Navigating enhanced cybersecurity regulations

Audit Insights

April 2023

Navigating enhanced cybersecurity regulations

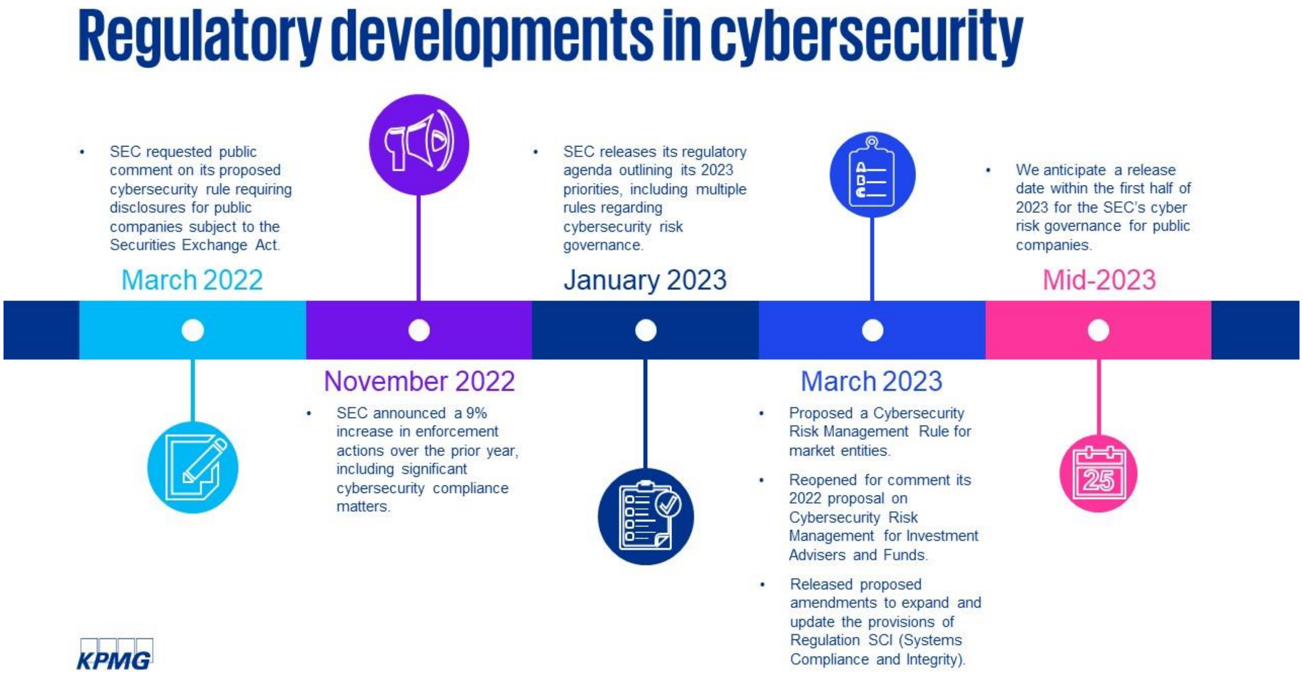
Companies are facing cyberattacks every day, with large organizations across industries reporting hackers gaining access to customer information, taking down IT systems and often making demands for ransom payments. As cyberattacks become more frequent and sophisticated, organizations are facing increased stakeholder calls and regulatory requirements to show they are protecting their information appropriately. According to a recent KPMG survey[1], 83% of companies suffered a cyberattack in the past year, and respondents said it took them an average of one month to fully contain the attack.

The Securities and Exchange Commission (SEC) is undertaking a comprehensive effort to increase cybersecurity preparedness and resilience for all registrants. This spring, new cybersecurity reporting requirements[2] for public companies are expected, enhancing and standardizing risk management, strategy, governance and incident disclosures. The SEC also released proposed cybersecurity rules for broker-dealers and other market entities[3] and opened comments on rules for registered advisers and funds[4] in March 2023. At the same time, the SEC is enforcing large penalties against some companies for misleading disclosures around past cyberattacks. Additionally, in April 2023, the Public Company Accounting Oversight Board listed cybersecurity among its top priorities for this year's inspections.[5]

With the increased focus on cybersecurity from regulators, customers and investors, executives have a growing responsibility to understand their company's cyber risks and the state of cyber programs. As a baseline, with oversight from the board, management should be preparing now to comply with the SEC's final rules on cybersecurity disclosures. Going beyond regulatory compliance, it's imperative to understand how your organization is positioned to detect, mitigate and remediate any cybersecurity threats and vulnerabilities with respect to information systems as well as business continuity and overall cyber incident reliance.

[1] KPMG LLP, "A triple threat across the Americas: KPMG 2022 Fraud Outlook," 2022, https://kpmg.com/xx/en/home/insights/2022/01/kpmg-fraud-outlook-survey.html.
[2] KPMG LLP, "SEC proposes cybersecurity rules," March 2022, https://frv.kpmg.us/reference-library/2022/sec-cybersecurity-guidance.html.
[3] KPMG LLP, "SEC Proposals on Cyber Risk Management for Market Entities," 2023, https://advisory.kpmg.us/articles/2023/sec-roposals-on-cyber-risk-management-for-market-entities.html.
[4] KPMG LLP, "Cybersecurity: SEC Proposal for Adviser/Fund Risk Management, 2022, https://advisory.kpmg.us/articles/2022/sec-cybersecurity-reg-alert-feb-2022.html.
[5] Public Company Accounting Oversight Board, "Spotlight: Staff Priorities for 2023 Inspections, April 2023, https://assets.pcaobus.org/pcaob-dev/docs/default-source/documents/priorities-spotlight.pdf

Regulatory developments in cybersecurity



March 2022

- SEC requested public comment on its proposed cybersecurity rule requiring disclosures for public companies subject to the Securities Exchange Act.

November 2022

- SEC announced a 9% increase in enforcement actions over the prior year, including significant cybersecurity compliance matters.

January 2023

- SEC releases its regulatory agenda outlining its 2023 priorities, including multiple rules regarding cybersecurity risk governance.

March 2023

- Proposed a Cybersecurity Risk Management Rule for market entities.
- Reopened for comment its 2022 proposal on Cybersecurity Risk Management for Investment Advisers and Funds.
- Released proposed amendments to expand and update the provisions of Regulation SCI (Systems Compliance and Integrity).

Mid-2023

- We anticipate a release date within the first half of 2023 for the SEC's cyber risk governance for public companies.

KPMG

You are here: Assessing your organization's current cyber risk

As a first step, management should evaluate the organization's current situation, laying the groundwork for a strategy for enhancing the organization's cyber maturity, achieving SEC compliance and reassuring customers, investors and other stakeholders that appropriate safeguards are in place. Key questions may include:

- Does management understand how mature the organization's cyber programs are in relation to others in the same industry?
- Is there appropriate insight into the current and future business, regulatory and compliance impacts of cyber risks on the organization's supply chain, both upstream and downstream?
- Has any risk assessment been performed to understand how the organization may be impacted by the current or future SEC proposals and regulations?

Third-party assessments and attestations are tools for management and the board to understand the organization's current cyber readiness and respond to stakeholder demand for transparency. A cyber maturity assessment is a way for the financial reporting and internal controls function to get a clear, easily digestible view of the organization's current cyber program benchmarked against other organizations of similar size and industry. A cybersecurity-focused SOC report can provide attestation for cyber controls.

Leaders should consider assessments that include potential vulnerabilities along the supply chain, which are often exploited by bad actors. With increased pressure from stakeholders throughout the supply chain to obtain varying levels of cybersecurity assurance, management may look to shift the organization's assessment of its cybersecurity posture from the historically acceptable self-attestation approach to assessments or attestation engagements performed by an independent third party. This level of independent attestation can clearly demonstrate to vendors and customers that appropriate governance and controls are in place to protect their sensitive data and reduce exposure to their IT environment.

Mapping out the future

With an understanding of the organization's starting point, management can plot out a path to compliance with SEC cyber regulations, transparency in response to stakeholder demand and organizational resilience.

Updating the internal communications plan

Questions to ask:

- How does the Information Security function disseminate information to key stakeholders in financial reporting and internal controls, including the board, audit committee and controller?
- At what frequency do these communications occur?

Even when a cyber incident has not been identified, cybersecurity update meetings should be held at defined frequencies to ensure all key stakeholders are equipped with the latest pertinent information. Establishing clear communication and reporting lines for identified cyber incidents is critical for ensuring those charged with financial reporting and internal controls are informed at the appropriate time to consider implication on Internal Controls over Financial Reporting and achieve compliance with any SEC regulations.

Preparing for a potential cyberattack

Questions to ask:

- Does management, with oversight from the Audit Committee, have fulsome cybersecurity incident response and recovery plans and procedures in place?
- Does management understand how potential cybersecurity incidents will be triaged and ultimately communicated to key stakeholders responsible for reporting to the SEC if a breach is identified? Are those reporting mechanisms in place?

Management should review and update cyber incident response policies and procedures, including a clear delineation of responsibilities of the cybersecurity and risk management teams, management's disclosure committee, and the legal department, plus escalation procedures to determine materiality, and preparation and review of disclosures.

With board oversight, management should test the cyber response plan and procedures, including documenting the cyber incident, evaluating it for materiality, drafting the disclosure and reviewing incidents in the aggregate. In its rule for public companies, the SEC will expect a materiality determination to be made "as soon as reasonably practicable," which may require judgment. Audit committees and boards should confirm that management has a plan for escalating incidents to the disclosure committee and legal team to make the final materiality determination.

Know before you go

As regulatory requirements around cybersecurity increase and threats from cybercriminals become more severe, it will be crucial to manage risks by ensuring governance is in place to protect sensitive information. Management can lead the way through uncharted waters by bolstering cyber maturity ahead of coming regulations.

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

Maksim Vander
Managing Director
Technology Assurance - Audit
KPMG LLP
212-872-7934
mvander@kpmg.com

Christopher Montone
Director
Technology Assurance - Audit
KPMG LLP
267-256-7000
cmontone@kpmg.com

Ruixiang Wu
Director
Technology Assurance - Audit
KPMG LLP
212-954-4006
ruixiangwu@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

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.