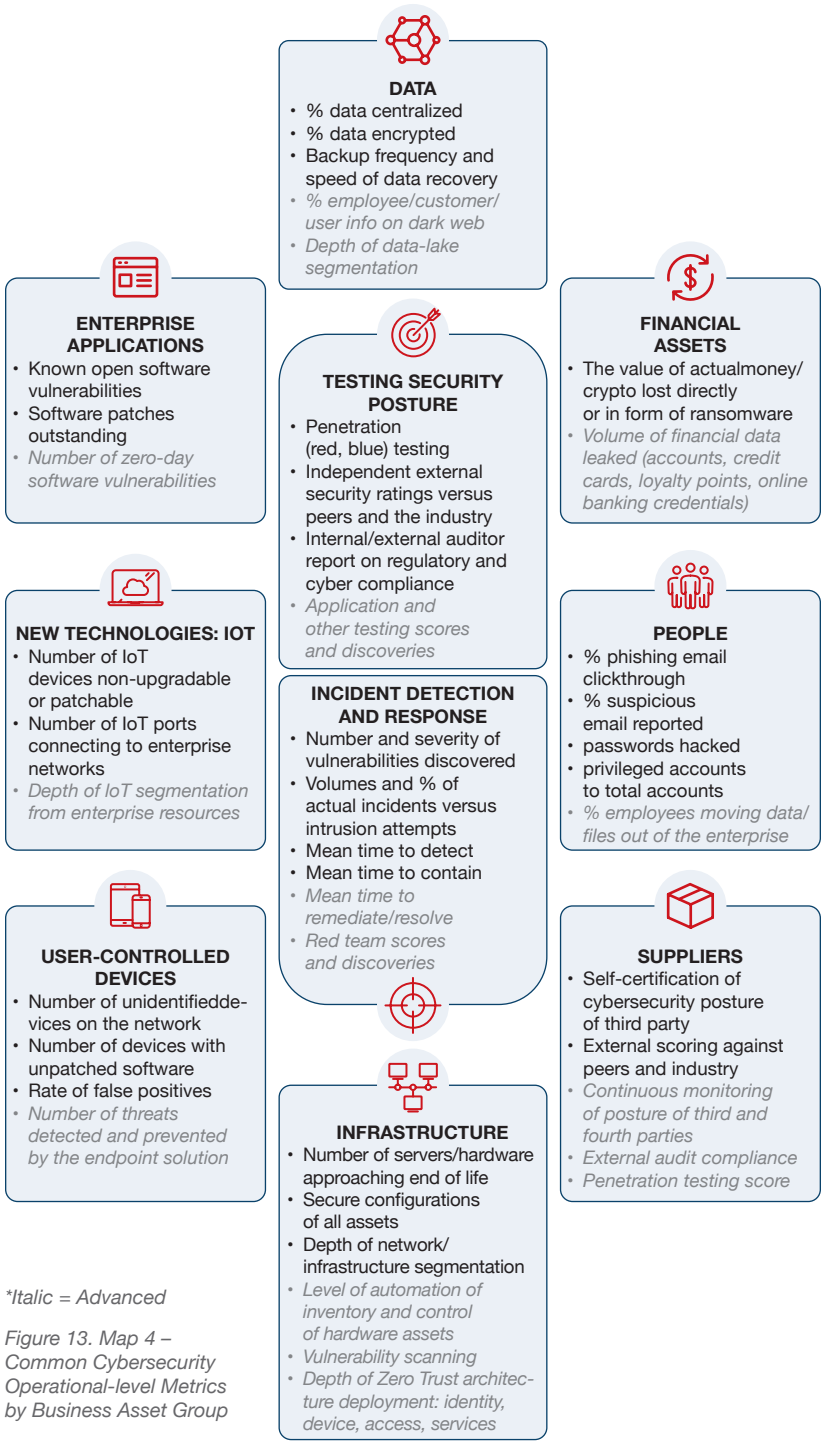
Operational-level Metrics

Security teams use operational metrics to track and report on cybersecurity activities and outcomes. When shared with the board of directors' risk or audit committees, these key performance indicators illuminate the organization's cybersecurity capabilities and the efficiency of cyber controls while also helping the board of directors evaluate the adequacy of investments in technology and talent.

Operational-level metrics should focus on crucial security impacts rather than only easily quantifiable data, including evaluating cybersecurity controls' functionality and recognizing any gaps. Data collected from continuous monitoring and detection of digital assets and related activities form the basis of these metrics. These capabilities are enhanced by integrating services from multiple vendors and incorporating new features to extract additional insights.

We have selected from a common set of operational-level metrics to provide board members with a clear view of protection mechanism performance. These metrics, categorized by asset groups, are further enriched with testing scores and benchmarking, detection, and mitigation metrics. Figure 13 depicts a selection of common metrics that are widely employed by cybersecurity professionals to measure the effectiveness of protection mechanisms as well as those of incident detection and response and benchmarking.

TYPICAL OPERATIONAL-LEVEL KEY PERFORMANCE INDICATORS



**Italic = Advanced*

Figure 13. Map 4 – Common Cybersecurity Operational-level Metrics by Business Asset Group

Consolidate and Correlate Metrics to Amplify Value

Effective utilization of operational-level metrics should align with a company's cyber program maturity. For instance, measuring the mean time to remediate/resolve a breach (i.e., the amount of time it takes to remediate and resolve a breach) may not be beneficial if the company does not have adequate threat detection and remediation capabilities.

Measuring progress and identifying improvement areas by comparing current practices with past performance and industry benchmarks is crucial. Regular examination and validation of the data behind these metrics is essential, as flawed data can lead to erroneous conclusions. Utilizing internal and external auditors, along with industry benchmarks, can help ensure metric validity and identify best practices.

While standardized metrics and tools often have a narrow focus, consolidating data from business-wide sources can enhance metric accuracy. Correlating metrics from different tools can identify trends, anomalies, and common outcomes.

Companies typically categorize metrics, provide descriptions, and assign benchmark or target ranges to make sense of the data. Cybersecurity operational metrics usually involve a mix of Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs). Board of directors' committees overseeing cybersecurity should distinguish between these two types for effective governance.

Lastly, the maturity levels of the Federal Financial Institutions Examination Council (FFIEC) Cyber Assessment Tool (CAT) can help track cybersecurity capabilities. This tool, applicable to non-financial institutions as well, assesses a company's inherent risk profile and defines the maturity level of the cybersecurity program across five categories: Baseline, Evolving, Intermediate, Advanced, and Innovative.

Board-level Metrics

Board-level metrics are crucial for assessing the maturity of the cybersecurity program and tracking cybersecurity risk. These metrics assist board members in executing their fiduciary and oversight responsibilities – allowing them to adopt a shareholder, regulatory, and risk-informed view. This understanding is critical in identifying gaps and weaknesses in the cybersecurity program and its roadmap

and determining the level of investment required to address these vulnerabilities. Board-level metrics are less standardized than operational-level metrics but are essential to enabling a board member to gauge the organization's overall cyber risk susceptibility.

For transparency in their decision-making, a board of directors should have a cyber dashboard that, at minimum, tracks the following information:

A. Assessment of cybersecurity culture
B. Assessment of cybersecurity program efficacy and regulatory compliance
C. Assessment of cybersecurity threat and enterprise risk profile
D. Assessment of investment levels and insurance coverage
E. Assessment of the organization's readiness to manage cyber breach impact

A. Assessment of Cybersecurity Culture

Much of cybersecurity success is rooted in an organization's cybersecurity culture, which includes the level of cybersecurity IQ, functional accountability and practical ownership, and executive engagement. While it is not easy to assess the organization's security culture, here are some dimensions to consider.

The level of cyberIQ: Every company should strive to attain a high cyberIQ across the organization. Board members can look for activities that increase and maintain a high cyberIQ level including regular education and training of employees, contract labor, and third-party partners, and demonstrating that teams can work together to achieve secure business outcomes.

The responsibility for building a culture of cyber awareness shouldn't rest solely with the CISO and their team, nor should they be the only ones held accountable for cybersecurity attacks and related failures.

Functional accountability and practical ownership: Cybersecurity accountability must extend across the entire organization, not just the technology functions. The responsibility for building a culture of cyber awareness shouldn't rest solely with the CISO and their team, nor should they be the only ones held accountable for cybersecurity attacks and

related failures. To achieve better business outcomes, security practices need to be fully incorporated into the corporate strategy. When business leaders share accountability for cyber success and failure, aided by the CISO's team, it demonstrates successful cybersecurity integration. In this setup, the CISO assumes a supportive role, and cybersecurity becomes an integral part of the business strategy rather than an isolated function.

Executive engagement: The CEO and other executives must engage in cybersecurity programs and possess a broad understanding of the strategic value of the security function. The CEO should have general cybersecurity knowledge, with decision-making and prioritization responsibilities delegated to a ranking executive. This executive is tasked with establishing materiality values to guide the identification of the company's top material cyber risks.

The appointed executive should receive regular updates on operational-level cybersecurity metrics, the program's maturity, regulatory compliance, threat assessments, and the enterprise risk profile. They should also be involved in determining the level of investment, insurance coverage, and the company's response plan in the event of a cyber breach.

HOW TO MEASURE THE CEO'S ENGAGEMENT

To measure the CEO's cybersecurity engagement (or that of other executives), the board of directors can assess the level of engagement between the CEO and internal teams, external advisors, and subject-matter experts. They can evaluate the CEO's ability to explain existing security gaps, the reasons behind them, and the steps being taken to address them. The board of directors should also consider the CEO's understanding of the company's resilience against cyber threats and the CEO's ability to discern when personal involvement is required versus when to delegate responsibilities.

B. Assessment of Cybersecurity Program Efficacy and Regulatory Compliance

Previously we provided a sample of common operational-level metrics owned by the CISO and security team that the ranking executive in charge of cybersecurity, the CEO and other executive team members, and a board of directors' committee should review. These operational-level metrics provide a model for the company to determine the efficacy of the organization's cybersecurity program and regulatory compliance and should identify gaps and shortcomings. The conclusions of these assessments should be summarized in several overall ratings and included in the company's cybersecurity dashboard.

C. Assessment of Cybersecurity Threat and Enterprise Risk Profile

Companies should incorporate KRIs that assess cybersecurity threats into their existing risk metrics to model their unique enterprise cyber risk. Specific to each company, these models form part of their comprehensive enterprise risk modeling.

In the Risk chapter, we explored the types of risks a cyber breach can cause, comparing and contrasting them with other enterprise risks. We recommend that organizations set trigger limits (green, amber, and red) for specific cyber breaches that could pose the most significant risks. For instance, we emphasized in the Risk chapter that business continuity risk, frequently caused by ransomware, should take priority.

Ransomware is often introduced via phishing emails, so companies should have KRIs that alert them based on the historical success rate of such emails and the strength of their defenses. Additional KRIs can assess the readiness of remediation mechanisms, such as backup/restore processes and network segregation.

D. Assessment of Investment Levels and Insurance Coverage

Investment levels should align with the threat environment and the cyber risks that the business seeks to avoid. Typically, large companies allocate 5-10 percent of their information technology budget to cybersecurity. Much of the company's IT budget will be dedicated to establishing a resilient and secure digital infrastructure, and cybersecurity expenditure is included in this budget as a natural extension of digital investment and should be considered as such.

For smaller organizations, cybersecurity budgets may exceed 5-10 percent of their IT budget due to the costs associated with building a minimum defense ecosystem. In such instances, these organizations might consider outsourcing their cybersecurity needs to third parties that offer fully managed programs with up-to-date technology stacks. Regardless of size, all organizations are recommended to procure independent vulnerability scanning services, penetration testing, and other types of testing, as discussed in Chapter 6.

As a company's cybersecurity program matures over time, the CISO should be able to differentiate and quantify the investment allocated to the defense ecosystem from the investment that enables innovation and business growth.

Cyber liability insurance is an effective risk management tool, with the amount of coverage depending on the size of the organization's technology stack and attack surface, which together determine overall risk exposure. Tools like self-insurance, larger retentions, and higher deductibles can be utilized to reduce premiums. We delved deeper into cyber insurance in Chapter 3 — Identifying and Addressing Cybersecurity Risk.

E. Assessment of Organization's Readiness to Manage Cyber Breach Impact

While security incidents can be project-managed by the security team, they should be led by business leaders. After all, most incidents stem from human error or business process failure, making it essential for these leaders to conduct business impact assessments both before significant digital decisions and after incidents to understand and address gaps.

Companies should not only manage cyber incidents but also their impact on customers. Understanding customer expectations and potential harm from poor security and privacy practices is critical. Business managers should go beyond mere compliance, promoting the company's security-related actions to customers. Understanding customer expectations and potential

Understanding customer expectations and potential harm from poor security and privacy practices is critical.

harm from poor security and privacy practices is critical. They should candidly discuss any inconveniences and emphasize the benefits of the company's efforts to customers. Good cybersecurity practices could establish trust with customers.

Revenue impact and intangible effects are other key considerations. Companies must measure, analyze, and use any revenue loss following security incidents to predict future losses. These assessments should be shared with key executives, including the CEO, to inform investment decisions. Moreover, companies should quantify intangible impacts, such as loss of customer confidence, damage to market reputation, decreased employee morale, loss of partner trust, and overall brand value impact. The cost of these adverse intangible impacts should be included to provide a comprehensive understanding of security incidents.

Chapter 8. **Closing Thoughts and Reflections**

Similar to any other business function, cybersecurity has gone through a period of forming, storming, norming, and, as the profession matures, performing. As organizations continue to evolve and change, so do the associated business risks. In parallel, cybersecurity practices must adapt and evolve to keep pace. This process is familiar to business leaders, but it moves much more rapidly now than in the past due to digital transformation impacting every aspect of the business.

As the business expands its digital footprint and ecosystem, it must strive to excel in delivering digital capabilities that allow customers, partners, and employees to achieve their business objectives from anywhere in the world and at any time, with minimal hurdles. Thanks to incredible technological innovations, the way technology is utilized would have been unimaginable just a few decades ago. Businesses now have access to a broad range of innovative technologies that are easily accessible, transparently scalable, and manageable in cost — and so do the competitors. In order to stay ahead, businesses must take advantage of digital reinvention, modernization, and transformation opportunities to deliver new services, drive new efficiencies, and tap into new markets. All of this must be done quickly while ensuring safety and security, and instilling trust in customers and other stakeholders.

Technology leaders are expected to create, adopt, and deliver technology solutions that support business goals while operating at a high speed. However, as the technology infrastructure expands, so does the attack surface. The volume of data increases exponentially, along with its value, which, in turn, heightens the potential risk to business growth. Cybersecurity measures must continually evolve to protect a vast, amorphous, and rapidly expanding digital landscape that is filled with unknown agents, ever-evolving risks, and lurking threats.

Board members must help drive a business-first, business-aligned mindset when it comes to cybersecurity and all technologies utilized by the organization. When considering security measures within the

business and the ongoing demands for investments in this area, it is important to maintain a balanced view and keep in mind the following five points:

1. **Cybersecurity is not the business, it protects and enables the business.** Cybersecurity can be viewed as a business enabler rather than a cost-center function. It is necessary to enable businesses to deliver products and services safely and quickly, that otherwise it could not do, as well as to support standard business functions.

   It may be necessary to reconsider the meaning of return on investment in the context of cybersecurity. To draw upon a common analogy, investing in better brakes doesn't make a race car drive any faster. However, it allows the driver to take full advantage of the engine's capabilities, including horsepower and torque, and to navigate turns more aggressively, with the assurance that the brakes will operate at a higher level when necessary. Similarly, a high-performing security function allows other areas of the business to perform more aggressively and create a competitive edge because cyber risks are being effectively managed.

   Going back to a traditional business model, the business may see an indirect return on the investment in security as it considers opening new markets (online sales, international supply chains, additional market segments), or lowered costs (as fraud and ransomware costs are lowered), or faster time to value (because the digital processes are functioning more reliably and consistently). Regardless of the direction in which businesses seek to expand, a robust security function plays a crucial role in protecting and preserving the value of the organization.

   Detractors may argue that cybersecurity is an endless drain on budgets. However, in reality, the risks addressed by high-performing cybersecurity programs are not solely cybersecurity concerns. Rather, they are business problems that the cybersecurity teams are attempting to address. What may look like mere security investments are actually business investments. These investments are necessary to safeguard a company's digital and physical assets and critical processes, ensuring that they remain secure and protected.

2. **Organizations should integrate cybersecurity reporting into each business update rather than handle it as a separate or adjacent discussion.** The cybersecurity function should be viewed through the lens of value preservation, protecting business functions, capabilities, delivery, and other aspects of the business that generate value. The discussion around cybersecurity should be driven by the business function, with line managers taking ownership of cyber risk. While the security function should provide guidance and support and be responsible for cybersecurity operations, it should not drive or assume cyber risk responsibility for the business. Business leaders should be prepared to discuss current and future risks and how proposed actions will affect risk calculations.

3. **Great technology is not a substitute for great leaders.** Organizations should prioritize the selection of capable leaders to helm their cybersecurity function, accompanied by a capable support team. All too often, discussions concerning cybersecurity begin and end with technology, threats, attacks, and incidents, overlooking the significance of the leader's role.

   Organizations and boards of directors should consider many aspects of cybersecurity leadership including but not limited to "What kind of leader should we rely on to give us thoughtful, informed, and informative updates on cybersecurity? What qualities are most important? Are they credible? Do they have the right skills and competencies to provide board members with the information necessary to execute their duty of care?"

4. **Companies should invest thoughtfully, whether financially or through resources; be responsive to business needs, but not over-responsive.** Companies should prioritize investing in activities that provide broad or long-term value to ensure shareholder return. Over-optimizing cybersecurity investments may result in continuously investing in new solutions to solve minor variations on an original problem. While it's important to address emerging risks with new cybersecurity solutions, it's also important to understand that accounting for all risks will never be possible. Evolving business practices, adopting new technologies, and motivated adversaries create the constant need to learn and respond to new threats over time.

5. **Companies and boards of directors should act before they react, and guide before they deride.** Despite the best efforts of the company and its leadership in investing in top-of-the-line cybersecurity solutions and diligently preventing security breaches, cyber breach events can still occur. Even in the absence of errors and with an exceptionally dedicated and proficient team at the helm, incidents are bound to transpire. It is vital to prepare for such occurrences.

   It is crucial for the company to understand the professional and emotional impact of cyberattacks on the cybersecurity team and to establish a framework that ensures the team understands the board of directors' expectations for informing them of incidents, including what qualifies as a material incident. By doing so, the team will be aware that the board members appreciate the nature of risk and will not fault them for their role in informing the board of directors. Establishing this framework will avoid divergence between the board of directors' objectives and the cybersecurity team's understanding of them, which could result in inaccurate assumptions. It is best to communicate the board of directors' requirements to the team beforehand to ensure their needs are met during a crisis.

   During a crisis, there is no time to devise and organize a plan. It is wise to prepare in advance while the teams have sufficient time to prepare adequately.

OUR FINAL THOUGHTS

Although technology advances at an exponential rate, the bedrock principles of security evolve at a comparatively slower pace. While these principles do evolve, the pace of change is not so swift as to reduce the value of fundamental concepts and terminology in the field. By acquiring fluency in this language, board members gain a more comprehensive understanding of the challenges posed by cybersecurity and can effectively articulate thoughts and ideas. This knowledge makes board members more informed and effective in having a deeper dialogue in the midst of these constantly evolving times.

Glossary

- **Adaptive Trust:** A dynamic security approach that modifies user access levels based on real-time behavior, context, and risk factors, ensuring the right access is granted at the right time.

- **Alert Storms:** When an alerting system generates so many alerts that it overwhelms the ability of the organization to analyze them properly to identify true problems.

- **Alerting:** A notification or system of notifications that make an organization aware of perceived or actual threats, or suspicious behavior.

- **Attack Surface:** The total of all the points in an organization's hardware, software, and networks where unauthorized users can attempt to gain access or extract data. The larger the attack surface, the more vulnerabilities there are for potential cyberattacks.

- **App Security:** Today, applications come from many sources and are not just internally created. Many of the applications businesses use on a daily basis may not be owned or controlled by the organization itself. Additionally, applications often utilize code from external sources. This realm of cybersecurity ensures these attack vectors are protected and users can access applications safely, as applications are gateways to business data. This domain includes secure development tools, DevSecOps, and web security.

- **CISA:** Certified Information Systems Auditor is a globally recognized certification offered by Information Systems Audit and Control Association (ISACA) that validates a professional's ability to assess, audit, and control an organization's business and IT systems.

- **Cloud Security:** Cloud security is a branch of cybersecurity focused on protecting cloud computing systems and the networking needed to use cloud-based infrastructure. Securing web traffic is part of network security, but securing traffic to and from a cloud and

between clouds is also considered cloud security. Companies need data to be kept safe and private for all cloud-based infrastructure, applications, and platforms. Cloud security protects cloud-based systems, data, and infrastructure. In contrast, web security protects websites and web applications from threats.

- **COBIT:** Control Objectives for Information and Related Technologies is a framework developed by Information Systems Audit and Control Association (ISACA) that provides best practices for IT governance and management, helping organizations align IT processes with business objectives.

- **COSO:** Committee of Sponsoring Organizations of the Treadway Commission is a joint initiative that provides a framework for enterprise risk management, internal control, and fraud deterrence, aiming to improve organizational performance and governance.

- **Credential Management:** The process of creating, storing, managing, and updating digital identities and access permissions within a system or network.

- **Data Protection:** The goal of data protection as a cybersecurity domain is, as the name suggests, to secure data assets. This includes protecting data repositories, transactional information, and how data assets are used. Data is now ubiquitous in all businesses. It is constantly being created in huge volumes. But before data can be protected, companies must understand what data they have. Therefore, organizations need tools that enable them to determine what data they have and then evaluate that data in terms of its importance. Crown jewel data assets should receive the greatest protection and allocation of cybersecurity resources. How much companies spend on data protection should be determined based on how data is used and monetized within the business.

- **Device Security:** Device security is a branch of cybersecurity concerned with protecting devices from attacks. This is one of the most mature areas of cybersecurity, which began with anti-malware systems for personal computers, and has expanded to cover the many devices now in use. Device security includes IoT security and endpoint protection.

- **DevSecOps:** Development, Security, Operations, which is the idea that security should be integrated into every aspect of the software development and operations life cycle.

- **Encryption:** The method of shielding data or information by using codes that conceal the asset's true meaning.

- **Identity Management:** Identity management is a framework of business processes, policies, and technologies that facilitate the management and authentication of electronic or digital identities for people, machines, IoT assets, and other aspects linked to a network. It is a way to control and manage access to the critical information within an organization.

- **Identity Orchestration:** A process that manages and coordinates the various components of digital identity across different systems, platforms, and applications. It involves synchronizing the user's identity information, such as usernames, passwords, and roles, across multiple identity and access management (IAM) systems. Identity orchestration aims to ensure a seamless and secure user experience, simplify the administration of digital identities, and enhance security by providing consistent and accurate identity data across all systems.

- **Incident Management:** When attacks occur, companies need to have incident management practices, strategies, and tools in place to reduce and avoid harm. Incident management involves identifying, analyzing, and responding to cybersecurity incidents.

- **ISO:** International Organization for Standardization is an independent, non-governmental international organization that develops and publishes standards to ensure the quality, safety, and efficiency of products, services, and systems across various industries.

- **LAN:** Local-area network, which is a computer that links to other computers on a local network within a single physical location.

- **Multi-factor Authentication (MFA):** Confirms a user's identity by requiring two or more evidence factors before granting access to a system or data. These can include a combination of something the user knows, such as a password; something the user has, like

a smartphone app that generates a one-time code or a physical security token; and something biometric like fingerprints or facial recognition. MFA increases the difficulty of unauthorized access since compromising one factor, like a password, wouldn't be sufficient without the other required factor(s).

- **Network Security:** Secure connectivity involves protecting connections by using encryption and other protocols to ensure the security of data moving over a network. This can include firewalls and SD-WAN for corporate network security. For cloud network security that connects clouds and data centers together, protection comes from cloud-based security components that are part of public cloud platforms. Network security includes protection for web traffic and traffic to and from cloud infrastructure.

- **NIST:** National Institute of Standards and Technology is a U.S. government agency that develops and promotes measurement standards and technology to enhance productivity, innovation, and security.

- **NOC:** The Network Operations Center of an organization, which is the centralized location through which IT staff monitors the organization's network activity.

- **People Security:** There is perhaps no bigger vulnerability within enterprise security than the people who work at an organization. Unintentionally, whether by clicking on the wrong email link, or connecting from unsecured devices, people can expose a business to many cybersecurity threats. The domain of people security therefore involves proper training for staff to avoid predictable risks. It also includes having tools and procedures to identify potential insider threats. It should set a framework for being able to determine who can be fully versus partially trusted, and who cannot be trusted at all. It should protect an organization from bad actors, accidental actions, and insiders who act maliciously.

- **Phishing:** A type of cybersecurity attack in which attackers try to trick trusted users into accidentally making a wrong decision, such as clicking a dangerous link or downloading attachments that then give the attackers access to the corporate network.

- **Policies (or Security Policies):** How an organization defines and documents its approach to cybersecurity and threat management.

- **SD-WAN:** A software-defined approach to a wide-area network, which is a centralized and virtualized service that enables the users of a corporate network to connect securely from anywhere.

- **Secure Access Service Edge (SASE):** An architecture for unified, cloud-delivered cybersecurity that integrates network security functions like Secure Web Gateway (SWG) and Firewall-as-a-Service (FWaaS) with secure access services such as Cloud Access Security Broker (CASB), Zero Trust Network Access (ZTNA), and Software-defined WAN (SD-WAN). Delivered as a service, SASE offers a scalable and flexible solution for securely connecting users and devices to on-premises or cloud resources, eliminating the need for hardware or software installation and maintenance. It efficiently protects against threats and vulnerabilities while ensuring data protection everywhere.

- **Security Communication and Collaboration Tools:** The communication and collaboration tools enterprises rely on to function are also some of their largest cybersecurity vulnerabilities. This includes email and collaboration tools like Slack, Chat, and iMessages. These channels must be protected from phishing, social engineering, and other impersonation-based attacks.

- **Security Service Edge (SSE):** A converged, cloud-native security solution that integrates vital security technologies into a unified platform, forming a key component of the Secure Access Service Edge (SASE) architecture. It provides comprehensive visibility and control over data across various sources, decoding and analyzing the cloud traffic that is beyond the capabilities of traditional security measures. Using Zero Trust principles, SSE is scalable and flexible, adapting to an organization's needs and allowing customization to meet specific security requirements. Beyond policy enforcement, effective SSE fosters a culture of security by coaching employees and encouraging safe data behavior.

- **SOC:** The Security Operations Center of an organization, which is the team responsible for monitoring, preventing, detecting, and responding to cybersecurity threats.

- **Supply Chain Security:** Today's supply chains are vast and much more complicated than in the past. They are composed of hardware, software, and managed services from third-party vendors, suppliers, and other providers. Companies need protocols and tools in place to secure their supply chain both from cyber risks and physical and geographical threats that can cause disruptions.

- **TCP/IP:** Transmission Control Protocol/Internet Protocol, which is an array of communication protocols used to connect network devices on the internet. It is a set of rules and procedures that can also be used as a communications protocol in a private computer network.

- **Threat Detection:** Threat detection within cybersecurity entails monitoring and analyzing an ecosystem to find any malicious activity that could threaten the network. This can include deception, which is a type of attack in which attackers impersonate trusted users to gain unwarranted access to the network. When a threat is detected, then mitigation efforts must be used to minimize the impact of potential attacks.

- **WAN:** Wide-area network, which is a network that is distributed across a large geographical area, or even globally.

- **Web Security:** The measures taken to ensure that websites and web applications are safe from threats on the internet. It protects personal and organizational public-facing websites from DDoS attacks, malware, data breaches, and other cyber threats.

THE CYBER SAVVY BOARDROOM

> Cybersecurity is definitely a hot topic for boards of directors everywhere. The Cyber Savvy Boardroom is a must-read about the risks and rewards of cybersecurity.
>
> **Ana Botín, Executive Chair of Santander Group**

> This book should be read at least once by each board of directors to get a full view of cybersecurity and how organizations should be protected. On the basis of these focused explanations, all board members can reach out to their CISO and expect to fully understand the risk in their business.
>
> **Bernard Gavgani, Group CIO, BNP Paribas**

> Cybersecurity knowledge is now essential at the board level, especially for risk management. This book therefore is a must read. It translates a complicated topic with many nuances into easily understood concepts that help every board director feel better prepared.
>
> **John Thompson, Partner, Lightspeed Ventures, and former Chair, Microsoft**

> Much has been written about cybersecurity. But this excellent, thoughtful and practical book puts the issues in proper perspective. A good read for any board member.
>
> **Seifi Ghasemi, Chairman, President and CEO, Air Products and Chemicals, Inc.**

09/23 BK-693-2