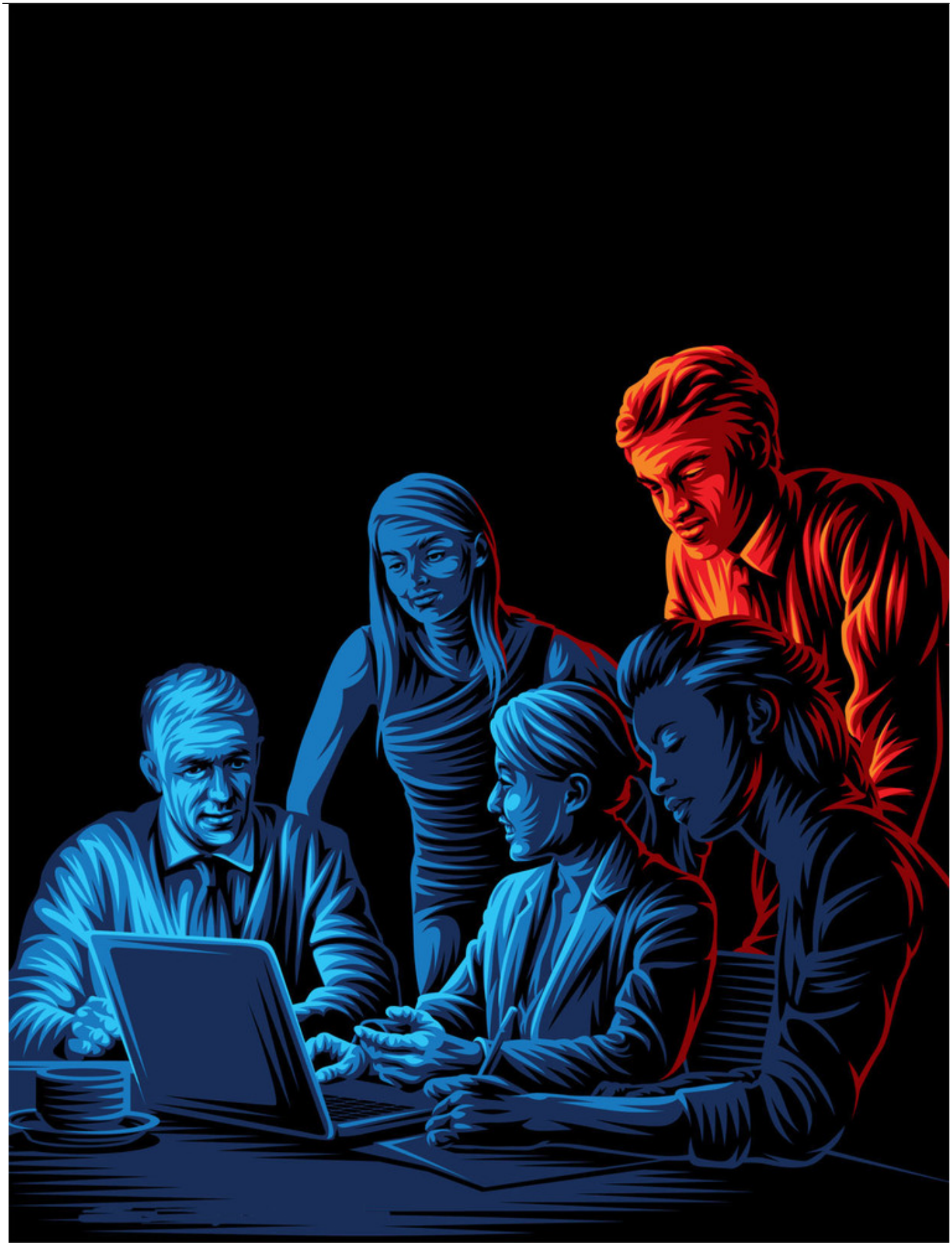
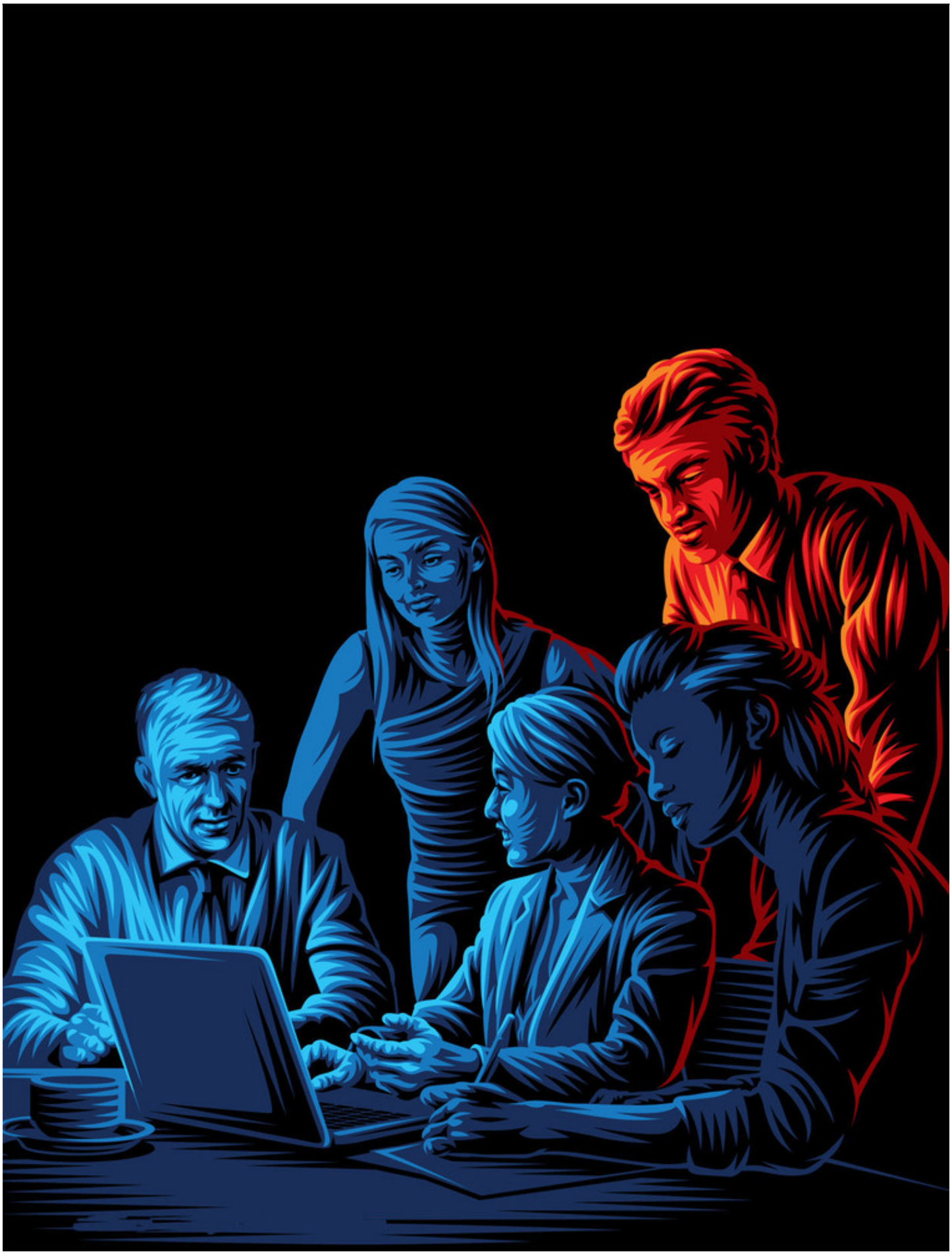
It's Coming from Inside: How to Educate Your Board of Directors on Insider Threats

Technology, Privacy, and eCommerce





CHEAT SHEET

- ***Insider threat.*** An insider threat originates from within the company under cyberattack, often by a present or former employee, officer, or stakeholder.
- ***In the know.*** The board of directors should develop a high-level understanding of cyber risks through briefings from the company's executives and management.
- ***Up-to-date.*** At a minimum, the board of directors must be kept up-to-date on plans for the implementation of an insider policy, communication and cultural awareness, activity monitoring, and cyber liability insurance.
- ***Liability.*** Class-action litigation against the company usually follows a severe cyber data breach, and individual directors may be personally liable for any failure to properly monitor risk.

If you follow the news, chances are that you know about the plethora of recent data breaches and cybersecurity threats. Historically, the corporate data breaches that make the news are carried out by outside individuals or entities. You may recall the data breaches suffered by Equifax in 2017, Anthem in 2015, Home Depot in 2014, and Target in 2013. However, the business world has picked up on a new, disturbing, and potentially costly trend. Over the past several years, insider data breaches have been on the rise. In 2015, Intel Security (now McAfee) found that internal actors were responsible for 43 percent of all data breaches, and a 2016 study conducted by the Ponemon Institute found that insider threats are now more prevalent than any other computer security threat.[1]

This new trend is especially troublesome because, while the financial cost of any single data breach often reaches into the hundreds of thousands or millions of dollars, outside breaches have received more attention from corporate executives and boards of directors. To date, outside breaches have, for the most part, been addressed with traditional security measures more thoroughly. In response to this trend, security personnel and company executives have recognized the need to devote more personnel hours and resources to identifying, preventing, and mitigating insider threats. In order to successfully navigate this issue and mitigate risk, the company's board of directors, who have a duty to oversee all aspects of the company's risk management programs, must champion this effort.

But for all that, boards are responsible for the current business climate, how do the company's employees and executives, particularly those with cybersecurity responsibilities, secure the board's full attention and focus? This article first summarizes the board of directors' duties with respect to insider cybersecurity threats and identifies the scope of these threats, then provides tips on engaging the board with regard to these threats.

1. See Ponemon Institute: 2016 Cost of Data Breach Study: Global Analysis, June 2016.

Duty to protect company assets from insider threats

The board of directors has a duty to protect corporate assets by monitoring and overseeing corporate risk. Increasingly, more and more of those assets are taking the form of information. Accordingly, the boards' interest and participation in discussions regarding cybersecurity and risk must mirror the

discussions on topics such as revenue performance, growth, and investment. This does not mean that boards are required to become cybersecurity experts, but they should develop a high-level understanding of cyber risks through briefings from the company's executives and management.

Failure to properly monitor and oversee the company's cybersecurity carries significant risk to the company and, possibly, board members in their individual capacities. A severe cyber data breach can materially disrupt a company's business; harm the company's brand, reputation, and goodwill; and cause significant secondary harm to the company's customers and business partners. Class-action litigation against the company typically follows, and under certain circumstances, individual directors may be personally liable for any failure to properly monitor risk.[2]

2. Failure to monitor risk can only be imputed to individual board members where: (a) the directors utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations, thus disabling themselves from being informed of risks or problems requiring their attention. *Caremark Int'l Derivative Litig.,* 698 A.2d 959 (Del. Ch. 1996). "In either case, imposition of liability requires a showing that the directors knew that they were not discharging their fiduciary obligations." *Stone v. Ritter,* 911 A.2d 362, 370 (Del. 2006) (citing *Caremark*).

What is an insider threat?

An insider threat is simply defined as a security threat that originates from within the company being attacked, often by an employee, officer, or stakeholder. An insider threat does not have to be a present employee, officer, or stakeholder. Attacks from former employees, officers, or anyone who had access to the company's proprietary or confidential information is considered an insider threat. The company's contractors, business partners, and any other individuals or third-party entities who have knowledge of the company's security practices or access to the company's protected networks or databases also fall under the umbrella of an insider threat. Lastly, an insider threat may also be described as a threat that traditional security measures, which focus on traditional hacking methods and preventing unauthorized access to networks from outside of the organization, cannot prevent.

Generally, insider threats can be categorized as follows: malicious insiders, exploited insiders, negligent insiders, and external insiders. Malicious insiders engage in intentional attacks, whereas attacks from exploited and negligent insiders are unintentional (from the employee's perspective). External insider attacks can be intentional or unintentional. Below is a brief description of each category.

- **Malicious insiders.** Malicious insiders engage in intentional cyber attacks on the company by using their knowledge of and access to sensitive information. Malicious insiders can often legitimately bypass the company's security measures. These individuals are often disgruntled employees, who may or may not intend to leave the company soon, or employees who are in financial distress. Due to the ease of access and large window of opportunity, these attacks are the most difficult to detect and are often the most costly.
- **Exploited insiders.** Exploited insiders are high-value employees, such as system administrators, information technology help desk teams, and company executives. Attackers commonly target these individuals with spear-phishing emails to gain sensitive information that the attacker can use to gain access to the employee's computer.[3] Once inside the employee's computer, attackers can capture their privileged credentials, further escalate them, and gain domain-level access and control over the company's larger network. Exploited insiders are just as much of a victim as the company.

- **Negligent insiders.** Negligent insiders are employees who are not out to intentionally attack the company or steal sensitive information — these employees are simply doing their job. During the execution of their job responsibilities, however, these employees may send the company's sensitive information through less secure means, via personal email for example, or store it in less secure locations such as Dropbox. At first glance, these actions may seem harmless, but they can unintentionally put the company's data and network at risk.
- **External insiders.** External insiders are third parties, such as contractors, vendors, and other business partners, that the company allows to remotely access their internal networks. Similar to the company's employees, these individuals can turn into malicious, exploited, or negligent insiders.

Regardless of the type of insider threat, all of them have one thing in common: They target the data and systems to which they have access.

However, the end goal is not always the same. Common end goals include disrupting the business, stealing money, or exfiltrating data.

3. Spear-phishing is a targeted attempt, typically through email or other online messaging, to steal sensitive information, such as account credentials or financial information from a specific victim. Attackers aim to acquire personal details on the victim and then disguise themselves as a trustworthy friend or entity to acquire sensitive information. Spear-phishing is widely considered the most successful form of acquiring confidential information on the internet.

Strategies to focus the board of directors' attention on insider threats

A. Establish expertise in the basics

In today's business climate, managing insider cybersecurity is analogous to managing quality and safety. What was once the responsibility of small, specialized departments is now a company-wide endeavor, which begins with the board. Become a resource for the board, not just an authority. Inform the board of the strategy and resources available to help facilitate decision-making related to risk identification and how to mitigate them. If necessary, engage third-party professionals to provide the board with the technical understanding to make proper decisions.

At a minimum, the board must be kept updated on the company's plans for the following:

- **Implementation of a robust insider policy.** This policy should address what people must do or not do to deter insiders who introduce cybersecurity risks through carelessness, negligence, or mistakes. The policy must be concise, free of complicated technical jargon, and clear about the penalty for policy violations. Employees should receive regular training on these policies, and violations must be enforced.
- **Communication and cultural awareness.** Communicate to employees that the company can and will observe their day-to-day cyberactivity as legally permitted, and encourage employees to report unusual or prohibited technologies (e.g., the presence of a portable drive in an area where data is usually accessed via the network) or behavior (e.g., an unauthorized employee or vendor asking for data).
- **Activity monitoring.** Diligently monitor the activity and privileges of all employees, particularly those with the highest levels of access to the company's systems, and deploy malware-detection software.
- **Obtain proper cyber liability insurance.** Cyber liability insurance is a crucial, fundamental

step in an effective internal security risk management strategy. These policies typically cover the company's losses and expenses related to a breach: hiring a security forensics firm, notification mailing costs, public relations, and legal services. Many policies also cover third-party losses, such as third-party claims based on the failure to protect confidential information, data loss, and fines and penalties.

In today's business climate, managing insider cybersecurity is analogous to managing quality and safety. What was once the responsibility of small, specialized departments is now a company-wide endeavor, which begins with the board.

B. Effectively explain why security matters

There is not a more boring cybersecurity presentation than one full of internal company data and external metrics focused on nothing more than whether the company is or is not compliant with some law or regulation. This is certainly not to suggest that companies refrain from using data and metrics; they are necessary for tracking and planning. But when engaging the board on internal cybersecurity, focus the board's attention on the difference between compliance (the bare minimum) and actual security (the ultimate goal).

Cybersecurity is no longer just an unwanted cost; it is now an important, competitve differentiator, something that can help the company win and retain business.

Just because the company is in compliance with a certain set of laws or security standards does not mean the company's data won't be compromised by an internal threat. Boards care about risk mitigation, and a discussion regarding actual security is apropos to their concerns. Focus less on rigid compliance and more on the company's business strategy. Explain how internal cybersecurity fits within that strategy.

Use language that is understandable to the board, and to the company's employees, to explain what the company is doing and why the company is doing it. Discussions full of technobabble and jargon are ineffective and may encourage the board to dig deeper into the weeds, which encroaches on management's autonomy.

Consider creating active scenarios (participation exercises) in which the board can act out the roles of employees and management. For example, if intellectual property is the most important thing that your company needs to protect, a participation exercise will allow the board to feel what would happen if a business unit lost a product, due to an internal security breach, that they had been working on for several years. How much revenue would the business unit lose if they were not able to bring the product to market? What does the manager say to his or her employees regarding their wasted efforts? What is the financial and cultural impact of having to eliminate some of those employees? Working through these types of issues creates a visceral experience for the board. It takes them out of the theoretical world and into the world of actual compliance.

C. Tie security efforts to the business

Convince the board that you are a business person first and a security person second. Emphasize to the board that you are there to support the business, and demonstrate that you have a clear understanding of why the business exists: to provide services or products to its customers and in turn

make money. Probe the board regarding the company's risk and growth strategies, and create an active dialogue with the board regarding how its decisions on those issues will affect the internal cybersecurity needs of the business and vice versa. Identify how the company can design internal cybersecurity measures to positively affect market share, revenue, and profit margins. Eventually, everything the company does with respect to internal cybersecurity, at some point, has to and will support the business in meeting its objectives.

D. Focus on the future

Instead of focusing on whether the company's current internal security plans, with respect to budgets, spending, and capabilities, are aligned with the current business strategies, focus on whether they are in line with the company's future growth strategies. If the company's current security plans are aligned only with the company's current position, it is impossible to know if the company will be ready when new technology enters the business via new engagements, partnerships, or lines of business.

For example, the company may not be using Internet of Things (IoT) technology at the moment, but down the road, it probably will.[4] Thus, discussions must be had at the board level regarding how the company can start ramping up its structural and technological capabilities and improving the skillsets of its human capital. If done with the appropriate forethought, the security specialists within the company will be prepared when the business asks how it can implement a particular IoT device safely. The board will also be prepared to approve a strategy that is ready to go.

In addition, help the board anticipate how the company's technological roadmap will change as the products and services within the company's development pipeline come to fruition. Supply the board with a map of the company's digital ecosystem, and keep it up to date. Include not only the backend technology, but also the business partner and customer-facing technologies (websites, mobile apps, etc.) as well. Under this approach, the board can seamlessly integrate internal cybersecurity strategies into its discussions regarding future business strategies.

4. IoT is the concept of connecting any device or machinery with an on and off switch to the internet, and/or to another device or machine. This includes almost any device that you can think of, such as cellphones, coffee makers, washing machines, headphones, lamps, and wearable devices. It could also apply to machinery, such as jet engines in an airplane or the drill of an oil rig. Jacob Morgan, "A Simple Explanation of 'The Internet of Things." *Forbes,* May 13, 2014.

Conclusion

Conventional wisdom views cybersecurity, including internal cybersecurity, as a compliance-focused cost center that is slow, reactionary, and not responsive to the business. Under this approach, data collection and assessments are completed by hand, and cybersecurity personnel are isolated from the rest of the enterprise. This is the antiquated view that focuses only on compliance and "checking the cybersecurity box."

Effectively engaging the board on internal cybersecurity requires a shift from this mindset. Cybersecurity is no longer just an unwanted cost; it is now an important, competitive differentiator, something that can help the company win and retain business. The new mindset is forward looking and integrates cybersecurity into every aspect of the business. It leverages existing technologies to enhance and automate the gathering, analysis, and presentation of security information, which

creates efficiencies, fosters collaboration, and ultimately enables the business.

Reachel Beichley

Vice President of Human Resources, General Counsel, and Corporate Secretary

MRI Global

Anthony Grice

Partner

Husch Blackwell LLP

He specializes in labor and employment matters for technology and manufacturing companies.

Virginia Fry

Partner

Husch Blackwell LLP

She specializes in healthcare, education, and life sciences.