Blogs
March 10, 2022
The SEC Proposes Cybersecurity Disclosure Rules! 4 Things to Know

Yesterday, the SEC **proposed** cybersecurity disclosure rules. Here's the **129-page proposing release** - and here's the **fact sheet**. This proposal was much anticipated as it's no secret that cybersecurity incidents are one of the more serious types of risk that any company faces today. As highlighted in **SEC Chair Gary Gensler's statement,** the intent of the rules is to make disclosures regarding cybersecurity more "consistent, comparable, and decision-useful." Overall, the proposed rules are fairly prescriptive, consistent with other recent SEC proposals and a departure from the more principles-based focus of rulemaking under the prior SEC Chair. For cybersecurity topics, the specificity may be helpful to companies in determining how to craft disclosures. But, as noted in **Commissioner Hester Peirce's dissenting statement,** "the proposed rules pressure companies to consider adapting their existing policies and procedures to conform to the Commission's preferred approach." The comment period extends until the later of May 9th or 30 days after publication in the Federal Register. Here are four things to know about the proposal: **1. Form 8-K Disclosure of Cyber Incidents, With Materiality-Linked Trigger:** The proposed rules include new Form 8-K Item 1.05, which would be triggered by a company's determination that it has experienced a *material cybersecurity incident*. Notably, like other Form 8-K items that rely on materiality determinations, the proposal provides that an untimely filing would not result in a loss of Form S-3 or Form SF-3 eligibility. By making the disclosure trigger dependent upon a company's determination that a material incident has occurred, the proposal provides needed flexibility in what can be a complicated process of assessing the effect of an incident. The proposal also places guardrails on this flexibility, including an instruction that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." But, in her comments during the open Commission meeting, Commissioner Allison Herren Lee called on commenters to provide insight on whether this flexibility makes the disclosure threshold too flexible. Similarly, the proposing release asks whether Form 8-K disclosure should be triggered by *any* cybersecurity incident. If the final rules were to require Form 8-K disclosure of all cybersecurity incidents, companies probably would face incredibly burdensome challenges in making meaningful and accurate disclosure in all cases, particularly considering the four-business day reporting requirement. This is one of more challenging areas for disclosure controls and materiality determinations. Companies on the one hand don't want to jump the gun and disclose a cybersecurity incident that makes it look more serious than it is. But they also should want to get disclosure about an incident out there as soon as possible - if it's material - to stave off any potential litigation. It's a tough road to navigate, particularly if the extent of an incident takes time to sleuth out accurately once the incident is detected.

---

2. Periodic Report Disclosures for Updating Form 8-K Disclosures: Two parts of proposed new Regulation S-K Item 106 would create requirements to update or supplement Form 8-K disclosures regarding cybersecurity incidents: - Proposed Item 106(d)(1) would require disclosure of material changes, additions or updates to information included in the Form 8-K. - If a company experienced a series of immaterial cybersecurity incidents that have become material in the aggregate, proposed Item 106(d)(2) would require disclosure in a periodic report (Form 10-Q or Form 10-K for the fourth quarter) for the quarter in which the company determines the incidents are material in the aggregate. These requirements are akin to many other SEC reporting requirements for quarterly updates.

---

3. Form 10-K Disclosures: Proposed Regulation S-K Item 106 also covers disclosures that would be provided annually in Form 10-K in two categories: - *Risk management and strategy* - Companies would be required to discuss, as necessary to adequately describe their policies and procedures, topics including risk assessment programs, risks associated with third-party service providers, and risks and incidents that have affected or are reasonably likely to affect the company's results of operations or financial condition. - *Governance* - Companies would be required to discuss both the board's role in oversight of cybersecurity risk, and management's role in assessing and managing cybersecurity risks and implementing related policies, procedures, and strategies. For

management's role, the proposal calls for disclosure of the relevant expertise of the company's chief information security officer (CIO) and other members of management responsible for measuring and managing cybersecurity risk. A disclosure requirement about management expertise - which would potentially include managers beyond a company's executive officers - would be unusual in the SEC's disclosure framework.

---

4. Proxy Disclosure of Board Cybersecurity Expertise: The proposal would also amend Regulation S-K Item 407 to elicit disclosure regarding the cybersecurity expertise of board members, if any. This disclosure would be included in Part III of Form 10-K, meaning it would typically be disclosed in the proxy statement. Unlike the board financial expert disclosure that is already required, the proposal would require disclosure of any details necessary to describe the nature of the expertise. For good reason, there already has been a push by many boards to add directors with cybersecurity expertise. For those boards that don't currently have directors with this kind of expertise, the SEC's proposal might serve as a wake-up call.

Explore more in

Corporate Law