Client Alert | US Public Company Advisory Group, Mergers & Acquisitions, Data, Privacy & Cybersecurity

SEC Adopts Mandatory Cybersecurity Disclosure Rules

August 1, 2023

On July 26, 2023, the Securities and Exchange Commission ("SEC"), in a 3-2 vote, adopted rules that will require public companies to make prescribed cybersecurity disclosures.[1] The rules are designed to elicit "consistent, comparable, and decision-useful"[2] disclosures by requiring:

(i) **Incident reporting:** mandatory, material cybersecurity incident reporting under a new Form 8-K item for domestic issuers and on Form 6-K for foreign private issuers; and

(ii) **Risk management and governance disclosure:** mandatory annual disclosures on companies' governance and risk management with respect to cybersecurity risks, including board oversight of cybersecurity risks, under a new disclosure item required in Form 10-K and Form 20-F.

The SEC's newly adopted rules represent a significant expansion of the disclosures previously required by SEC rules, but are a somewhat "slimmed down" version of the rules originally proposed in March 2022.[3] The rules expand on the SEC's previously issued interpretive guidance from 2011[4] and 2018,[5] in which the SEC provided its views on how existing disclosure obligations would apply to cybersecurity risks and incidents and continue the SEC's move toward a more prescriptive rule-making approach and away from the prior administration's principles-based approach.[6]

In explaining the necessity of the new rules, the adopting release highlighted the inconsistent timing, content and location of current disclosures on cybersecurity risks and incidents. It also noted the increasing prevalence of cybersecurity incidents and attacks, as well as the significant impact such an attack may have on a company, in addition to noting recent developments in artificial intelligence which may exacerbate such threats.

1 The rules are available here, the fact sheet is available here and the press release is available here.

2 *See* SEC Chair Gary Gensler's "Statement on Public Company Cybersecurity Disclosures," available here.

3 For more information, *see* "SEC Proposes Mandatory Cybersecurity Disclosure Rules", available here.

4 *See* CF Disclosure Guidance: Topic No. 2- Cybersecurity (Oct. 13, 2011), available here.

5 *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166], available here, and our prior alert, "SEC Issues Interpretive Guidance on Public Company Cybersecurity Disclosures: Greater Engagement Required of Officers and Directors."

6 Both Commissioner Peirce's and Commissioner Uyeda's dissents focused on what is, in their view, the overly-prescriptive nature of the new rules. Commissioner Uyeda criticized the SEC's approach, opining that "rather than using a scalpel to fine-tune the principles-based approach of the 2018 Interpretive Release, today's amendments swing a hammer at the current regime and create new disclosure obligations for cybersecurity matters that do not exist for any other topic." Commissioner Peirce also criticized the "prescribe[d] granular disclosures, which seem designed to better meet the needs of would-be hackers rather than investors' need for financially material information" and questioned the SEC's "reject[ion of] financial materiality as the touchstone for its disclosures, and [its] fail[ure] to offer in its place a meaningful intelligible limit to its disclosure authority." *See* Commissioner Peirce's dissent, available here, and Commissioner Uyeda's dissent, available here.

Effective Dates

- **Risk management and governance disclosure**: All registrants must provide the new disclosure under Item 106 of Regulation S-K (or comparable requirements for FPIs in Form 20-F) beginning with annual reports for fiscal years ending on or after **December 15, 2023**. Therefore, calendar-year companies must comply with the new rules in their upcoming annual reports.

- **Incident disclosure**: All registrants (other than smaller reporting companies) must begin complying with the incident disclosure requirements in new Item 1.05 of the Form 8-K and in Form 6- K starting on **December 18, 2023** (or, if later, **90 days** after the date of publication of the new rules in the Federal Register). Smaller reporting companies will have an additional 180 days and must begin complying with Form 8-K Item 1.05 starting on June 15, 2024 (or, if later, **270 days** after the date of publication in the Federal Register).

- **Inline XBRL**: All registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement. Therefore, for the annual report disclosure, companies must begin tagging in Inline XBRL starting with annual reports for fiscal years ending on or after **December 15, 2024**, and for Form 8-K and Form 6-K disclosure, companies must begin tagging responsive disclosure starting on **December 18, 2024** (or if later, 465 days after the date of publication in the Federal Register).

Cybersecurity Incident Disclosure

The new rules provide for:

(1) ***Material Cybersecurity Incidents as a Form 8-K Event.*** New Item 1.05 of Form 8-K requires companies to file a Form 8-K if "the registrant experiences a cybersecurity incident that is determined by the registrant to be material." The Form 8-K must be filed within four (4) business days after the company *determines* that it has experienced a *material* cybersecurity incident. The Form 8-K must describe:

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

- the material impact or reasonably likely impact[7] on the registrant, including its financial condition and results of operations.[8]

In response to comments expressing concern that disclosure could exacerbate cybersecurity threats by providing details to actual and potential threat actors, the final rules no longer call for disclosure regarding the incident's remediation status, whether it is ongoing or whether data was compromised. In addition, Instruction 4 to Item 1.05 specifically provides that "a registrant 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 the registrant's response or remediation of the incident." The release notes that the SEC believes the adopted standard "more precisely focuses the disclosure on what the company determines is the material impact of the incident, which may vary from incident to incident", rather than on requiring details regarding the incident itself.

Timing of Disclosure: The trigger for an Item 1.05 Form 8-K is the date on which a company ***determines that a cybersecurity incident it has experienced is material***, rather than the date of discovery of the incident, in order to focus the disclosure on incidents that are material to investors. The adopted rules state that companies must make this determination "without unreasonable delay", (rather than, as originally proposed, "as soon as reasonably practical"). In explaining this standard, the

---

7 Commissioner Uyeda took issue with the forward-looking nature of this requirement, arguing that the new rules "break new ground by requiring real-time, forward-looking disclosure" regarding the reasonably likely impact of a breach as well as the requirement to update this information, stating that "[n]o other Form 8-K event requires such broad forward-looking disclosure that needs to be constantly assessed for a potential amendment."

8 The adopting release notes that the "rule's inclusion of 'financial condition and results of operations' is not exclusive; companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident." For example, harm to a company's reputation, customer or vendor relationships, or competitiveness may have a material impact on the company, as could the possibility of litigation or regulatory investigations or actions.

adopting release notes that "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" (emphasis added). It also warns that actions such as intentionally delaying a board meeting necessary to determine materiality or revising incident procedures to support a delayed materiality determination would constitute an unreasonable delay.

The SEC's adopting release clarifies that the materiality determination is made using the same standard that applies generally under the federal securities laws,[9] but notes that "doubts as to the critical nature...should be resolved in favor of those the statute is designed to protect," namely investors. As the adopting release explains, some cybersecurity incidents may be material yet not cross a particular financial threshold, and the material impact of an incident "may encompass a range of harms, some quantitative and others qualitative." For example, the SEC notes that an incident that results in "significant reputational harm" 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. Likewise, the SEC notes that an incident may be material due to the "scope or nature of harm to individuals, customers or others," rather than based on any quantitative financial measures.

In making a materiality determination, in "the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered" and each registrant will "develop information after discovery until it is sufficient to facilitate a materiality analysis." While not prescribing whether the materiality determination should be performed "by the board, a board committee or one or more officers," the adopting release notes that a company "may establish a policy tasking one or more persons to make the materiality determination" and that "companies should seek to provide those tasked with the materiality determination information sufficient to make disclosure decisions." In this regard, the SEC did not exempt registrants from providing disclosures regarding cybersecurity incidents on third party systems they use, but, consistent with SEC rules regarding disclosure of information that is difficult to obtain, the final rules "generally do *not* require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers" (emphasis added).[10]

The SEC acknowledged the widespread concern that forcing disclosure so soon after a materiality determination could lead to vague or misleading information being conveyed to investors, but noted that investors are best served by knowing quickly about the existence of the incident and the Company's materiality determination. The Commission believes that because the required disclosure is focused on the incident's "basic identifying details" and its material or reasonably likely material impacts, companies should have this information available at the time disclosure is triggered.

Definition of "Cybersecurity Incident":[11] [12] Under the adopted rules, the definition of "cybersecurity incident" is to be construed broadly, and also extends to "a series of related unauthorized occurrences", reflecting the fact that "cyberattacks sometimes compound over time, rather than

---

9 TSC Indus. v. Northway, 426 U.S. 438, 449 (1976); Matrixx Initiatives v. Siracusano, 563 U.S. 27, 38-40 (2011); Basic, 485 U.S. at 240. Also s*ee* 17 CFR 230.405 (Securities Act Rule 405) and 17 CFR 240.12b-2 (Exchange Act Rule 12b-2).

10 See footnote 124 of the adopting release.

11 The complete definition is "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." *See* new Item 106(a).

12 The adopting release points to the proposing release for examples of cybersecurity incidents that may, if determined by the company to be material, trigger the proposed Item 1.05 disclosure requirement, including: "An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data; [a]n unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems; [a]n 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 registrant; [a]n incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or [a]n incident in which a malicious actor has demanded payment to restore company data that was stolen or altered."

present as a discrete event."[13] Accordingly, when a company finds that 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 results from multiple intrusions that are each on their own immaterial.

Limited National Security Exception: Pursuant to Item 1.05(c), a registrant may delay filing a Form 8-K if the United States Attorney General (the "AG") determines that immediate disclosure would pose a "substantial risk to national security or public safety" and notifies the SEC of such determination in writing. Initially, disclosure may be delayed for up to 30 days, as specified by the AG. The delay may be extended for an additional period of up to 30 days if the AG determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the AG determines that disclosure continues to pose a substantial risk to national security and notifies the SEC of such determination in writing. The adopting release explains that the SEC has already consulted with the Department of Justice ("DOJ") to establish an interagency communication process to allow for the AG's determination to be communicated to the SEC in a timely manner.[14]

In addition to this exception, the adopting release explicitly references Exchange Act Rule 0-6,[15] which can allow for the omission of information that has been classified by an appropriate department or agency of the Federal government for protection "in the interests of national defense or foreign policy." As the adopting release notes, "if the information a registrant would otherwise disclose on an Item 1.05 Form 8-K or pursuant to Item 106 of Regulation S-K or Item 16K of Form 20-F is classified, the registrant should comply with Exchange Act Rule 0-6."

Impact of Failure to File: Consistent with the SEC's approach to certain other Form 8-K disclosure items requiring a company to make a rapid evaluation of materiality, failure to timely report under new Item 1.05 (i) will *not* impact Form S-3 eligibility and (ii) will be subject to the limited safe harbor from certain public and private claims under Section 10(b) and Rule 10b-5 of the Securities Exchange Act of 1934, as amended (the "Exchange Act").[16]

(2) ***Updates on Disclosed Cybersecurity Incidents in Amendments to Form 8-K.*** In a change from the proposed rules, companies are not required to disclose any material updates to the Item 1.05 information in their quarterly or annual reports, but instead are required to provide certain updates in an amended Form 8-K. Specifically, Instruction 2 to Item 1.05 of Form 8-K directs a registrant to include in its Item 1.05 Form 8-K a statement identifying any information called for in Item 1.05 that is not determined or available at the time of the required filing, and then later file an amendment to its Form 8-K with this information (within four business days after the registrant, without unreasonable delay, determines such information or within four business days after the information becomes available). The adopting release notes that, "[o]ther than with respect to such previously undetermined or unavailable information, the final rules do not separately create or otherwise affect a registrant's duty to update its prior statements." However, the adopting release reminds companies that they may have a duty to correct prior disclosure if it is determined to be untrue or a duty to update disclosure that becomes materially inaccurate after it was made, and that companies should also consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

---

13 For example, if "the same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, [and] they are either quantitatively or qualitatively material." Another example provided in the release "is a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially."

14 The adopting release goes on to explain that the DOJ "will notify the affected registrant that communication to the Commission has been made, so that the registrant may delay filing its Form 8-K."

15 *See* footnote 131 of the adopting release.

16 This limited safe harbor applies only to a failure to timely file a current report on Form 8-K—not to any other anti-fraud violation or failure to maintain disclosure and controls under the Exchange Act—and extends until the due date of the company's next quarterly report on Form 10-Q or annual report on Form 10-K, whichever comes first.

Risk Management and Governance Disclosure in Annual Reports

The new rules also require enhanced disclosure on companies' cybersecurity risk management and governance in both annual reports on Form 10-K and Form 20-F. Specifically, companies must disclose:

(1) ***Cybersecurity Risk Management and Strategy***. New Item 106(b) of Regulation S-K requires a company to describe in its Form 10-K (or Form 20-F), as applicable:

a. Its processes, if any, for the assessment, identification and management of the material risks from cybersecurity threats, in sufficient detail for a reasonable investor to understand these processes, including:

i. Whether and how the described cybersecurity processes have been integrated into the registrant's overall risk management system or processes;

ii. Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

iii. Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.[17]

b. 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 the registrant, including its business strategy, results of operations, or financial condition and if so, how.[18]

These disclosure requirements were narrowed from those proposed, in response to comments, in that the final rules do not require detailed disclosure regarding prevention and detection activities, continuity and recovery plans or how previous incidents have informed policy, governance or technology changes. Following widespread concern that the proposed rules were so prescriptive as to affect companies' risk management and decision making, the adopting release explicitly noted that the purpose of the rules is to inform investors, and "not to influence whether and how companies manage their cybersecurity risk".

(2) ***Cybersecurity Governance***. New Item 106(c) of Regulation S-K requires disclosure in a company's Form 10-K (or Form 20-F) of:

a. **Board oversight** of risks from cybersecurity threats, including, if applicable:

i. identifying any board committee or subcommittee responsible for oversight, and

ii. describing the process by which the board or committee is informed about such risks[19]; and

b. **Management's role** in assessing and managing the registrant's *material* risks from cybersecurity threats including, as applicable, the following non-exclusive list of disclosure items:

i. "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[20];

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

---

17 *See* new Item 106(b)(1).

18 *See* new Item 106(b)(2).

19 *See* new Item 106(c)(1).

20 An instruction to Item 106(c) notes that expertise of management in cybersecurity risk assessment may include, for example, prior work experience in cybersecurity; any relevant degrees or certifications; and any knowledge, skills, or other background in cybersecurity.

iii. 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."[21]

The SEC did not adopt proposed changes that would have required disclosure as to whether and how the board integrates cybersecurity into its business strategy, risk management and financial oversight function, the frequency of board discussions on cybersecurity, and whether directors have expertise in cybersecurity. However, the adopting release noted that, depending on context, some registrants' descriptions of the processes by which their board or relevant committee is informed about cybersecurity risks may include the frequency of board or committee discussions.[22]

Inline XBRL Tagging

The new rules require companies to tag the information specified by Item 1.05 of Form 8-K and Item 106 of Regulation S-K in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual, to allow investors and other market participants "to more efficiently perform large-scale analysis and comparison of this information across [companies] and time periods."

Application to Foreign Private Issuers[23]

(1) ***Periodic Disclosure.*** The new rules amend Form 20-F to add Item 16J, which requires a foreign private issuer ("FPI") to include in its annual report on Form 20-F the same cybersecurity risk management and governance disclosure as is called for in Item 106 of Regulation S-K and described above.

(2) ***Incident Disclosure.*** The new rules amend Form 6-K General Instruction B to add "material cybersecurity incidents" as a potential reporting event. FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or publicize in a foreign jurisdiction, to any stock exchange[24] or to security holders.

Practical Considerations

(1) **Evaluate Cybersecurity Risk Management Systems and Incident Response Plan in Light of New Disclosure Requirements.** Cybersecurity risk management and governance disclosures will be required in Form 10-Ks filed in 2024 for the fiscal year ending in 2023, and incident reporting will be required starting December 18, 2023. In light of these upcoming disclosures, companies should review and consider any appropriate updates to their cybersecurity and risk management systems, with a focus on any recent changes in their technology infrastructure, changes in the cybersecurity threat landscape, and insights gleaned from any recent security incidents.

In addition, companies should review their incident response plan in light of the new rules to ensure that the appropriate team is constructed and made aware of the timeline for disclosure and the process for escalation, if necessary. This process should include when and how to raise significant or material incidents with senior management and/or the board. The brief window for reporting means that this process needs to happen quickly and efficiently. Preparedness is essential, and companies should perform mock incident sessions with the incident response team at least annually, to ensure familiarity with the incident response plan and to sharpen any inefficiencies. Secure communication methods will need to be utilized and maintained through the resolution and remediation of any material cybersecurity incidents, given the requirement to provide updates to the disclosure.

---

21 *See* new Item 106(c)(2).

22 For example, the adopting release notes that "if the board or committee relies on periodic (e.g., quarterly) presentations by the registrant's chief information security officer to inform its consideration of risks from cybersecurity threats, the registrant may, in the course of describing those presentations, also note their frequency."

23 The new rules do not apply to Form 40-F filers given that "the MJDS generally permits eligible Canadian FPIs to use Canadian disclosure standards and documents to satisfy the Commission's registration and disclosure requirements."

24 The rules of the New York Stock Exchange and the Nasdaq Stock Market require that companies disclose promptly to the public through any Regulation FD compliant method any material information that would reasonably be expected to affect the value of securities or influence investors' decisions.

(2) **Revisit Disclosure Controls and Procedures.** While the "materiality" threshold is well-known to public companies, registrants should revisit the materiality framework they have established for cybersecurity incidents and the disclosure controls and procedures that are designed to facilitate the analysis of incidents in real time. There should be a team in place, comprised of company leadership, information technology ("IT") and legal personnel, to make any materiality determinations with respect to an incident.[25] There should also be appropriate procedures for reporting and escalating to the legal team and senior management who will make the materiality determinations. This will require greater involvement of IT and data security professionals at the outset, including independent third-party cybersecurity firms that specialize in performing forensic investigations, to ensure the risks and potential operational and business impacts are properly identified. The SEC has recently brought enforcement actions against companies for inadequate disclosure controls and procedures involving cybersecurity incidents in which there was a breakdown in communication between the IT and financial reporting functions, leading to inaccurate disclosures to investors.[26] It is important to remember that in this context, disclosures will need to be considered and prepared while the company is also in the process of evaluating a breach and planning its containment and remediation strategy. Clear processes and chains of command will be necessary in order to ensure coordination and that neither activity is impeded by the other.

(3) Limited Scope of "National Security or Public Safety" Exception: The determination as to whether a reporting delay should be requested is solely in the DOJ's discretion, based on how the agency determines the cybersecurity incident impacts national security and public safety.[27] Factors in the DOJ's determination could include, among others, the presence of a significant foreign nexus related to the cybersecurity incident and the likelihood of early disclosure jeopardizing a DOJ investigation or otherwise causing unintended material adverse consequences to the public, such as by providing a path for further exploitation by bad actors. This exception is narrowly tailored and is not currently expected to result in a significant number of delayed disclosures. If a company determines that a material cybersecurity incident involves factors relevant to the DOJ's analysis, these factors should be promptly communicated to the SEC and to the DOJ.

(4) **Revisit Cybersecurity Policies and Procedures, including with Respect to Third-Party Providers.** The final rules do not exempt registrants from providing disclosures regarding incidents originating on the systems of their third party` providers; however, companies are not required to perform any special inquiry into third party systems, into which they may have reduced visibility. Companies should ensure they have effective communication protocols in place with third-party service providers to facilitate timely assessment and disclosure. In addition, companies should evaluate the adequacy and formality of their existing cybersecurity policies and procedures, to ensure that their cybersecurity programs are generally comparable with those of competitors, as the strength of companies' cybersecurity protocols could be a factor weighed by investors.

(5) **Review and Assess Governance and Oversight Structure**. Companies should evaluate their existing cybersecurity risk oversight structures at the board and management level, and consider whether any improvements are needed, such as delegating tasks to a dedicated board committee, scheduling additional cybersecurity updates on board agendas or increasing the amount of time spent addressing cybersecurity, and strengthening processes for timely communications between management and board members.

---

25 The 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."

26 *See, for example, In the Matter of Blackbaud, Inc.,* (March 9, 2023), available here.

The following White & Case attorneys authored this alert:

Maia Gez, F. Paul Pittman, Michelle Rutta, Danielle Herrick and David Jividen

White & Case Team Members:

Colin J. Diamond
Elodie Gal
Maia Gez
David Johansen
Scott Levi
Michelle Rutta
Kimberly C. Petillo-Décossard
Melinda Anderson
Patti Marks
Danielle Herrick
Sarah Hernandez