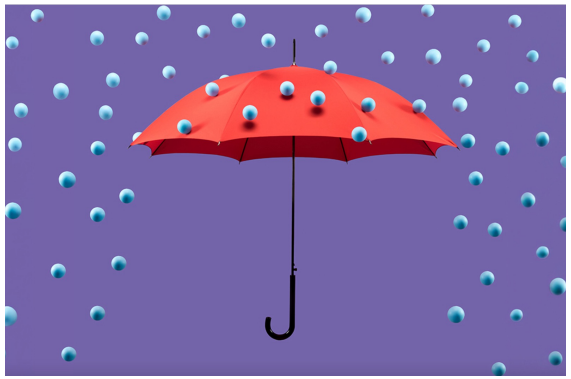
Harvard Business Review

Sander Zeijlemaker
Chris Hetner
Michael Siegel

June 2, 2023

4 Areas of Cyber Risk That Boards Need to Address



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."

...

TO CONTINUE, SCAN QR CODE

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.* **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.* **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.*