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

SEC's New Rules for Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Go into Effect

Article By:

Ralph V. De Martino

Cavas S. Pavri

Johnathan C. Duncan

Marc E. Rivera

Cody C. Boender

Jeffrey J. Kennedy

On December 18, 2023, the US Securities and Exchange Commission's (SEC) new rules enhancing and standardizing disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by companies who are subject to the Securities and Exchange Act of 1934 (including foreign private issuers) went into effect. As such, companies will want to be aware of how best to comply.

In particular, the new rules require (1) reporting of any material cybersecurity incidents and (2) annual reporting of the company's process for assessing, identifying, and managing material risks from cybersecurity threats and previous cybersecurity incidents, including the board and management's role in identifying and managing such material cybersecurity risks.

All companies, other than smaller reporting companies, must report material cybersecurity incidents on Form 8-K or Form 6-K beginning on December 18, 2023 — the effective date of the final rules. Smaller reporting companies have an additional 180 days and must comply with the reporting requirements within 270 days from the effective date, or June 15, 2024.

All companies with fiscal years ending on or after December 15, 2023, must include the cybersecurity risk management, strategy, and governance disclosures in their annual report on Form 10-K, or Form

20-F for foreign private issuers.

Cybersecurity Incident Reporting on Form 8-K

The final rules amend Form 8-K to add a new Item 1.05, which requires companies to disclose “material cybersecurity incidents” within four days after the determination that the cybersecurity incident was material. This contrasts with the originally proposed rules triggering an Item 1.05 disclosure upon discovery of the incident itself.

Required Disclosure

Upon the triggering of an Item 1.05 disclosure, the company must disclose the following:

- A detailed description of the material aspects of the nature, scope, and timing of the cybersecurity incident
- The material impact or reasonably likely material impact on the company’s operations and financial condition

Companies do not need to disclose a detailed description of technical or specific information about the company’s anticipated response to the incident or the company’s cybersecurity systems if it would impede the company’s response or remediation of the incident.

When determining if an incident qualifies as material, the SEC directs companies to engage in a materiality analysis in the same way it would for securities laws in general, considering qualitative and quantitative factors.

The SEC defines a cybersecurity incident broadly to include any unauthorized occurrence, or series of related occurrences, on or conducted through a company’s information systems that jeopardized the confidentiality, integrity, or availability of those systems or information contained within them. As a result, a series of related occurrences may be deemed material in the aggregate, even if such individual occurrences are considered immaterial.

Delaying Disclosure

In response to concerns expressed during the comment period following the release of the proposed amendments to Form 8-K, the final rule created exceptions in the interest of national security or public safety. There is now a delay provision baked into Item 1.05 that allows for a delay of disclosure up to 30 days if the US Attorney General determines delay is necessary to prevent a substantial risk to national security or public safety. This delay can be extended for another 30 days if determined necessary by the Attorney General and, in extraordinary circumstances, a final additional period of up to 60 days. The SEC has established a process of communication between the Attorney General, the SEC, and the company seeking the delay.

While Item 1.05 doesn’t give instructions on how to seek the delay from the Attorney General, the Federal Bureau of Investigation (FBI) has recently given companies some guidance. Detailed in the official guidance, companies should provide the FBI with a written notice of its delay. Among other things, the notice must contain detailed information about the company’s mitigation or remediation efforts, its points of contact, and any information gathered about the culprits of the incident.

Amending Disclosure

Where information required to be disclosed under Item 1.05 of Form 8-K either was not determined or was not yet available at the time of the filing, the company must state that such information is missing in the initial filing and file an amendment within four business days of the determination or availability of the information.

Risk Management Disclosure on Form 10-K

The final rules adopted by the SEC also amend Form 10-K to add a new Item 1C and Regulation S-K to add a new Item 106. Together, these new disclosure requirements require companies to report their internal processes for identifying, assessing, and managing material risks from cybersecurity threats, including but not limited to:

1. the board's oversight of such risks;
2. management's role in assessing and managing such risks;
3. the persons responsible for assessing and managing such risks and their relevant expertise;
4. the process by which such persons are informed about and monitor the prevention of cybersecurity incidents; and
5. whether such risks are reported to the board or board committees.

Foreign Private Issuers

The new rules pertaining to cybersecurity incidents also apply to foreign private issuers and amend Form 6-K to require disclosure of cybersecurity incidents if the issuer discloses or is required to disclose such incidents in accordance with the law of the jurisdiction in which it is organized. Additionally, foreign private issuers are required, under the amended Form 20-F, to disclose their risk management processes.

Clayton Spivey contributed to this article.

National Law Review, Volume XIII, Number 354