Cooley

SEC Adopts Comprehensive Cybersecurity Disclosure Requirements

August 2, 2023

On July 26, 2023, the Securities and Exchange Commission (SEC) voted at an open meeting to adopt **final rules to mandate standardized cybersecurity disclosures by public companies**. The final rules will:

- Require a company to disclose specified material information about a material cybersecurity incident under new Item 1.05 of Form 8-K within four business days of the company making the determination that the cybersecurity incident was material, subject to a narrow exception for disclosures that would pose a substantial risk to national security or public safety. An instruction to Item 1.05 will require a company to make their materiality determinations "without unreasonable delay," while an additional instruction will require a company to include a statement identifying any required information that is not determined or unavailable at the time of the required filing, and then file an amendment to the initial Item 1.05 Form 8-K containing such information within four business days after such information becomes available.
- Require annual disclosure in reports on Form 10-K pursuant to Item 106 of Regulation S-K regarding:
  - A company's processes, if any, for assessing, identifying and managing material risks from cybersecurity threats.
  - Whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect a company's business strategy, results of operations or financial condition.
  - The board of directors' oversight of risks from cybersecurity threats.
  - Management's role in assessing and managing material risks from cybersecurity threats.

The final rules will become effective 30 days after publication in the Federal Register. Companies other than smaller reporting companies will be required to comply with the incident disclosure requirements in Item 1.05 of Form 8-K on the later of 90 days after the date of publication of the adopting release in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days and will be required to comply with Item 1.05 on the later of 270 days from publication of the adopting release in the Federal Register or June 15, 2024. All companies will be required to comply with the annual disclosure requirements in Item 106 of Regulation S-K beginning with annual reports for fiscal years ending on or after December 15, 2023. Therefore, for calendar year-end companies, the first report requiring compliance with Item 106 will be the Form 10-K for the 2023 fiscal year filed in 2024.

The following table compares at a high level the requirements proposed versus those adopted in the final rules.

Item	**Proposed requirement**	**Adopted requirement**
Form 8-K Item 1.05 – **Material cybersecurity incidents**	Companies would be required to disclose any cybersecurity incident they experience that is	Companies must disclose any cybersecurity incident they experience that is determined to be material and describe the **material** aspects of its:

	determined to be material and disclose, to the extent known at the time of filing: ▪ 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. An Item 1.05 Form 8-K would be required to be filed within four business days of determining an incident was material.	▪ Nature, scope and timing. ▪ Impact, or reasonably likely impact, on the company, including its financial condition and results of operations. An Item 1.05 Form 8-K must be filed within four business days of determining an incident was material, subject to a narrow exception if disclosure would pose a substantial risk to national security or public safety. To the extent information required by Item 1.05 is not determined or is unavailable at the time of the required filing, companies must include a statement to that effect, and then file an amendment to the initial Form 8-K to disclose such information within four business days after determining such information or after such information becomes available. An untimely filing of an Item 1.05 8-K will not result in a loss of Form S-3 eligibility.
Regulation S-K Item 106(d) –**Updated incident disclosure**	Companies would be required to quarterly disclose in Forms 10-Q and 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. ▪ When a series of individually immaterial cybersecurity incidents become material in the aggregate.	Removed. Note: The definition of "cybersecurity incident" was extended to "a series of related unauthorized occurrences," which would still require companies to aggregate incidents under certain circumstances.

Regulation S-K Item 106(b) – **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, other litigation and legal risk, and reputational risk.	Companies must describe their processes, if any, for the assessment, identification and management of material risks from cybersecurity threats and describe whether any risks from cybersecurity threats have materially affected, or are reasonably likely to materially affect, their business strategy, results of operations or financial condition.
Regulation S-K Item 106(c) – **Governance**	Companies would be required to: ▪ Describe the board's oversight of cybersecurity risks. ▪ Describe management's role in assessing and managing cybersecurity-related risks, as well as its role in implementing the company's cybersecurity policies, procedures and strategies.	Companies must: ▪ Describe the board's oversight of risks from cybersecurity threats. ▪ Describe management's role in assessing and managing **material** risks from cybersecurity threats.
Regulation S-K Item 407(j) – **Cybersecurity expertise**	Companies would be required to disclose the cybersecurity expertise (if any) of members of the company's board.	Removed.

Please see the **SEC's press release** for the final rules and the **condensed fact sheet** for further details. For more background on the final rules and information on the SEC commissioners' views and statements regarding the rules, which passed by a vote of 3 – 2 along party lines, see our **July 2023 PubCo blog post**.

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 and Regulation S-X that may require disclosure with respect to cybersecurity matters – such as risk factors, management's discussion and analysis of financial condition and results of operations, description of business, legal proceedings, board leadership structure and role in risk oversight, financial statements, and disclosure controls and procedures.

In 2011, the SEC's Division of Corporation Finance (Corp Fin) 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 additional interpretive guidance in 2018** to reinforce and expand upon the earlier Corp Fin staff (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 **this March 2018 Cooley client 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 adopted these final rules. Despite adoption of the final rules, however, the 2011 and 2018 interpretive guidance will remain in place.

Final rules

Cybersecurity incident reporting

The final rules add new Item 1.05 to Form 8-K, which requires disclosure of material cybersecurity incidents within four business days of the company making the determination that the cybersecurity incident is material – not discovery of such incident. In a change from the stricter language proposed, an instruction to Item 1.05 will require companies to make their materiality determinations "without unreasonable delay." Notably, the disclosure requirement also applies to cybersecurity incidents on third-party systems a company uses that have a material impact on the company.

In the adopting release, the SEC made clear that the "materiality" determination for cybersecurity incidents will 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 release also notes that a materiality analysis should take into consideration qualitative factors alongside quantitative factors in assessing the materiality of the cybersecurity incident, such as "harm to a company's reputation, customer or vendor relationships, or competitiveness," or the "possibility of litigation or regulatory investigations or actions." In many circumstances, a company may not be able to make such a determination until after a thorough investigation is performed by a forensic firm on the company's systems.

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

1. The material aspects of the nature, scope and timing of the incident.
2. The material impact, or reasonably likely material impact on the company, including its financial condition and results of operations.

New Item 1.05 also will include an instruction providing that to the extent any required information is not determined or is unavailable at the time of the required filing, a statement to this effect should be included in the initial Form 8-K followed by an amendment to the Form 8-K with this missing information within four business days after the information becomes available or is determined by the company, "without unreasonable delay."

In addition, new Item 1.05 will include an instruction providing that a company does not need to "disclose specific or 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, the final rules allow for a delayed filing under Item 1.05 in cases where the US attorney general has notified the SEC in writing that the disclosure poses a substantial risk to national security or public safety. Initially, the delay would only last for a time period specified by the attorney general, up to 30 days following the date when the disclosure was otherwise required. The delay may be extended for an additional 30 days if the attorney general determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC in writing.

In "extraordinary circumstances," disclosure may be delayed for a further 60 days if the attorney general determines that disclosure continues to pose a substantial risk to national security and notifies the SEC in writing. Beyond these 120 days of potential delay, if the attorney general indicates that further delay is necessary, the SEC will consider additional requests and grant any relief through an SEC exemptive order. However, Item 1.05 will not allow for a reporting delay for other federal agencies or non-federal law enforcement agencies. In addition, note that this provision does not relieve a company of its obligations under other securities laws, such as Regulation FD.

There is an additional narrow delay provision when the disclosure would conflict with a Federal Communications Commission (FCC) rule for breaches of customer proprietary network information. This provision allows for a delayed filing of the Item 1.05 Form 8-K up to the seven-business day period following the required notifications specified in the applicable FCC rule, with written notification to the SEC via an EDGAR correspondence filing no later than the date when the disclosure would have otherwise been required under Item 1.05. However, the final rules do not provide for a delay where the incident may be subject to any other federal requirements or regulators.

While the SEC did not adopt a definition for "cybersecurity," it did include 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" is defined as "an unauthorized occurrence, or a series of related unauthorized occurrences, 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."
    - The SEC reiterated in the adopting release that, in general, it "believe[s] that an accidental occurrence is an unauthorized occurrence," and that an accidental occurrence may therefore be a cybersecurity incident under its definition, "even if there is no confirmed malicious activity."
- "Cybersecurity threat" is defined as "any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity or availability of a registrant's information systems or any information residing therein."
- "Information systems" are defined as "electronic 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."

Lastly, disclosure under Item 1.05 on Form 8-K will be required to be filed, rather than furnished, with the SEC, but an untimely filing will **not** impact a company's eligibility to use registration statements on Form S-3. Further, the final rules amended Rules 13a-11(c) and 15d-11(c) under the Securities Exchange Act of 1934 (Exchange Act) to include new Item 1.05 disclosure in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) and Rule 10b-5 under the Exchange Act of 1934

Risk management, strategy and governance reporting

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

Risk management and strategy

With respect to risk management and strategy, a company will be required to describe its processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The final rules provide that this disclosure should include, as applicable, a discussion of:

- Whether and how the described cybersecurity processes have been integrated into the company's overall risk management system or processes.
- Whether the company engages assessors, consultants, auditors or other third parties in connection with any of these processes.
- Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

The final rules also clarify that this list is nonexclusive, and that companies should also disclose whatever information is necessary, based on their facts and circumstances, for a reasonable investor to understand their cybersecurity processes.

In addition, the final rules will require companies to disclose "[w]hether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how."

Governance

1. Board oversight: Under the final rules, companies will be required to:
    a. Describe the board's oversight of risks from cybersecurity threats.
    b. If applicable, identify the board committee or subcommittee responsible for this oversight of risks from cybersecurity threats.
    c. Describe the processes by which the board or this committee is informed about these risks.
2. Management's role: Companies also will be required to describe management's role in assessing and managing material risks from cybersecurity threats. In crafting this description, the final rules direct companies to consider including, but not limited to, disclosure of the following information:
    a. Whether and which management positions or committees are responsible for assessing and managing these risks, and the relevant expertise of such persons or members in enough detail as necessary to fully describe the nature of the expertise.
    b. The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents.
    c. Whether such persons or committees report information about these risks to the board or a committee or subcommittee of the board.

In determining the "relevant expertise" of a person for purposes of the governance-related disclosures, the final rules add an instruction to Item 106(c) that explains 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.

Structured data

Under the final rules, companies will be required to tag information specified in Item 1.05 of Form 8-K and Item 106 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 final rules, but companies may nonetheless disclose quantitative amounts if material.) Compliance with the Inline XBRL requirements will be required one year after initial compliance with the related disclosure requirement, described above.

Foreign private issuers

The final rules apply similarly to foreign private issuers (FPIs), subject to certain differences as a result of the different reporting regimes. FPIs are not required to file current reports on Form 8-K; however, the final rules add "material cybersecurity incidents" as a reporting topic under Form 6-K that may trigger the filing of a Form 6-K. In addition, the final rules add new Item 16K to annual reports on Form 20-F, which will require cybersecurity disclosures that are consistent with the requirements in Item 106 of Regulation S-K discussed above, but these disclosure requirements were not added to Form 40-F filings.

For reporting material cybersecurity incidents on Form 6-K, if triggered, FPIs will be required to comply on the later of 90 days after the date of publication of the adopting release in the Federal Register or December 18, 2023. FPIs must comply with the annual disclosure requirements in Item 16K beginning with annual reports for fiscal years ending on or after December 15, 2023. Therefore, for calendar year-end companies, the first report requiring compliance will be the Form 20-F for the 2023 fiscal year filed in 2024.

Observations and commentary

- **The final rules make changes from the initial proposal in mostly welcome ways.** The final rules make changes from the proposed rules in ways that streamline the disclosure requirements and better mitigate the possibility that the disclosures provide additional information to threat actors and expose the company to additional cybersecurity incidents. In this regard, the final rules focus the disclosure on the impacts of a material cybersecurity incident, rather than on specific details regarding the incident itself. The new delaying provision for national security and public safety also may benefit some companies, though it has a narrow application, and the release was not clear about how companies would contact the attorney general for this determination. In addition, while the final rules removed the requirement for companies to provide quarterly disclosure in Form 10-Qs (or Form 10-Ks for the fourth quarter) regarding updates with respect to previously disclosed incidents or disclosure when a series of individually immaterial cybersecurity incidents become material in the aggregate, separate incidents may still need to be aggregated given the extension of the definition of "cybersecurity incident" to "a series of related unauthorized occurrences."

  In another helpful change, the disclosures required under Item 106 related to risk management, strategy and governance were streamlined from the proposal and provide companies with more flexibility in disclosing their cybersecurity processes, although these disclosures will still require careful consideration when drafting. Lastly, the final rules removed the proposed addition of the requirement to disclose the cybersecurity expertise of a company's board. While leaving this requirement out of the final rules provides companies with more flexibility in determining how they would like to manage and disclose this expertise, this disclosure is still requested by proxy advisory firms and many institutional investors, and disclosure regarding the expertise of management or committees responsible for assessing and managing cybersecurity risks is still required under the final rules.
- **Review existing cybersecurity-related processes and internal controls.** Companies should promptly conduct a legally privileged review of their existing cybersecurity-related policies, procedures, controls and incident-response measures in light of the final rules and each company's own threat environment. We note that conducting such reviews under legal privilege, where possible, is highly advised, as such reviews often identify issues that should be addressed. The final rules include an extensive disclose-what-you-do framework that will require companies to disclose their cybersecurity processes. 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 – how they identify and manage cybersecurity risks.

Companies that do not have cybersecurity processes should consider the impact of this new reporting framework and should work toward designing and implementing them. Companies that do have cybersecurity processes for assessing, identifying and managing cybersecurity risks should reflect on how they will disclose and describe those processes and whether any updates may be advisable in response to any of the features highlighted in the final rules. In addition, for companies that have not yet done so, now is the time to closely evaluate whether there are any gaps in their control environment and implement additional controls where needed, which should also occur going forward on a regular basis. Recent SEC enforcement actions have applied the internal control provisions of the Exchange Act expansively to include policies and procedures concerning the disclosure of cybersecurity incidents. This trend – combined with the incident disclosure requirements in the final rules – makes it even more critical that companies have internal controls and processes in place for identifying and reporting cybersecurity incidents.

- **Review existing governance structure and risk management framework in relation to cybersecurity matters.** Companies also should undertake a legally privileged review of 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 advisable in relation to cybersecurity oversight at the board or committee level, and in relation to management's role in assessing and managing cybersecurity risks. While many companies have assigned cybersecurity oversight to the audit committee, the publication of these rules may be a good occasion to consider whether this delegation is aligned with the committee members' expertise and is appropriate in light of the bandwidth of each board committee. In addition, companies may elect to implement additional processes to ensure that cybersecurity is receiving sufficient attention – including ensuring timely communications are made on material cybersecurity matters and adequate time is dedicated to such discussions at the board or committee level – and that address the areas highlighted in the final rules, such as management reporting to the responsible board or committee 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. Some best practices in this regard include, among many others:

  - Ensuring that the board is regularly and adequately informed regarding the company's cybersecurity risk management and incident-response preparedness.
  - Implementing a direct reporting line from the chief information security officer to the board.
  - Documenting the board's role in and oversight of the cybersecurity and incident response program.
  - Modernizing applications and overall IT systems.
  - Conducting regular threat assessments and mock breach exercises.
  - Approving a written security road map for enhancing cybersecurity oversight, which should be continuously reassessed to confirm its ongoing efficacy.

  Lastly, the requirement to discuss management's expertise may well increase demand for chief information officers and chief information security officers, so companies considering hiring for these positions are advised to act promptly. In addition to soliciting new disclosures on cybersecurity risk management, similar to the proposed climate disclosure rules, the final rules ask for discussion of the integration of cybersecurity processes into overall risk management systems. For many companies, any such discussion would be their first substantive public disclosure regarding their enterprise risk management processes. As a result, companies may want to consider how they will disclose and describe these processes and evaluate the robustness and formality of their general risk management systems and related stakeholder expectations.

- **Review existing disclosures and board expertise.** Companies should review their existing disclosures relating to the board's role in risk oversight as required under Item 407(h) of Regulation S-K. In addition, despite the removal of the requirement to describe the board's cybersecurity expertise, many investors still expect board skills matrices and disclosures concerning board expertise or knowledge relating to cybersecurity matters. Therefore, in order to gather this information, companies should consider adding questions to their directors and officers 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 may feel

pressure to prioritize this expertise in searches for new director candidates. Consequently, director candidates with cybersecurity expertise will likely continue to find themselves in high demand. In addition to identifying and recruiting directors with existing expertise, companies also should consider additional management and board education and training on cybersecurity matters, including disclosure requirements under the new rules.

- **Review incident response plans and playbooks as they relate to cybersecurity incident response, escalation, materiality 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 should review their existing disclosure controls and policies in light of the new mandatory reporting requirement for material (whether individually or in the aggregate) cybersecurity incidents to ensure that the appropriate channels are in place so that relevant information about cybersecurity incidents is processed and reported to appropriate personnel for making disclosure decisions. Given the four-day requirement from the date of determination of materiality, these controls should ensure the information flows in a timely manner to the disclosure decision-makers, while taking appropriate steps to preserve the legal privilege wherever possible. Appropriate personnel, including those in IT and information security, also should be made aware of these requirements and appropriately and regularly trained. Companies also should assess their processes for the evaluation of incident materiality. In connection with this, companies should consider business-specific factors that may impact materiality determinations and be prepared to articulate standards for incident materiality to the Staff.
- **Be prepared to regularly review the evolving impacts of cybersecurity incidents to determine if current or periodic disclosure is appropriate.** Under the final rules, a company's materiality determination regarding a cybersecurity incident must be made "without unreasonable delay" after discovery of the incident. In addition, to the extent that information required by Item 1.05 of Form 8-K is not determined or is unavailable at the time of the required filing, companies are required to include a statement to this effect, and then file an amendment to the initial Item 1.05 8-K containing such information within four business days after the company, "without unreasonable delay," determines such information, or within four business days after such information becomes available.

  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. The SEC stated in the adopting release that, other than with respect to the previously undetermined or unavailable information referenced in the initial Form 8-K filing, the final rules "do not separately create or otherwise affect a registrant's duty to update its prior statements." As a practical matter, however, and as additional material facts come to light during such an investigation, companies should be prepared to regularly review and, depending on the circumstances, consider whether to update existing cybersecurity incident disclosures – even before the next periodic or annual report – to avoid having outdated information in the public domain or having the accuracy or completeness of their initial disclosures questioned. Companies also should continue to review and enhance their broader Forms 10-K and 10-Q disclosures in light of any material cybersecurity incidents to ensure the description of risks remains fulsome and accurate. In this respect, we expect that, in practice, companies that have previously disclosed material incidents may find it necessary to discuss those incidents and updates thereto on a quarterly basis, including in management discussion and analysis, legal proceedings, risk factors and notes to financial statements, as applicable.
- **24/7 incident response team.** In the event of a suspected data incident, members of Cooley's data incident and breach response team can be reached at any time using the contact information below.

Cooley Breach Hotline
cyber/data/privacy

incident.response@cooley.com
(844) 476-1248 Work
(415) 693-2888 Work

Notes

1. See *TSC Indus. v. Northway*, 426 US 438, 449 (1976); see also *Basic Inc. v. Levinson*, 485 US 224, 232 (1988).

Key Contacts

Brad Goldberg New York	bgoldberg@cooley.com +1 212 479 6780
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Amanda Weiss New York	alweiss@cooley.com +1 212 479 6858
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018
Sarah Sellers New York	ssellers@cooley.com +1 212 479 6370
Christian Lee San Francisco	christian.lee@cooley.com +1 415 693 2143
Michael Mencher San Francisco	mmencher@cooley.com +1 415 693 2266
Beth Sasfai New York	bsasfai@cooley.com +1 212 479 6081
Reid Hooper Washington, DC	rhooper@cooley.com +1 202 776 2097

Stephanie Gambino Seattle	sgambino@cooley.com +1 206 452 8748