

SEC Adopts Cybersecurity Disclosure Rules for Public Companies

On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted new disclosure rules relating to cybersecurity matters for public companies.

The new disclosure requirements include the following:

- A new trigger for Form 8-K filings. Under new Item 1.05 of Form 8-K, if there is any cybersecurity incident that a registrant experiences that is determined to be material, a Form 8-K must be filed describing the material aspects of: (1) the nature, scope and timing of the incident; and (2) impact or reasonably likely impact of the incident. Registrants must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file an Item 1.05 Form 8-K generally within four business days of such determination.
- A registrant must describe, in its annual report on Form 10-K pursuant to new Item 106 of Regulation S-K, its processes, if any, for the assessment, identification and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect its business strategy, results of operations or financial condition.
- Item 106 of Regulation S-K will also require Form 10-K disclosure of the board's oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats.

There is a provision to delay Form 8-K disclosure of a material cybersecurity incident if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. If the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief through possible exemptive orders. Although the promulgating release discusses procedures for the SEC to coordinate with the U.S. Department of Justice for such delays, it seems likely that most cybersecurity incidents will not qualify for a national security or public safety standard.

The final rules will be effective 30 days following publication of the adopting

POSTED:

Jul 31, 2023

RELATED PRACTICES:

[Corporate Law](#)

<https://www.reinhartlaw.com/practices/corporate-law>

RELATED SERVICES:

[Securities](#)

<https://www.reinhartlaw.com/services/securities>

[Data Privacy and Cybersecurity](#)

<https://www.reinhartlaw.com/services/data-privacy-and-cybersecurity>

RELATED PEOPLE:

[Benjamin G. Lombard](#)

<https://www.reinhartlaw.com/people/benjamin-lombard>



release in the Federal Register. With respect to the periodic disclosures required by Item 106 of Regulation S-K, all registrants must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. With respect to compliance with the current disclosure requirements for material cybersecurity incidents required by Item 1.05 of Form 8-K, all registrants (other than smaller reporting companies) must begin complying 90 days after publication of the adopting release in the Federal Register or December 18, 2023, whichever is later. Smaller reporting companies have an additional 180 days from the non-smaller reporting company compliance date, so those registrants must begin complying with Item 1.05 of Form 8-K 270 days after publication of the adopting release in the Federal Register or June 15, 2024, whichever is later.

In order to prepare for the rules, a public company should review its disclosure controls and procedures and cybersecurity response plan to ensure that appropriate personnel are aware of the 8-K filing requirement and the need to make a determination as to materiality without unreasonable delay. Public companies should also review their cybersecurity processes and procedures with a view to the new requirements for public disclosure.

If you have any questions about the amended rules, changes to your policies and procedures or other securities law matters, please contact [Benjamin Lombard](#), another member of the Reinhart Securities Team or your Reinhart attorney.

These materials provide general information which does not constitute legal or tax advice and should not be relied upon as such. Particular facts or future developments in the law may affect the topic(s) addressed within these materials. Always consult with a lawyer about your particular circumstances before acting on any information presented in these materials because it may not be applicable to you or your situation. Providing these materials to you does not create an attorney/client relationship. You should not provide confidential information to us until Reinhart agrees to represent you.