March 10, 2022

# SEC Proposes Sweeping New Cybersecurity Disclosure Rules for Public Companies

Yesterday, the SEC proposed new wide-ranging cybersecurity-related disclosure rules. The proposal represents the SEC's boldest effort yet to set national expectations for cyber-related disclosures, risk management, and corporate governance. If adopted as proposed, the rules would require public companies to disclose cybersecurity incidents more often and with greater specificity; explain the board's role in cybersecurity risk oversight and governance; discuss management's approach to cybersecurity risk mitigation and its impact on corporate strategy; highlight director and management-level expertise on cybersecurity; and describe cybersecurity policies and procedures.

The scope of the proposed rules—which echo those proposed last month for registered investment advisers and funds—is likely to generate substantial interest and comment through the SEC's rulemaking process. In accompanying remarks, SEC Chair Gensler emphasized the importance to investors of having "consistent, comparable, and decision-useful" information from public companies about cybersecurity practices and incidents. Complementary rules for registered broker-dealers and other market intermediaries are forthcoming.

The proposed rules principally address the following topics:

*Cybersecurity Incident Disclosures and Updating of Prior Disclosures*: Under the proposed rules, companies would be required to disclose under a new Form 8-K line item any material cyber incident within four business days of determining that the incident was material (applying traditional materiality standards). Undue delay in making that determination is specifically discouraged: registrants would be required to "be diligent" and assess materiality "as soon as reasonably practicable after discovery of the incident." As proposed, disclosable incidents would reach breaches involving information resources "used by" the registrant even if not "owned" by the issuer (*i.e.*, third-party systems). For all cyber incidents, companies would have to disclose the nature, scope, and operational impact of the incident, whether data was stolen or compromised, and whether remediation efforts are ongoing or complete.

The proposed rules recognize that the materiality of a detected incident may not be immediately discernable. But they also, by design, offer no relief from the disclosure deadline because an investigation is pending or where applicable state laws or other regulatory regimes might explicitly excuse or permit a delayed disclosure due to law enforcement or other investigatory imperatives. Finally, the proposed rules would establish a continuous reporting regime requiring material changes and updates to previously-disclosed information about any prior cyber incident to be included in a company's subsequent Form 10-Q or Form 10-K.

*Cybersecurity Governance and Strategy Disclosures*: The proposed rules would amend Regulation S-K to require that companies provide recurring disclosures describing their cybersecurity policies and procedures. The required disclosures would cover how and whether cybersecurity risks are factored into business strategy, and how each of management and the board of directors allocate responsibility for controlling and overseeing cybersecurity risk. The proposed rules are prescriptive and contemplate governance disclosures on, among other

things, post-incident continuity and recovery plans, the frequency of board briefings on cyber risks, and strategies for managing cybersecurity risks associated with third-party service providers. The proposed rules also require discussion and assessment of how cybersecurity risk matters affect a company's financial planning and capital allocation decisions, and whether the cybersecurity policies and procedures address identification and management of reputational and operational risks arising from cyber breaches.

*Director and Management Expertise Disclosures*: The proposed rules would amend Regulation S-K to require disclosure of management's role and expertise in assessing and managing cyber risk and implementing related policies and procedures, and they would require disclosure of board members' cybersecurity expertise. The SEC has proposed a non-exclusive list of criteria for companies to consider in determining whether a director has cybersecurity expertise, including whether the director has obtained a certification or degree in cybersecurity and has knowledge in areas such as security architecture. Whether a director's technical sophistication generally or ability to engage effectively on cybersecurity-related matters would alone meet SEC expectations under the proposed rules is unclear, and that question should attract substantial commentary. After all, one need not necessarily have granular, cyber-specific technical expertise to meaningfully enhance board-level discussion of cybersecurity.

*Applicability to Foreign Private Issuers*: Foreign private issuers would also be subject to new cybersecurity disclosures for their Form 20-F and Form 6-K filings.

*No S-3 Ineligibility Risk/Extension of 10b-5 Safe Harbors*: Notably, under the proposed rules a company's failure to timely file a Form 8-K disclosure regarding a cyber incident would not result in loss of eligibility to register securities on Form S-3. And the proposed rules would extend the limited safe harbor from Section 10(b) and Rule 10b-5 liability to include untimely Form 8-K disclosures of cyber incidents.

* * *

As comprehensive federal cybersecurity legislation remains pending in Congress, and state regulators and enforcers exert greater muscle in advancing their own expectations for cybersecurity hygiene and governance, the SEC has sought to claim the regulatory high ground. While some aspects of the proposed rules will no doubt change after notice and comment before taking effect, all public companies would be wise to scrutinize their current cybersecurity-related policies and procedures to identify and address any notable gaps between existing approaches and the SEC's forthcoming standards.

John F. Savarese
Wayne M. Carlin
Sarah K. Eddy
Sabastian V. Niles
David M. Adlerstein
Jeohn Salone Favors