STINSON

News & Insights

SEC Proposes Public Company Cybersecurity Disclosure Rules

Alert

03.21.2022

On March 9, 2022, the Securities and Exchange Commission (SEC) proposed amendments to its rules that would require certain cybersecurity-related disclosures by public companies. The proposed rules are intended to enhance and standardize disclosures for cybersecurity incident reporting, strategy, risk management and governance.

The proposed amendments mark a change from the prior administration's principles-based approach to a more prescriptive method. If adopted, the proposed rules will supplement the SEC's previous guidance issued in 2011 and 2018, which included the SEC's views regarding disclosure requirements for cybersecurity risks and incidents under existing rules, and emphasized the importance of cybersecurity to enterprise risk management.

The proposed amendments would require:

- Current reporting of material cybersecurity incidents and periodic updates regarding the developments of previously reported cybersecurity incidents, as well as the reporting of cybersecurity incidents which, in the aggregate, become material.
- Periodic reporting about:
  - A company's policies and procedures for identifying and managing cybersecurity risks
  - Oversight of cybersecurity management by the board of directors
  - Management's role and expertise in implementing a company's cybersecurity policies, procedures and strategies
  - Annual reporting about the board of directors' cybersecurity expertise

SEC Proposes Public Company Cybersecurity Disclosure Rules

CYBERSECURITY INCIDENT DISCLOSURE

Form 8-K would be amended by proposed Item 1.05, which would require a registrant to disclose information about a material cybersecurity incident within four business days of occurrence. A company would be required to report:

- When the incident was discovered and whether it is ongoing
- A brief description of the nature and scope of the incident
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose
- The effect of the incident on the company's operations
- Whether the company has remediated or is currently remediating the incident

The trigger for an Item 1.05 Form 8-K would be the date a company determines a cybersecurity incident it experienced was material, not the date of the incident. The materiality threshold is consistent with the various cases addressing materiality in securities laws. Information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if such information "significantly alter[s] the 'total mix' of information made available."

Failure to timely report Item 1.05 would not result in a loss of Form S-3 or Form SF-3 eligibility. Under the proposed rules, Rule 13a-11(c) and Rule 15d-11(c) of the Securities Exchange Act would be amended to include Item 1.05 as eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 of the Exchange Act.

Required Updates on Disclosed Cybersecurity Incidents

Proposed Item 106(d)(1) of Regulation S-K would require public companies to disclose any material changes, additions, or updates to information required to be disclosed under Item 1.05 of Form 8-K in the company's quarterly report filed on Form 10-Q or annual report filed on Form 10-K.

Disclosure of Cybersecurity Incidents that Have Become Material in the Aggregate

Proposed Item 106(d)(2) of Regulation S-K would require disclosure of previously undisclosed cybersecurity incidents when they become material in the aggregate. Such incidents would need to be disclosed in the periodic report for the period in which a company has made a determination that the incidents are material in the aggregate.

SEC Proposes Public Company Cybersecurity Disclosure Rules

CYBERSECURITY RISK MANAGEMENT, STRATEGY AND GOVERNANCE DISCLOSURES

The proposed rules related to risk management, strategy and governance are intended to increase transparency for public companies' strategies and actions in managing cybersecurity risk.

Risk Management and Strategy

Proposed Item 106(b) of Regulation S-K is intended to require companies to provide consistent and informative disclosures for their cybersecurity risk management and strategy and would require a company to disclose whether:

- The company has a cybersecurity risk assessment program and if so, to provide a description of such program.
- The company engages assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program.
- The company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third party service provider, including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers.
- The company undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents.
- The company has business continuity, contingency, and recovery plans in the event of a cybersecurity incident.
- Previous cybersecurity incidents have informed changes in the company's governance, policies and procedures, or technologies.
- Cybersecurity related risk and incidents have affected or are reasonably likely to affect the company's results of operations or financial condition and if so, how.
- Cybersecurity risks are considered as part of the company's business strategy, financial planning, and capital allocation and if so, how.

Governance

Proposed Item 106(c) of Regulation S-K would require disclosure of a company's cybersecurity governance, including the board's oversight of cybersecurity risk and a description of management's role in assessing and managing risk, management's cybersecurity expertise, and its role in implementing cybersecurity-related policies, procedures and strategies.

The Board's Cybersecurity Expertise

To build upon existing disclosure requirements in Items 401(e) and 407(h) of Regulation S-K, proposed Item 407(j) of Regulation S-K would require disclosure about the cybersecurity expertise of the members of the board of directors, if any. A company would be required to disclose any board member with cybersecurity expertise and describe the nature of such expertise. The proposed Item 407(j) disclosure would be required in a company's proxy or information statement when action is to be taken with respect to the election of directors, and in its Form 10-K.

Proposed Item 407(j) would not define "cybersecurity expertise." However, proposed Item 407(j)(1)(ii) would include a non-exclusive list of criteria a company should consider in determining whether a director has cybersecurity expertise.

To alleviate any concerns for cybersecurity experts considering board service, proposed Item 407(j)(2) would state that a person deemed to have expertise in cybersecurity will not be deemed to be an expert for any purpose, including for purposes of liability under Section 11 of the Securities Act, as a result of being identified as a director with expertise in cybersecurity under proposed Item 407(j). Further, proposed Item 407(j) would not impose any additional duties, obligations, or liabilities on such a board member identified as having cybersecurity expertise.

FOREIGN ISSUER DISCLOSURES

Foreign private issuers are not required to file current reports on Form 8-K. Instead, they are required to provide on Form 6-K copies of all information the foreign private issuer: (i) makes or is required to make public under the laws of its jurisdiction of incorporation, (ii) files, or is required to file under the rules of any stock exchange, or (iii) otherwise distributes to its security holders. The proposed rules would amend General Instruction B of Form 6-K to reference material cybersecurity incidents among items that may trigger a current report on Form 6-K.

Form 20-F would be amended to add Item 16J to require a foreign private issuer to include in its annual Form 20-F report the same type of disclosures proposed in Items 106 and 407(j) of Regulation S-K in periodic reports filed by domestic registrants. However, since foreign private issuers are not subject to SEC rules for proxy or information statement filings, they would only be required to include the proposed Item 407(j) disclosure about board expertise in their annual reports. Form 20-F would also be amended to require, on an annual basis, foreign private issuers to disclose any previously undisclosed material cybersecurity incidents that occurred in the reporting period and any previously undisclosed immaterial cybersecurity incidents that have become material in the aggregate.

INLINE XBRL TAGGING REQUIREMENTS

To make the disclosures readily available and easily accessible to investors, market participants and others for aggregation, comparison, filtering and other analysis, the proposed amendments would require Item 1.05 of Form 8-K and Items 106 and 407(j) of Regulation S-K to be tagged in Inline XBRL, in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

The public comment period will remain open until May 9, 2022 or 30 days following the publication of the proposing release in the Federal Register, whichever period is longer.

RELATED CAPABILITIES

Corporate Finance

Cybersecurity & Data Privacy

Governance, Risk & Compliance

Public Companies, Securities & Capital Markets