Lowenstein Sandler

Capital Markets & Securities

March 22, 2022

SEC Proposes New Rules Related to Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure By Public Companies

By Steven M. Skolnick, Kate Basmagian, Kathleen A. McGee, Jeffrey M. Shapiro, and Daniel C. Porco

Requirements under the proposed rules would include the disclosure of:

- **Material cybersecurity incidents within four business days of the determination that a material cybersecurity incident has occurred in a Form 8-K**
- **Updates to any previously disclosed material cybersecurity incidents in Forms 10-Q and 10-K**
- **Registrant's cybersecurity policies and governance practices in Form 10-K**
- **Board of directors' cybersecurity expertise in Form 10-K**

On March 9, 2022, the Securities and Exchange Commission (SEC or Commission) proposed new rules (the Proposed Rules)[1] in an effort to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies." The Proposed Rules would require a host of new disclosures regarding material cybersecurity incidents[2] and registrants' cybersecurity risk management, strategy, and governance.

Background and Context

Since 2011, the SEC has periodically published interpretive guidance related to disclosure of cybersecurity incidents. Up until now, the guidance maintained that despite there being no existing requirement explicitly referring to the disclosure of cybersecurity risks and cyber incidents, companies nonetheless may be required to disclose such risks and incidents by existing obligations.[3] Existing SEC guidance has also emphasized thExisting SEC guidance has also emphasized the importance of cybersecurity policies and procedures including disclosure controls related to cybersecurity risk and incidents.[4]

With the increased digital nature of the conduct of business today, the reliance on information technologies, and the rising number of cybersecurity threats and incidents throughout the world, the SEC cites the increased risk of the effect of cybersecurity incidents on the economy at large, as well as on individual registrants, as the reasoning behind the Proposed Rules. In light of these bases, the SEC explains that investors must have access to timely and consistent disclosure about cybersecurity incidents, and because of the observed variations in current disclosure

[1] The Proposed Rules can be found here.
[2] Under the Proposed Rules, "cybersecurity incident" means "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."
[3] *CF Disclosure Guidance: Topic No. 2*
[4] SEC Release No. 33-10469

practices among public companies of all sizes, the Proposed Rules aim to provide investors with "consistent, comparable and decision-useful" disclosures.

Proposed Rules

Incident Disclosure

The Proposed Rules would amend Form 8-K to add an Item 1.05, requiring the disclosure of a material cybersecurity incident within four business days after a registrant determines that a material cybersecurity incident has occurred. Item 1.05 would require the disclosure of:

- When the incident was discovered
- A brief description of the nature of the incident (no sensitive or technical information is required)
- Whether any data was stolen, altered, accessed, or used for an unauthorized purpose
- The effect of the incident on operations of the registrant
- Whether the incident has been remediated or if there have been remediation efforts undertaken

The SEC has pegged the trigger date of the new Item 1.05 to the date on which a registrant determines that an incident is material, and not the date on which the registrant discovers the incident. The SEC chose this timing in order to focus disclosures on incidents and events that are material to investors. To avoid the intentional delay of reporting, the new Item 1.05 will require that upon discovery of an incident, a registrant "shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable."

Information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important"[5] in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."[6] However, the SEC provides a non-exhaustive list of incidents it believes would typically be material in this context:

- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network), or violated the registrant's security policies or procedures; incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data
- An unauthorized incident that has caused degradation, interruption, loss of control, damage to, or loss of operational technology systems
- An incident in which an unauthorized party has accessed, or a party has exceeded authorized access, and altered or stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant
- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data
- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered

Once a company has determined that an incident is "material," an Item 1.05 Form 8-K would be due within four business days, despite any ongoing investigation into the incident. The SEC considered the potential need for a delay in reporting to allow for an internal investigation, or to allow law enforcement to investigate, but found that investors' need for timely information outweighs these needs.

Notably, the Proposed Rules specify that the untimely filing of an 8-K under Item 1.05 would not impact a registrant's ability to use Form S-3 so long as the registrant's Form 8-K reporting is current at the time the Form S-3 is filed.

Further, the Proposed Rules would extend the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act of 1934, meaning that an untimely filing of an Item 1.05 Form 8-K will not be deemed a violation of Section 10(b) or Rule 10b-5 of the Exchange Act.

Updating Previously Reported Cybersecurity Incidents in Forms 10-Q and 10-K

The Proposed Rules would also amend Regulation S-K by adding new Item 106(d)(1). Item 106(d)(1) would require registrants to disclose any material changes, additions, or updates to information disclosed pursuant to Item 1.05 of Form 8-K in the registrant's quarterly report filed with the Commission on Form 10-Q or annual report filed with the Commission on Form 10-K for the period in which the material change, addition, or update occurred.

---

[5] *TSC Industries v. Northway*, 426 U.S. 438, 449 (1976).
[6] Id. See also the definition of "material" in Securities Act Rule 405, 17 CFR 230.405; Exchange Act Rule 12b-2, 17 CFR 240.12b-2.

The SEC stated that while the Proposed Rules are intended to produce timely disclosure, registrants will likely need time to investigate an incident in order to assess the full magnitude of the incident. For example, after a registrant has initially disclosed a material cybersecurity incident in Form 8-K, the registrant's investigation may uncover additional material information regarding the incident. In this instance, the SEC gave a nonexclusive list of information that should be disclosed:

- Any material impact of the incident on the registrant's operations and financial condition
- Any potential material future impacts on the registrant's operations and financial condition
- Whether the registrant has remediated or is currently remediating the incident
- Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes

Disclosure of Cybersecurity Incidents That Have Become Material in the Aggregate

Proposed Item 106 of Regulation S-K would require a registrant to disclose when a series of previously undisclosed incidents have become material in the aggregate. The series of incidents would need to be disclosed in the periodic report for the period in which a registrant has made a determination that they are material in the aggregate, and such disclosure would need to include all of the following:

- When the incidents were discovered and whether they are ongoing
- A brief description of the nature and scope of such incidents
- Whether any data was stolen or altered
- The impact of such incidents on the registrant's operations and the registrant's actions
- Whether the registrant has remediated or is currently remediating the incidents

Therefore, registrants must continually assess the materiality of each incident individually, but also must assess and continuously track materiality of a series of incidents in the aggregate.

The Proposed Rule has requested comment on whether any final rule should also require an Item 1.05 Form 8-K to be filed once such a materiality determination has been made.

Disclosure of a Registrant's Risk Management, Strategy, and Governance Regarding Cybersecurity Risks

Proposed Item 106(b) of Regulation S-K would require registrants to provide disclosure regarding cybersecurity risk management, including the existence of any relevant policies and procedures, to the extent a registrant has established any, in Form 10-K. The Proposed Rules would require disclosure regarding:

- *Risk management and strategy:* including (i) the existence of a cybersecurity risk assessment program; (ii) whether the registrant engaged consultants, auditors, or other third parties in connection with its cybersecurity program; (iii) the existence of any policies and procedures relating to cybersecurity risks associated with use of third-party service providers (including whether and how cybersecurity considerations affect the selection of providers); (iv) measures undertaken to prevent, detect, and minimize effects of cybersecurity incidents; (v) business continuity, contingency, and recovery plans in the event of a cybersecurity incident; (vi) whether previous cybersecurity incidents have informed changes in the registrant's policies and procedures; (vii) whether previous cybersecurity incidents have affected or are reasonably likely to affect the results of operations or financial condition, and if so, how; and (viii) whether cybersecurity risks are considered part of the registrant's business strategy, financial planning, and capital allocation, and if so, how
- *Governance:* including (i) whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks; (ii) the processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and (iii) whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight
- *Management's oversight of cybersecurity risk:* including (i) whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons or members; (ii) whether the registrant has designated a chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any

such persons; (iii) the processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and (iv) whether and how frequently such persons or committees report to the board of directors or a committee of the board of directors on cybersecurity risk

Disclosure Regarding the Board of Directors' Cybersecurity Expertise

The Proposed Rules would also amend Regulation S-K by amending existing Item 407. The proposed amendments to Item 407 would require disclosure about the cybersecurity expertise of members of the board of directors of the registrant, if any.

The term "cybersecurity expertise" is not defined in the Proposed Rules, but the SEC did include a nonexclusive list of criteria that a registrant should consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager, or business continuity planner
- Whether the director has obtained a certification or degree in cybersecurity
- Whether the director has knowledge, skills, or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning

The Proposed Rules would state that a person who is determined to have expertise in cybersecurity will not be deemed an "expert" for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act.

Key Takeaways for Public Companies and Their Boards of Directors and Management

1. *Materiality analyses and DCP.* Registrants must be diligent in creating thRegistrants must be diligent in creating the required disclosure control procedures (DCP) in order to be able to identify, assess, and determine whether to disclose cybersecurity incidents. The initial assessment of materiality, which will drive the initial Form 8-K reporting, will require coordination among many different constituents, including consultants, forensics, third-party vendors, etc., and management. This analysis may take time. Further, a system should be implemented to continually assess whether, and when, certain immaterial incidents become material in the aggregate. Registrants should work with counsel to develop these procedures.
2. *Ignorance is no longer a defense.* Cybersecurity incidents are becoming increasingly prevalent, and it is only a matter of time before a registrant, of any size, may experience an incident. If they have not done so already, management and boards of directors should move to gain an understanding of their company's technology and cybersecurity infrastructure. This assessment could include the engagement of a technology and/or information systems consultant who can analyze the adequacy of a company's existing capabilities, identify vulnerabilities, and help implement policies. Prior to the engagement of any third-party vendor, companies should consult with counsel to insure privilege is and will be maintained at all times.

   Having an understanding of the type of data their company maintains or possesses, where that data resides, and who has access to the data will enable management and boards of directors to more efficiently gauge the materiality of any potential cybersecurity incident, which will allow for timely Item 1.05 Form 8-K reporting pursuant to the Proposed Rules.
3. *Update D&O questionnaires.* While this is not yet required, identifying directors and management who have cybersecurity experience can start now. Much like how boards of directors assess whether a director qualifies as an "audit committee financial expert" via questions contained in a registrant's standard D&O questionnaire, boards of directors and management should work with counsel to update D&O questionnaires to include questions and/or prompts that elicit a candidate's experience in this field. These proposed rule changes will likely increase demand for board nominees with the requisite experience.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

STEVEN M. SKOLNICK
Partner
Chair, Capital Markets & Securities
Vice Chair, Transactions & Advisory Group
T: 973.597.2470
jshapiro@lowenstein.com

KATE BASMAGIAN
Partner
T: 646.414.6941
kbasmagian@lowenstein.com

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

JEFFREY M. SHAPIRO
Partner
T: 973.597.2470
jshapiro@lowenstein.com

DANIEL C. PORCO
Counsel
T: 646.414.6811
dporco@lowenstein.com