Cooley

SEC Proposes Sweeping Cybersecurity Disclosure Framework

March 16, 2022

On March 9, 2022, the Securities and Exchange Commission **announced** that it proposed **rules** that would expressly mandate cybersecurity disclosures by public companies. The rules would require disclosure of material cybersecurity incidents, as well as disclosure regarding a company's cybersecurity risk management and strategy, and governance, and board of directors' cybersecurity expertise. In keeping with SEC Chair Gary Gensler's oft-repeated **refrain** of the benefits of "consistent, comparable, and decision-useful" disclosure, the proposal seeks to provide investors "with more uniform and timely disclosure about material cybersecurity incidents and disclosure" that is "comparable to the disclosure provided by other registrants."

The proposed rules were not without opposition, with SEC Commissioner Hester Peirce providing a dissenting statement and, among other things, stating that the proposal "flirts with casting [the SEC] as the nation's cybersecurity command center, a role Congress did not give us." For more information on Peirce's dissent and other commissioner statements, refer to our **Cooley PubCo blog post**.

The SEC is soliciting comments on the proposed rules. The comment period will be open until the later of 30 days after the proposing release is published in the Federal Register or May 9, 2022 (60 days from the date that the rules were proposed). Interested parties can submit comments **here**.

Background

Under the existing public company reporting framework, there are no explicit disclosure requirements relating to cybersecurity matters. However, there are several disclosure requirements under Regulation S-K or Regulation S-X that may encapsulate cybersecurity matters, such as risk factors, management's discussion and analysis of financial condition and results of operations, description of business, legal proceedings, financial statements, and disclosure controls and procedures.

In 2011, the SEC's Division of Corporation Finance published **interpretive guidance** to provide direction to companies on how cybersecurity risks and incidents should be discussed under the existing disclosure rules, as well as examples of when disclosure may be required. Recognizing the growth in cybersecurity incidents, the SEC published **interpretive guidance** in 2018 to reinforce and expand upon the earlier Staff guidance, and to discuss the importance of disclosure controls and procedures in addressing cybersecurity risks and incidents, as well as the application of insider trading prohibitions and Regulation FD in the context of cybersecurity incidents. For more information on the 2018 interpretive guidance, refer to our **March 2018 Cooley alert**.

According to the SEC, while cybersecurity disclosures improved following the issuance of the interpretive guidance, the Staff had observed, among other things, that disclosures, in terms of content and timing, were inconsistent. Accordingly, the SEC has proposed these new rules to "enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies." Regardless of whether the proposed rules are adopted, the 2011 and 2018 interpretive guidance will remain in place.

Proposed rules

Cybersecurity incident reporting

Current reports

The proposed rules would add new Item 1.05 to Form 8-K, which would require disclosure within four business days after a company **has determined that** it has experienced a material cybersecurity incident, not discovery of such of incident. While the SEC stated that, in some cases, the date of discovery and the date of the company's materiality determination may be the same date, in other cases, it expects companies "to be diligent in making a materiality determination in as prompt a manner as feasible." To that end, it added an instruction to Item 1.05 that would provide that a company "shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." In many circumstances, a company may not be able to make such a determination until after a thorough investigation performed by a forensic firm on the company's systems.

In the proposing release, the SEC made clear that the "materiality" determination for cybersecurity incidents would remain consistent with existing case law – i.e., information is material if there is a substantial likelihood that a reasonable shareholder would consider this information important in making an investment decision, or if the information would have significantly altered the total mix of information made available.[1] The SEC also noted in the proposing release that a materiality analysis should take into consideration both quantitative and qualitative factors surrounding the cybersecurity incident.

In reporting a material cybersecurity incident, a company would be required to disclose, to the extent known at the time of filing:

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

While the SEC did not propose a definition for "cybersecurity,"[2] it did propose definitions for "cybersecurity incident," "cybersecurity threat" and "information systems," which would apply to disclosures required in Item 1.05 of Form 8-K and Item 106 of Regulation S-K.

- "Cybersecurity incident" would be defined 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."
- "Cybersecurity threat" would be defined as "any potential occurrence that may result in, an unauthorized effort to adversely affect the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."
- "Information systems" would be defined as "information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations."

The SEC provided a non-exclusive list of examples of cybersecurity incidents that may, if determined by a company to be material, require disclosure under Item 1.05 of Form 8-K, including:

- An unauthorized incident – whether stemming from accidental exposure of data or from a deliberate attack to steal or alter data

– that has compromised the confidentiality, integrity, or availability of an information asset (data, system or network), or violated the company's security policies or procedures.

- An unauthorized incident that caused degradation, interruption, loss of control, damage to or loss of operational technology systems.
- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the company.
- 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.

In the proposing release, the SEC stated that it would not expect any company 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 as would impede the registrant's response or remediation of the incident." Importantly, however, proposed Item 1.05 would not allow for a reporting delay when there is an ongoing internal or external investigation related to the cybersecurity incident, or where state laws would allow a company to delay providing public notice about a data breach incident or notifying certain constituencies of such an incident – even if law enforcement determines that notification would impede a civil or criminal investigation.

In addition, disclosure under Item 1.05 on Form 8-K would be required to be filed, rather than furnished, with the SEC, but an untimely filing would **not** impact a company's eligibility to use registration statements on Form S-3. A failure to file an Item 1.05 disclosure on Form 8-K would be subject to the limited safe harbor from liability under Section 10(b) and Rule 10b5-1 in Rules 13a-11(c) and 15d-11(c) under of the Securities Exchange Act of 1934.

Periodic reports

The proposed rules would add new Item 106(d) to Regulation S-K, which would add material cybersecurity incident disclosure obligations in quarterly reports on Form 10-Q and annual reports on Form 10-K.

1. **Material updates:** Under the proposed rules, companies would be required to disclose in Form 10-Q and Form 10-K any material changes, additions or updates to the information disclosed under Item 1.05 of Form 8-K that had occurred within the applicable reporting period (which is the fourth fiscal quarter in the case of an annual report). Under this proposed rule, the SEC included the following non-exclusive examples of the types of disclosure that should be provided, if applicable:
    a. Any material effect of the incident on the company's operations and financial condition.
    b. Any potential material future impacts on the company's operations and financial condition.
    c. Whether the company has remediated or is currently remediating the incident.
    d. Any changes in the company's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.
2. **Material in the aggregate:** Companies also would be required to disclose when a series of individually immaterial cybersecurity incidents become material in the aggregate. Accordingly, the SEC stated that companies "would need to analyze related cybersecurity incidents for materiality, both individually and in the aggregate." Under this proposed rule, companies would be required to disclose, to the extent known to management:
    a. A general description of when the incidents were discovered and whether they are ongoing.
    b. A brief description of the nature and scope of the incidents.
    c. Whether any data was stolen or altered in connection with the incidents.

d. The effect of the incidents on the company's operations.

e. Whether the company has remediated or is currently remediating the incidents.

Risk management, strategy and governance reporting

The proposed rules would add new Items 106(b) and (c) of Regulation S-K, which would require companies to disclose in an annual report on Form 10-K matters related to cybersecurity risk management and strategy, board oversight of cybersecurity risk, and management's role in assessing and managing cybersecurity risk, and implementing the company's cybersecurity policies, procedures and strategies.

Risk management and strategy

With respect to risk management and strategy, companies would be required to describe their policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including, but not limited to, 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. The proposed rule provides that disclosure should include, as applicable, a discussion of whether:

- The company has a cybersecurity risk assessment program and, if so, a description of the 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, but not limited to, those providers that have access to the company's customer and employee data. If so, the company must describe these policies and procedures, 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. If so, the company must provide a description of the types of activities undertaken.
- The company has business continuity, contingency and recovery plans in the event of a cybersecurity incident.
- Previous cybersecurity incidents informed changes in the company's governance, policies and procedures, or technologies.
- Cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the company's strategy, business model, 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

1. **Board oversight:** Under the proposed rules, companies would be required to describe the board's oversight of cybersecurity risk, including, as applicable:
   a. Whether the entire board, specific board members or a board committee is responsible for the oversight of cybersecurity risks.
   b. The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic.
   c. Whether and how the board or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.
2. **Management's role:** Companies also would be required to describe management's role in assessing and managing cybersecurity-related risks, its relevant expertise, and its role in implementing the company's

relevant policies, procedures and strategies, including, but not limited to, the following information:

a. 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 in such detail as necessary to fully describe the nature of the expertise.

b. Whether the company has a designated chief information security officer or someone in a comparable position and, if so, to whom that individual reports within the company's organizational chart, and the relevant expertise of any such persons in such detail as necessary to fully describe the nature of the expertise.

c. The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents.

d. 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.

In determining the "relevant expertise" of a person for purposes of the governance-related disclosures, the SEC has proposed to add an instruction Item 106(c) that would explain that this may include, for example, prior work experience in cybersecurity, any relevant degrees or certifications, or any knowledge, skills or other background in cybersecurity.

Board of directors' cybersecurity expertise

In addition to the cybersecurity incident and cybersecurity governance reporting discussed above, the proposed rules would add new paragraph (j) to Item 407 of Regulation S-K, which would require certain disclosures about the cybersecurity expertise (if any) of members of the company's board of directors. This disclosure would be required in Part III, Item 10 of annual reports on Form 10-K, and pursuant to Item 7(b) of Schedule 14A when action is to be taken with respect to the election of directors in annual meeting proxy statements.

Under the proposed rules, the company would be required to disclose the name(s) of any such director(s) and provide detail as needed to fully describe the nature of the expertise. In determining whether any director has expertise, the proposed rules provide that the company should consider, among other things:

- 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.

Similar to audit committee financial experts, directors designated as having cybersecurity expertise would be subject to a safe harbor pursuant to which they would not be deemed an expert for any purpose, including, without limitation, Section 11 of the Securities Act of 1933, nor would designating this person as having cybersecurity expertise impose any duties, obligations or liability greater than such as are imposed on that individual as a member of the board of directors, absent that designation.

Structured data

Under the proposed rules, companies would be required to tag information specified in Item 1.05 of Form 8-K and Items 106 and

407(j) of Regulation S-K in Inline XBRL format, using block text tagging for narrative disclosures, and detail tagging for any quantitative amounts disclosed within the narrative disclosures. (There are no explicit quantitative disclosure requirements in the proposed rules, but companies may nonetheless disclose quantitative amounts.)

Foreign private issuers

The proposed rules would apply similarly to foreign private issuers, subject to certain differences as a result of different reporting requirements. FPIs are not required to file current reports on Form 8-K; however, the SEC has proposed adding "cybersecurity incidents" as a reporting topic under Form 6-K that may trigger the filing of a Form 6-K. In addition, the SEC has proposed adding new Item 16J to annual reports on Form 20-F, which would require cybersecurity disclosures that are consistent with the requirements in Items 106 and 407(j) of Regulation S-K discussed above, but did not propose to make these disclosures applicable to Form 40-F filings.

Observations and commentary

- **Review existing cybersecurity-related policies and procedures.** Notwithstanding this early stage of rulemaking – and given the increased congressional and regulatory focus on cybersecurity matters – companies would be wise to get a head start on reviewing their existing cybersecurity-related policies, procedures, controls, and incident response measures in light of the proposed rules and each company's own threat environment. The SEC is proposing a sweeping disclose-what-you-do framework that would require companies to disclose their cybersecurity policies and procedures. With the increased scrutiny this disclosure may draw from the SEC and investors, public companies and companies looking to go public in the near term should assess or reassess, as the case may be, their policies and procedures relating to cybersecurity. Companies that do not have cybersecurity policies and procedures may want to consider the impact of this new proposed reporting framework, and whether to work toward designing and implementing cybersecurity policies and procedures. Companies that have cybersecurity policies and procedures may want to think about how they would disclose and describe these policies and procedures, and whether any updates to these policies and procedures may be desirable in response to any of the features highlighted in the proposed rules, such as oversight of cybersecurity risks relating to third-party service providers.
- **Review existing governance structure and risk management framework in relation to cybersecurity matters.** Companies may also want to review their current governance structure and risk management framework in relation to cybersecurity matters in light of their own threat environment. This review may include assessing whether any updates may be desirable in relation to cybersecurity oversight at the board or committee level, and in relation to management's role in assessing and managing cybersecurity risks. In addition, companies may elect to implement additional policies and procedures (1) to ensure that cybersecurity is receiving sufficient attention, including ensuring timely communications are made on material cybersecurity matters, and that adequate time is dedicated to such discussions at the board or committee level, and (2) that address the areas highlighted in the proposed rules, such as frequency of discussions at the board or committee level, and information related to management expertise and reporting structures. For companies where cybersecurity matters are mission-critical risks, the company should consider tailoring its governance structure and risk management framework to appropriately reflect the heightened importance that is placed on these matters from a board oversight and fiduciary duties perspective.
- **Review existing disclosures and board expertise.** Companies may also want to review their existing disclosures relating to the board's role in risk oversight as required under Item 407(h) of Regulation S-K, as well as any board skills matrices or disclosures relating to board expertise or knowledge relating to cybersecurity matters. If the rules are adopted as proposed, companies will want to ensure that any director who has previously been identified in a board skills matrix or otherwise as having cybersecurity knowledge is sufficiently qualified to be named as having cybersecurity expertise under the new rules. As part of this review – and if the rules are adopted as proposed – companies could consider adding questions to their D&O questionnaires that are similar to the questions regarding the qualification of audit committee financial experts. Companies that do not have cybersecurity expertise on their board or do not have cybersecurity expertise that would qualify under the proposed rules may feel pressure to prioritize this expertise in searches for new director candidates. Consequently, director candidates with cybersecurity expertise may find themselves in higher demand.
- **Assess disclosure controls and procedures as they relate to cybersecurity incidents and disclosure.** While the 2018

interpretive guidance encouraged companies to assess the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure, companies may want to review their existing disclosure controls and policies with a view toward the proposed rules that would require mandatory reporting for material (whether individually or in the aggregate) cybersecurity incidents to ensure that the appropriate channels are in place so relevant information about cybersecurity incidents is processed and reported to appropriate personnel to make disclosure decisions.

- **Be prepared to regularly review and update cybersecurity incident disclosures.** Under the proposed rules, if a company were to determine that a cybersecurity incident is material "as soon as reasonably practicable after discovery of the incident" – and therefore trigger a disclosure obligation under Item 1.05 of Form 8-K – the company would need to be prepared to disclose any material changes, additions, or updates to the information disclosed previously on the Form 8-K in its periodic and annual reports. In addition, the SEC has stated that "there may be situations where a registrant would need to file an amended Form 8-K to correct disclosure from the initial Item 1.05 Form 8-K, such as where that disclosure becomes inaccurate or materially misleading as a result of subsequent developments regarding the incident." Practically speaking, given the complexity and duration of cybersecurity incident investigations, it might take weeks or months for a company to understand the full scope and impact of such an incident. As additional material facts come to light during such an investigation, companies should be prepared to regularly review and, depending on the circumstances, update existing cybersecurity incident disclosures – even before the next periodic or annual report – to avoid having outdated information in the public domain.

---

1. See *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976); see also *Basic Inc. v. Levinson*, 485 U.S. 224, 232 (1988).
2. In its request for comment, the SEC inquired whether defining "cybersecurity" would be helpful, and stated that it could define the term as "any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat."

Key Contacts

Brad Goldberg New York	bgoldberg@cooley.com +1 212 479 6780
Chadwick Mills San Francisco	cmills@cooley.com +1 650 843 5654

Jason Kent New York	jkent@cooley.com +1 212 479 6044
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018