No. 2022-01
10 March 2022

To the Point

SEC – proposed rule

SEC proposes requiring more cybersecurity disclosures

The proposed rules are aimed at enhancing and standardizing registrants' disclosures related to cybersecurity risk management, strategy and governance.

What you need to know

- The SEC proposed new rules that would require registrants to disclose information about a material cybersecurity incident on Form 8-K within four business days of determining that the incident is material.
- Registrants would have to provide updated disclosures in periodic reports about previously reported incidents, describe their policies and procedures, if any, for the identification and management of risks from cybersecurity threats and provide disclosures about the board's oversight of cybersecurity risk and management's role in assessing and managing this risk and in implementing cybersecurity policies.
- Registrants would also have to disclose whether they have cybersecurity expert(s) on the board of directors and, if so, provide their name(s) and a description of their experience.
- Comments are due at the later of 30 days after publication of the proposal in the Federal Register or 9 May 2022.

Overview

The Securities and Exchange Commission (SEC) **proposed** new rules to enhance and standardize disclosures that registrants make about cybersecurity incidents, their cybersecurity risk management, strategy and governance.

In its proposing release, the SEC said new rules are needed because cybersecurity risks have increased and registrants' current disclosures about cybersecurity incidents and risks vary widely, making it difficult for investors to analyze the information. Gary Gensler, the SEC

Building a better working world

chair, noted that the SEC has also proposed requiring registered investment advisers and funds to make more cybersecurity disclosures.

The proposed rules would codify many of the concepts in the interpretive guidance on cybersecurity that the SEC issued in 2018 (the 2018 Interpretive Release[1]) and in the Division of Corporation Finance's 2011 staff guidance[2] on cybersecurity disclosures. But it would also go beyond that guidance, requiring more disclosures about cybersecurity risk governance and the board's expertise in that topic.

The proposed rules would apply to nearly all registrants that are required to file periodic reports (e.g., Form 10-K, Form 20-F) with the SEC, including smaller reporting companies and foreign private issuers (FPIs).

Key considerations

Incident disclosures

Form 8-K reporting requirements

The proposed rules would require registrants to provide updated information to investors in Forms 10-Q and 10-K on previously disclosed material cybersecurity incidents.

The proposed rules would amend Form 8-K to add Item 1.05, which would require registrants to disclose a material cybersecurity incident within four business days of determining that a cybersecurity incident is material, rather than the date they discover the incident.

The proposed rules would require registrants to disclose the following information about such material incidents in Form 8-K, to the extent it is known at the time of the filing:

- When the incident was discovered and whether it is still 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 purposes
- The effect of the incident on the registrant's operations
- Whether the registrant has remediated or is currently remediating the incident

The proposing release includes examples of cybersecurity incidents that may trigger Form 8-K reporting, including an unauthorized incident that compromised a registrant's confidential data and an unauthorized incident that caused a registrant to lose control of its operational technology system.

The proposing release states that what constitutes materiality for purposes of determining whether an incident must be reported in a Form 8-K would be consistent with the Supreme Court definition of materiality, and registrants would need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances of the cybersecurity incident, including both quantitative and qualitative factors.

The proposing release also clarifies that a registrant would not be expected to publicly disclose specific, technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail that it would impede its response or remediation of the incident.

When a registrant is under an ongoing internal or external investigation by law enforcement authorities, a timely filed Form 8-K would still be required if the registrant has experienced a material cybersecurity incident.

How we see it

In its 2018 Interpretive Release, the SEC said registrants had an obligation to use Form 8-K to disclose information about material incidents. Although the proposal would formalize the timing and specify the content and location of cybersecurity incident disclosure, the use of materiality as the threshold for providing disclosure about incidents would not change.

Updates to previously filed Form 8-K disclosure in periodic reports

The proposed rules would add Item 106(d) to Regulation S-K to require registrants to provide updates in Forms 10-Q and 10-K on previously disclosed material cybersecurity incidents. Item 106(d) would also require registrants to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. In this situation, a registrant would be required to disclose the same information as described above for the Form 8-K reporting of material cybersecurity incidents.

The proposed rules identify the minimum disclosure that should be provided in Forms 10-K and 10-Q, such as any material impact of the incident on the registrant's current operations and financial condition or potential future impact, whether the registrant has remediated or is remediating the incident, and any changes to the registrant's cybersecurity policies and procedures due to the incident.

The proposed rules also would amend Form 20-F to require FPIs to provide similar cybersecurity disclosures.

How we see it

Although the SEC provided an example of a series of undisclosed individually immaterial cybersecurity incidents to illustrate how such events could become material in the aggregate, we expect that the SEC will get feedback from companies and other stakeholders to clarify how this guidance should be implemented.

Risk management, strategy and governance disclosures

The proposed rules would add Item 106 to Regulation S-K, and Item 16J to Form 20-F, to require registrants to disclose their cybersecurity risk management, strategy and governance.

Risk management and strategy

The proposed rules would require registrants to disclose their policies and procedures, if any, to identify and manage cybersecurity threats, including operational risks, intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risk, and reputational risk. For example, a registrant would have to disclose whether it has a risk assessment program and, if so, describe the program, disclose whether it uses assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program, and disclose whether cybersecurity risks are considered part of its business strategy, financing planning and capital allocation.

Governance

The proposed rules would also require registrants to disclose the board's role in overseeing cybersecurity risk and management's involvement in assessing and managing cybersecurity risk and implementing cybersecurity policies, procedures and strategies.

A registrant would be required to disclose whether the entire board, specific board members or a board committee oversees cybersecurity risks, how the board is informed about cybersecurity risks and the frequency of its discussions on this topic, and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

The proposed rules would also require disclosures about management's role in managing cybersecurity risks, including whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, and whether the registrant has a designated chief information security officer.

Cybersecurity expertise

The proposed rules would amend Item 407 of Regulation S-K and Form 20-F to require registrants to disclose whether board members have cybersecurity expertise. If they do, the registrant would be required to disclose their names and a description of their relevant experience, including prior work experience, certification or degree, knowledge, skills or other background in cybersecurity.

Registrants would also be required to include the disclosures under proposed Item 407 of Regulation S-K in their proxy statements.

How we see it

Boards should consider whether their committee structures are appropriate and whether they are allocating sufficient time on their agendas to address the areas that would need to be disclosed under the proposed rules related to cybersecurity oversight and board members' expertise.

Endnotes:

1 *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, 26 February 2018.

2 *CF Disclosure Guidance: Topic No. 2: Cybersecurity*, 13 October 2011.