Updates
April 15, 2022

SEC Proposes New Cybersecurity Disclosure Rules on Incident Reporting, Risk Management, Strategy, and Governance

As cybersecurity threats to the private and public sectors increase, the government has continued its efforts to enhance cybersecurity outside of government-controlled systems. On March 9, 2022, the U.S. Securities and Exchange Commission (SEC) issued proposed rules regarding cybersecurity risk management, strategy, governance, and incident disclosure for public companies subject to the reporting requirements of the Securities Exchange Act of 1934. These rules are distinct from the February 2022 proposed rules covering registered funds and advisers and are intended to enhance and standardize public companies' disclosures.

The SEC cited long-standing concerns about the need for companies to maintain secure and reliable information systems, and also highlighted new and increased vulnerabilities and threats such as digitalization, remote work, reliance on cloud and other third-party services, digital and virtual payments, and sophisticated ransomware and malware campaigns. These factors create risk to the overall economy and create costs and consequences for businesses and investors. As a result, the SEC found that "cybersecurity is among the most critical governance-related issues for investors" and that there "may also be a positive correlation between a registrant's stock price and investments in certain cybersecurity technology." The SEC further assessed that cybersecurity-related disclosures based on its 2018 Interpretive Release did not follow consistent substantive or procedural standards and were not always distinguished from other, unrelated disclosures.

Accordingly, the SEC determined that investors would benefit from "more timely and consistent disclosures" by public companies of several categories of cybersecurity-related information: (1) material cybersecurity incidents, (2) risk management and strategy, (3) governance, and (4) cybersecurity expertise among board members. The SEC's proposed reporting requirements are discussed in greater detail below.

Material Cybersecurity Incidents

The SEC proposes to amend Form 8-K to require disclosure of "material" cybersecurity incidents within four business days. The four-day period would begin after a company determines that a cybersecurity incident was material, and not from the date of the incident itself. In that regard, the rule would require a company to make a materiality determination "as soon as reasonably practicable" after an incident was discovered. Notably, the proposed rule does not contain any provision for delaying a report to avoid impeding an internal—or external—investigation.

The definition of "materiality" serves an important role in scoping this reporting requirement. The SEC proposed the familiar definition courts apply in security cases: information is material "if there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if a disclosure would "significantly alter[] the 'total mix' of information made available" to investors. *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976); *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988). In the cybersecurity context, a materiality analysis would include quantitative and qualitative assessments of both the likelihood and potential magnitude of loss.

The SEC provided the following examples of incidents that would trigger the reporting obligation if a company found that they were material: the compromise of confidentiality, integrity, or availability of data or a network; an impact on operational technology systems; the theft, unavailability, or authorization of sensitive business information; extortion-related threats to release stolen information; and ransomware attacks.

The proposal would require a company to report, to the extent known: (1) when an incident was discovered and whether it remained ongoing; (2) a brief description of the incident; (3) whether data was taken, changed, accessed, or used for any unauthorized purpose; (4) how the incident affected the company's operations; and (5) whether the company had remediated, or was in the process of remediating, the incident. The SEC would *not* expect such disclosures—which would be public—to include specific or technical information about its response plans, its security systems, its networks, its vulnerabilities, or other information that could assist attackers or obstruct remediation efforts. The proposed rule would thus balance the SEC's assessment of what investors need to know quickly against the potential risks of detailed public disclosure.

The SEC further proposes to amend forms 10-Q and 10-K to update disclosures previously made about cybersecurity incidents, including past and potential impacts on the company, the status of remediation efforts, and forthcoming changes to the company's cybersecurity posture. The amendments would also require disclosure of any series of individually nonmaterial cybersecurity incidents that became material when taken together as a whole.

Risk Management and Strategy

A proposed amendment to Regulation S-K would require "consistent and informative" disclosure of cybersecurity risk management and strategy. In addition to requiring disclosures of a company's own cyber risk management, the new rule would include disclosures of how a company chooses and oversees third-party service providers to manage and mitigate cyber risk. The rule would further require disclosure of how a company factors into its overall business strategy and planning the cyber risks associated with its business model, such as collection and handling of sensitive data or increased reliance on technology. The rule is intended to equip investors with information sufficient to evaluate the risk to a company and how the company is working to manage those risks and their potential impact. To that end, the rule would require disclosure, as applicable, of whether (1) the company has a cybersecurity risk assessment and management program (if so, the rule would require a description); (2) the company engages third parties in connection with the program; (3) the company has policies and procedures in place to evaluate cyber risks associated with third-party service providers, and considers third-party providers' risks in selecting and overseeing those providers; (4) the company's cybersecurity programs are informed by prior cybersecurity incidents; (5) cybersecurity risk and incidents have affected or reasonably could affect the company; and (6) cybersecurity risks are considered as part of the company's business strategy, planning, and capital allocation (and how).

Governance

The SEC further proposes to amend Regulation S-K requirements to require companies to disclose how both the board and management take responsibility for cyber risk. Proposed disclosures would include details of "cybersecurity governance, including the board's oversight of cybersecurity risk." In particular, required disclosures will include (1) whether oversight of cybersecurity risks is the duty of the entire board, a committee, or specific board members; (2) processes for informing the board about cybersecurity risks and how often the board discusses those risks; and (3) whether and how the board (or committee) evaluates cyber risk as part of its overall strategy, risk management, and financial oversight.

In addition to a description of board responsibilities, the proposed rule would require "a description of management's role in assessing and managing cybersecurity risks." Companies would be required to describe management's cybersecurity expertise and its role in implementing cybersecurity measures. For example, disclosures would include (1) managers' or management committees' responsibilities for evaluating and managing cyber risk, including mitigation, and their relevant expertise; (2) whether the company has a chief information security officer (CISO) or similar role, the management chain to which that role reports, and the incumbent's relevant expertise; (3) the process by which managers responsible for cybersecurity are informed of and monitor cybersecurity efforts, including identification and remediation of cybersecurity incidents; and (4) whether and how often managers responsible for cybersecurity report to the board (or board committee) regarding cyber risk.

Expertise

Another amendment to Regulation S-K would require disclosure of directors' cybersecurity expertise. Companies would identify by name those directors with relevant expertise and would describe the nature of that expertise, which could include prior work experience, degrees or certifications, and relevant knowledge and skills. Describing a director as a cybersecurity expert in such a disclosure would not cause that director to be deemed a cybersecurity expert for other purposes; would not impose upon that director any additional duties, obligations, or liability; and would not reduce other directors' duties and obligations.

Note: The comment period for the proposed rules ends on May 9, 2022. Please seek counsel for assistance with any questions regarding the proposed rules and their effects on an individual or business, and for guidance in satisfying the reporting requirements once they go into effect.

Authors

David Aaron

Senior Counsel
DAaron@perkinscoie.com

Explore more in

Privacy & Security Investment Management

Related insights

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers

Update

Employers and Immigration Under Trump: What You Need To Know