HIGHLIGHTS FROM THE SEC'S FINAL RULES ON CYBERSECURITY DISCLOSURE

JULY 2023

GLOBAL RISK INSTITUTE

The U.S. Securities and Exchange Commission's (SEC) final rules[1] on cybersecurity disclosure, released on July 26 2023, provide updated requirements on material incidents disclosure, enhanced annual reporting and governance guidance for public companies. In the final rules, the SEC has aimed to streamline disclosure elements and narrow the scope of disclosure, while also varying the effective dates for the new rules.

1. SUMMARY

The SEC newly approved final rules require registered companies (including foreign companies doing business in the U.S.) to disclose material cybersecurity incidents within four business days from the materiality determination. Additionally, registered companies are required to share details of their cybersecurity risk management, strategy, and governance with the commission on an annual basis. The final rules will take effect 30 days after publication of the adopting rules in the Federal Register, with compliance dates for specific reporting ranging from 90 to 270 days.[2] Foreign private issuers must comply with disclosure requirements similar to domestic issuers and must also furnish information about material cybersecurity incidents disclosed in foreign jurisdictions.

2. HIGHLIGHTS

2.1 Material Incident Reporting

Under the new rules, companies are required to provide the SEC with relevant details of a given material incident's "nature, scope and timing" and offer information on how they believe the event will impact them, including financial condition and results of operations, within four business days of the company deciding the incident is material.

The notification trigger is the determination of the incident materiality, not the incident occurrence. However, the final rules provide for a delay in disclosure for 30 to 60 days if the Attorney General of the United States determines that disclosure "poses a substantial risk to national security or public safety" and notifies the SEC of such determination in writing.

Main changes from the proposed rules

The final rules narrow the scope of disclosure "to better balance investors' needs and registrants' cybersecurity posture".[3] The new rule focuses on the impact or reasonably likely impact of the incident, rather than on the details of the incident itself, such as remediation status.

1 https://www.sec.gov/news/press-release/2023-139

2 https://www.sec.gov/files/rules/final/2023/33-11216.pdf p. 107

3 https://www.sec.gov/files/rules/final/2023/33-11216.pdf p. 28

The new rule adds "a limited delay" for disclosures that would pose significant risks to national security or public safety, and has eliminated the disclosure requirement from the proposed rules on remediation status, whether it is ongoing and whether data were compromised, and further clarifies the type of disclosure required.

The SEC also dropped proposed Item 106(d)(1) that would have provided additional details on material impacts, potential future impacts and remediation following an Item 105 disclosure, in favour of a new instruction in the final rule noting that updated incident disclosure should be provided in a Form 8-K amendment (instead of Form 10-Q and 10-K).

2.2 Risk Management and Strategy

The final rules add a new Item 106(b) to Regulation S-K on risk management and strategy, requiring registrants to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents.

Main changes from the proposed rules

In the final rules, the Item 106 disclosure must describe whether risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition, thus reducing the scope of the initially proposed version by referring to "material" effects only.

The final rules also adopt the term "processes" to avoid disclosing operational details that could be exploited by threat actors and to comprehensively assess registrants' cybersecurity practices, regardless of whether they have written policies and procedures.

2.3 Board of Director and Management Oversight

Regulation S-K Item 106(c) imposes disclosure requirements regarding boards of directors. It requires registrants to describe the board's oversight of risks from cybersecurity threats, as well as to describe management's role in assessing and managing material risks from cybersecurity threats, to be provided in the annual report on Form 10-K.

The final rule 106(c)(1) and (2) mandates a description of the board's oversight and management's role in assessing and managing risks from cybersecurity threats. Board oversight includes identifying any committee responsible for cybersecurity oversight and explaining the processes for informing such committee. The description of management's role may include disclosing responsible positions, expertise, and processes for managing cybersecurity incidents, as well as reporting such information to the board or its committees. Additionally, disclosure on consultants and third parties related to such processes is also required.

Main changes from the proposed rules

The final rules on board oversight are less granular than the proposed rule and, most significantly, no longer require companies to disclose detailed information on the cybersecurity expertise of members of the board of directors, which is now on management.

The final rules have also been simplified compared to the proposed rules, removing disclosure on whether and how the board integrates cybersecurity into its business strategy, risk management, and financial oversight as well as removing a requirement to report on the frequency of the board or committee's discussions on cybersecurity.

2.4 Compliance Dates

The final rules will become effective 30 days following publication of the adopting release in the Federal Register.

Regarding Regulation S-K Item 106 and the comparable requirements in Form 20-F, all registrants must include these disclosures in their annual reports beginning with fiscal years ending on or after December 15, 2023.

For compliance with the incident disclosure requirements in Item 1.05 of Form 8-K and Form 6-K, registrants other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the Federal Register or December 18, 2023.

Smaller reporting companies will have an additional 180 days from the non-smaller reporting company compliance date to start complying with Item 1.05 of Form 8-K, on the later of 270 days from the effective date of the rules or June 15, 2024.

2.5 Foreign Private Issuers

Foreign private issuers will be required to furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction to any stock exchange or to security holders. They will also be required in Form 20-F to describe the board's oversight of risks from cybersecurity threats and describe management's role in assessing and managing material risks from cybersecurity threats.

3. LOOKING AHEAD

In anticipation of publication in the Federal Register, it is to be expected that affected companies will be checking disclosure controls and procedures to ensure they contemplate cybersecurity incidents and to determine whether to mandate a specific board committee with oversight of cybersecurity matters. A review of management processes to monitor cybersecurity risk and reporting may also be in order, as well as a review of any risk tied to third-party partners.