KPMG

Mitigating Cyber Risk

Audit Insights

May 2022

Mitigating risk in an increasingly digitized world

In an increasingly digitized world, it's more vital than ever that businesses and organizations develop effective internal controls to identify and mitigate cybersecurity risks. Last year, more data compromises[1] took place in the U.S. than in any year since the first state data breach notification law became effective in 2003. Cyberattacks show no signs of slowing: according to a KPMG survey of senior risk executives[2], 84% say cybersecurity risks will grow in 2022, and 74% expect compliance risks to rise in tandem.

Investors, regulators, and other stakeholders increasingly demand transparency about how companies are managing evolving cybersecurity risks to better understand the factors that could materially impact a company financially. Audit committees, which often oversee the entity's cybersecurity risks, can play a proactive role in helping organizations understand the impact on their financial reporting and in reevaluating their privacy and security standards.

Understand the risk and regulatory environment

In March 2022, on the heels of several large-scale data breaches, the SEC released new proposed amendments[3] on cybersecurity risk and incident disclosures for public companies. A month prior, the SEC proposed rules to require registered investment advisers and funds[4] to adopt and implement cybersecurity risk management policies and procedures.

These evolving cybersecurity reporting requirements certainly raise pressure for public companies. Over 80% of senior risk executives in the U.S.[5] report that rigorous enforcement, increasing regulatory burdens, and potential penalties increase the time and attention that their corporate leaders pay to compliance issues. For boards and audit committees, the set-and-forget approach to internal cybersecurity controls is no longer sufficient.

Know your risk environment and appetite

An organization's data security and privacy plan should be tied to its corporate strategy and growth objectives. Organizations' customers and stakeholders are increasingly demanding transparency regarding how companies process the myriad of personal data they collect. To protect the value such data generates,

---

[1] Identity Theft Resource Center, *2021 Annual Data Breach Report*, https://notified.idtheftcenter.org/s/2021-data-breach-report.
[2] KPMG US, *A triple threat across the Americas: KPMG 2022 Fraud Outlook,* January 2022, https://advisory.kpmg.us/articles/2022/2022-kpmg-fraud-outlook.html.
[3] U.S. Securities and Exchange Commission, "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," March 9, 2022, https://www.sec.gov/news/press-release/2022-39.
[4] U.S. Securities and Exchange Commission, "SEC Proposes Cybersecurity Risk Management Rules and Amendments for Registered Investment Advisers and Funds," February 9, 2022, https://www.sec.gov/news/press-release/2022-20.
[5] KPMG US, *A triple threat*.

organizations must invest in privacy and security capabilities and services to effectively oversee internal and external data uses while demonstrating to stakeholders a proactive and consistent cybersecurity strategy and implementation.

Stay up to speed on regulatory requirements

Evolving regulations on a global scale can pose a wide range of challenges, especially for sensitive data (e.g. financial transactions, healthcare and personal data). These regulations can range from the SEC's disclosure requirements, to data privacy laws such as the EU General Data Protection Regulation and the California Consumer Privacy Act, to wide-ranging oversight over financial crimes and operational risks. Ensuring all these regulations are met, while paying close attention to new regulatory developments, will improve the overall compliance of organizations and reduce their cybersecurity risk level.

Be proactive about supply chain risk

It is essential to recognize that some regulations, such as the SEC's updated disclosure guidance, may also apply to service providers of the organizations. Therefore, dedicated assurance programs can verify cybersecurity protocols, strengthen vendor relationships, and maximize cybersecurity-related regulatory compliance across the supply chain.

Supply chain risk has become top of mind for organizations, with a number of large supply chain hacks in the past 18 months affecting clients downstream. One of the most complex was a sophisticated supply chain hack[6] in late 2020 where a malicious code was introduced into a software platform during the software design process. Another example is the January 2022 ransomware attack on a workforce management software platform which made headlines when it cut off thousands of employers' access to timecards and other services. And recently, a global automotive company was forced to temporarily shut down domestic production due to a supply chain cyberattack.

Third-party cybersecurity risk should be part of every audit. Managing this risk is crucial to protecting companies' data. Setting security standards for outside vendors is a good start, but in order to be effective, companies must run security checks in a continuous, real-time process.

Data integrity is the centerpiece of cyber assurance

Data presents one of the biggest challenges facing businesses and organizations because data silos often accumulate over a company's lifetime. These silos come both from internal functions and external service providers. According to a KPMG data privacy survey[7] in 2021, more than 60% of business leaders say their organization should be doing more to strengthen existing data protection measures. The board and audit committee should take time to ensure the company can break down unnecessary data silos as needed while exerting robust controls over data practices across its supply chain.

When a cyberattack happens

The 2022 KPMG Fraud Outlook[8] finds that 62% of surveyed senior risk executives say their company experienced an economic loss due to cybercrime in the past year. If a cyber incident occurs, businesses

[6] Sudhakar Ramakrishna, "New Findings From Our Investigation of SUNBURST," Orange Matter – SolarWinds, January 11, 2021, https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/.
[7] KPMG US, *Corporate data responsibility: Bridging the consumer trust gap,* August 2021, https://advisory.kpmg.us/content/dam/advisory/en/pdfs/2021/corporate-data-responsibility-bridging-the-consumer-trust-gap.pdf
[8] KPMG US, *A triple threat*.

must consider the most immediate economic impact of the incident and resulting operational roadblocks in their financial statement.

Without appropriate controls in place, data breaches can lead to costly litigation. Additionally, failing to reassure investors and customers about cybersecurity and privacy standards may damage a company's brand reputation, which could further impact the company's financial results.

Enhancing the role of boards in pivoting to the new cybersecurity horizon

In light of evolving cybersecurity challenges and pressure, boards and audit committees must commit to proactively reviewing cybersecurity risk management plans. Because of the ever-changing nature of cybersecurity risks, constant monitoring and assessment of all controls are needed to make sure that they remain relevant, and that continuous improvement can be achieved so organizations can meet emerging risks.

Boards should ask management for information on cyber incidents and threats, risk assessments, and safeguards to help develop a holistic cybersecurity and privacy strategy. As detailed in the KPMG Board Leadership Center report "On the 2022 board agenda,"[9] boards may also create a broader data governance framework that includes compliance with privacy laws and regulations as well as the company's policies and protocols regarding data ethics, data integrity, and other key areas.

Questions to ask:

- Does the company have a data governance framework that makes clear how and what data is being collected, stored, managed, and used?
- Which business leaders are responsible for cybersecurity and privacy across the enterprise?
- How does the board confirm assignment, coordination, and accountability for the company's cybersecurity and data privacy policies?
- Does the company have a plan for responding to a data breach, and what does it include? If a ransomware attack occurs, is the company willing to pay ransom? Does it know how to locate and prioritize data for recovery? Does it detail responsibilities for partner, customer, and regulator notification?

Competing in the cyber-compliant world

Business leaders should view cybersecurity as an opportunity rather than just a risk. The wheel towards enhanced cybersecurity controls is already turning in the board rooms of many businesses and organizations. According to the KPMG Technology Industry Survey[10], more than half of technology company leaders say their cyber security strategy is integrated with their growth strategy and even more view their information security as a competitive advantage.

---

[9] KPMG US, *On the 2022 board agenda*, December 9, 2021, https://boardleadership.kpmg.us/relevant-topics/articles/2022/on-the-2022-board-agenda.html.
[10] KPMG US, *Tech companies lean on cyber to go faster and gain trust*, February 2022, https://advisory.kpmg.us/insights/tech-industry-cyber-report-02-22.html.

This opportunity can start with building an auditable plan, with a goal of forming a strong assurance strategy with fulsome considerations and reliable metrics. Boards and audit committees can help translate this race towards cybersecurity readiness into a competitive advantage that facilitates growth, enables stakeholder trust, and fosters organizational resiliency.

Heather Paquette
National Technology Assurance Leader - Audit
+1 415 963 8998
hpaquette@kpmg.com

Doron Rotman
Managing Director, National Cyber and Privacy Co-Leader, Technology Assurance - Audit
+1 408 367 7607
drotman@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

kpmg.com/socialmedia