Published on *The National Law Review* https://natlawreview.com

SEC Adopts Final Rules to Enhance Cybersecurity Disclosure [PODCAST]

Article By:

Tara N. Cho

Theodore F. Claypoole

Ting Zheng

Rajiv Radia

Sid Shenoy

On July 26, 2023, the SEC adopted new rules[1] to enhance and standardize disclosures pertaining to cybersecurity risk management, strategy, governance, and material cybersecurity incidents.

The SEC's decision to introduce these amendments follows prior interpretive guidance issued in 2011[2] and 2018[3] on the application of existing disclosure requirements to cybersecurity risks and incidents. Despite improvements in cybersecurity-related disclosures, the SEC observed inconsistency in reporting practices. The objective of the new rules is to achieve uniform, comparable, and decision-useful disclosures that empower investors to make well-informed evaluations of a company's cybersecurity posture.

Form 8-K Item 1.05 - Cybersecurity Incident Disclosure

Under this new Item of Form 8-K, public companies must disclose any cybersecurity incident they determine to be material. This disclosure must address the nature, scope, and timing of the incident, as well as its material impact or the reasonably likely material impact on the company, particularly its financial condition and results of operations. Companies must file the Form 8-K within four business days after making the determination of materiality, which determination must be made by the company without unreasonable delay. Notable changes from the proposed rule include the following:

- The SEC narrowed the amount of information companies are required to disclose, in an effort strike the right balance between investors' need for information and a company's cybersecurity posture. Moreover, the disclosure is now focused primarily on the impacts of a material cybersecurity incident, rather than on the details of the incident itself.
- A company may delay making this filing if the United States Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing.
- A company must provide certain updated incident disclosure in an amendment to its Form 8-K (instead of in subsequent Forms 10-Q and 10-K).
- A company will not be required to provide periodic report disclosure when a series of previously undisclosed immaterial cybersecurity incidents becomes material in the aggregate.

Regulation S-K Item 106 - Cybersecurity Risk Management and Strategy

Under the new rule, companies must describe their processes for assessing, identifying, and managing material risks arising from cybersecurity threats. In providing this disclosure, companies should address, as applicable:

- Whether and how such processes have been integrated into the company’s overall risk management systems or processes;
- Whether the company engages assessors, consultants, auditors or other third parties in connection with any such processes; and
- Whether the company has processes to oversee and identify risks from cybersecurity threats associated with its use of any third-party service provider.

Companies must also disclose whether any risks from cybersecurity threats, including as a result of previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, and if so, how. The new rule also requires companies to disclose the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing a company’s material risks from cybersecurity threats. Notable changes from the proposed rule include the following:

- The SEC eliminated or narrowed certain elements from the proposed rule. For example, the SEC did not adopt requirements to discuss prevention and detection activities, continuity and recovery plans and previous incidents.
- Companies will not be required to disclose cybersecurity expertise of individual board members.

Next Steps

The final rules will take effect thirty (30) days after publication in the Federal Register. Compliance deadlines for different disclosure requirements noted above are as follows:

Form 8-K Item 1.05: Companies other than smaller reporting companies must comply on the later of 90 days after publication in

the Federal Register or December 18, 2023. Smaller reporting companies must comply beginning on the later of 270 days from the effective date of the rules or June 15, 2024.

Regulation S-K Item 106: All companies must provide the required disclosures in their annual reports for fiscal years ending on or after December 15, 2023.

Companies must tag disclosures required under the final rules in Inline XBRL starting one year after initial compliance with the related disclosure requirement.

In advance of the new disclosure requirements, public companies should review and update their disclosure controls and procedures to prepare for the new incident reporting requirements, and prepare draft disclosures of their cybersecurity risk management and strategy to review and align with internal departments and external advisors.

National Law Review, Volumess XIII, Number 336