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

More Disclosures Required for Public Companies with the SEC's New Cybersecurity Rules

Article By:

David J. Lavan

Marisa E. Bens

The SEC has adopted final rules requiring public companies subject to the reporting requirements of the Securities Exchange Act of 1934, to disclose material cybersecurity incidents and material information regarding their cybersecurity risk management, strategy and governance. In adopting the rules, the SEC intends to benefit investors, companies and the markets by requiring more consistent and comparable disclosures across registrants on cybersecurity incidents and risk management.

Effective Date

The final rules will become effective 30 days following publication of the adopting release in the Federal Register. The specific compliance dates for each disclosure are as follows:

	Compliance Dates
Form 10-K; Form 20-F *(Item 106 of Regulation S-K; Item 16K)*	Beginning with annual reports for fiscal years ending on or after December 15, 2023
Form 8-K; Form 6-K *(Item 1.05)*	Smaller reporting companies: • 270 days after the date of publication in the Federal Registrar or June 15, 2024, whichever is later All other registrants: • 90 days after the date of publication in the Federal Registrar or December 18, 2023, whichever is later
Inline XBRL	All registrants must begin tagging responsive disclosures in Inline XBRL 1 year after initial compliance: • For 10-K/20-F: annual reports of fiscal years ending on or after December 15, 2024 • For 8-K/6-K: 465 days after the date of publication in the Federal Registrar or December 18, 2024, whichever is later

Overview of Final Rules

Form 8-K Item 1.05

Under the new Form 8-K Item 1.05, issuers must disclose that a material cybersecurity incident has occurred within four days of making such determination. The disclosure must include:

1. the material aspects of the nature, scope and timing of the incident; and

2. the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations.

The issuer must make the materiality determination “without unreasonable delay” once the incident has been discovered. Materiality under this disclosure applies the same definition from standard securities law. Information is material if there is a substantial likelihood that a reasonable investor would consider the information important when making an investment decision.

In situations where the U.S. Attorney General determines that immediate disclosure, in accordance with the new final rule, would pose a substantial risk to national security or public safety, the Form 8-K may be delayed for 30 days, and potentially up to 120 days, if the risk is considered ongoing. The U.S. Attorney General will notify the SEC of the national-security exemption for the issuer.

Further, issuers must update the Form 8-K with an amendment if required information that was unavailable at filing later comes to light. An amendment must be made within four business days of the registrant, without unreasonable delay, determining such information, or within four business days

of the new information becoming available.

Annual Report on Form 10-K

On top of cybersecurity incident disclosures, issuers also must now include information regarding their cybersecurity risk management, strategy and governance within their Annual Reports on Form 10-K. These disclosures must detail:

1. the issuer's specific processes for assessment, identification and management of material risks from cybersecurity threats;

2. whether any risks from cybersecurity threats have materially affected, or are reasonably likely to materially affect, the issuer's business strategy, results of operations or financial conditions;

3. the board of director's oversight of risks from cybersecurity threats, including whether any specific board committee or subcommittee is tasked with oversight of this specific concern; and

4. management's role and expertise in assessing and managing material risks from cybersecurity threats, including which management positions are responsible for assessment of cybersecurity risks, the processes by which such persons or committees are informed about, and monitor, the prevention, detection, mitigation and remediation of incidents, and if such persons or committees report about such risks to the board of directors, a board committee and/or a board subcommittee.

Foreign Private Issuers

The final rule includes parallel requirements for foreign private issuers when filing Forms 6-K and 20-F.

Next Steps

In response to the new final rules from the SEC, issuers should carefully scrutinize their current cybersecurity policies and procedures, among other steps, including:

1. Educating the board of directors and management of the new rules and the importance of their oversight in dealing with cybersecurity incidents and risks;

2. Identifying gaps in current policies and procedures and taking steps to address them;

3. Ensuring adequate incident reporting, evaluation procedures and mitigation practices exist to determine when an incident occurs and whether it is material such that it must be timely disclosed; and

4. Developing cybersecurity expertise among management and other key departments of the issuer.

National Law Review, Volumess XIII, Number 216