Navigating the SEC's new cybersecurity disclosure rules

The SEC finalized its cybersecurity disclosure rules for public companies, and now the race to comply is on. The frequency and impact of cyberattacks affecting both shareholder and stakeholder interests, fueled a strong demand for cybersecurity transparency. But the rules go far beyond just incident disclosure; they also require improved and standardized risk management, strategy, and governance over what has mostly been outside the arena of financial reporting.

Never before have reporting requirements been tethered to a scope of technology risks that are as rapidly evolving, challenging to quantify, and far more complex than those traditionally aligned to financial reporting processes. And risks associated with adjacent technologies and capabilities, such as artificial intelligence (AI), are almost inextricably linked. In fact, 78% of executives believe AI and machine learning also present unique cybersecurity challenges. So while the rules provide greater transparency, they require companies to keep pace with rapid shifts in technology that are likely to continue compounding as technology further enables businesses, financial reporting, and the audit.

Those responsible for financial reporting, internal controls, and compliance for 8-K and 10-K disclosures may now find themselves in uncharted territory. These rules provide greater transparency for investors and the capital markets and require companies to maintain pace with rapid shifts in technology that increasingly impact both financial reporting and third-party auditing and assessment.

So what do finance leaders, especially CFOs, need to know and do in preparation for rule compliance? Here are four key areas to focus on:

1. Confirm scoping and materiality assessments and adjust your processes to ensure compliance.

Companies that began preparing for compliance during rule proposal period may need to adjust their processes according to the final SEC requirements: cataloguing documented incidents, making materiality determinations, and drafting disclosures. Notably, the final rule includes a 30-day disclosure delay if the federal government determines the disclosures pose a risk to national security or public safety – which was not included in the original proposal. Revisit your cybersecurity processes for integration with your overall risk management system.

2. Build for speed.

Under the new rules, companies must disclose material cybersecurity incidents in their 8-K within 4 business days after they determine that the incident is material. This creates complexity, as determinations need to be

made “as soon as reasonably practicable,” and consider the perspective of a “reasonable shareholder” making an investment decision. It is crucial for companies to prepare a thoughtful, standard incident review process that include those who are responsible for disclosures and who can balance quantitative and qualitative factors for incidents that impact the company – and then engage the reporting process effectively.

Further, annual reports must also include disclosures on the company’s processes to identify, assess and manage material risks from cybersecurity threats, including management’s role in those processes and the board’s oversight. Given the newly required speed to disclosure, now is the time for organizations to test their cyber response processes and controls, and ability to draft disclosures with proper documentation.

3. Align and integrate your cyber risk management, strategy, and governance.

Companies must disclose in the annual report their strategy for preventing future cyberattacks and integrating cybersecurity processes into their overall risk management approach. Questions they should consider include: How are cybersecurity processes integrated into the overall risk management system? How are auditors and other third-party assessors engaged on these processes? And how is a company identifying vendors’ cyber risks?

Companies must carefully evaluate whether cybersecurity threats, including past incidents, have had a material impact or are reasonably expected to be material to their operations. This assessment may require a more comprehensive tracking of cyber attacks. Companies should consider tracking the nature and relationship of all cyber incidents to inform judgements required under the new rules. Third-party assessments and attestations can support this undertaking. A cyber maturity assessment can help companies benchmark against peers, and attestation vehicles like the System and Organization Controls (SOC) for Cybersecurity report can provide internal and external stakeholders with assurance over the organization’s cybersecurity governance and control effectiveness.

4. Oversight and third parties.

Compliance requires companies to have line of sight into their own procedures – and beyond. The new rule emphasizes the need for appropriate oversight to be in place for key stakeholders – including the board, audit committee, and controller – to assess materiality and make timely disclosures. Early testing of existing systems to confirm that they work with the expanded disclosure rules, is essential.

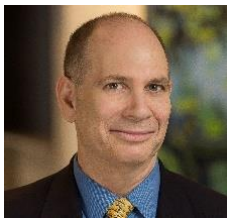
More importantly, incidents with third parties may be considered material. A cyber breach that occurs on a third-party system can still be deemed material and disclosed. Processes to oversee and identify material risks from third parties should be included within your firm’s 106b disclosure.

Previously companies have relied on third-party attestation to verify the consistent and comparable delivery of cybersecurity control information. This update may necessitate increased and ongoing partnerships.

Complying with the SEC’s new cybersecurity disclosure rules requires organizations to navigate potentially uncharted waters. By understanding materiality determinations, ensuring proper controls are in place, and focusing on risk management, strategy, and governance, companies can meet the new standards and proactively enhance transparency and trust.

Authors

Matthew Johnson
National Tech Assurance Leader - Audit
KPMG LLP
404-222-3491
mpjohnson@kpmg.com



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

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

We would like to thank our contributors: Ruixiang Wu and Christopher Montone.

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