KPMG

Taking a byte out of cybercrime

Audit Insights

January 2023

Three cyber security considerations for technology company boards

Technology executives are bracing for an influx of cyber-attacks.

More than eight out of 10 technology, media and telecom (TMT) executives recently surveyed by KPMG foresee increased cyber risk in the coming year. However, only 39% of respondents said their company can identify a cyber breach or attack within a week of it taking place and only 21% can contain it within a week of discovery.[1] With breaches, ransomware, malware and other forms of attack on the rise, TMT companies have a lot to lose from a cyber event—intellectual property, customer information, network infrastructure, data center access, competitive standing and, importantly, profits. According to IBM, the average total cost of a data breach in 2022 rose to $4.35 million globally and $9.44 million in the United States.[2]

If we narrow the scope to technology companies specifically, the largest of which have millions of customer touchpoints and are already under intense public scrutiny, the operational, reputational, regulatory and financial risks become that much greater. With stakes like these, mitigating cyber risk has never been more critical.

From conversations with technology company boards, their audit committees and management, we've identified three key actions boards should take to mitigate cyber risk:

1. Level up monitoring of management's cyber preparedness to address the growing sophistication of threats

Boards are already making significant strides in monitoring management's cyber security effectiveness. According to the KPMG Board Leadership Center's *On the 2023 board agenda*, boards are increasingly operating with greater IT and cyber expertise and sharpening their focus on how management implements company-specific dashboard reporting to identify critical risks and opportunities, assess cyber security talent, war-game various attack scenarios and more.[3]

And yet, despite this progress, the sophistication of threats is only accelerating, forcing companies and their boards to function in a continual state of catch-up. This phenomenon is particularly prevalent in the technology sector, as well as across media and telecom, where 83% of executives reportedly saw an

[1] KPMG LLP, "Telecoms, Media & Entertainment, Technology (TMT): KPMG 2022 Fraud Outlook," 2022, https://advisory.kpmg.us/articles/2022/kpmg-2022-fraud-outlook-tmt.html.
[2] IBM, "Cost of a Data Breach Report 2022," https://www.ibm.com/reports/data-breach.
[3] KPMG LLP, "On the 2023 board agenda," December 2022, https://boardleadership.kpmg.us/relevant-topics/articles/2023/on-the-2023-board-agenda.html.

increase in frequency of at least one type of cyber-attack over the past year.[4] Like many other sectors, technology companies are prone to phishing and scamming incidents. However, they are also uniquely vulnerable to a range of more sophisticated cyber tactics. Per *KPMG's 2022 Fraud Outlook*, TMT executives were more likely than those in any other industry to report growth in malware (30% compared to 22% on average), social hacking (23% to 17%) and SQL injection attacks (18% to 11%).[5]

So, what makes technology companies, specifically, so vulnerable? Aren't the most technologically savvy companies the most prepared for cyber events? Not necessarily. For one, technology companies are not only collecting, storing and managing data, they are also creating it. Constant innovation keeps these companies on the leading edge, but it also attracts bad actors. This is an industry-wide issue with cyber criminals targeting multiple technology companies at once to see where they can gain footing before striking.

Supply chain vulnerability is also a key concern. Technology companies face enhanced accountability for the security of their products—whether software, hardware or otherwise—up and down the supply chain, from the initial development of the technology to each customer touchpoint. In other words, the responsibility to mitigate cyber risk does not stop at point of sale. After all, a customer who purchases a new computer wants reasonable assurance that the company that sold it will remain vigilant of cyber vulnerabilities over the course of the computer's life. Supply chain protection is particularly top-of-mind for management: 79% of technology executives surveyed by KPMG view protecting their partner ecosystem and supply chain as just as important as building their own organization's cyber defenses.[6]

Then, of course, there is reputational risk. We're living in an era of intense scrutiny over how a company protects *and uses* customer data. Key stakeholders—from customers to regulators to policymakers—are increasingly telling the largest technology companies, "Just because you can doesn't mean you should." The long-lasting reputational impact of a cyber-attack may in fact outweigh the financial repercussions.

In light of the above challenges, technology company boards—and their audit committees—may need to sharpen their oversight in a number of critical areas, including:

- How sensitive management is to early warning signs of cyber events;
- The extent to which management embeds cyber considerations into the design process for new products and internal systems;
- Whether the company's crisis response plan is robust and ready to go, taking into account the potential loss of critical infrastructure, such as data centers;
- The quality of processes and controls in place over cyber risk management, and whether they are keeping pace with the ever-evolving threat landscape;
- The cyber risks posed by the company's entire supply chain; and
- If or when a cyber incident occurs, management's ability to identify the source of the incident efficiently and effectively (i.e., a deficiency in internal controls) and put new procedures in place to prevent future incidents.

2. Keep a close eye on the regulatory environment and plan accordingly

As companies across sectors contend with the evolving cyber security landscape, understanding the impact of cyber risk on the company's financial results and position is mission critical. Cyber security incidents can

[4] KPMG LLP, "Telecoms, Media & Entertainment, Technology (TMT): KPMG 2022 Fraud Outlook."
[5] KPMG LLP, "Telecoms, Media & Entertainment, Technology (TMT): KPMG 2022 Fraud Outlook."
[6] KPMG LLP, "Technology companies lean on cyber to go faster and gain trust," 2022, https://advisory.kpmg.us/insights/tech-industry-cyber-report-02-22.html.

lead to additional expenses (including increased insurance premiums and legal liabilities), losses in revenue and diminished future cash flows.[7] And, without appropriate controls in place, they also can lead to long-term litigation and reputational damage, impacting the company far beyond the current fiscal year.[8]

Regulators are working to bring greater clarity to the connection between cyber risk and financial reporting. Under 2018 regulation from the U.S. Securities and Exchange Commission (SEC), companies that experience a cyber event are expected to provide reasonable assurance that information about the range and magnitude of financial impacts from that event be incorporated into financial reporting on a timely basis.[9] This includes future effects as well, such as reduced revenues, increases in litigation, cyber security and insurance costs and the possibility of assets becoming impaired.[10]

In March 2022, the SEC took an even firmer stance, proposing new rules related to cyber risk management, strategy, governance and disclosure requirements for public companies.[11] If enacted, the rules would increase the prominence of required disclosure on cyber security incidents in a number of corporate filings, including annual filings. They would also require disclosure of cyber events within four days of any incident being deemed material, and greater detail surrounding companies' cyber security policies and procedures, management's role in cyber security governance and the board's level of oversight and expertise.[12]

With final SEC action on the proposed rule expected in the spring of 2023, companies across sectors, and their boards, need to prepare. For technology company boards, this should prompt an increased focus on the company's:

- **Cyber security and privacy standards within the context of financial reporting.** Audit committees must play a key role in overseeing the impact of a breach or another cyber event on the financial statements.
- **Inventory of all third-party relationships.** Dedicated assurance programs can verify cyber security protocols, strengthen vendor relationships and maximize related regulatory compliance across the supply chain.[13]
- **Assessment of how future cyber regulation may impact the business.** While technology companies are already bound to extensive data privacy legislation, such as the General Data Protection Regulation and the California Consumer Privacy Act, they must also consider what future regulation from the SEC, the Federal Trade Commission or another governing body may mean for operations, strategy and reporting.
- **Understanding of who will do the heavy lifting on regulatory compliance.** Boards may use new SEC reporting requirements as a marker to evaluate the composition of the company's disclosure committee, making sure appropriate functional leaders (i.e., chief supply chain officer, chief information security officer and others) are included.[14] They may also evaluate internally who will monitor compliance. The

---

[7] KPMG LLP, "Defining Issues: SEC issues guidance on cybersecurity," February 2018, https://frv.kpmg.us/reference-library/2018/sec-cybersecurity-guidance.html.
[8] KPMG LLP, "Mitigating Risk in an Increasingly Digitized World," May 2022, https://info.kpmg.us/news-perspectives/advancing-the-profession/mitigating-risk-in-a-digitized-world.html.
[9] U.S. Securities and Exchange Commission, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures,* February 2018, https://www.sec.gov/rules/interp/2018/33-10459.pdf.
[10] KPMG LLP, "Defining Issues: SEC issues guidance on cyber security."
[11] U.S. Securities and Exchange Commission, "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," March 2022, https://www.sec.gov/news/press-release/2022-39.
[12] KPMG LLP, "SEC on ESG: Proposed enhancements to cybersecurity disclosures," March 2022, https://frv.kpmg.us/reference-library/2022/sec-cybersecurity-guidance.html.
[13] KPMG LLP, "Mitigating Risk in an Increasingly Digitized World."
[14] KPMG LLP, "On the 2023 audit committee agenda," December 2022, https://boardleadership.kpmg.us/relevant-topics/articles/2023/on-the-2023-audit-committee-agenda.html.

audit committee is traditionally tasked with cyber risk oversight, but the increased workload of SEC reporting may necessitate expansion to additional directors and committees.[15]

3. Recognize the link between cyber security and data governance

Once a standalone responsibility for the audit committee, we're beginning to see cyber risk viewed under the larger umbrella of data governance. Companies and their boards are building robust data governance strategies to identify and address risks associated with cyber security, data privacy, data ethics and hygiene and artificial intelligence. While cyber risk has historically been the purview of the audit committee—and audit committees clearly have a continued role in cyber risk oversight—the heightened complexity of the landscape means that oversight is increasingly touching multiple points on the board agenda. Where exactly it sits at the committee level depends on several factors, including the nature of the business, the company's current level of cyber preparedness, the bandwidth of board committees and the unique skill sets of directors.[16]

For technology companies, this consolidation means that boards and audit committees must be ready to discuss and monitor cyber risk within the context of broader data governance issues. For example, fast-emerging technologies that will likely require increased board and committee focus include:

- **Facial recognition software:** How is facial recognition data collected? Where is it stored? What are the associated privacy concerns and how is management mitigating them?
- **Artificial intelligence and machine learning:** What are the ethical considerations? As technology continues to learn and adapt, what biases are implicit and how is management addressing them? What regulatory compliance (including E.U. regulations) and reputational risks are triggered by the company's use of this technology?

Ultimately, how the board and management work together to address issues of data governance is the basis for digital trust: the confidence stakeholders have in the ability of an organization to harness digital technology to protect their interests and uphold societal expectations and values.[17] As we've seen countless times on the national and global scale, failing to preserve digital trust can have detrimental repercussions, financially, reputationally, legally and more.

Accountability and mitigation are critical

In today's environment, technology companies must stay vigilant for data vulnerability. Cyber, privacy and other related data governance risks run rampant across the sector. Whether they arise in the earliest stages of product innovation or in customer data collection and storage, in machine learning or up and down the supply chain, technology company board members have their work cut out for them to anticipate and work with management to mitigate these risks.

The board must hold management accountable for action, or inaction, and should help leadership send and reinforce the message that the company's security is the responsibility of every employee. Employee training, weaving data governance best practices into company culture and allowing for regular touchpoints between the board and the technology function are all integral to success. There is no one-size-fits-all approach. Instead, leaders say it takes a village, manned by skilled professionals who continually assess and identify emerging threats and develop comprehensive programs to address them.[18] With the blistering pace of

[15] KPMG LLP, "On the 2023 board agenda," December 2022.
[16] KPMG LLP, "Oversight of cybersecurity and data governance," 2021, https://boardleadership.kpmg.us/relevant-topics/articles/2021/oversight-of-cybersecurity-and-data-governance.html.
[17] KPMG LLP, "Cyber trust insights 2022," 2022, https://advisory.kpmg.us/articles/2022/cyber-trust-insights-2022.html.
[18] KPMG LLP, "Technology companies lean on cyber to go faster and gain trust."

innovation in the technology sector, this is a tall order. However, by establishing a strong cyber risk management strategy today, technology companies can enjoy a sizeable competitive advantage tomorrow.

Authors

Janel Riley
National Audit Industry Leader, Technology
KPMG LLP
408-761-2792
janelriley@kpmg.com

John Rodi
Leader, KPMG Board Leadership Center
KPMG LLP
1-800-808-5764
us-kpmgmktblc@kpmg.com

Kyle Kappel
U.S. Leader for Cyber
KPMG LLP
312-953-9079
kylekappel@kpmg.com

Jason Schneider
Audit Partner
KPMG LLP
619-517-6800
jwschneider@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia