SEC Approves Public Company Cybersecurity Disclosure Requirements

By Susan Lindberg and Jeff Haughey
July 28, 2023

On July 26, 2023, the Securities and Exchange Commission (SEC) voted to approve its final rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. The rule, proposed in March 2022, includes requirements about current disclosure of material cybersecurity incidents, and periodic disclosures about a registrant's processes to assess, identify, and manage material cybersecurity risks; managements role in assessing and managing material cybersecurity risks; and the board of directors' oversight of cybersecurity risks.

Who must comply with the rule?

Public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. There are no limits on the scope of disclosures for smaller reporting companies (SRCs) or emerging growth companies.

When is compliance required?

For disclosures of material incidents (Item 1.05 of Form 8-K and Form 6-K), compliance is required beginning on the later of December 18, 2023, or 90 days after the date the rule is published in the Federal Register. For SRCs, this date is the later of June 15, 2024 or 270 days after Federal Register publication.

For disclosures required in annual reports (Item 106 of Regulation S-K), the first such disclosure is required beginning with annual reports for fiscal years ending on or after December 15, 2023.

Beginning one year after the initial compliance date, registrants must tag the required disclosures in Inline XBRL.

What does the rule require?

- Reporting of cybersecurity incidents on an **Item 1.05 Form 8-K** within four business days of a determination that the incident is material.
    - materiality determination must be made "without unreasonable delay" rather than "as soon as reasonably practicable," as proposed;
    - disclosure must include material aspects of (i) the incident's nature, scope and timing, and (ii) impact or reasonably likely impact;
    - if any required information is not available at the time of filing, the Form 8-K must be amended to provide such previously undetermined or unavailable information;
    - the untimely filing of an Item 1.05 Form 8-K will not cause the loss of Form S-3 eligibility; and

- Item 1.05 is eligible for the liability safe harbor under Section 10(b) and Rule 10b-5 under the Exchange Act.

- Information to be reported annually on **Form 10-K**:

  - registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats;
  - whether any risks from such threats have materially affected or are reasonably likely to materially affect the company's business strategy, results of operations, or financial condition; and
  - describe the board of directors' oversight of risks from cybersecurity threats, and identify any board committee or subcommittee responsible for overseeing cybersecurity risks, if any, and describe the process by which the board or relevant committee is informed about such risks.

- Foreign private issuers must make comparable disclosures on **Form 6-K** for material incidents and on **Form 20-F** for cybersecurity risk management.

Are any exceptions available?

The final rules were revised to provide that current disclosure of material incidents may be delayed if the U.S. Attorney General determines that timely disclosure would pose a substantial risk to national security or public safety, and so notifies the SEC in writing. The delay period may be extended for an additional 30 days – and, in extraordinary circumstances, for a further 60 days -- if the AG determines the substantial risk has continued and so notifies the SEC in writing. In addition, disclosure may be delayed up to seven business days following notification of the Secret Service and FBI pursuant to an FCC notification rule for breaches of customer proprietary network information with notice to the SEC.

What are the key definitions in the rule?

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 systems: 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.

Materiality: the Commission declined to create a special definition of materiality for cyber incidents. It is clear from the Commission's discussion that "materiality" is to be construed as it normally is in the context of the SEC's regulations. The Commission reiterated 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. In determining whether an incident is material, the Commission expects the registrant to consider all relevant circumstances, which may include both quantitative and qualitative factors.

What changed from the originally proposed rule?

Many commenters pointed to the possibility that too much disclosure could erode companies' ability to protect against future cyber attacks and also the administrative burden of excessive disclosure. In response to comments, the Commission modified (and substantially streamlined) its original proposal. The modifications in the final rule include:

- More general information, and a shorter list of required information, required for in the Form 8-K disclosures than initially proposed. This means public companies will not be required to disclose the incident's remediation status or whether data has been compromised, among other things.

- Addition of the ability to request an extension of time to protect national security.

- Material new information on the incident will need to be disclosed in an amendment to the Form 8-K originally disclosing the incident rather than in a periodic report, such as a 10-Q or 10-K.

- The following proposed disclosures were omitted from the final rules:

    - The requirement to disclose the frequency of board discussions of cybersecurity matters or the cybersecurity qualifications of individual board members. The Commission acknowledged that "directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise," and that a registrant would likely disclose any specific board-level expertise that it deems necessary to cyber risk management.
    - Whether data was stolen and the status of any remediation.
    - "Specific or technical information" regarding the cybersecurity system or its potential weaknesses.
    - Information regarding a series of individually immaterial incidents that become material in the aggregate.

- Inclusion of a materiality qualifier for the information required to be provided in the 10-K and 20-F. The Commission confirmed that the purpose of the disclosures is to inform investors, not to provide an advantage to threat actors or to influence decisions on cybersecurity risk.

Is the Commission's previous guidance on cyber disclosures still relevant?

The Commission has issued guidance to registrants in the past, including its 2018 Commission Statement and Guidance on Public Company Cybersecurity Disclosures. In the rule, the Commission specifically stated that the final rules supplement and do not replace the Commission's prior guidance.

What should registrants do to prepare?

- Review internal policies and processes regarding disclosure, cybersecurity investigations, and cyber incident response to ensure that information on cyber attacks is appropriately communicated within the organization so the process of determining the materiality of an incident can be made without unreasonable delay as part of the company's disclosure controls and procedures.

- Review cyber expertise within the company and its other providers of such services.

- Consider the company's past discussion of cybersecurity in Form 10-K and determine what, if any, modifications will need to be made in the next annual report to comply with the rule.

Commission support for the rule:

The Commission's vote was split 3-2, with Commissioners Peirce and Uyeda voting against the final rule. Both dissenting Commissioners pointed out that public companies face a wide variety of risks besides cybersecurity that could become material. They expressed concern about regulatory overreach of a specific rule for cybersecurity, and about the cost versus benefit of compliance. They voiced skepticism of the rule's consistency with the SEC's Congressional mandate. See at Commissioner Peirce's written statement.

Chairman Gensler cited statutory support, including the Sarbanes-Oxley Act, for the Commission's action.

For questions regarding the SEC's new Cybersecurity Disclosure Requirements, please contact your GableGotwals attorney or a member of our Corporate & Securities Group or Cybersecurity and Data Privacy Group.

Susan Lindberg
918-595-4826
slindberg@gablelaw.com

Jeffrey T. Haughey
918-595-4837
jhaughey@gablelaw.com