BDO BULLETIN

THE SEC'S NEW CYBERSECURITY DISCLOSURE RULES ARE HERE

AUGUST 2023

SUMMARY

The SEC voted 3:2 to adopt new rules that require registrants to disclose material cybersecurity incidents in Form 8-K and make annual disclosures regarding their policies and procedures to identify and manage cybersecurity risk, the board's oversight of risks from cybersecurity threats, and management's role in assessing and managing material risks from cybersecurity threats. The timeline until effectiveness is short. Most registrants will be required to make the new annual disclosures in their 2023 reports on Form 10-K (or Form 20-F) and to report material cybersecurity incidents in Form 8-K as early as December 18, 2023.

CYBERSECURITY INCIDENT DISCLOSURES IN FORM 8-K

New Item 1.05 of Form 8-K requires registrants to disclose cybersecurity incidents within four business days from the date they determine the incident(s) to be material. A delay in the four-business day requirement is permitted only in circumstances when the U.S. Attorney General notifies the SEC in writing that such disclosure poses a substantial risk to national security or public safety.[1] While the date of the materiality determination may be the same date or after the date of the incident's discovery, registrants must make their materiality determinations without "unreasonable delay." Foreign private issuers (FPIs) are required to make similar disclosures on Form 6-K.

The materiality evaluation of a cybersecurity incident is consistent with the evaluation of any other event or risk that a registrant may face. Accordingly, an incident is material if "*there is substantial likelihood that a reasonable shareholder would consider it important*" or if it would have "*substantially altered the 'total mix' of information made available from the perspective of a reasonable investor*." Considerable judgment may be required in the materiality determination; registrants must consider all relevant facts and circumstances, including both quantitative and qualitative factors.

When disclosure is triggered under Item 1.05, the registrant must disclose the material:

- Aspects of the scope, nature, and timing of the cybersecurity incident[2]
- Impact or reasonably likely material impact on the registrant's financial condition and results of operations

If the information required to make these disclosures is not available or determined at the time of filing, the registrant is required to include a statement to that effect and file an amendment to Form 8-K within four business days after the information becomes available. Unlike in the proposed rules, registrants are not required to continually provide updated information about the incident in Form 8-K or their periodic reports in Forms 10-Q and 10-K. However,

[1] The initial delay period of up to 30 days may be extended by the U.S. Attorney General up to a total of 90 days after which the SEC will consider additional requests for delay and potential relief through exemptive order.

[2] Specific or technical information about the registrant's cybersecurity system, planned response to the incident, or potential system vulnerabilities is not required.

registrants have a duty to update any disclosure that becomes materiality inaccurate (or omitted a material fact necessary to make the disclosure not misleading).

Disclosures made in Item 1.05 are eligible for the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act.

RISK MANAGEMENT, STRATEGY, AND GOVERNANCE DISCLOSURES

Item 106 of Regulation S-K and Item 16K of Form 20-F require registrants to disclose information about their cybersecurity risk management, strategy, and governance in sufficient detail for a reasonable investor to understand. While such disclosures are required in Forms 10-K and 20-F, registrants should consider the materiality of cybersecurity risks and incidents when preparing disclosures in connection with registration statements.

Risk Management and Strategy

Item 106(b) requires registrants to describe:

- Their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats
- Whether any risks from cybersecurity threats have materially affected (or are reasonably likely to materially affect) their business strategy, results of operations, or financial conditions

In providing these disclosures, registrants are required to address, at a minimum, the following:

- Whether and how cybersecurity processes have been integrated into the registrant's overall risk management process
- Whether the registrant engages third parties in connection with such processes
- Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with third-party service providers
- Any other information necessary for a reasonable investor to understand their cybersecurity processes

Governance

Item 106(c) requires registrants to describe:

- The board's oversight of risks from cybersecurity threats and if applicable, any board committee or subcommittee responsible for the oversight of these risks and the related processes by which such committee is informed about the risks
- Management's role in assessing and managing material risks from cybersecurity threats

In providing these disclosures, registrants are required to address, at a minimum, the following:

- Which management positions or committees are responsible for assessing and managing cybersecurity risks
- The relevant expertise of members of management responsible for assessing and managing cybersecurity risks
- How members of management or committees are informed about and monitor cybersecurity incidents
- How such information is reported to the board of directors or board committee

The proposed rules would have required disclosure about the cybersecurity expertise, if any, of members of the registrant's board of directors. The SEC dropped the proposed requirement because it concluded that effective cybersecurity processes are designed and administered largely by management.

DEFINITIONS IN ITEM 106 OF REGULATION S-K

The new requirements include the following definitions:

Cybersecurity Incident: an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Cybersecurity Threat: any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Information System: electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

BDO INSIGHTS: ROBUST PROCESSES AND CONTROLS WILL BE NEEDED TO ADDRESS THESE REQUIREMENTS

The definition of a cybersecurity incident in the proposed rule was revised to include "a series of related unauthorized occurrences" to reflect that cyberattacks sometimes compound over time, rather than at a point in time. The SEC gave the following examples:

- The same malicious actor engages in small but continuous cyberattacks against the registrant
- A series of related attacks from multiple actors attack the same vulnerability

Evaluating whether a series of related unauthorized occurrences are collectively material to the registrant may require the application of professional judgment, based on the facts and circumstances.

The definition of an information system includes resources "used by" the registrant. Accordingly, cybersecurity incidents that occur on third-party systems used by the registrant are required to be considered for reporting.

Registrants will need robust processes and controls so that such events are properly considered for disclosure.

SCOPE AND ADOPTION TIMELINE

The amendments are applicable to virtually all registrants, except for asset-backed issuers who are exempt from these new disclosure requirements.

The cybersecurity incident disclosures are required in Form 8-K (Form 6-K for FPIs) beginning the later of 90 days after publication in the Federal Register or December 18, 2023. Smaller Reporting Companies (SRCs) have an additional 180 days to comply with the Form 8-K requirements (that is, the later of 270 days after publication in the Federal Register or June 15, 2024).

The new risk, strategy, and governance disclosures in Forms 10-K and 20-F are required for registrants beginning with fiscal years ending on or after December 15, 2023. There is no delay for SRCs for these requirements.

Link to **Final Rule**

Link to **Fact Sheet**