EgonZehnder

Rewiring Boardroom Cybersecurity

Boards must act now to safeguard their organizations from cyberattacks. This playbook lays out tangible actions for boards to strengthen cyber-preparedness and protect organizations from current and emerging threats.

April 2023

Author:

Dr. Moudy Elbayadi
SVP, Chief Technology Officer, Shutterfly, Inc.
Author of *Big Breaches: Cybersecurity Lessons for Everyone*

Contributors:

Karena Man, William Houston, Scott Texeira, and Drew McFeetors
Consultants, Egon Zehnder
Rod Hackman, Board Member

Foreword

In late 2013, Target's systems were breached when a third-party contractor fell victim to a phishing attack. The hackers were able to install malware on Target's point-of-sale (POS) systems, which allowed them to steal the credit and debit card information of approximately 40 million customers, as well as the personal information of 70 million customers including names, addresses, and phone numbers. Target had to pay out millions of dollars in settlements and fines, including a $18.5 million settlement with 47 states and the District of Columbia, as well as a $10 million class-action lawsuit settlement with affected customers. The breach also led to a drop in sales and stock prices, with Target reporting a $17 million loss in profits during the fourth quarter of 2013. Multiple board members, including Kenneth Salazar, Mary Dillon, Roxanne Austin, and CEO Gregg Steinhafel were called to testify before Congress.

Four years later in 2017, Equifax suffered one of the largest data breaches in history. The breach involved hackers accessing the personal and financial information of approximately 143 million Equifax customers, including names, birth dates, Social Security numbers, and credit card information. The breach also exposed driver's license numbers for some customers. Equifax had to pay out millions of dollars in settlements and fines, including a $700 million settlement with the Federal Trade Commission (FTC) and other government agencies, and a $380.5 million settlement with affected consumers. The breach also led to a drop in Equifax's stock price, and the resignation of several high-ranking executives. Richard Smith, then CEO of Equifax, was summoned before Congress in October 2017. Testimony also included current and former board members, including Mark Feidler, John McKinley, and Edith Cooper.

It's well-understood today that the threat of cyberattacks poses a significant risk to companies in reputation, business continuity, and financial losses. Yet despite these and many other high-profile examples, companies and boards continue to make fundamental mistakes in their cybersecurity policies such as relying on regulatory compliance as a complete defense or relegating cybersecurity to a simple IT issue. Even as the level of awareness on this imminent threat has increased, it hasn't necessarily translated into the required level of commitment at the board level, or ideally the appointment of a director with a spike on cybersecurity.

The time for boards to act is now.

With such high stakes on the line, it's clear that cybersecurity is an indispensable competence in the boardroom. In this e-book, author Dr. Moudy Elbayadi, CTO of Shutterfly and author of Big Breaches: Cybersecurity Lessons for Everyone, offers a concise and practical playbook for boards of directors to improve their understanding of cybersecurity issues and challenges, create a systemic approach to improve their company's defenses, and prepare for potential attacks with an integrated, holistic plan.

Our hope is that these resources take your organization's cyber-preparedness to the next level. Are you ready to rewire your board?

Karena Man, William Houston, Scott Texeira, Drew McFeetors
Members of Egon Zehnder's Cybersecurity Practice Group

Purpose of this e-book

According to the World Economic Forum, 60 percent of the Global GDP is now digital. It is now clear that the majority of the world's economic output relies on technology being reliable, available – and importantly – secure from unauthorized parties that may wish to disrupt it. Given the immense risk that cyberattacks pose to the economy, regulators in the United States are beginning to take action. In March 2022, the U.S. Securities and Exchange Commission (SEC) proposed new rules to bring greater focus and accountability. There have been several changes regarding cybersecurity regulations, including the requirement to report material cybersecurity incidents and the requirement for boards to disclose their level of oversight of cybersecurity risk and board member cybersecurity expertise. In addition, there is now an increased emphasis on the role of management in implementing cybersecurity policies and procedures, as well as identifying and managing cybersecurity risks. In short, security is no longer just an "IT issue."

Our purpose in writing this e-book is to help directors and leaders of all levels engage in the right conversations about cybersecurity and digital risk. Not only to prepare and get ahead of the new SEC rules but also to implement improved governance and cyber resilience. In addition, we aim to inspire the next generation of directors to take on this critical challenge and lead with greater digital impact. A recent MIT study concluded that companies that had digital-savvy directors on the board had 38 percent higher revenue growth, 34 percent higher ROA, and 34 percent higher market gap growth.

Our primary thesis is simple: Cyber-risk is a part of enterprise risk, a form of systemic risk to all companies, which can only be dealt with and contextualized by understanding the underlying systems. When boards get curious and begin having the right conversations with security and technology leaders, they will be able to provide better oversight and reduce the risks of a cyberattack and increase the resilience of their firms. These "right conversations" can happen only when all participants speak the same language and are educated and organized for cybersecurity success. This is not only possible, but essential as the moment for leadership and action is now. This e-book is your playbook for this change journey.

Chapters Overview

Chapter One takes a deep dive into the reasons behind organizations' continued vulnerability to cyberattacks despite their increased investments in cybersecurity. The chapter highlights two dangerous mindsets that hinder progress in cybersecurity: compliance-focused programs and treating cybersecurity as an IT-only issue. Compliance-focused programs may meet the minimum regulatory standards but fail to address real-world risks while treating cybersecurity as an IT-only issue fails to address the human factor in cybersecurity. The chapter emphasizes the importance of addressing the human factor and highlights the need for a comprehensive, systemic approach to cybersecurity that involves all aspects of the corporation, including employees, processes, and technology. The approach would help organizations develop a more strategic cybersecurity plan, addressing enterprise risks while engaging the board of directors in a more meaningful way.

Chapter Two focuses on the board of directors' responsibility for cybersecurity governance and the importance of understanding the business ecosystem. We recommend elevating the Chief Information Security Officer (CISO) role, establishing Cybersecurity Risk Committees, and promoting continuous education to foster an enterprise-wide culture of managing and governing cyber-risk. By making organizational, educational, and cultural changes, organizations can substantially improve their cybersecurity governance and proactively tackle cyber risks.

Chapter Three highlights the importance of involving the CISO in board discussions as businesses adapt to the new reality of remote work and digital transformation. Regular conversations with the CISO can help boards better understand the organization's cybersecurity strategy, potential risks, and the financial impact of cyber incidents. Furthermore, the chapter emphasizes the need for open dialogue and encourages board members to ask questions without fear, fostering a better understanding of cyber risks and the board's role in managing them. Engaging with the CISO ensures that organizations are prepared to respond to cyber threats effectively.

Chapter Four emphasizes the importance of understanding technical debt and its impact on cybersecurity. Technical debt, which accumulates when organizations prioritize short-term gains over long-term technology investments, can lead to outdated and vulnerable systems. The chapter highlights the importance of discussing tech debt with the board and investing in technology upgrades to improve security. Regular security assessments can help identify and prioritize areas of tech debt that need to be addressed. The board plays a critical role in understanding and managing technical debt by asking the right questions about the organization's strategy, budget, and the role of the CISO in addressing tech debt. Proper management of technical debt helps reduce the risk of cyberattacks and strengthens the organization's security posture.

Chapter Five emphasizes the importance of hiring experts with diverse backgrounds to strengthen an organization's cybersecurity. A diverse team brings multiple dimensions of expertise, including industry-specific knowledge, experience in high-pressure environments, and alternate perspectives from non-traditional industries. Military veterans, professionals from critical infrastructure sectors, and individuals with diverse cultural, gender, and age backgrounds contribute to better problem-solving and decision-making. Boards of directors are advised to prioritize diversity in recruitment and selection to create a comprehensive approach to cybersecurity, identifying vulnerabilities and mitigating potential threats more effectively.

Chapter Six discusses critical questions that boards of directors should be asking their CISO and senior technology executives to ensure effective cybersecurity. Boards need to inquire about the organization's overall cybersecurity posture, protection of critical assets, addressing emerging threats, measuring the effectiveness of cybersecurity controls, and preparing for potential breaches. By engaging in regular conversations with the CISO and senior technology executives, boards gain insights into the organization's cybersecurity posture and take necessary steps to mitigate risks. Asking the right questions ensures that boards are actively involved in maintaining strong cybersecurity measures, preparing for emerging threats, and fostering a supportive environment for the CISO and technology executives.

Chapter Seven emphasizes the importance of creating an effective cybersecurity risk subcommittee within an organization to provide guidance and advice to the board of directors on cybersecurity matters. The chapter outlines several key steps that organizations can take to establish an effective subcommittee, including defining the subcommittee's purpose and scope, identifying members with diverse expertise, providing cybersecurity training, assigning a chairperson, establishing a regular meeting schedule, developing a work plan, and reporting to the board of directors regularly. The subcommittee's agenda should cover various topics such as cybersecurity risk management, emerging threats, incident response planning, cybersecurity insurance, third-party risk management, employee training, regulation and compliance, budget allocation, data protection, technology debt, technology roadmap, and cybersecurity metrics and reporting. By establishing an effective cybersecurity risk subcommittee, organizations can enhance their cybersecurity governance and risk management capabilities.

Chapter Eight focuses on the importance of preparing organizations for the worst-case scenario: a major data breach and outage. The chapter emphasizes the importance of having a robust incident response plan and conducting regular tests to ensure preparedness. Key steps include appointing a breach response team, identifying critical systems and data, containing the breach, investigating the breach, notifying affected parties, implementing remediation measures, communicating with stakeholders, and reviewing and improving security measures. The chapter also highlights the value of conducting simulated breaches (wargames) and employing white-hat hackers to test and strengthen an organization's cybersecurity defenses. By preparing for a major data breach and outage, organizations can mitigate the risks and minimize the impact of a cyber incident.

Chapter Nine highlights the importance of celebrating victories in cybersecurity, which is often overlooked due to the nature of the field. Success in cybersecurity means that nothing happened, which can make it challenging to identify and celebrate accomplishments. However, recognizing and celebrating successes is vital for building morale, motivation, and fostering a positive culture. This chapter emphasizes the role of the board in acknowledging and celebrating the security and technology team's efforts through formal recognition programs, awards, or simply appreciating their contributions. It is also important to celebrate both individual and organizational successes to build a positive corporate culture, foster unity, and encourage collaboration across departments. By celebrating victories in cybersecurity, organizations can create a sense of pride, purpose, and commitment in their cybersecurity teams, which can help improve their cybersecurity posture and reduce the risk of cyber incidents.

CHAPTER 1

The Broken State of Cybersecurity Governance

Despite the increase in cybersecurity and technology investments, organizations still object that they don't feel any safer. We realize that firms of all shapes and sizes are taking steps to protect their data and systems, yet they mostly remain vulnerable to attackers. The "blast radius" of an incident is still large and unwieldy. This chapter will explore the reasons why the traditional approach – viewing cybersecurity as primarily an isolated "IT issue" and making compliance the goal – is inadequate in defending against the growing threat of cyberattacks. By recognizing cybersecurity as a business risk on par with other enterprise risks, such as supply chain and capital structure, organizations can adopt a more comprehensive strategy that encompasses all aspects of the enterprise.

> *"Leadership is about making the tough calls, not just the easy ones. It's about recognizing when something isn't working and being willing to pivot, even if it means admitting failure and starting over."*
>
> **Ben Horowitz**
> Co-founder of Andreessen Horowitz and Opsware

Two Dangerous Mindsets That Thwart Cybersecurity Progress

Given the complex and ever-evolving threat landscape, organizations are constantly facing new challenges to securing and protecting their networks and systems from cyberattacks. Despite investing significant resources into cybersecurity, many organizations still struggle to achieve the desired resilience. There are two paradigms that are holding organizations back from contextualizing systemic cyber risk and making more progress faster: the first is a compliance-focused "check-the-box" security program, and the other is treating cybersecurity as an "IT-only" issue.

Mistake 1: Having Only a Compliance-Focused Program

A compliance-focused security program is a paradigm where organizations focus primarily on meeting regulations and standards, such as PCI DSS, HIPAA, and ISO 27001. While compliance is an important aspect of cybersecurity and must be satisfied, it only partially protects organizations from cyber threats. An additional danger is that compliance can deliver the board false comfort that cybersecurity governance is being satisfied. Compliance-focused security programs are piecemeal, reactive and defensive

in nature. They only address known risks and vulnerabilities. In today's rapidly changing threat landscape, this approach is insufficient as cybercriminals are constantly finding new ways to attack organizations. Also, while the attacks are executed systematically, the compliance programs are implemented in fragments.

Phil Venables, the highly regarded Chief Information Security Officer for Google Cloud and formerly Goldman Sachs, writes, "Compliance is a necessary but insufficient condition for security. Many compliance regimes do, in fact, represent a baseline level of security that is useful and necessary, but sustaining compliance does not equate to the security you might need in your context." Simply put, as cyberattacks become more advanced, coordinated, and sophisticated, companies will need an equally well-coordinated and systemic approach to cybersecurity to have a better chance of successfully defending against those threats. Compliance-first approaches do not take into account the constantly evolving nature of cyber threats. Organizations must be proactive in their defense and stay ahead of the curve by implementing comprehensive security strategies that take into account the changing nature of cyber threats.

It is important to note that compliance with regulations should not be ignored. However, this should not be the sole focus of an organization's cybersecurity governance. Organizations need to take a comprehensive approach that integrates regulatory requirements into a larger, more comprehensive security strategy and addresses the changing nature of cyber threats.

Mistake 2: Security as an IT Problem

Treating cybersecurity as an IT problem only perpetuates the notion that cybersecurity is an isolated technical issue and not a business risk deserving of board oversight. It is both! This narrow approach fails to consider the full spectrum of cyber threats and the impact they can have on an organization. In the event of a breach, the company could face significant financial losses, reputational damage, and a loss of trust among its customers and shareholders. This can have long-term consequences that far outweigh any investments required to prevent such events. While IT professionals are critical to defending against cyber threats, they cannot do so effectively in isolation. Cybersecurity requires a cross-functional, integrated systems approach and corporate culture change that involves the entire organization, including a board of "digital savvy" directors (see MIT study).

When cybersecurity is viewed as an IT problem, it is often siloed and treated as a low priority compared to other business initiatives. This can lead to inadequate and suboptimal allocation of investment in cybersecurity and a lack of accountability at the highest levels of an organization. Furthermore, this approach can create a false sense of security as the focus on IT-specific solutions may overlook the importance of non-technical factors such as employee training, incident response planning, and third-party risk management.

These two dangerous mindsets highlight the need for organizations to adopt a more comprehensive and systemic approach to cybersecurity. By viewing cybersecurity as a business problem and an enterprise risk, organizations can develop a more strategic approach that involves all aspects of the corporation, including employees, processes, and technology.

Humans are still the Weakest link

One of the primary reasons the above approaches fail is the lack of attention to the human factor. No matter how secure a company's technology is, the weakest link in the security chain is often the employees. A company may have the latest firewalls and endpoint protection, but if its employees are not trained in basic cybersecurity best practices, such as identifying phishing emails, the organization remains vulnerable to attack.

According to Deloitte, a staggering 91 percent of successful cyberattacks began with a phishing email, highlighting the critical role of addressing the human factor in cybersecurity governance. It is our belief that implementing intelligent security measures that are user-friendly and don't create

significant obstacles will encourage employees to comply with cybersecurity protocols. For instance, a 90-day password change policy can be cumbersome and less effective than requiring longer passphrases that don't expire as frequently and have demonstrated greater effectiveness in the real world.

Lack of Board Involvement

The lack of involvement from boards of directors is the final major factor contributing to the broken state of cybersecurity governance. Board members are often not knowledgeable about cybersecurity risks and may not understand the importance of having a robust cybersecurity strategy in place. This can result in a lack of support for cybersecurity initiatives and a lack of resources allocated toward the development of a comprehensive security program. While some companies are adopting and adding digital savvy directors, many are still operating in the old way, where technology and system risk are not considered at the board level. The following chapters outline a new approach to cybersecurity that brings the board of directors closer to this area of enterprise risk and will aid in improving the relationship and coordination between the board and security and technology executives. With the right conversations and investments in key areas, organizations can make meaningful progress in their journey toward a more secure future.

CHAPTER 2

Board Responsibility for the Ecosystems They Govern

The board of directors bears the ultimate responsibility for cybersecurity governance, one which cannot be transferred to management. Cyber-risk is a form of systemic risk that can only be governed by understanding your business ecosystem, a regularly interacting or interdependent group of elements and subsystems which comprise your business function. Ecosystem elements include assets, processes, and the people who interact with one another both internally and externally. Despite the complexity and changing nature of the ecosystem, boards can effectively govern by committing to firm-wide organizational, educational, and cultural reforms which lead to the development of an understanding of the ecosystem sufficient for good governance. Cyber risk cannot be contextualized and governed without understanding this ecosystem. There are no "check-the-box" solutions.

> *"The biggest issue for a typical board to focus on is how to become cyber-resilient quickly."*
>
> **Brad Smith**
> President and Chief Legal Officer, Microsoft

Change Board Culture on Cybersecurity

Cyber-risk is becoming more complex and chaotic. Market, regulatory and legal pressures are mounting for boards to get control of and develop better cybersecurity governance practices. Economic damage and litigation exposure are increasing at the same time, while cyber insurers are charging more and covering less. As discussed, the SEC is proposing "SOX-like" disclosure requirements that will drive new board composition and behavior. This leads to the conclusion that major changes in board cultures are inevitable. Boards must choose to become proactive to get ahead of this problem or to remain reactive with unknown consequences. Some practical steps and recommendations for changing the board culture follow:

- **Inform** - Directors must be regularly informed about the organization's cybersecurity posture, emerging threats, and the potential business impact of cyber incidents. In addition to providing an internal perspective, providing real-life examples and case studies of other organizations that have experienced significant financial or reputational damage due to cyberattacks can help drive home the importance of this issue.
- **Self-learning** - Education will enable the board to better understand the complexities of cybersecurity and appreciate its critical role in the organization's overall risk management strategy.
- **Engage Experts** - Cybersecurity and technology experts can advise the board on specific threats, best practices, and industry trends. These qualified technology experts (QTEs) can offer valuable insights, ensuring that the board remains up-to-date with the rapidly evolving cyber threat landscape.
- **Engage with the Cyber Community** - Encourage board members to attend cybersecurity conferences, workshops, and training sessions to deepen their understanding of the subject matter. Being around the cyber community and other digital savvy directors will demystify what might seem a foreign and intractable issue.
- **Create a Culture of Accountability** by assigning specific cybersecurity responsibilities to individual directors. This can include appointing dedicated board members with cybersecurity expertise or establishing a cybersecurity subcommittee responsible for overseeing the organization's cyber risk management efforts.

Organizing for Cyber Resiliency

A strong signal of the importance of cybersecurity as part of enterprise risk management is to elevate the Chief Information Security Officer (CISO) role to report to the C-Suite and also have direct channel to the cybersecurity subcommittee, if one exists. Additionally, boards should establish Cybersecurity Risk Committees at both the board and management level. Both committees should interact on a regular basis to evaluate and mitigate existing risks and new risks introduced by changes to the business ecosystem. Changes could include new digital technologies, acquisitions, divestitures, changing third-party relationships, etc. The management committee should include representatives from all functional areas of the enterprise and be led by the CISO. Additionally, the charter for the committee should establish clear authorities and responsibilities for committee heads.

Keys to Understanding the Ecosystem

To create a robust cybersecurity culture within an organization, it's essential for all stakeholders, including board members, to grasp the key concepts and vocabulary related to cybersecurity. Begin by inviting external advisors to collaborate with your management team and board to explore, clarify, and explain the various components of your organization's cybersecurity ecosystem, using easy-to-understand business language. This process can be integrated into the broader risk assessment studies that typically examine potential cybersecurity vulnerabilities.

Broaden the educational scope to encompass the C-Suite, ensuring that both management and the board develop a shared understanding of the ecosystem. Including the CISO in these discussions will enable them to better comprehend the company's risk mitigation objectives. As the fundamental concepts are grasped, continue the education process across all levels of the organization. This shared understanding will facilitate better communication and collaboration between the board, management, and the CISO.

To initiate meaningful discussions, consider addressing the following questions:

- What are your business' most valuable information assets?
- Which data is the most crucial to protect?
- Where is your most critical data hosted?

- Are there any design flaws in your ecosystem that could be improved?
- How resilient is your ecosystem against inevitable cyberattacks?
- What are the cyber vulnerabilities within your ecosystem, and can they be mitigated or eliminated?

As the board and management develop a common language and understanding, it becomes possible to delve deeper into more complex issues. In later chapters, we will expand on these questions to explore topics such as technical debt and the organization's overall security posture. However, comprehending the business ecosystem forms a solid foundation for ongoing conversations and adapting to changes within your organization, whether they stem from digital transformation, shifts in business strategy, or other factors.

The road to proactive cybersecurity governance involves nurturing an enterprise-wide culture that views cyber-risk management from an ecosystem perspective. Investing in organizational, educational, and cultural changes today will significantly enhance your cybersecurity governance. In the following chapters, we will delve deeper into the roadmap for proactive governance.

CHAPTER 3

Inviting the CISO In

The COVID-19 pandemic has led to a major shift in the way businesses operate. Companies of all shapes and sizes have been forced to adapt to a new reality where remote work and socially distanced customer interactions are the norms. This has led to an acceleration of digital transformation efforts, particularly in the area of "touchless" technology, which allows customers to interact with businesses without physical contact. A 2020 study by the Pew Research Center found that by 2025, massive generational shifts will force 75 percent of organizations to adapt their hybrid work strategies to include demands for radical flexibility. As a result of this shift, it is now more important than ever for boards of directors to understand the importance of cybersecurity and the role of the Chief Information Security Officer (CISO) in managing the associated risks. It is also important for the CISO to understand the enterprise from the board's perspective.

Conversation with the CISO

The CISO is responsible for developing and implementing an organization's cybersecurity strategy, which includes identifying and mitigating potential vulnerabilities, detecting and responding

to cyber threats, and implementing best practices for data protection. One of the best ways to educate a board of directors on cybersecurity and its challenges is to invite the CISO to present to the board's risk committee on a regular basis and to the full board at least once a year. This provides an opportunity for the CISO to provide an overview of the organization's risk framework, and cybersecurity posture, including any potential risks, vulnerabilities, and incidents that have occurred. It also gives the board an opportunity to ask questions and gain a deeper understanding of the organization's cybersecurity strategy and the actions being taken to protect against cyber threats.

The CISO can also serve as a valuable resource to help the board understand the business ecosystem and build a resilient organization that has fiduciary strength. They can provide guidance on best practices for managing cyber risks, such as incident response plans, regular security assessments, and comprehensive cybersecurity strategies. The CISO can also help the board understand the financial impact of a cyber incident, such as the cost of recovery and potential loss of revenue. Finally, the CISO can help the board understand what they can do, such as leading "wargames" or tabletop exercises for simulated breaches to better understand their role in incident response.

Confidence to Ask Questions

Not only must the board understand the complexities of cybersecurity. It is equally important for the CISO to develop an understanding of the enterprise from the board's perspective to be able to explain complex issues in a non-technical manner. The Chair of the board should encourage open dialogue and encourage all members to ask questions without the fear of being perceived as unknowledgeable. This helps to ensure that both sides have the knowledge and understanding they need to effectively manage cyber risks.

While it may seem intimidating to engage in a conversation with technical executives such as the CISO, their role is to make complex cyber-risk topics simple and to provide contextual relevance to the business ecosystem. Interaction with the board is crucial for ensuring that an organization is prepared and able to respond to cyber threats. By fostering open communication and encouraging all board members to ask questions, the Chair can ensure that the board has the knowledge and understanding it needs to manage cyber risks effectively. Some of the specific areas of inquiry are detailed in the following chapters.

CHAPTER 4

Understanding Tech Debt in the Context of Cybersecurity

Tech debt defined

One of the biggest challenges organizations face when it comes to cybersecurity is the presence of technical debt. “Tech debt” is a term used to describe the accumulation of outstanding technical development work that occurs when an organization chooses to prioritize short-term gains over required, long-term technology investments. This can result in an outdated and vulnerable technology infrastructure that is prone to cyberattacks.

Conversions about Systems

When it comes to cybersecurity, it is important to have conversations with the board about the current state of the systems that are being protected. This includes discussing the impact of tech debt on the overall security posture of the organization. Tech debt can have a significant negative impact on an organization’s ability to protect sensitive data and respond to cyber threats. It is, therefore, crucial that the board understands the risks associated with accumulated tech debt and the importance of investing in technology upgrades.

Think of tech debt as the plaque that builds inside our arteries. Over time, this plaque can cause serious health problems, such as heart attacks. Similarly, tech debt can cause serious problems for organizations such as data breaches and cyberattacks. Just like plaque, tech debt can slowly build up over time, making it difficult to see the full impact it is having on the organization. But when it reaches a critical level, it can cause serious harm.

Phil Venables, again, writes, “It can be a mistake to only invest in cybersecurity controls while neglecting broader technology upgrades and modernization, this would be like building on a foundation of sand. You have to manage this as a portfolio of risks. On a positive note, companies that have the best cyber defenses and track record also typically have the most modern IT platforms, the best agility, the best technology risk mitigation overall and deliver significant business or mission advantage from this.”

One of the key reasons why tech debt can pose a threat to cybersecurity is that it often results in outdated systems and applications. As technology evolves and new security threats emerge, it is important for organizations to keep their systems up-to-date and secure. However, when tech debt is present, organizations are constantly “behind the curve” and may be unable to make the necessary investments in technology upgrades. This leaves their systems vulnerable to cyberattacks and makes it more difficult for them to respond to security incidents.

One of the most important things that organizations can do to safeguard their systems is to prioritize technology investments. This means

making the necessary investments in technology upgrades and replacing outdated systems with modern, secure alternatives. By doing so, organizations can improve their overall security posture and reduce their exposure to cyber threats.

Another important step that organizations can take to reduce tech debt is to engage in regular security assessments. These assessments can help organizations identify areas of tech debt that need to be addressed and prioritize the most important investments. They can also help organizations understand the potential risks associated with tech debt and the impact it may have on their overall security posture.

Asking the right Questions

When it comes to technical debt and its impact on enterprise risk and cybersecurity, the board of directors has a critical role to play. As the guardians of the organization, it is important for them to understand the current state of the systems being protected and to ask the right questions to ensure that the organization is effectively managing its technical debt. Here are some helpful tips for board members to ask questions that will help them better understand technical debt and its impact:

1. **Start by asking about the current state of the systems**: Before diving into the details of technical debt, the board should start by asking about the current state of the systems being protected. This includes asking about the age and version of software, the number of patches and upgrades required, and the overall state of the technology infrastructure.
2. **Ask about the impact of technical debt on the organization**: Technical debt can have a significant impact on the organization, including increased operational costs, reduced efficiency, and increased cybersecurity risks. The board should ask about the specific impact of technical debt on the organization and how it is being managed.
3. **Ask about the organization's strategy for managing technical debt**: A comprehensive strategy for managing technical debt is essential for reducing the risk of a cyberattack. The board should ask about the organization's strategy for managing technical debt and what measures are in place to prevent it from accumulating.
4. **Ask about the risks of not addressing technical debt**: Technical debt can have a serious impact on the organization if left unaddressed. The board should ask about the specific risks of not addressing technical debt and what measures the organization is taking to mitigate these risks.
5. **Ask about the budget for addressing technical debt**: Addressing technical debt requires a significant investment of time and resources. The board should ask about the budget for addressing technical debt and how it is being allocated to ensure that the organization is effectively managing this risk.
6. **Ask about the role of the CISO**: The Chief Information Security Officer (CISO) is responsible for developing and implementing the organization's cybersecurity strategy, including managing technical debt. The board should ask about the CISO's role in managing technical debt and how they are working with the CTO, CIO, and other parts of the technology organization to ensure that the systems are secure.
7. **Ask about the security assessment process**: Regular security assessments are an important part of managing technical debt and reducing the risk of a cyberattack. The board should ask about the security assessment process and what measures are in place to ensure that the assessments are effective.

Understanding the impact of technical debt on enterprise risk and cybersecurity is critical for the board of directors. By asking the right questions and engaging in open communication with the technology and security teams, the board can ensure that the organization is effectively managing its technical debt and reducing its risk of a cyberattack.

CHAPTER 5

Uncover Your Blind Spots: Hire Experts of Diverse Backgrounds

Organizations must have the right experts onboarded with diverse backgrounds to help mitigate risks. There are a number of ways of looking at the pool of candidates; we believe that taking a diverse approach to the selection is key.

It is essential for boards of directors to know their organizations have the right experts onboarded with diverse backgrounds to help mitigate risks. There are a number of ways of looking at the pool of candidates; we believe that taking a diverse approach to recruitment and selection is key. Ideal cybersecurity organizations have multiple dimensions of expertise: They need to have expertise in the best practices of running

a modern cybersecurity program. They need to understand systems. Next, they need to have a deep understanding of the industry (for example, a CISO of an automaker, having knowledge of autonomous self-driving as well as internet-connected cars would be valuable to overseeing the firm). The third dimension must cover a range of perspectives and backgrounds. We list several examples here:

Military Veterans

The military is one example of a background that can provide valuable skills and experience in the field of cybersecurity. Military personnel are trained to operate in high-pressure situations and to make quick decisions in the face of danger. These are critical skills in the field of cybersecurity. Military personnel are also used to working in highly controlled environments, which is essential for maintaining the security of sensitive information.

Non-Traditional Industries

Many unconventional industries are also rich in skills and experience in cybersecurity. One example is nuclear power, which is heavily regulated and require strict security protocols to be in place. This is because a nuclear power plant is a high-value target for cyber attackers. Individuals who have experience running a nuclear power plant have a deep understanding of the importance of security and the measures that need to be taken to protect critical infrastructure. Other industries involving critical infrastructure such as oil and gas, aviation, and communications can offer alternate perspectives and additional pools of skilled candidates.

Diversity of Perspective

When it comes to cybersecurity, diversity is key. A diverse team of experts can bring a range of perspectives and skill sets to the table. The CISO and her team should consider and represent all stakeholders, including individual users, technical practitioners, finance, shareholders and more, and perhaps should have varied career backgrounds to better understand their perspectives. Additionally, diversity of culture, gender, age, and other qualities leads to better debate, enhanced problem-solving skills, and improved decision-making. Diversity creates an environment for a more comprehensive approach to cybersecurity, which can help to identify potential vulnerabilities and mitigate potential threats.

In short, hiring experts with diverse backgrounds is essential for protecting organizations from cyber threats. The military, as well as diverse industry backgrounds and other qualities skills and experience land themselves well in the field of cybersecurity. A diverse team of experts can bring a range of perspectives and skill sets to the table, which can lead to broader analysis and help to identify potential vulnerabilities and mitigate potential threats. The board of directors should take the necessary steps to hire experts with diverse backgrounds in order to protect their organization from cyber threats.

CHAPTER 6

Critical Questions

As technology continues to advance more and more to the cloud and to SaaS, and as the threat landscape evolves, it is essential that boards of directors are aware of emerging risks to their organization and take steps to mitigate them. As previously stated, one of the key ways to do this is by regularly engaging with the organization's Chief Information Security Officer (CISO) to understand the state of the company's cybersecurity posture. Once the CISO is in the room, what do we ask beyond the general "How secure are we?" In this section, we will explore the types of questions that boards should be asking their CISOs and senior technology executives to ensure that their organization is well-protected against cyber threats.

What is our overall cybersecurity posture?

The first question that boards should ask their CISO and senior technology executives is about the overall cybersecurity posture of the organization. This should include information on the current state of the company's security controls, the effectiveness of these controls, and any gaps or vulnerabilities that have been identified. The CISO and senior technology executives should also provide information on any recent cyberattacks or breaches that have occurred and what steps were taken to mitigate them. The numbers of incidents and metrics from a bounty program – which help find and track the number of security vulnerabilities – are also good indicators of the organization's posture.

What are our most critical assets, and how are they protected?

Another important question boards should ask is about the organization's most critical assets and how they are protected. We love this question because it connects the three most strategic elements: (1) **business operations**, (2) **the state of the technology and the most critical data that powers the enterprise**; (3) **the security capabilities to monitor, detect, prevent, and alert.** This includes information on the types of data and systems that the organization relies on, the level of access that different users have to these assets, and the controls in place to protect them. The CISO and senior technology executives should also provide information on any recent vulnerabilities or threats that have been identified and the steps that have been taken to address them. As part of the question, understand the nature and impact of any tech debt, and whether it has come about from a legacy application or a recent acquisition.

How are we addressing emerging threats?

As the cybersecurity threat landscape continues to evolve, it is critical for organizations to stay ahead of emerging threats. To accomplish this, boards must actively engage with their CISO and senior technology executives to inquire about the measures being taken to proactively address new and emerging threats. This includes

seeking information on any new technologies or approaches being adopted, as well as any employee training or awareness programs being implemented to promote safe online practices.

Ransomware: A Critical Threat

Ransomware is a type of malicious software (malware) that encrypts a victim's data, effectively locking them out of their own files or systems. The attacker then demands a ransom, usually in the form of cryptocurrency, in exchange for the decryption key needed to regain access to the data. Ransomware attacks have become increasingly prevalent, with numerous variants and iterations posing a severe threat to businesses worldwide. These attacks put boards in a challenging position, as they must make difficult decisions in response to such incidents. For example, the FBI discourages paying the ransom in response to a ransomware attack. However, boards must weigh the potential consequences of not paying the ransom, such as the loss of critical data or prolonged operational disruptions, against the ethical considerations of giving in to extortion.

This complex situation highlights the urgent need for companies to understand evolving threats and make the necessary investments to protect their operations. Some issues, such as ransomware attacks, may require immediate attention and cannot wait for board meetings. By proactively addressing emerging threats like ransomware, organizations can position themselves to effectively respond to new challenges, minimize the risk of data breaches, and maintain the trust of their stakeholders. To successfully navigate the complexities of ransomware attacks, boards should foster a culture of cybersecurity awareness, invest in robust security measures, and develop comprehensive incident response plans. This proactive approach can help organizations minimize the impact of ransomware attacks and ensure they are better prepared to make informed decisions when faced with such incidents.

How are we measuring the effectiveness of our cybersecurity controls?

Another important question for boards to ask is how the organization is measuring the effectiveness of its cybersecurity controls. This should include information on the metrics that are being used to evaluate the performance of different security controls and the results that have been achieved. The CISO and senior technology executives should also provide information on any recent audits or assessments that have been conducted and the results that have been achieved. We recognize there is no standard way to measure effectiveness, it is important to use benchmarks as well as many data points to help us triangulate the overall effectiveness.

How are we preparing for potential breaches?

Boards should ask their CISO and senior technology executives about the steps that the organization is taking to prepare for potential breaches. This should include information on the incident response plan that is in place and the steps that have been taken to test and validate it. The CISO and senior technology executives should also provide information on any recent simulations or exercises that have

"Look for people who have lots of great questions. Smart people are the ones who ask the most thoughtful questions, as opposed to thinking they have all the answers. Great questions are a much better indicator of future success than great answers."

Ray Dalio
founder of Bridgewater Associates

been conducted and the results that have been achieved. Due to the ransomware attacks on the rise, the ability to fully recover from data loss is a vital part of an incident response. How often are these controls tested, and can the organization fully recover from a complete loss of its systems?

Ask the CISO or Tech Executive: "What is the one thing we can do to help you?"

Finally, boards should ask their CISO and senior technology executives to share one thing they need in terms of support from the board. Listen carefully to what is said and also not said. Is the CISO struggling to get support and cooperation from the executive team? Is the CISO feeling all alone and with many open vulnerabilities that other departments are not taking seriously? Are business leaders "accepting risks" they don't fully understand? By asking the question, the board is communicating their support for the CISO as a person who might be feeling overwhelmed by the number of threats, and not having enough support to do anything about it.

Cybersecurity governance is a critical aspect of any modern business, and dialogue with the board of directors plays a vital role in ensuring that the organization is well-protected against cyber threats. By regularly engaging with their CISO and senior technology executives, boards can gain a better understanding of the organization's cybersecurity posture and take steps to mitigate any risks that have been identified. The questions outlined in this chapter provide a good starting point for boards to begin their engagement with their CISO and senior technology executives and to ensure that their organization is well-protected against cyber threats. The ability to engage with candor is of paramount importance for the CISO and other senior executives. Encouraging honest conversations about cyber risks can lead to more effective decision-making and risk mitigation strategies.

Some of key reasons why candid communication is essential in cybersecurity governance:

- **Identifying the right problems**: Open communication allows the CISO and other executives to raise concerns about the most pressing cybersecurity issues facing the organization. By highlighting these risks, the board can prioritize resources and efforts towards addressing the most critical vulnerabilities.
- **Promoting trust and collaboration**: When the CISO and senior technology executives can openly discuss risks without fear of reprisal or blame, it fosters a culture of trust and collaboration. This atmosphere enables the board and the C-Suite to work together effectively to develop and implement comprehensive cybersecurity strategies.
- **Informed decision-making**: Candid communication about known risks helps the board make informed decisions regarding cybersecurity investments, policies, and procedures. This understanding allows the board to allocate resources more effectively and prioritize initiatives that will have the most significant impact on the organization's security posture.
- **Enhancing stakeholder confidence**: Transparent and open communication about cyber risks and the steps being taken to address them can help build stakeholder confidence in the organization's commitment to cybersecurity.

In summary, candid and open communication between the CISO, senior technology executives, and the board of directors is crucial for effective cybersecurity governance. The questions outlined in this chapter serve as a valuable starting point for boards to engage with their CISO and senior technology executives, ensuring that their organizations are well-protected against cyber threats. By fostering an environment of candor, organizations can more effectively identify and address the most pressing cybersecurity risks, ultimately safeguarding their reputation, financial stability, and overall business success.

CHAPTER 7

Establishing an Effective Cybersecurity Risk Subcommittee

As we have outlined in previous chapters, it is critical for all organizations to have a robust cybersecurity risk management framework in place to protect their assets, data, and reputation. By setting up a cybersecurity risk subcommittee, organizations can ensure that they have a dedicated group of experts who are focused solely on this issue, and who can provide regular guidance and advice to the board of directors. Whether a company is private or public, these steps can help enhance cybersecurity posture and ensure that it is well-prepared to manage and respond to cyber threats.

Step 1: Define the Subcommittee's Purpose and Scope

The purpose of the subcommittee should be clearly defined and communicated to all board members. This includes the subcommittee's role in advising the board on matters related to cyber risk and digital resilience, as well as the limits of its authority. The scope of the subcommittee should also be defined and communicated. This includes the areas of focus for the subcommittee, such as reviewing the organization's cybersecurity risk management practices, emerging threats, and digital resilience.

Step 2: Identify Subcommittee Members

The subcommittee should consist of board members who have a strong understanding of technology and cybersecurity, as well as those who bring diverse perspectives and expertise to the table. It is important to have the right mix of skills, knowledge, and experience to ensure that the subcommittee is effective. Consider including members with a background in technology, cybersecurity, risk management, and legal and regulatory compliance.

Step 3: Provide Cybersecurity Training for Committee Members

Most likely, not all committee members will be technology and cybersecurity experts and will need additional training to ensure that they are equipped to carry out their responsibilities effectively. The subcommittee should provide regular training sessions for its members on cybersecurity and technology-related topics. This can include in-person training, online courses, and workshops.

Step 4: Assign a Chairperson

The subcommittee should have a chairperson who is responsible for overseeing its operations and ensuring that its meetings are productive and focused. The chairperson should be a board member who has a strong understanding of technology and cybersecurity, and who is committed to the subcommittee's success.

Step 5: Establish a Regular Meeting Schedule

The subcommittee should meet regularly, at least quarterly, to review the organization's cybersecurity risk management practices and discuss any emerging issues. Preparation should cover all relevant information and data, including regular reports from the organization's cybersecurity risk management team. We recommend that the chair builds rapport with the CISO and CIO that oversee the operational and day-to-day responsibilities.

Step 6: Establish a Work Plan

The subcommittee should develop a work plan that outlines its priorities and objectives for the year. The work plan should include regular reviews of the organization's cybersecurity risk management practices, as well as any specific initiatives or projects that the subcommittee plans to undertake.

Step 7: Regularly Report to the Board of Directors

The cybersecurity risk subcommittee should provide regular reports to the board of directors on its activities and findings. The subcommittee should also provide recommendations for any changes or improvements that are needed to enhance the organization's cybersecurity risk management practices. The subcommittee's reports should be comprehensive and should highlight any areas of concern or areas for improvement.

Proposed Agenda Topics

While each organization is unique, we outline some of the important elements that the subcommittees should include on their annual agenda. We have shared 12 areas, which can be divided into 3 topics per quarterly review.

1. **Review of the organization's cybersecurity risk management framework**: This includes reviewing the policies, procedures, and practices that the organization has in place to manage cyber risk and ensure digital resilience.
2. **Emerging threats and vulnerabilities**: The subcommittee should stay informed about the latest cyber threats and vulnerabilities and assess the organization's exposure to these risks.
3. **Incident response planning**: The subcommittee should review the organization's incident response plan and ensure that it is up-to-date and effective.
4. **Cybersecurity insurance**: The subcommittee should assess the organization's need for cybersecurity insurance and recommend any changes to the organization's coverage.
5. **Third-party risk management**: The subcommittee should review the organization's approach to managing third-party risk, including due diligence and vendor risk assessments.

6. **Employee training and awareness**: The subcommittee should review the organization's employee training and awareness programs and recommend any changes or improvements.
7. **Regulation and compliance**: The subcommittee should review the organization's compliance with relevant cybersecurity regulations and standards and recommend any changes to the organization's approach.
8. **Budget and resource allocation**: The subcommittee should review the organization's budget and resource allocation for cybersecurity and recommend any changes to ensure that the organization has the resources it needs to manage cyber risks effectively.
9. **Data protection, encryption, and recovery**: The subcommittee should review the organization's data protection and recovery strategies, including backup and disaster recovery plans, to ensure that the organization's critical data is protected and can be recovered in the event of a breach or other cyber incident. In addition, the organization's encryption strategy should also be part of the focus and assess if it is adequate to protect sensitive data, both at rest and in transit.
10. **Technology debt**: The subcommittee should review the organization's technology debt and assess the impact on cybersecurity risk. This includes evaluating the security implications of outdated software and systems and recommending strategies for reducing tech debt.
11. **Technology roadmap**: The subcommittee should review the organization's technology roadmap and assess the impact on cybersecurity risk. This includes evaluating the security implications of new technology deployments and recommending strategies for integrating cybersecurity into the broader technology roadmap.
12. **Cybersecurity metrics and reporting**: The subcommittee should review the organization's cybersecurity metrics and reporting and recommend any changes to ensure that the organization is effectively measuring and managing cyber risk.

CHAPTER 8

Preparing for the Worst: Navigating a Major Data Breach and Outage

The worst-case scenario for any organization is a data breach. Not only can it result in significant financial losses, but it can also damage an organization's reputation and brand. In today's digital age, news of a data breach spreads quickly, and it can take a long time for an organization to recover from the damage done. Given the increasing sophistication of cyber threats and the growing number of connected devices and systems, the likelihood of a breach happening continues to rise. That is why it is essential that boards and executive management be prepared to navigate a major data breach and an outage if they occur simultaneously.

Incident Response Plan

To be prepared for the worst, organizations need a robust incident response plan. This plan should outline the steps to be taken in the event of a breach or an outage, who is responsible for each step, and the resources required. It should be tested regularly to ensure that it is up-to-date and that all stakeholders know their roles and responsibilities. Given today's threat landscape, it is no longer a question of "if" a breach will happen but "when" one will occur. We have mentioned in prior chapters the need to build a plan that focuses on resilience. A fundamental aspect of that incident response and resilience is having effective methods for recovering and restoring data.

The following are specific steps that organizations can take to prepare for and respond to a data breach and outage:

- **Appoint a breach response team**: This team should consist of representatives from various departments, including IT, legal, public relations, and human resources. The team should be led by a senior executive who has the authority to make decisions quickly.
- **Identify critical systems and data**: The first step in responding to a breach is to identify which systems and data have been compromised. This information is crucial in determining the extent of the damage and in responding appropriately.
- **Contain the breach**: The breach response team should have a plan to contain the breach as quickly as possible to limit the damage. This may involve disconnecting affected systems from the network, shutting down servers, or closing down applications.

- **Investigate the breach**: The breach response team should know how to conduct a systematic and thorough investigation to determine the cause of the breach and to identify any additional systems or data that may have been affected.
- **Notify affected parties**: Organizations must have a communication plan to notify affected parties, including customers, partners, and regulators, as soon as possible. This can be a delicate process, and organizations should work closely with their legal and public relations teams to ensure that they comply with all applicable laws and regulations.
- **Implement remediation measures**: The breach response team should anticipate the remediation measures required to prevent a breach from happening again. This may include patching systems, changing passwords, and upgrading security systems.
- **Communicate with stakeholders**: Organizations should communicate regularly with stakeholders, including customers, employees, and shareholders, to keep them informed of the situation and to show that they are taking the matter seriously.
- **Review and improve**: After a breach, organizations should conduct a thorough review of their incident response plan and identify areas for improvement. They should also review their security systems and processes to ensure that they are robust enough to prevent similar breaches from happening in the future.

Emphasizing Preparedness: Tabletop Exercises and Breach Simulations for Executives

One crucial aspect of improving an organization's cybersecurity preparedness is regularly conducting tabletop exercises and breach simulations. These exercises involve creating hypothetical cyberattack scenarios and engaging the company's executives, board members, and relevant stakeholders in a collaborative, problem-solving process. By simulating actual breach situations, executives can better understand the challenges and complexities of responding to a real cyber incident and help their organizations be better prepared for such events.

The importance of tabletop exercises and breach simulations cannot be overstated. Here are a few key reasons why they are essential for executive involvement and overall organizational preparedness:

1. **Enhance decision-making skills**: Tabletop exercises and breach simulations provide executives with the opportunity to practice making strategic decisions under pressure. By working through various cyber scenarios, executives can develop and refine their decision-making skills, enabling them to respond more effectively to real incidents.
2. **Strengthen cross-functional collaboration**: Cybersecurity incidents often require a coordinated response from multiple departments, including IT, legal, human resources, and public relations. Tabletop exercises and breach simulations promote cross-functional collaboration, ensuring that

"In preparing for battle I have always found that plans are useless, but planning is indispensable."

Dwight D. Eisenhower

all relevant parties understand their roles and responsibilities during an incident and can work together efficiently.

3. **Test incident response plans**: Regularly conducting tabletop exercises and breach simulations allows executives to evaluate the effectiveness of their organization's incident response plans. By identifying potential gaps or weaknesses in the plan, they can make necessary adjustments and improvements, ensuring that the organization is better prepared to handle a real cyber incident.

4. **Raise cybersecurity awareness**: By actively participating in tabletop exercises and breach simulations, executives demonstrate their commitment to cybersecurity and reinforce the importance of cybersecurity preparedness throughout the organization. This engagement can help foster a culture of cybersecurity awareness and vigilance among all employees.

5. **Build stakeholder confidence**: When executives are well-prepared to handle cybersecurity incidents, it sends a strong message to stakeholders, including customers, partners, and investors. This proactive approach to cybersecurity preparedness can help build trust and confidence in the organization's ability to protect its assets and maintain business continuity.

Regularly conducting tabletop exercises and breach simulations with executive involvement is an invaluable tool for enhancing an organization's cybersecurity preparedness. By embracing these exercises, executives can help ensure that their organizations are better equipped to handle cyber threats and protect their reputation, financial stability, and overall business success.

White-hat Hackers

Some organizations that are particularly susceptible to cyberattacks may need to go one step further by actually attacking themselves. The use of so-called "white hat hackers," individuals hired by organizations to test systems and networks by trying to break into them, is a powerful way to evaluate their cybersecurity defenses. Also known as "ethical hackers" these individuals are true hackers familiar with the tactics that malicious hackers use to compromise systems but are used to find vulnerabilities before the bad guys do.

Many organizations use ethical hackers as a proactive approach to strengthen an organization's cybersecurity defenses and protect against potential threats. They attempt to penetrate the organization's systems and identify vulnerabilities that could be exploited by attackers, but with the organization's permission and under a strict set of rules of engagement. Once they identify these vulnerabilities, they provide the organization with a report detailing their findings and recommendations for how to address the vulnerabilities. This approach can be highly effective for organizations to get an informed, outside perspective and catch vulnerabilities which they might have overlooked.

In summary, a data breach and an outage can have a devastating impact on organizations, and it is essential that boards and executive management be prepared to navigate these situations. By having a robust incident response plan, practicing their roles if a breach occurs, and testing critical systems through real-world attack techniques, organizations can mitigate the damage and protect their reputation and brand.

CHAPTER 9

Celebrate Victories

Why Celebrations are Overlooked

Celebrating victories in cybersecurity are uncommon because, in many ways, it is about proving the negative or showcasing what did not happen or has been prevented. Success in managing cybersecurity and digital risk often means nothing happened – no breach or attack occurred, the systems remain available and operational, and no data was lost or unrecoverable. This lack of obvious outcomes can make it challenging to celebrate victories. After all, we don't celebrate the lack of business losses; we celebrate and praise leaders for beating quarterly expectations. Yet cybersecurity teams, like all of us, need recognition to feel valued and appreciated by their organizations. Creating a culture that recognizes and celebrates successes is an important step in creating a high-performing cybersecurity team.

> *"Train people well enough so they can leave, treat them well enough so they don't want to."*
>
> **Sir Richard Branson**
> British entrepreneur

When Board Members Notice

Organizations know they need to celebrate victories to help build morale, increase motivation, and create a positive and proactive culture. The technology and security teams are no different; they need to know their work matters, and each person makes a difference in managing cyber risks. The board can play a crucial role in this by acknowledging and celebrating the successes of the security and technology team. Board participation can be done through formal recognition programs, awards, or simply taking the time to acknowledge and appreciate the team's efforts.

Earlier in my career, I was the CIO of a public company, where security had become a top concern. We were investing and accelerating many programs across the technology and security groups. It was meaningful when one of the board members, who had taken ownership of driving the digital risk agenda, pulled me aside and said, "We all see what you're doing, and we

appreciate the long nights and pain that you and the team are feeling... you guys are making us a better company."

The message by the board member was short, powerful, and lingered with me. I ended up sharing this with my entire organization at the CIO all-hands meeting, and just that tiny recognition was felt and reverberated throughout the technology team. Small recognitions by board members communicate to the security and technology team that they are invested in the progress of the security program and care about the organization's well-being. The example I shared helped foster a positive and proactive security culture, where everyone was motivated to improve and protect the organization against cyber threats continuously.

Tips for Celebrating Victories

The board can celebrate victories and show their appreciation in a number of ways. The team should be recognized and celebrated when a new security solution is implemented, and no security incidents occur for a set period of time. Again, a low-tech solution as simple as a "shout-out" at a team meeting, a company-wide email, or even a team-building activity. These small acts of recognition go a long way in motivating the team to continue working towards a common goal.

In addition to individual successes, it is also essential to celebrate organizational victories. When the organization successfully defends against a significant threat or when the security posture improves, this should be celebrated as a collective effort and a demonstration of the organization's commitment to security. Celebrating these victories not only helps to build a positive corporate culture but also helps to foster a sense of unity and strengthens the team's resolve to continue to protect the organization.

Finally, it is important to celebrate successes not just within the IT and security departments but across the entire organization. When the sales team closes a deal with a new client, and the information security team is able to secure the client's data, this is a victory for the entire organization and should be celebrated as such. By creating a culture that celebrates victories across departments, organizations can break down silos and foster collaboration, which is essential in today's interconnected and interdependent business environment.

Conclusion

In today's rapidly evolving digital landscape, cybersecurity has become a top priority for organizations across industries. Cyber threats have become more sophisticated and frequent, with the potential to cause significant financial losses and damage to an organization's reputation. It is essential that boards of directors and technology leaders take an active role in managing cyber risks and build highly resilient organizations that can withstand cyberattacks and outages.

To achieve this goal, organizations need to adopt a comprehensive, systemic approach to cybersecurity. This approach involves addressing all aspects of the corporation, including employees, processes, and technology. The board must play an active role in cybersecurity governance and establish a culture of managing and governing cyber risks. Elevating the CISO's role, establishing Cybersecurity Risk Committees, promoting continuous education, and understanding technical debt are critical components of building a strong cybersecurity posture.

It is also essential to hire experts with diverse backgrounds, prioritize diversity in recruitment and selection, and create a comprehensive approach to cybersecurity. Boards of directors must engage in regular conversations with the CISO and senior technology executives to ensure effective cybersecurity, mitigate risks, and prepare for emerging threats.

Establishing an effective cybersecurity risk subcommittee can provide guidance and advice to the board of directors on cybersecurity matters. The subcommittee should cover various topics such as cybersecurity risk management, emerging threats, incident response planning, cybersecurity insurance, third-party risk management, employee training, regulation and compliance, budget allocation, data protection, technology debt, technology roadmap, and cybersecurity metrics and reporting.

Preparing for the worst-case scenario, a major data breach and outage, requires a robust incident response plan, regular tests to ensure preparedness, appointing a breach response team, identifying critical systems and data, containing the breach, investigating the breach, notifying affected parties, implementing remediation measures, communicating with stakeholders, and reviewing and improving security measures. Conducting simulated breaches (wargames) and employing white-hat hackers to test and strengthen an organization's cybersecurity defenses can also help prepare for a potential cyberattack.

Celebrating victories in cybersecurity is often overlooked due to the nature of the field. Success in cybersecurity means that nothing happened, which can make it challenging to identify and celebrate accomplishments. However, recognizing and celebrating successes is vital for building morale, motivation, and fostering a positive culture. Boards of directors can acknowledge and celebrate the security and technology team's efforts through formal recognition programs, awards, or simply appreciating their contributions. Celebrating both individual and organizational

successes can build a positive corporate culture, foster unity, and encourage collaboration across departments.

Throughout this e-book, we have argued that cybersecurity is a critical aspect of any organization's success in today's digital age. Boards of directors and technology leaders must take an active role in managing cyber risks and building highly resilient organizations that can withstand cyberattacks and outages. By adopting a comprehensive, systemic approach to cybersecurity, promoting diversity, engaging in regular conversations with the CISO and senior technology executives, establishing an effective cybersecurity risk subcommittee, preparing for potential cyberattacks, and celebrating victories in cybersecurity, organizations can effectively manage and mitigate cyber risks, protect their reputation, and achieve long-term success. We hope we have been able to inspire you to take up this challenge and lead with greater impact. We need you!

Written by:

Dr. Moudy Elbayadi
SVP, Chief Technology Officer, Shutterfly, Inc.
Author of *Big Breaches: Cybersecurity Lessons for Everyone*
moudye@gmail.com

As Shutterfly's Chief Technology Officer (CTO), Dr. Elbayadi leads the company's technology, eCommerce transformation, cybersecurity, software development, mobile apps, AI-driven personalized experiences. Dr. Elbayadi has led large software development teams and provided strategic vision and direction to drive growth and innovation in consumer products, SaaS, and enterprise technology. As an investor, Dr. Elbayadi has a unique perspective on the intersection of technology, business, and crossing the chasm to scale.

Contributors:

Karena Man
Consultant, Egon Zehnder, San Francisco
karena.man@egonzehnder.com

Scott Texeira
Consultant, Egon Zehnder, Palo Alto
scott.texeira@egonzehnder.com

William Houston
Consultant, Egon Zehnder, Washington, D.C.
william.houston@egonzehnder.com

Drew McFeetors
Consultant, Egon Zehnder, Toronto
drew.mcfeetors@egonzehnder.com

Rod Hackman
Board Member
rod.hackman@gmail.com

Mr. Hackman has extensive experience heading the cybersecurity oversight function of an NYSE company. His career has been dedicated to capital formation, M&A, corporate development, and the creation of shareholder value as an advisor and entrepreneur. Mr. Hackman is a former member of several public and private Boards of Directors and has served as lead director and as the head or member of all chartered committees. As a former nuclear engineer, Mr. Hackman understands the importance of protecting and building resilience into complex digital business ecosystems.

EgonZehnder

Egon Zehnder's Approach to Cybersecurity

At Egon Zehnder, our network of global cyber consultants can help your organization evaluate the structure of its cybersecurity function. We can help you build teams with the right competencies and recruit leaders who can balance security requirements with business objectives. Our cybersecurity consultants help refine the constructs of your company's job roles and devise career tracks that increase talent retention and build robust, high-performing cybersecurity teams.

We partner closely with both fast-growing cybersecurity firms, as well as more traditional companies. We use this combined insight to help our clients identify, assess, and develop cybersecurity consultants for team leader positions, who can help them rapidly and strategically scale their departments.

About Egon Zehnder

Egon Zehnder is the world's preeminent leadership advisory firm, inspiring leaders to navigate complex questions with human answers. We help organizations get to the heart of their leadership challenges and offer honest feedback and insights to help leaders realize their true being and purpose.

We are built on a foundation that supports partnership in the truest sense of the word and aligns our interests with the interests of our clients. Our 560 consultants across 63 offices and 36 countries are former industry and functional leaders who collaborate seamlessly across geographies, industries and functions to deliver the full power of the Firm to every client, every time.

We partner closely with public and private corporations, family-owned enterprises, and non-profit and government agencies to provide a comprehensive range of integrated services, including executive search, leadership solutions, CEO search and succession, board advisory and diversity, equity & inclusion. Our leadership solutions cover individual, team and organizational effectiveness, development and cultural transformation. We work with world-class partners including Mobius Executive Leadership, a transformational leadership development firm.

We believe that together we can transform people, organizations and the world through leadership.

For more information, visit www.egonzehnder.com and follow us on LinkedIn and Twitter.