GUNDERSON DETTMER

SEC Adopts Mandatory Cybersecurity Disclosure Framework for Public Companies

Insights
September 28, 2023

New rules require enhanced and standardized disclosures related to cybersecurity for nearly all public companies.

Current reporting about material cybersecurity incidents within four business days is required beginning in December 2023 (June 2024 for smaller reporting companies). Annual reporting about cybersecurity risk management, strategy and governance is required beginning with the next Form 10-K for all calendar-year-end companies.

On July 26, 2023, a divided U.S. Securities and Exchange Commission (SEC or Commission) voted 3-2 to require enhanced and standardized disclosures related to cybersecurity for public companies, including emerging growth companies (EGCs), smaller reporting companies (SRCs) and foreign private issuers (FPIs).

In summary, the final rules mandate:

- Form 8-K disclosure of material cybersecurity incidents within four business days of determining the incident's materiality; and

- Form 10-K disclosure of cybersecurity risk management, strategy and governance practices, including company cybersecurity risk management processes, and the roles of management and the board of directors in cybersecurity oversight and governance.

The SEC's adopting release is available here, related Fact Sheet here and Small Entity Compliance Guide here. Gunderson Dettmer has also prepared a two-page quick reference guide summarizing the most significant aspects of the final rules, which is available here.

If you have any questions or would like assistance in complying with the new cybersecurity disclosure requirements discussed in this client alert, please reach out to your regular Gunderson Dettmer attorney or any member of our Public Companies or Data Privacy and Cybersecurity practice teams.

Key Compliance Dates

Form 8-K Disclosure

All companies other than SRCs must comply with the Form 8-K incident reporting req beginning on or after **December 18, 2023**.

SRCs must comply with the Form 8-K incident reporting requirements beginning on o **2024**.

Form 10-K Disclosure

All companies (including SRCs) must comply with the Form 10-K risk management, s governance disclosure requirements beginning with annual reports for **fiscal years e after December 15, 2023** (meaning, for calendar-year-end companies, the fiscal 202 filed in 2024).

Inline XBRL

Inline XBRL tagging must begin one year after the initial compliance dates described

What to Do Now

The new disclosure obligations will increase the time and cost of compliance; regulatory, investor and other stakeholder scrutiny; and reputational, enforcement and litigation risks. To prepare, in addition to becoming familiar with the new disclosure rules—which we summarize below—public companies can take the following practical steps:

Preparing for New Form 8-K Disclosures

- Review what internal disclosure controls and procedures are in place or should be adopted to ensure that information concerning cybersecurity incidents is timely escalated to the team responsible for making SEC disclosure decisions (and special trading blackout decisions under the insider trading policy).

    - *An accurate materiality determination needs to be made "without unreasonable delay" following detection of the incident, and any required Form 8-K disclosures must be made within four business days of the determination.*

- Determine who will make the materiality determination (the board, a board committee or certain company officer(s)), and identify who will be involved in the disclosure process (e.g., cybersecurity, financial reporting, legal and other professionals).

- Establish or enhance controls and procedures for ongoing updates, as necessary, to any cybersecurity incident disclosed in a Form 8-K, such as for previously undetermined or unavailable information, additional material facts, changes in the incident's impact, or other corrections or updates.

- Include processes for tracking and evaluating potentially related or similar incidents that individually are not material but cumulatively may have a (quantitative or qualitative) material impact.

- Confirm disclosure controls and procedures account for protecting privilege, where appropriate.

- Review incident response and notification guidelines to update as necessary for the new disclosure obligations and timelines.

- Consider scheduling a tabletop exercise to test and assess preparedness and readiness to make disclosure decisions and meet disclosure timelines.

Preparing for New Form 10-K Disclosures

- Consider how company cybersecurity risk management processes will be disclosed, and whether any adjustments to those processes may be necessary or advisable in light of the enhanced transparency.

- Evaluate existing cybersecurity governance and reporting structures at the board and management levels, including updating board committee charters, as necessary, to ensure board oversight duties are clearly delineated.

- Confirm the board or appropriate board committees receive regular updates from management and outside advisors (as relevant) regarding cybersecurity matters, and that such updates are memorialized in board and/or committee minutes.

- Assess the cybersecurity expertise of members of management responsible for managing cybersecurity risks, and consider how to support or, as necessary, supplement that expertise.

    - *The final version of the rules dropped the proposed requirement to identify board-level cybersecurity expertise, instead requiring disclosure of management's expertise in managing cybersecurity risks.*

- Ensure the new Form 10-K disclosures are consistent with any existing disclosures about cybersecurity in other SEC filings and corporate sustainability reports.

- Consider adding a cybersecurity team member to the disclosure committee.

Form 8-K Disclosure of Material Cybersecurity Incidents

The final rules amend Form 8-K to add new Item 1.05, which requires companies to disclose the following information about a material "cybersecurity incident" **within four business days after the company determines the incident is material** (rather than within four business days after discovery of the incident, though the two dates may coincide):

- The material aspects of the nature, scope and timing of the incident; and

- The material impact or reasonably likely material impact on the company, including its financial condition and results of operations.

The SEC notes that inclusion of the phrase “financial condition and results of operations” is not meant to be exclusive, and that **companies should consider qualitative factors alongside quantitative factors in assessing the material impact of a cybersecurity incident**. The adopting release provides the following examples:

- Harm to a company’s reputation, customer or vendor relationships, or competitiveness may be examples of a **material impact** on the company.

- The possibility of litigation or regulatory investigations or actions may constitute a **reasonably likely material impact** on the company.

Information concerning the incident’s remediation status, when it was discovered, whether it is still ongoing and whether any data were compromised is not required under the final rules (as originally proposed), although the adopting release explains that disclosure about such items may be required if material: “While some incidents may still necessitate, for example, discussion of data theft, asset loss, intellectual property loss, reputational damage or business value loss, [companies] will make those determinations as part of their materiality analyses.”

An instruction to Form 8-K provides that a company need not 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 [its] response or remediation of the incident.”

Item 1.05 disclosures will be considered filed, not furnished, for purposes of liability under the Securities Exchange Act of 1934 (Exchange Act).

Broad Definition of Cybersecurity Incident

"**Cybersecurity incident**" is defined as "an unauthorized[1] 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 notes that what constitutes a "cybersecurity incident" should be construed broadly, encompassing a range of event types. The term "cybersecurity" is not separately defined.[2]

"**Information systems**" is defined as "electronic information resources, owned or used by[3] 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."

Materiality Determination

Timing

Companies are required to make a materiality determination regarding a cybersecurity incident "**without unreasonable delay after discovery of the incident**."[4] Although "without unreasonable delay" is not explicitly defined—and the final rules prescribe no specific timeline between the incident and the materiality determination—the SEC explains that "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance" with this requirement.

The SEC believes that although a company may not have complete information about an incident, it may know enough to determine whether the incident was material. Accordingly, "a company being unable to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the

need for continued investigation regarding the incident, should not delay the company from determining materiality." Other examples of what the SEC would consider an "unreasonable delay" provided in the adopting release include:

- "[I]f the materiality determination is to be made by a board committee, intentionally deferring the committee's meeting on the materiality determination past the normal time it takes to convene its members."[5]

- "[I]f a company were to revise existing incident response policies and procedures in order to support a delayed materiality determination for or delayed disclosure of an ongoing cybersecurity event, such as by:

  - extending the incident severity assessment deadlines,

  - changing the criteria that would require reporting an incident to management or committees with responsibility for public disclosures, or

  - introducing other steps to delay the determination or disclosure."

In addition, the adopting release clarifies that a company's decision to share information with other companies or government actors about emerging threats does not, in itself, constitute a determination of materiality triggering an Item 1.05 disclosure obligation: "A [company] may alert similarly situated companies as well as government actors immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for determining materiality." As such, a company's decision to comply with contractual or regulatory obligations to notify third parties of a cybersecurity incident or threat does not necessarily render that incident or threat "material" for purposes of triggering the Item 1.05 disclosure requirement.

Substance

What constitutes “materiality” for purposes of cybersecurity-related disclosure is consistent with the Supreme Court definition of materiality—i.e., information is material if “there is a substantial likelihood that a reasonable shareholder would consider it important” in making an investment decision, or if it would have “significantly altered the ‘total mix’ of information made available.”[6] The adopting release stresses, consonant with prior Commission guidance, that “[d]oubts as to the critical nature” of the relevant information “will be commonplace” and should “be resolved in favor of those the statute is designed to protect,” namely investors.[7]

As part of its materiality analysis, a company should take into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors. The adopting release states that “[a] lack of quantifiable harm does not necessarily mean an incident is not material” and provides the following examples:

- “[A]n incident that results in significant reputational harm to a [company] may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material.”

- “[W]hereas a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the [company] that results from the scope or nature of harm to individuals, customers or others, and therefore may need to be disclosed.”

- “[W]hen a [company] experiences a data breach, it should consider both the immediate fallout and any longer term effects on its operations, finances, brand perception, customer relationships, and so on, as part of its materiality analysis.”

Third-Party Cybersecurity Incidents

Cybersecurity incidents on a third-party system (e.g., cloud-based or hosted systems) may trigger the required Form 8-K disclosure. The adopting release notes the SEC has expressly determined not to exempt companies from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor to provide a safe harbor for information disclosed about third-party systems, citing companies' rapidly increasing reliance on third-party service providers for information technology services, including cloud computing technology, and the rising prevalence of third-party cybersecurity incidents.

The adopting release states that "the materiality of a cybersecurity incident is contingent neither on where the relevant electronic systems reside nor on who owns them, but rather on the impact to the [company]. We do not believe that a reasonable investor would view a significant data breach as immaterial merely because the data are housed on a cloud service."

The adopting release adds that "[d]epending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither." In light of reduced visibility into third-party systems, companies "should disclose based on the information available to them." While companies should ensure they maintain normal contact with their third-party service providers, the new rules "generally do not require that [companies] conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with [companies]' disclosure controls and procedures."[8]

Narrow, Time-Limited National Security/Public Safety Reporting Delay

Incident disclosure on Form 8-K may be delayed, initially for up to 30 days, if the U.S. Attorney General determines immediate disclosure would pose a "**substantial risk to national security or public safety**" and notifies the SEC of such determination in writing prior to the Form 8-K deadline. The delay may be extended for an additional 30-day period and (in extraordinary circumstances) for a final additional 60-day period in a similar fashion. To extend the delay beyond 120 days, the SEC must grant relief through an exemptive order.

Despite the objections of numerous commenters, this provision does not extend to other law enforcement authorities (such as state, local or foreign law enforcement) or when law enforcement believes disclosure will hinder their efforts to identify or capture the threat actor. The SEC notes in the adopting release that the final rules do not preclude other federal agencies or non-federal law enforcement agencies from requesting that the Attorney General determine that the disclosure poses a substantial risk to national security or public safety and communicate that determination to the SEC. However, it believes that designating the Department of Justice (DOJ) as the Commission's single point of contact on such delays "is critical to ensuring that the rule is administrable."

In addition, this delay provision does not relieve a company of its obligations under other federal securities laws, such as Regulation FD. Under Regulation FD, material nonpublic information related to cybersecurity incidents and risks disclosed to any investor (e.g., through investor outreach activities) would be required to be disclosed publicly, subject to limited exceptions.

The adopting release notes that the SEC and the DOJ have established an interagency communication process to allow for the Attorney General's determination to be communicated to the SEC in a timely manner. The DOJ will notify the affected company that communication to the SEC has been made, so that the company can delay its Form 8-K filing. No further details about this process are provided.[9]

As a practical matter, it is not clear how companies would contact the Attorney General for this determination or how feasible it will be to obtain the determination prior to the four-business-day Form 8-K reporting deadline. The DOJ is reportedly planning to issue clarifying guidance before year-end. We expect that such determinations from the Attorney General will be rare.

Consequences of Late Filings

As is the case with other Form 8-K disclosure items that require management to quickly assess the materiality of an event to determine whether a disclosure obligation has been triggered, the final rules provide that untimely disclosure of material cybersecurity incidents on Form 8-K will not result in the loss of Form S-3

eligibility and also will fall within the limited safe harbor from liability under Section 10(b) of the Exchange Act and Rule 10b-5 thereunder.

- **Eligibility to Use Form S-3**. The final rules amend the general instructions to Form S-3 to add new Item 1.05 to the list of Form 8-K items that, if untimely filed, do not result in the loss of eligibility to use Form S-3 registration statements, so long as Form 8-K reporting is current at the time the Form S-3 is filed.

- **Limited Safe Harbor from Exchange Act Section 10(b) and Rule 10b-5 Liability**. The final rules also amend Exchange Act Rules 13a-11(c) and 15d-11(c) to include new Item 1.05 in the list of Form 8-K items that are eligible for a limited safe harbor from public and private claims under Exchange Act Section 10(b) and Rule 10b-5 in the event of an untimely filing.

Updates to Previously Filed Form 8-K Disclosure

To the extent that any required information about a material cybersecurity incident is not determined or is unavailable at the time the company prepares the initial Item 1.05 Form 8-K, the company must include a statement to this effect in the filing and then file a Form 8-K amendment containing such information within four business days after such information is determined or becomes available (rather than disclosing such information in subsequent annual and quarterly reports, as proposed).

The SEC explains that updated reporting is not required for *all* new information and that, other than with respect to such previously undetermined or unavailable information, the final rules do not separately create an obligation to update prior statements in an earlier Item 1.05 Form 8-K. However, the SEC cautions that companies may still have (i) a *duty to correct* prior disclosure that they subsequently determine was misleading or untrue at the time it was made (for example, if the company later discovers contradictory information that existed at the time of the initial disclosure) or (ii) a *duty to update* prior disclosure that becomes materially inaccurate after it was made (for example, when the original statement is still being relied on by reasonable investors). Companies are advised to “consider whether they need to

revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident."

Aggregation of Related Immaterial Incidents

While the final rules omit the proposed requirement that companies disclose in their periodic reports individually immaterial cybersecurity incidents that become material when considered in the aggregate, they expand the proposed definition of "cybersecurity incident" for purposes of the Item 1.05 Form 8-K disclosure to capture "a series of related unauthorized occurrences" that collectively may have a (quantitatively or qualitatively) material impact, recognizing that cyberattacks sometimes compound over time, rather than present as a discrete event.

The adopting release underscores that when a company concludes it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact of each individual intrusion is by itself immaterial. While the SEC declined to explicitly define the term "related," the adopting release suggests events may be related if they involve, for instance, the same malicious actor or exploitation of the same vulnerability.[10]

Form 10-K Disclosure of Cybersecurity Risk Management, Strategy and Governance

The final rules amend Form 10-K to add new Item 106 of Regulation S-K, which requires companies to disclose detailed information about their cybersecurity risk management, strategy and governance practices.

In response to concerns voiced by commenters that the prescriptiveness of the rule proposal could be seen as an attempt to micromanage companies' cybersecurity defenses and constrain their risk management and strategy decision-making, the SEC asserts in the adopting release that "the purpose of the [new Item 106 disclosures] is, and was at proposal, to inform investors, not to influence whether and how companies manage their cybersecurity risk" or otherwise operate their cybersecurity programs. The SEC further emphasizes that the "final rules are

indifferent as to whether and to what degree a [company] may have identified and chosen to manage a cybersecurity risk" and that it seeks to "foreclose any perception that the rule prescribes cybersecurity policy."

Although the SEC declined to require Item 106 disclosures in registration statements, the adopting release reiterates the Commission's 2018 interpretive guidance that companies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure required in registration statements.

Risk Management and Strategy

Under new Item 106(b) of Regulation S-K, companies must describe:

- Their processes[11] (if any) for assessing, identifying and managing material risks from cybersecurity threats "in sufficient detail for a reasonable investor to understand those processes," including the following non-exclusive disclosure items (as applicable):
    - 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 such processes;[12]
    - Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider; and
- Whether and how 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 company, including its business strategy, results of operations or financial condition.

"**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."

While the final rules, to avoid being overly prescriptive, omit the specified types of risks from cybersecurity threats enumerated in the proposal (i.e., intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risk, and reputational risk), the SEC retains them in the adopting release as "guidance," noting that it continues to believe these are the types of risks companies may face in this context and thus may wish to keep in mind when drafting their disclosures.

Governance

Board Oversight

Under new Item 106(c)(1) of Regulation S-K, companies must describe the board of directors' oversight of risks from cybersecurity threats, including (as applicable):

- The identity of any board committee or subcommittee responsible for such oversight; and

- The processes by which the board or such committee is informed about such risks. [13]

No Requirement to Disclose Board Expertise

In a key departure from the draft rules, the SEC did not adopt the proposed requirement for companies to disclose whether any member of the board of directors has cybersecurity expertise and, if so, the director's name and a detailed description of the nature of their expertise. The adopting release notes that, after considering significant pushback during the public comment period, the SEC is "persuaded that effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise." The SEC adds that companies that deem board-level expertise to be a critical component of their cybersecurity risk management may choose to highlight that information if they wish. However, as discussed below, companies must disclose the "relevant expertise" of management or committees responsible for assessing and managing the company's material risks from cybersecurity threats.

Role of Management

Under new Item 106(c)(2) of Regulation S-K, companies must describe management's role, and relevant expertise, in assessing and managing material[14] risks from cybersecurity threats, including the following non-exclusive disclosure items (as applicable):

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members "in such detail as necessary to fully describe the nature of the expertise"; [15]

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

- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

Examples of relevant management expertise include prior work experience in cybersecurity; any relevant degrees or certifications; and any knowledge, skills or other background in cybersecurity.

Foreign Private Issuers

Comparable disclosure requirements will apply to FPIs on Forms 6-K and 20-F.

Inline XBRL

The new cybersecurity disclosures are required to be presented in Inline XBRL, including block-text tagging of narrative disclosures and detail tagging of any quantitative amounts disclosed within the narrative disclosures.

As noted above, compliance with the structured data requirements will be deferred for one year beyond initial compliance with the disclosure requirements.

Prior Disclosure Rules and SEC Investigation and Enforcement Background

Under the previous public company reporting framework, there were no SEC disclosure requirements that explicitly referred to cybersecurity risks or incidents, and cybersecurity disclosure conventions to date have varied widely across companies. Although the SEC acknowledged that companies' disclosures of both material cybersecurity incidents and cybersecurity risk management, strategy and governance practices have improved in terms of quality and frequency since the issuance of Commission-level cybersecurity guidance in 2018, which reinforced and expanded on the staff-level cybersecurity guidance published in 2011,[16] it believes under-

disclosure regarding cybersecurity persists and that “current cybersecurity reporting may be inconsistent, not timely, difficult to locate and contain insufficient detail.”

To address these concerns, the new cybersecurity disclosure framework substantially augments the Commission’s existing principles-based guidance with a precise set of detailed and prescriptive mandatory disclosure rules intended to elicit more timely, informative, consistent and comparable (in terms of both content and location) information that investors can use to better evaluate companies’ exposure to material cybersecurity incidents and risks as well as their ability to manage and mitigate those risks.

The new rules were adopted against the backdrop of the Commission’s intensified investigation and enforcement focus on public companies’ cybersecurity disclosures and related controls and procedures. Over the past two years, the SEC, in settled actions, has charged multiple companies with deficient cybersecurity disclosures, inadequate cybersecurity disclosure controls and procedures, and misleading disclosures that characterized actual cybersecurity incidents as merely hypothetical risks, including most recently in March (see, for example, here, here and here). Civil penalty amounts assessed in connection with the settlement of such cases have been increasing. In May 2022, the SEC nearly doubled the size of its Crypto Assets and Cyber Unit in the Division of Enforcement, which is expected to continue “to identify disclosure and controls issues with respect to cybersecurity” and bring enforcement actions in this area.

In June, SolarWinds Corporation disclosed that certain of its current and former executive officers and employees, including the chief financial officer and chief information security officer, have received Wells notices from the SEC enforcement staff, alerting them of potential civil enforcement actions stemming from the SEC’s investigation of a previously disclosed cyberattack. Also in June, the SEC Enforcement Director delivered remarks before an industry conference on enhancing cyber resiliency, in which he signaled the SEC is taking an aggressive stance against public companies that fail to take the right steps after experiencing a cyber incident, and articulated several principles that guide the Commission’s work to ensure public companies “take their cybersecurity and disclosure obligations seriously.”

Notable Changes from Proposed Rules

In response to commenters' concerns, the final rules reflect several significant changes to the March 2022 rule proposal (discussed in-depth in our earlier client alert here), including:

- Narrowing the scope of required disclosure about a material cybersecurity incident, to focus primarily on the material impacts of the incident rather than on details of the incident itself;
- Adding a limited (up to 120 days) delay in reporting where disclosure would implicate national security or public safety concerns, as determined by the U.S. Attorney General;
- Delaying SRCs' required compliance date for the Form 8-K incident disclosures (but not the Form 10-K risk management, strategy and governance disclosures, which they must provide on the same timeline as other companies) by an additional six months from the non-SRC compliance date (the final rules do not provide reduced disclosure requirements or any other disclosure accommodations for SRCs or EGCs);
- Requiring material updates to past incident disclosure in a Form 8-K amendment (rather than in subsequent Forms 10-Q/10-K);
- Removing the proposed requirement to disclose in periodic reports when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate, instead expanding the proposed definition of "cybersecurity incident" to include a "series of related unauthorized occurrences," which would still require companies to aggregate separate incidents under certain circumstances;
- Streamlining the proposed disclosure elements related to risk management, strategy and governance, with an emphasis on company processes as opposed to specific policies and procedures; and
- Eliminating the proposed requirement to provide proxy statement disclosure regarding the cybersecurity expertise of board members, instead focusing on management's expertise in managing cybersecurity risks.

---

[1] The adopting release states that an accidental occurrence is an unauthorized occurrence; therefore, an accidental occurrence may be a cybersecurity incident under this definition, even if there is no confirmed malicious activity: "For example, if

a company's customer data are accidentally exposed, allowing unauthorized access to such data, the data breach would constitute a 'cybersecurity incident' that would necessitate a materiality analysis to determine whether disclosure under Item 1.05 of Form 8-K is required."

[2] While the adopting release does not include specific examples of cybersecurity incidents that may require disclosure on Form 8-K if determined to be material, the proposing release had provided the following non-exhaustive list: (i) an unauthorized incident 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. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data; (ii) an unauthorized incident that caused degradation, interruption, loss of control, damage to or loss of operational technology systems; (iii) 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; (iv) an incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; and (v) an incident in which a malicious actor has demanded payment to restore company data that were stolen or altered.

[3] The adopting release emphasizes that the phrase "used by" specifically contemplates information resources owned by third parties and used by the company, thus implicating cybersecurity incidents on third-party systems.

[4] The proposed rules would have directed companies to make their materiality determination regarding a cybersecurity incident under a stricter standard of "as soon as reasonably practicable" after discovery of the incident. The SEC states in the adopting release that materiality determinations necessitate "an informed and deliberative process," and the revised language is meant to alleviate undue pressure on companies to make premature determinations before they have sufficient information.

[5] The adopting release notes that "Form 8-K Item 1.05 does not specify whether the materiality determination should be performed by the board, a board committee, or one or more officers. The company may establish a policy tasking one or more persons to make the materiality determination. Companies should seek to provide those tasked with the materiality determination information sufficient to make disclosure decisions."

[6] See *TSC Indus. v. Northway, Inc.*, 426 U.S. 438, 449 (1976); *Basic, Inc. v. Levinson*, 485 U.S. 224, 232 (1988); and *Matrixx Initiatives v. Siracusano*, 563 U.S. 27 (2011).

[7] *TSC Indus. v. Northway, Inc.*, 426 U.S. at 448.

[8] The SEC notes this approach is consistent with the Commission's general rules regarding the disclosure of information that is difficult to obtain, including Exchange Act Rule 12b-21, which provides that required information need be disclosed only insofar as it is known or reasonably available to the company.
[9] The delay provision for substantial risk to national security or public safety is separate from Exchange Act Rule 0-6, which provides for the omission of information that has been classified by an appropriate department or agency of the federal government for the protection of the interest of national defense or foreign policy. If the information a company would otherwise disclose on an Item 1.05 Form 8-K (or pursuant to Item 106 of Regulation S-K, as discussed below) is classified, the company should comply with Exchange Act Rule 0-6, meaning that such information should not be disclosed.
[10] The adopting release offers the following non-exclusive examples of "related" incidents: (i) "the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material" and (ii) "a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially."
[11] The final rules substitute the term "processes" for the proposed "policies and procedures," which the SEC believes more fully encompasses companies' cybersecurity practices, which may not be formally codified. The adopting release explains the shift to "processes" also was made "to avoid requiring disclosure of the kinds of operational details that could be weaponized by threat actors" and increase a company's vulnerability to cyberattack. However, the SEC indicates it still expects disclosure in sufficient detail to allow investors to ascertain a company's cybersecurity practices (such as whether it has a risk assessment program in place) and to understand the company's unique cybersecurity risk profile.
[12] While the SEC believes investors should know the level of a company's in-house versus outsourced cybersecurity capacity, neither the names of, nor the specific services provided by, third parties are expected to be disclosed.
[13] While the final rules delete the proposed obligation to disclose the frequency of board and management discussions on cybersecurity, the SEC notes that, depending on context, some companies' descriptions of the processes by which their board or relevant committee is informed about cybersecurity risks may include discussion of frequency: "For example, if the board or committee relies on periodic (e.g., quarterly) presentations by the [company]'s chief information security officer to inform its consideration of risks from cybersecurity threats, the [company] may, in the course of describing those presentations, also note their frequency."
[14] The SEC notes that an analogous materiality qualifier has not been included with respect to the board's oversight of cybersecurity risks because "if a board of directors

determines to oversee a particular risk, the fact of such oversight being exercised by the board is material to investors. By contrast, management oversees many more matters and management's oversight of non-material matters is likely not material to investors."

[15] While the SEC did not adopt the proposed requirement that companies specifically disclose whether they have a designated chief information security officer (or someone in a comparable position), it notes this information would typically be encompassed within the more general disclosure about management expertise.

[16] The 2011 and 2018 interpretive guidance was designed to assist companies in determining when they may be required to disclose information regarding cybersecurity incidents, risks and governance under existing disclosure rules (such as in risk factors, MD&A, description of business, legal proceedings, board leadership structure and risk oversight, or the financial statements), but imposes no prescriptive disclosure obligations. The 2018 guidance also addresses the importance of establishing and maintaining effective cybersecurity policies and procedures, including related disclosure controls and procedures, as well as the application of insider-trading prohibitions in the cybersecurity context and the obligation to refrain from making selective disclosures of material nonpublic information related to cybersecurity incidents and risks before making full disclosure of that same information to the general public. The SEC emphasizes that the final rules supplement, but do not replace, the existing cybersecurity guidance, which will remain in effect and should be used to inform potential disclosure obligations not specifically addressed in the final rules.

Related Services

Data Privacy

Public Companies/Public Offerings

Featured Insights

FIRM NEWS

Gunderson Dettmer Commemorates 2025 Asian American and Pacific Islander Heritage (AAPI) Month

CLIENT NEWS

Brazilian Carbon Capture Company Mombak Announces $30M Financing

CLIENT NEWS

Africa B2B OmniRetail Announces $20M Financing

CLIENT NEWS

Glacier Announces Series A Financing to Expand Robot Recycling Fleet

CLIENT NEWS

Dataminr Announces $100M Investment Led by Fortress Investment Group

CLIENT NEWS

Omnidian Announces $87M Series C for Renewable Energy Performance

INSIGHTS

Splitting the Pie: How Savvy Founders Divide Ownership and Navigate Other Founder Equity Decisions

CLIENT NEWS

Chainguard Announces $356 Million Series D Led by Kleiner Perkins and IVP

INSIGHTS

Client Insight: California AI Transparency Act

INSIGHTS

Client Insight: Prepare for BE-10 Benchmark Survey of US Direct Investment Abroad

INSIGHTS

Tech Brew Interviews Aaron Rubin in “Where the legal battle stands around copyright and AI training”

CLIENT NEWS

Latin America Fintech Belvo Announces $15M Funding