WINSTON & STRAWN LLP

BLOG

SEC Proposes New Rules Requiring Cybersecurity Disclosures

MAY 23, 2022

The SEC has proposed new rules that would require companies to make significant disclosures relating to cybersecurity incidents and preparedness. Specifically, the new rules would require a company to disclose: (i) material cybersecurity incidents; (ii) information about the company's cybersecurity risk management, strategy, and governance; and (iii) whether any member of the company's board of directors has cybersecurity expertise. Although companies are already disclosing some of this information pursuant to SEC guidance published in 2011 and 2018, the SEC believes that cybersecurity incidents are still underreported and untimely. Moreover, even when cybersecurity incidents are disclosed, the SEC has determined that the content of the disclosures varies greatly. The SEC intends for the new rules to provide investors and other market participants with timely, informative, and consistent disclosure about cybersecurity incidents, cybersecurity risk management and governance practices, and cybersecurity expertise.

1. Mandatory Disclosure of Material Cybersecurity Incidents, and Ongoing Disclosure of Past Cybersecurity Incidents

- The SEC proposes to add a new Item 1.05 to Form 8-K (current reports), requiring public companies to disclose certain information within four business days after the company determines that a material cybersecurity event has occurred. Note that this is not four days after the event occurs, but four days after the company makes an affirmative determination that the incident is material. The proposed rules do not include a firm threshold (e.g. number of users affected). However, the SEC indicated that the definition should be "construed broadly" and can include accidental exposures.
- The SEC proposes amending Forms 10-Q (quarterly reports) and 10-K (annual reports) to require public companies to update disclosures relating to material cybersecurity incidents disclosed in the past and to disclose when a series of separately immaterial cybersecurity incidents are material in the aggregate. This would include any "material changes, additions, or updates to information" that was disclosed pursuant to Item 1.05 of Form 8-K. This may include current or future material impacts on the company's operations and financial condition, whether the incident has been remediated or is still being remediated, and any changes to policies or procedures because of the cybersecurity incident. This also includes mandatory disclosure for individual, immaterial cybersecurity incidents if they become material when taken together.

Determinations of materiality should be made "as soon as reasonably practicable after discovery of the incident," but the proposal does not indicate penalties or metrics by which this could be judged. Untimely filing of material cybersecurity incidents on Form 8-K would be covered under Safe Harbor provisions and would not result in loss of Form S-3 or Form F-3 eligibility.

"Materiality" will be determined in accordance with existing SEC principles. That is, information is material if "there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered." The SEC proposes to define a "cybersecurity incident" as "an unauthorized occurrence 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." The definition of "material" does not change from its existing definition in 17 C.F.R. § 230.405, i.e., "matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered."

Notably, the disclosure requirement does not provide for a delay when there is an ongoing internal or external investigation into the incident. The SEC expressly notes that this may impact cybersecurity investigations by law enforcement, but affirmatively concludes that the four-day reporting requirement supersedes such considerations in favor of "well-functioning, orderly, and efficient markets."

2. Disclosure of Risk Management, Strategy, and Governance Regarding Cybersecurity Risks

- The SEC proposes adding a new Item 106 to Form 10-K (annual reports) to require disclosures regarding:
  - Policies and procedures for identifying and managing cybersecurity risks;
  - Cybersecurity governance, including board of directors' oversight role; and
  - Management's role and relevant expertise in assessing and managing cybersecurity-related risks and implementing related policies, procedures, and strategies.

The SEC's proposed rules also seek to increase transparency about cybersecurity policies and procedures, and management and board involvement in the development and implementation of such policies and procedures. In the proposed changes, the SEC notes that "most of the registrants that disclosed a cybersecurity incident in 2021 did not describe their cybersecurity risk oversight and related policies and procedures."

Proposed new Item 106(b) of Regulation S-K would require disclosures of policies and procedures to identify and manage cybersecurity risks. These risks include "operational risk; intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk." Required disclosures include, but are not limited to, whether the company has a cybersecurity risk-assessment program, how the company manages third-party providers under its cybersecurity risk-assessment programs, mitigation plans, contingency and continuity plans, and how previous cybersecurity risks and incidents have informed these decisions and business strategy.

Proposed new Item 106(c) of Regulation S-K would focus on governance activities, namely board oversight of a company's cybersecurity risk and how involved management is in overseeing the implementation of policies, procedures, and strategies. Required disclosures would include whether, and which, board members are responsible for oversight of cybersecurity risks, the processes by which the board is informed of cybersecurity risks, and how the board considers cybersecurity risks as part of its business strategy and risk management.

3. Disclosure of Board Cybersecurity Experience

- The SEC proposes adding a new Item 407(j) of Regulation S-K to require disclosures identifying individuals on the board with cybersecurity expertise and identifying the nature of that expertise.

The SEC proposes requiring disclosures of whether board members have cybersecurity expertise, identifying those board members who have such expertise, and descriptions of such expertise. The SEC does not dictate any minimum requirements for expertise—and expressly declines to define "cybersecurity expertise"—but proposes a list of criteria that could apply. Additionally, the SEC does not require having a person with such expertise on the board of directors. As proposed, identifying such an individual with cybersecurity expertise would not impose any additional duties, obligations, or liability on that individual.

The SEC has asked questions that demonstrate a potential hesitance to expressly name such board members, lest those individuals be deterred from serving in the role. The SEC also has asked whether a lack of cybersecurity expertise on the board should be expressly disclosed.

It is important to note that the SEC's final rules may differ from the proposed rules, for which it requested comments. The comments period closed on May 9, 2022. According to the SEC, the average time between publication of its proposed and final rules is 450 days, so no final regulations are likely until 2023.

Key Takeaways

The SEC's proposed new cybersecurity incident-disclosure requirements will shine a spotlight on company information governance and cybersecurity. This forthcoming transparency requirement should serve as a call to action for companies to ensure they are prepared to operate in a world where companies are required to disclose more information about internal cybersecurity issues.

We recommend that companies take the following steps now:

- Evaluate their information governance and cybersecurity policies and procedures to ensure they meet applicable legal requirements and align with best practices;
- Prepare a written incident-response plan to respond to cybersecurity incidents, which includes the new SEC reporting requirements;
- Evaluate their existing board members and proactively add board members with cybersecurity expertise;
- Review and update their risk factors in their periodic reports relating to specific cybersecurity risks; and
- Monitor the SEC's proposed cybersecurity rules and any guidance, and update their internal SEC reporting compliance processes accordingly.

We will continue to monitor these developments.

For more information, please contact Mike Blankenship or your Winston relationship partner.

5 Min Read

Authors

Michael J. Blankenship

David Houck

Related Locations

Houston | Washington, DC

Related Topics

Cyber Security | Securities and Exchange Commission (SEC) | Regulations | Disclosures | Compliance

Related Capabilities

Privacy & Data Security | Technology, Media & Telecommunications

Related Regions

North America

Related Professionals

Michael J. Blankenship

David Houck

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.