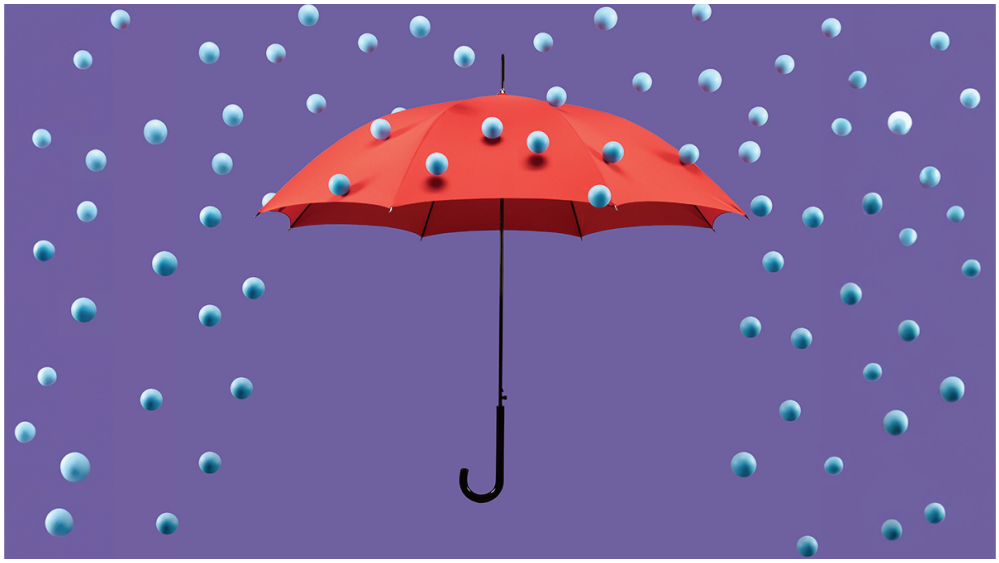
Harvard Business Review | Digital Article

Cybersecurity and Digital Privacy



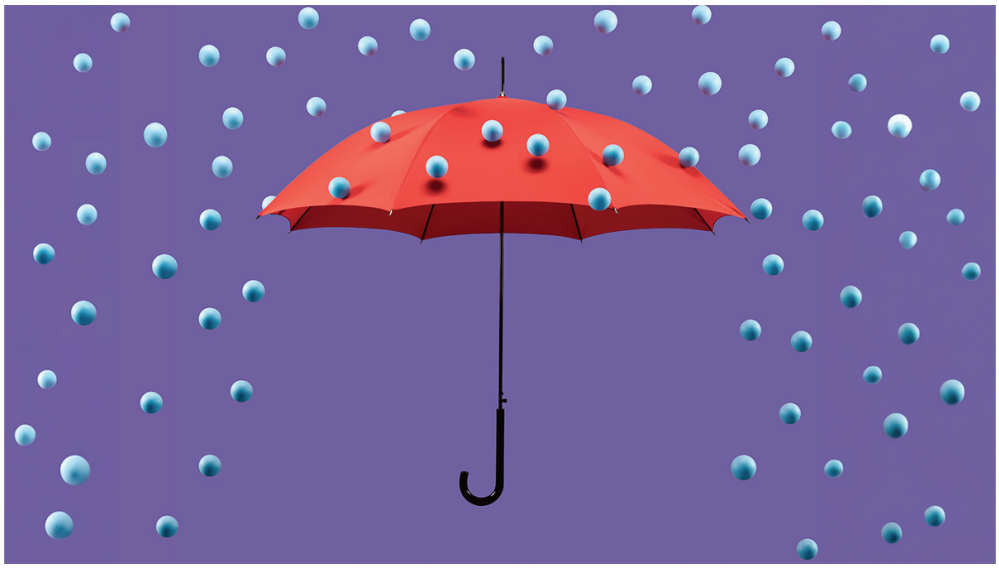
4 Areas of Cyber Risk That Boards Need to Address

How companies can build a long-term strategy that will keep them secure. **by Sander Zeijlemaker, Chris Hetner, and Michael Siegel**

4 Areas of Cyber Risk That Boards Need to Address

How companies can build a long-term strategy that will keep them secure. **by Sander Zeijlemaker, Chris Hetner, and Michael Siegel**

Published on HBR.org / June 02, 2023 / Reprint H07O3Z



PM Images/Getty Images

As technological innovations such as cloud computing, the Internet of Things, robotic process automation, and predictive analytics are integrated into organizations, it makes them increasingly susceptible to cyber threats. Fortune 1000 companies, for example, have a 25% probability of being breached, and 10% of them will face multi-million loss. In smaller companies, 60% will be out of business within six months of a severe cyberattack. This means that governing and assessing cyber risks becomes a prerequisite for successful business

performance — and that investors need to know how vulnerable companies really are.

This need for transparency has been recognized by the regulators and facilitated by the new cyber security rules. Currently, the U.S. Security and Exchange Commission (SEC) has increased its enforcement to ensure companies maintain adequate cybersecurity controls and appropriately disclose cyber-related risks and incidents.

Unfortunately, our research shows that cyber risk is not easy to understand. Organizations seem often to underestimate the financial loss related to cyber threats. These can include:

- Immediate effects, such as business interruptions, decreases in production, and delays in product launches, as well as additional costs to recover from an attack.
- Long-term consequences, such as damage to the company's competitiveness and reputational loss, as well as loss of revenues from intellectual property theft, data theft, or unauthorized use of proprietary information.
- There's also legal risks resulting from neglecting, for instance, cyber resilience obligations in products and services, breach reporting, safeguarding of sensitive data, or critical infrastructure protection.

There isn't a simple way forward, though. Overinvesting in cyber risk management or risk-management strategies that don't align with business needs can have equivalently negative impacts. This article explains the importance of the SEC's new cybersecurity rules and addresses the four essential topics investors should discuss with the board for evaluating the long-term effectiveness of their companies' cyber risk management strategy.

Transparency in Cyber-Risk Governance

Being transparent about cybersecurity isn't just best practice, it's now a requirement for U.S. companies. The SEC's new cybersecurity rules "require publicly enlisted companies to disclose their cybersecurity governance capabilities, including the board's oversight of cyber risk, a description of management's role in assessing and managing cyber risks, the relevant expertise of such management, and management's role in implementing the company's cybersecurity policies, procedures, and strategies."

This kind of disclosure allows investors to evaluate the attention of executives and business leaders to cyber risks. Management boards need to understand how these threats can cause material harm. For instance, the ransomware attack on Hanesbrands disrupted order fulfillment for three weeks, causing a $100 million loss in revenue. Another example is the IT outage caused by a cyber attack at Tenet Healthcare, which also resulted in $100 million of lost revenues. And the Kaseya VSA breach was the result of insecure operational software that ultimately let to the postponement of an initial public offering that sought to raise $875 million.

Under the new SEC guidelines companies are also required to report within four days of incidents that are deemed "material." The "materiality" determination is influenced by the incident's impact on the company's business, operations, and financial conditions. This mandatory incident reporting allows investors to evaluate the effectiveness of the firm's cyber risk policies and may provide learnings for future improvements in cyber risk management. And there is a significant opportunity for improvement since the cost of cyber crime — including the cost for recovery and remediation — are expected to grow to $10.5 trillion per year by 2025.

4 Critical Areas Investors Should Expect Boards to Address

These new cybersecurity rules should be considered a starting point for the dialogue about cyber-risk governance. To shore up their cybersecurity and stay ahead of the curve, companies need to consciously anticipate to changing internal and external environment and prioritize their cyber risk efforts accordingly.

Cyber risk can be hard to understand. Board members already deal with a lot of different strategic challenges, and when faced with issues around cyber risk — such as prioritizing product market growth versus its security, critical supplier dependency for secure service delivery, dealing with "heinous" aspects of ransomware attacks, or falling victim to geopolitical cyber tensions — they can be overwhelmed by the complexity and dynamic nature of the problems. Ultimately, this may cause cybersecurity-related blind spots, impacting the effectiveness of intended decisions and even yielding unintended consequences, which can lead to what is the "capability trap," an ongoing deterioration of essential organizational processes. An essential characteristic of this trap is that its effects remain hidden from management for a very long time, until it is too late. The capability trap happens more often than many decision-makers imagine.

To avoid this trap, companies need to focus on long-term effectiveness of their strategic decisions in four areas:

1. Align cyber risk management with business needs.
Boards have many corporate challenges to face and limited amounts of funding available to meet them, so being able to make the business case for this investment is essential. Clear insights into business, operational, and financial exposures: 1) generate language to discuss cyber risks, 2) connect to board members who do not have a technical background, and 3) put cyber risk on the agenda, as well as allow for comparing this

risk with other corporate challenges. It also helps the board explain the cyber risk exposure of the firm to investors. The National Association of Corporate Directors (NACD) recognizes this need and deployed a commercially available solution to its members.

2. Continuously monitor the cyber risk capability performance.
The people, processes, and technology that make up firms is changing — and there are more and more areas that need protection, imposing an ever-increasing and dynamically shifting burden on the security capabilities of the organization, making lapses more likely. Solving these problems may require significant security capability improvements, which may take several months or even years.

Continuous monitoring is essential to establish if the cyber-risk management strategy performs as intended. Often management reporting dashboards, combined with insights from cyber event exercises are used for this purpose. Currently, in their most advanced form, these activities can capture the near real-time situation. Yet, for bridging the timing gap for utilizing improvements decision-makers have a need to see what the future outcome of their strategic decisions. This evokes the need for simulation aided approaches to strengthen managerial foresight capabilities.

3. Proactively anticipate to the changing threat landscape.
Digital transformation also allows for faster, stronger, and more sophisticated attacks. This adversarial behavior strengthens the ongoing, changing, and emerging struggle between the offensive and the defensive. Both parties try to observe, learn, and anticipate each other. Consequently, adversaries introduce new, innovative techniques to remain successful.

Proactive cyber risk management enables defending organizations to learn from information sharing and exercises prior to cyberattacks. It

contributes to security capability improvement prior to attacks and therefore reduces the number of significant security incidents. Reactive learning is significantly costlier because organizational improvement takes place based on the lessons learned from cybersecurity incidents that they have suffered. Currently, 56% of knowledgeable decision-makers make costly, suboptimal decisions when it comes to cyber risk management. The overspending on cyber risk management affects the profitability of the firm.

4. Position security as a strategic business enabler.
Cyber-risk-management strategy implementation can be a challenge. As previously mentioned, the ongoing increase in surfaces that require protection and increasing adversarial behavior require more efforts from cybersecurity teams to improve the defensive posture. However, these teams are struggling with a lack of qualified security resources. Currently, the United States alone has more than 750,000 cybersecurity job openings. This makes focusing on today's workload already difficult, let alone preparing for the defense posture of the future by running a cyber risk management program.

Effective ongoing workload reduction becomes essential. Therefore, secure by design, collaboration with other parties, automation, and the realization of economies of scale are critical to achieving a future state of security. Organizations that cannot properly make these adjustments become increasingly exposed to unintended control lapses and reactive learning mechanism.

The SEC's new cybersecurity rules provide a solid basis for transparency about companies cyber-risk governance. These rules are a great basis for starting a dialogue about long-term effectiveness of cyber-risk governance with the board. This article provides four critical areas relevant to this dialogue.

Acknowledgements: This work is co-funded by "Fondo Europeo di Sviluppo Regionale Puglia POR Puglia 2014 – 2020 – Asse I – Obiettivo specifico 1a – Azione 1.1 (RS) – Titolo Progetto: Suite prodotti Cybersecurity e SOC" and BV TECH S.p.A. This work is co-funded by Cybersecurity at MIT Sloan (CAMS).

This article was originally published online on June 02, 2023.

SZ

Sander Zeijlemaker, is a Research Affiliate Cybersecurity at MIT CAMS, agenda contributor to the World Economic Forum, president of the Security, Stability and Resilience special interest group of the System Dynamics Society and managing director of Disem Institute.

CH

Chris Hetner served as the senior cybersecurity advisor to SEC chairs White and Clayton and currently is a senior advisor at The Chertoff Group, a special advisor for cyber risk at NACD, and Co-Chair Cybersecurity and Privacy, NASDAQ Center for Board Excellence Insights Council.

MS

Michael Siegel, is Principal Research Scientist and Director of Cybersecurity at MIT Sloan (CAMS). His research focusses on cyber risk management, cyber resilience management, IT/OT integration, and application of AI techniques.

