FOLEY & LARDNER LLP

SEC Proposes New Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Jessica S. Lochmann, Benjamin F. Rikkers, Aaron K. Tantleff, Jennifer L. Urban, John K. Wilson, Mary Kathleen Conterio
17 March 2022

Innovative Technology Insights
On March 9, 2022, the U.S. Securities Exchange Commission (the Commission) announced proposed amendments to its rules regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies to enhance and standardize disclosures.

Chair of the Commission Gary Gensler emphasized that the proposal would "strengthen investors' ability to evaluate public companies' cybersecurity practices and incident reporting." The proposed amendments are intended to ensure better-informed investors by mandating disclosure around a registrant's risk management, strategy, and governance regarding cybersecurity and requiring timely notifications of material cybersecurity incidents. In addition, the proposed amendments reinforce the increased significance of cybersecurity with the proposal acknowledging the "potential costs and damages that can stem from a material cybersecurity incident are extensive."

The proposal is currently open for comments and we expect that there will be significant interest and comments from investors, companies, and advisors. Commissioner Hester Pierce's dissent, which is summarized below, foreshadows some of the likely arguments to be put forward against the proposed amendments, which include that the mandated incident reporting could be counter-productive to the interests of registrants and their stakeholders and the disclosure requirements are a backdoor way to mandate desired governance goals.

Background

Although certain federal and state regulations and laws may require cybersecurity disclosures, neither Regulation S-K nor Regulation S-X currently contains any disclosure requirements explicitly requiring information regarding cybersecurity. However, in 2011 the Division of Corporation Finance issued interpretative guidance providing their views on a registrant's disclosure obligations regarding cybersecurity and issued follow-up interpretive guidance in 2018 (2018 Interpretative Release). The 2018 Interpretative Release asserted that Regulations S-K and S-X may require disclosure about cybersecurity under various items such as:

a. Risk Factors (Item 105)

b. Management's Discussion and Analysis of Financial Condition and Results of Operations (Item 303)
c. Description of Business (Item 101)
d. Legal Proceedings (Item 103)
e. Corporate Governance (Item 407)
f. Regulation S-X financial disclosures

In its discussion of the proposed amendments, the Commission noted that approximately 94% of Form 10-K filers provide cybersecurity disclosures in the Risk Factors section, but only 21% and 10% of filers provided such disclosure in the Description of Business or Management's Discussion and Analysis sections, respectively.

Summary

The proposed amendments would:

1. *Incident Reporting on Form 8-K*: Amend Form 8-K to add Item 1.05 requiring registrants to disclose information about a cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident (and not the date the registrant discovers the incident).
    - Item 1.05 would require registrants to disclose: (a) when the incident was discovered and whether it is ongoing; (b) a brief description of the nature and scope of the incident; (c) whether any data was stolen, altered, accessed, or used for any other unauthorized purpose; (d) the effect of the incident on the registrant's operations; and (e) whether the registrant has remediated or is currently remediating the incident.
    - Examples of cybersecurity incidents, if determined to be material, that would trigger Item 1.05 disclosures include: (a) an unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset; (b) an unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems; (c) an incident in which an unauthorized party accessed and altered or stole sensitive business information, personally identifiable information, intellectual property, or information that may result in a liability for the registrant; (d) an incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; and (e) an incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.
    - The proposal provides that untimely filing of a Form 8-K under Item 1.05 would not result in loss of Form S-3 or Form SF-3 eligibility.
    - The reporting deadline may not be delayed for any reason, including due to the ongoing investigation of the cybersecurity incident.

2. *On-Going Updates to Incident Reporting*: Amend Forms 10-Q and 10-K to require registrants to provide updated disclosure relating to previously disclosed cybersecurity incidents, as well as amend

Forms 10-Q and 10-K to require disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate.

- The Commission noted that the goal of the proposed amendments is to balance the need for prompt disclosure with the fact that a registrant may not have complete information about a cybersecurity incident at the time it files the Form 8-K.
- Examples of this disclosure are: (a) any material impact of the incident on the registrant's operations and financial condition; (b) any potential material future impacts on the registrant's operations and financial condition; (c) whether the registrant has remediated or is currently remediating the incident; and (d) 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.

3. *Disclosure of Policies and Governance*: Amend Form 10-K and add Section 106 of Regulation S-K to require disclosure regarding:
    a. A registrant's policies and procedures, if any, for identifying and managing cybersecurity risks, including cybersecurity risks associated with its use of any third-party service provider, including disclosure of:
        - Whether a registrant has a cybersecurity risk assessment program, and if so, a description of the program
        - Whether the registrant engages assessors, consultants, auditors, or other third parties in its cybersecurity risk assessment program
        - The efforts taken to prevent, detect, and minimize the impacts of cybersecurity incidents
        - Whether the registrant has business continuity and disaster recovery plans in the event of a cybersecurity incident
        - Previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies
        - Whether cybersecurity-related risks and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition
        - Whether cybersecurity risks are considered part of the registrant's business strategy, financial planning, and capital allocation
    b. A registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risk, including:
        - Whether the entire board, specific board members, or a board committee is responsible for the oversight of cybersecurity risks
        - The processes by which the board is informed about cybersecurity risks, including the frequency of such discussions
        - Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management, and financial oversight
    c. Management's role, and relevant expertise, in assessing and managing cybersecurity related

risks and implementing related policies, procedures, and strategies, including:

- Who is responsible for measuring and managing cybersecurity risk, whether it's certain management positions or committees
- Whether the registrant has a designated a chief information security officer or someone in a comparable position to whom such person reports, and the expertise of such person "in such detail as necessary to fully describe the nature of the expertise"
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents
- 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.

4. *Board Cybersecurity Expertise*: Amend Item 407 of Regulation S-K to require disclosure about whether any member of the registrant's board of directors has cybersecurity expertise, including prior experience in cybersecurity, a certification or degree in cybersecurity, and whether the director has knowledge or other background in cybersecurity.

5. *Applicability to Foreign Private Issuers*: Amend Form 6-K to add "cybersecurity incidents" as a reporting topic per General Instruction B and amend Form 20-F to require foreign private issuers to provide cybersecurity disclosures in their annual reports.
    - This would require the same type of disclosure proposed in Items 106 and 407(j) of Regulation S-K that would be required by domestic registrants

6. *Inline XBRL (Inline eXtensible Business Reporting Language) Tagging*: Item 1.05 of Form 8-K and Items 106 and 407(j) would require inline XBRL tagging, including detailed tagging of narrative disclosures.

Dissenting Voice

Commissioner Pierce penned a dissenting statement on the proposal, accusing the proposed amendments of guiding or creating a list of expectations about what an issuer's cybersecurity programs should look like or dictating an issuer's corporate governance, while remaining cloaked as a standard disclosure requirement. To support her position, Commissioner Pierce references the significant level of detail involved in the requirements.

Commissioner Pierce also expressed concern over the proposed incident reporting requirements. She noted that the root of the concern is that the Commission is acting "unduly dismissive of the need to cooperate with, and sometimes defer to, our partners across the federal government and state government." Commissioner Pierce foresees a situation where delaying disclosure about a material incident could actually

protect investors by, for example "increase[ing] the chances of recovery of stolen funds" and criticized how the reporting requirement does not allow for such delay.

Potential Implications of the Proposed Amendments for Registrants

The proposed amendments may create certain unintended consequences that registrants should begin considering now, even though the final rules are likely to differ from the proposed amendments. As such, registrants should consider how the proposed amendments may impact their disclosures and what steps a registrant should consider to ensure compliance and limit cybersecurity risks.

1. *Amending Cybersecurity Incident Response Plans*: To meet the disclosure obligations and deadlines under the proposed amendments, a registrant's cybersecurity incident response plans would need to be reviewed and amended, if applicable, to ensure the registrant has the ability to assess and escalate cybersecurity incidents quickly. Additionally, registrants should regularly test such plans, including the efforts necessary to provide timely and adequate reporting of such cybersecurity incidents in accordance with any disclosure requirements. Testing should include management and board members, as applicable, to ensure the ability of the organization to meet its disclosure obligations in connection with cybersecurity incidents.

2. *Management of Third Parties*: The proposed amendments would create additional compliance risks for registrants who rely upon "third party service providers for information technology services," which to some extent encompasses virtually all registrants as the proposed amendments govern all "information resources owned or used by the registrant." Most third-party service provider contracts have varying contractual obligations regarding whether and when they report a cybersecurity incident to their customer. Even with enhanced reporting obligations under a third-party service provider contract, it would be up to the registrant, not the third-party service provider, to determine whether the cybersecurity incident would be material and require disclosure. Therefore, registrants should consider a thorough review of all third-party service providers and their contracts to understand how existing service provider contracts would enable a registrant's ability to comply with its disclosure obligations. Once any new disclosure rules become final, registrants will likely have to amend existing contracts and ensure future contracts contain new requirements regarding cybersecurity and data privacy. Registrants will likely also have to conduct additional or enhanced diligence, including cybersecurity and privacy risk assessments and audits of all applicable third-party service providers. Registrants should also consider establishing or revisiting their existing third-party service provider management program to ensure such third-parties are providing sufficient information on a timely basis to enable a registrant to evaluate the incident and make its own determination relative to any required disclosure. Registrants should also consider what the third-party provider can or may disclose about an incident. This will likely be more complicated in situations involving third-party service providers that are registrants with their own disclosure

requirements, as customers that are registrants will have to consider how disclosure by the third-party service provider may affect its own disclosure analysis should the third-party service provider make a disclosure. Registrants should also be prepared to terminate agreements with third-party service providers who cannot comply with any new disclosure requirements.

3. *Cybersecurity Risks*: The detail required by the proposed amendments requires substantial disclosure of a registrant's cybersecurity risk management policies and procedures as well as any cybersecurity incident. While the intent of the proposed amendments may be to encourage registrants to improve their policies and procedures, registrants will have to weigh how any such disclosure has the potential to provide threat actors with information to enable them to design a targeted attack against perceived vulnerabilities and avoid detection. Disclosing details relating to an ongoing attack before the full containment and remediation may allow threat actors to further victimize a vulnerable organization and any impacted individuals and entities. This may also impact a registrant's ability to contain and remediate an attack where the registrant has to disclose information regarding an ongoing incident or may require disclosure regarding whether a registrant is subject to and their position and strategy regarding ransomware or extortion.

4. *Litigation Risks*: The proposed amendments require, within four business days of determining that an incident is a material cybersecurity incident, disclosure regarding the discovery of the cybersecurity incident, 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 registrant's operations, and the remediation status of the incident. This disclosure obligation would likely precede data breach notifications to individuals, state attorneys general, other regulatory authorities, and other required disclosures, as well as to others potentially impacted by the incident. This early disclosure, which is likely before the completion of the registrant's investigation, has the potential to create liability because the full scope of the incident is not likely to be fully understood at the time of disclosure. This may result in litigation before the registrant has a complete picture of the scope and impact of the incident on the organization and may impact attorney-client privilege associated with the ongoing investigation. This also has the potential to affect the analysis and timeliness of data breach notification obligations under applicable data breach protection and notifications laws.