Features

Quarter Four 2023

Volume 49, Number 4

Cyber Risk

IS A BUSINE

SS ISSUE

STOCK.ADOBE.COM/ GORODENKOFF

Understanding the nuances of cyber risks is an ongoing challenge. Boards that engage with a company's chief information security officer and learn the best practices of cyber-risk oversight can stay up to date on emerging issues and be prepared for a potential cyber crisis.

By Neal A. Pollard and Shelley B. Leibowitz

NEW RULES from the US Securities and Exchange Commission (SEC) that go into effect this year will require public companies to disclose their processes for managing material cyber risks, as well as the C-suite's and the board's roles in managing or governing those risks. This reflects a trend of boards sharing responsibility for cybersecurity with the company's most senior ranks. But many companies will need to overcome a communications gap that exists between the technical details and jargon that often accompany cybersecurity briefings and the fundamental questions, What is the risk to the business, and how do we know we are managing it effectively?

Many directors do not fully understand technical briefings from the organization's senior cybersecurity executive (usually the chief information security officer, or CISO) and how the data from those briefings translate to increasing or decreasing exposure to cybercrime. Companies can close this gap by treating cyber risk as a business problem, not a technology problem. Boards and management should elevate the discussion of cyber risk within a broader context of how digitalization—the development and monetization of data and digital platforms—drives business strategy, and how cyber and other risks can disrupt that strategy. To do so, companies need to change the risk conversation, particularly at the board level, as well as create a business partner in the CISO, and build the board's fluency in the language of digitalization.

Change the Risk Conversation

Some boards are considering whether to dedicate a seat to a cybersecurity expert so that at least one director understands the risk discussion when it goes down the rabbit hole of intrusion detection, patching, encryption, firewalls, and the like. But this dilutes risk governance into a technical discussion of cybersecurity operations. Moreover, it is not the proper focus when it comes to governing cyber risk. Simply put, cyber risk is the loss or liability that can arise by virtue of doing business connected to the Internet. "Loss or liability" here is not a technical concept: it is money out of your pocket, stolen property, lawsuits to defend, damage to your brand and reputation, lost customers, regulatory or even congressional scrutiny, and in extreme cases related to health care, transportation, or energy, threats to public safety or national security.

> **Simply put, cyber risk is the loss or liability that can arise by virtue of doing business connected to the Internet. It is money out of your pocket, stolen property, lawsuits to defend, damage to your brand and reputation, lost customers, regulatory or even congressional scrutiny, and in extreme cases related to health care, transportation, or energy, threats to public safety or national security.**

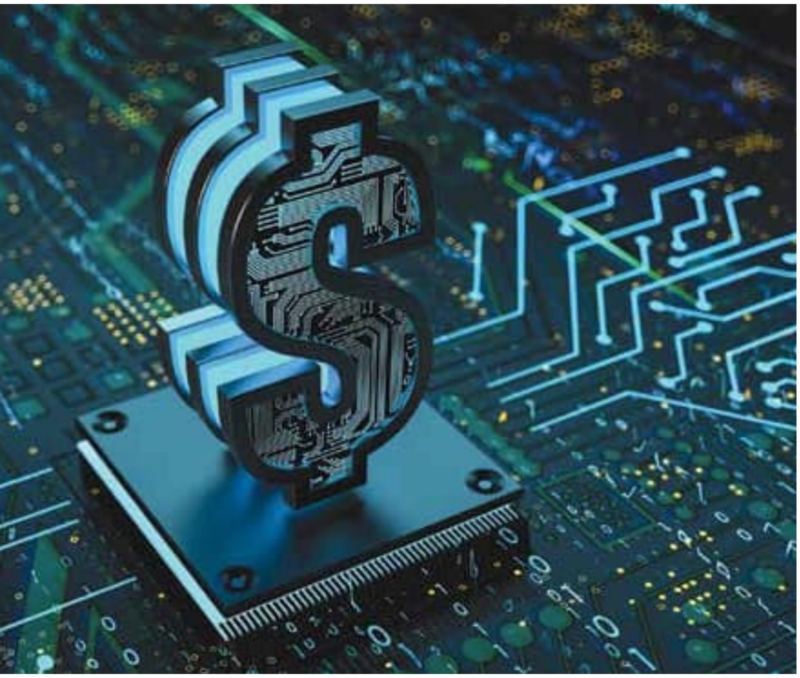
Start the conversation by asking these questions: What is our exposure to these kinds of losses? How would they happen, and to which parts of the business? What are we doing to avoid, mitigate, or transfer risks using strategy, controls, and insurance? What risks remain, and are they acceptable? Given risk data and metrics, is the company exercising due care? Is there any area in which it is an outlier compared with industry peers? Is there a risk management mechanism that is fundamentally broken, missing, or going in the wrong direction, and if so, what are we doing about it? What does the CISO need from management or the board? And lastly, how well prepared are we for when, not if, a breach does occur? In short, how well is the organization extending and protecting the value of digitalization?

Partner With the CISO

These are nontechnical questions that all directors can and should ask, and that a senior cybersecurity executive should be able to answer. Without context, technical statistics offer limited utility to the board and management to understand how the organization is managing risk. For many boards, a designated committee such as audit or risk will include cyber-risk governance among its responsibilities. This committee should engage with the CISO to define the parameters of due care—that is, the kind of cyber-risk management that is optimal for the organization, the appropriate level of investment and risk mitigation given its assets and risk appetites, and how this information should be reported.

This is where the CISO's technical expertise is useful: translating technical controls and data to fall under the organization's standard of due care, and communicating progress toward that standard to stakeholders, grounded in the language of business, not technology. There is a growing body of guidance, including from the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, the World Economic Forum, and NACD, that provides board directors and corporate executives with tools to have effective conversations about defining risk expectations for cybersecurity. This guidance will continue to evolve to keep pace with changing digital ecosystems and increasingly sophisticated cyber adversaries.

For a clear, business-focused dialogue to occur, the CISO must become a business partner, not a technical service provider. It is more important that the CISO understands the organization's strategy and how it creates value than it is for directors to understand the technical underpinnings of cybersecurity. This requires a CISO to have many of the same skills and experiences with engaging board directors as any officer in the C-suite. It also requires that companies place the CISO at an organizational level that confers independence and authority to understand business strategy, to have influence across the entire company, and to engage regularly with business and technology leadership beyond the periodic security and risk update. Boards should ask the CISO how the cybersecurity program is assuring and enabling corporate strategy, and how corporate strategy might challenge risk management. If the company launches a digital product, moves into a new region or market segment, joins a partnership, or builds a transformational platform, it should understand what cyber risks might follow and how they can be managed. Prudent cybersecurity creates and protects business value and ensures that the organization is seen as a trusted partner to all constituencies—customers, suppliers, partners, and employees.



Build the Board's Fluency

The role of digitalization in corporate strategy is a natural nexus between the CISO and the board. This is an area where directors must sharpen their acumen.

Cyber risk will probably always occupy an outsized space on the digitalization agenda, capturing the attention of boards, regulators, investors, media, lawmakers, and the general public, with billions of dollars invested and at risk annually. But it is only one important component of a broader digital competency that directors of large, global enterprises must develop. Boards should seek to infuse many or all directors with "digital DNA" so they can oversee the value and impact of machine learning and artificial intelligence, financial technology, and digital platforms that monitor net-zero carbon emissions and sustainability goals, to name but a few important innovations. The World Economic Forum has stated that 70 percent of new value created over the next decade will be from digitalization and digital-based business models. Boards should govern that value based on well-articulated strategy and by paying appropriate attention to all risks that could derail that strategy. Contributions should be spread among all directors; consequently, all directors should be fluent in the language of digitalization and the governance thereof involving strategy, risk, financing, sourcing, competing, partnering, and profiting.

Despite the best laid plans, things will go wrong. The new SEC rules also include requirements for the disclosure of material cyber incidents, adding to the complex and growing body of regulatory requirements in this area. Lawyers and regulatory experts have become an important part of the discussion and decision-making, and often are already critical advisors to the CISO, management, and the board. These individuals, along with the CISO, can help answer another important business question for the board and management: Are we ready for when things go wrong? During a cyber crisis, smart people sometimes do unwise things, and a poor response to a breach can cause as much or more damage than the breach itself. The CISO often acts as a lead executive in cyber crisis response, helping to determine when and what to escalate, whom to notify, and what constitutes a material incident, relying on ambiguous and rapidly changing facts all while interacting with a lot of worried senior executives who want to know what is happening and how they can help. This requires sound business judgment and operational experience in addition to technical acumen. Getting the plan right before a crisis occurs, becoming familiar with crisis conditions, and clearly defining roles and responsibilities through scenario planning and practice exercises are critical to running a business, and perhaps the most important area of cooperation and communication among the CISO, senior management, and the board.

Effective CISOs have at least two things in common with other operating executives. First, they understand the business strategy in a framework of value creation and risk mitigation. Second, they transcend technical jargon and put critical execution plans and required investment into business terms. Hence, the best CISOs tend to lessen the need for deep cybersecurity expertise on the board.

With digitalization comes high growth and value potential, but also business volatility, complexity, demands for ever increasing speed and agility, risky partnerships, supply chain uncertainty, and an ever-shifting global patchwork of privacy and security regulations. Business-savvy CISOs and digital DNA on boards will help organizations better understand that cybercrime is a business problem, not just a technical one, and most certainly not the only peril lurking on the Internet.

NEAL A. POLLARD is an adjunct professor at Columbia University, where he teaches graduate courses in cybersecurity as a business risk. Pollard has spent 30 years in cybersecurity as a technologist, operator, attorney, founder, board director, and policy advisor in government, industry, consulting, and academia. Formerly, Pollard was the group chief information security officer for UBS.

SHELLEY B. LEIBOWITZ is the founder and president of SL Advisory, whose focus is all things digital, including transformation, effectiveness, governance, and trust. Leibowitz is a seasoned corporate director and serves as an independent director for public and private companies in financial services and tech. Formerly, Leibowitz was the chief information officer for the World Bank Group.

ISTOCK/ ASBE