CARLTON FIELDS

SEC Deals New Cybersecurity Disclosure Requirements to Public Companies

September 28, 2023

On July 26, 2023, the SEC adopted new cybersecurity rules, which have two top-line impacts. First, registrants must disclose material cybersecurity incidents promptly on Form 8-K. Second, registrants must disclose new information regarding cyber risk management, strategy, and governance as part of their annual disclosures. These requirements apply to public company registrants with the SEC, including insurance companies (but not investment company registrants). As to current disclosures, the rules add Item 1.05 to Form 8-K, requiring the disclosure of material cybersecurity incidents, including the nature, scope, and timing of the incident. The disclosure will be generally due four business days after the registrant determines materiality, which some registrants will think makes them disclose their hand prematurely. There is an exception to that disclosure timeframe, if the U.S. attorney general determines there is a substantial risk to national security or public safety and so notifies the SEC in writing. But such an exception will likely be difficult to obtain within the rules' four-day deadline. As a practical matter, therefore, this disclosure might necessarily be high level and based on less-than-perfect information, because the investigation of such larger cybersecurity incidents often takes weeks or months. This is particularly true for events with multiple moving parts, such as a ransomware attack with data exfiltration and an extortion demand, where the impact on personal information may not even be known within the four-day period. As to annual disclosures, the rules add Item 106 to Regulation S-K, requiring the following new disclosures in the registrant's annual report on Form 10-K:

- A description of the registrant's processes for assessing, identifying, and managing material cybersecurity risks.
- Disclosures as to the material effects of previous cybersecurity incidents.
- Disclosures as to management's role and expertise in managing cybersecurity risks and as to the board's oversight of those risks.

Registrants will need to start planning for compliance immediately, as the rules took effect on September 5. The Form 10-K disclosures start on annual reports for fiscal years ending on December 15, 2023. The Form 8-K requirements start on December 18, 2023, although smaller reporting companies have an extension to June 15, 2024. Public companies should revisit their incident response plans, to see if they would benefit from additional processes to determine when a cyber incident could be material and, if so, who will be responsible for any necessary disclosures on Form 8-K within the four-business-day timeframe. Public companies should also work with their disclosure counsel to gather information for disclosure through new Item 106 on their annual reports.

Authored By

John E. Clabby

Related Practices

Securities Litigation and Enforcement
Cybersecurity and Privacy
Life, Annuity, and Retirement Solutions

Related Industries

Life, Annuity, and Retirement Solutions
Securities & Investment Companies
Life, Annuity, and Retirement Solutions