Westlaw Today
powered by Reuters

Five key takeaways from the SEC's final cybersecurity rules for public companies

By Evan D. Wolff, Esq., Matthew B. Welling, Esq., Jennie Wang VonCannon, Esq., and Anand Sithian, Esq., Crowell & Moring LLP*

AUGUST 7, 2023

On July 26, 2023, the SEC finalized long-awaited disclosure rules[1] (the "Final Rules") regarding cybersecurity risk management, strategy, governance, and incidents by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. While the end results are substantially similar to rules proposed by the SEC in March 2022,[2] there are some key distinctions.

The top five takeaways are:

1. Disclosure of cybersecurity incidents within 4 days of materiality determination. Public companies must now disclose in their Form 8-K Item 1.05 filings "any cybersecurity incident that they experience that is determined to be material" and describe "material aspects" of the reported incident, including a description of its nature, scope, timing, and impact on the company, within four business days of determining a cybersecurity incident is material.

Public companies would be well advised to consider retaining outside experts, including cybersecurity counsel, to help train directors in cybersecurity matters.

Recognizing that a materiality determination necessitates an informed and deliberate process, the Final Rules do, however, impose that such a determination needs to be done "without unreasonable delay." Such materiality analysis should be "consistent with the standard set out in the cases addressing materiality in the securities laws, that information is material if 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision, or if it would have 'significantly altered the 'total mix' of information made available.'"[3]

Per the SEC, "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance."[4] Thus, public company officers and directors should assess existing disclosure controls and procedures to ensure information about cybersecurity incidents are properly escalated, as appropriate, to management, the board, and any board committees with oversight of cybersecurity, and to ensure they are capturing what the Final Rules require.

Companies should ensure they have appropriate internal and outside experts and advisors to assist in making a materiality determination regarding a particular cybersecurity incident.

2. Board expertise requirement removed. Following substantial comments, the SEC declined to adopt in the Final Rules a proposed requirement for disclosure of cybersecurity expertise, if any, for a company's board of directors.[5] Among the comments opposing this proposed requirement were those noting a shortage of cybersecurity expertise in the marketplace, which would make this requirement difficult to fulfill.[6]

However, pursuant to Regulation S-K Item 106(b), public companies must now describe annually in their Form 10-K the board's oversight of risks arising from cybersecurity threats, as well as management's role in assessing and managing such material risks.[7]

Accordingly, public companies would be well advised to consider retaining outside experts, including cybersecurity counsel, to help train directors in cybersecurity matters, including on incident response, with periodic refresher trainings, to ensure appropriate oversight of cybersecurity risks and developments.

And while the SEC did not adopt the board expertise disclosure requirement, the Final Rules now require disclosure of the cybersecurity expertise for those members of management responsible for assessing and managing cybersecurity risks.[8]

3. Companies must disclose "processes," but no requirement to disclose cybersecurity procedures. Pursuant to Item 106(b) of Regulation S-K, public companies must now describe annually in their Form 10-K their processes, if any, for "assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes" and must also describe if the risks "have materially affected or are reasonably likely to materially affect" the company, "including its business strategy, results of operations, or financial condition and if so, how."[9]

The SEC declined to adopt a requirement in the Proposed Rules mandating the disclosure of cybersecurity "policies and procedures," thereby avoiding potential public disclosure of information that threat actors could then leverage to attack companies' cybersecurity defenses.

On this point, SEC Commissioner Hester Peirce voiced concern[10] that compliance with the Final Rules could increase the future risk of cyberattacks on companies. Commissioner Peirce pointed out that the "strategy and governance disclosures risk handing [cyber criminals] a roadmap on which companies to target and how to attack them."

The Final Rules provide a national security exception to the timing of a Form 8-K disclosure of a material cybersecurity incident.

She argued that compliance with the Final Rules could do more harm than good because maintaining compliance with the Final Rules, while at the same time describing cyberattacks without revealing incident response procedures, security controls, or being too descriptive about a company's network architecture, may be a difficult balance to maintain.

4. National security delay exception carries the day. The Final Rules provide a national security exception to the timing of a Form 8-K disclosure of a material cybersecurity incident.

Specifically, if the U.S. Attorney General determines that such a disclosure "poses a substantial risk to national security or public safety," companies may delay providing the Form 8-K disclosure until such period determined by the Attorney General, up to 30 days, which can be extended for additional 30 days if the Attorney General determines that disclosure would pose continuing risk.[11]

This disclosure can be further delayed by the Attorney General in "extraordinary circumstances." This national security delay exception appears to be in response to comments about how a delayed disclosure when there is an ongoing law enforcement investigation may not only facilitate the investigation but may be key to its success.[12]

5. Private companies. Although the SEC's Final Rules apply only to companies with securities registered with the SEC, the concepts captured by the Final Rules may be helpful for all companies, particularly when it comes to board oversight, management's cybersecurity expertise, a company's understanding of cybersecurity risks, and incident response. Moreover, as private companies consider strategic exits, including potential public offerings, the SEC's Final Rules may be considered as part of IPO readiness.

Effective dates

With certain exceptions, the Final Rules will become effective 30 days after the date of publication in the Federal Register. For companies that file their Form 10-K or Form 20-F annual reports on or after December 15, 2023, those filings must comply with Final Rules.

For registrants other than smaller reporting companies, Form 8-K disclosures (in which material cybersecurity incident-based reporting must be made) and Form 6-K disclosures (for foreign private issuers who disclose material cyberse curity incidents in a foreign jurisdiction, to any stock exchange, or to security holders) will be required beginning December 18, 2023 or 90 days after the date of publication of the Final Rules in the Federal Register, whichever is later. Smaller reporting companies will have an extra 180 days to comply.

Conclusion

The SEC's publication of these cybersecurity rules is yet another data point demonstrating that the U.S. government's focus on cybersecurity regulation and enforcement is trending toward increased accountability, with an increasingly "stick"-like approach.

Public companies, officers, directors, and chief information security officers would need to assess existing cybersecurity and disclosure controls and procedures, and work with cybersecurity and disclosure counsel to prepare for this new reporting and disclosure regime.

Notes

[1] https://bit.ly/3Qqq4oS

[2] https://bit.ly/3qkLtVR

[3] *See* Final Rules at 80.

[4] *See* Final Rules at 38.

[5] *See* Final Rule at 81.

[6] Final Rules at 83.

[7] *See* Final Rule at 171.

[8] *Id*.

[9] *See* Final Rules at 170–71.

[10] https://bit.ly/449KeH7

[11] *See* Final Rules at 184.

[12] *See* Final Rules at 22-23.

About the authors




(L-R) **Evan D. Wolff** is a partner at **Crowell & Moring LLP**, co-chair of the firm's privacy and cybersecurity group, and a member of the government contracts group. He is based in Washington, D.C., and can be reached at ewolff@crowell.com. **Matthew B. Welling** is also a partner in the firm's Washington, D.C., office, where he practices in the privacy and cybersecurity and energy groups. He can be reached at mwelling@crowell.com. **Jennie Wang VonCannon** is a partner in the firm's Los Angeles office, where she is a member of the white collar and regulatory enforcement and privacy and cybersecurity groups. She can be reached at jvoncannon@crowell.com. **Anand Sithian**, a counsel in the firm's New York office, is a member of the international trade and white collar and regulatory enforcement groups. He can be reached at asithian@crowell.com. The authors would like to thank partners William J. Bruno and Daniel Zelenko and senior counsel Alexander Urbelis and Christiana State for their contributions to this article. This article was originally published July 28, 2023, on the firm's website. Republished with permission.

This article was published on Westlaw Today on August 7, 2023.