Cooley

# SEC's Proposed Rules Highlight Continued Focus on Cybersecurity

March 15, 2022

On March 9, 2022, the Securities and Exchange Commission ("SEC") proposed new rules which, if adopted, would require public companies to promptly disclose material cybersecurity incidents and, more generally, to provide more detailed disclosures regarding cybersecurity risk management, strategy, and governance practices. The rules – the latest in a series of recent SEC cyber-related regulatory and enforcement actions – demonstrate that the agency is only increasing its scrutiny of this area.

The proposed rules, which are subject to a public notice and comment period, have two primary components. First, they would add material cybersecurity incidents to the list of events required to be disclosed in the SEC's Form 8-K current report filing. Public companies would be required to file a Form 8-K within four business days after determining that a material cybersecurity incident has taken place. The required disclosures would include:

- When the incident was discovered and whether it is ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incident.

The proposed rules would also require companies to update these disclosures with any material new information regarding the incident. Finally, if the rules are promulgated, companies would need to continually assess whether individually undisclosed cybersecurity incidents have become material in the aggregate.

In addition to requiring enhanced incident disclosure, the proposed rules would also require public companies to provide detailed information about their cybersecurity programs. Among other things, companies would be required to disclose information about their chief information security officers (CISOs); any board- or committee-level reporting framework; and processes for preventing, monitoring, and remediating cybersecurity incidents.

In support of the proposed rules, the SEC pointed to the impact of cybersecurity incidents on the economy as a whole, including critical infrastructure and national security, as well as the increasing costs that cybersecurity incidents and compliance impose on public companies. According to the SEC, "cybersecurity is among the most critical governance-related issues for investors, especially U.S. investors." As a result, "whether and how a registrant is managing cybersecurity risks could impact an investor's return on investment and would be decision-useful information in an investor's investment or considerations."

The SEC's increased presence in the cybersecurity regulatory environment comes even while the Federal Trade Commission and state regulators have continued to focus on incident reporting and response. Dissenting from the proposed rules, SEC Commissioner Hester Peirce argued that "egulators may have a role to play in working with companies on cybersecurity, but we are not the regulators with the necessary expertise."

As we have highlighted in the past, Chair Gary Gensler has demonstrated a close focus on cybersecurity in his first year at the SEC. If adopted, the proposed rules will not only present significant governance and disclosure challenges, they are likely to catalyze further scrutiny by the SEC's Enforcement Division. Areas of potential enforcement focus include:

- The failure to disclose purportedly material cybersecurity incidents, even in the absence of meaningful stock price movement;
- The failure to disclose multiple discrete cybersecurity incidents which, while immaterial when considered individually, may be material when viewed in the aggregate;
- The failure to accurately describe cybersecurity policies, procedures, controls, and/or governance, particularly in hindsight (after these safeguards have failed to prevent a material incident); and
- The failure to maintain adequate disclosure controls surrounding cybersecurity.

## Contributors

**Luke Cadigan**
**Bio**

---

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as “Cooley”). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices. Copyright © 2026