Governance & Securities Alert

Weil

From the Public Company Advisory Group of Weil, Gotshal & Manges LLP

July 28, 2023

SEC Adopts Cybersecurity Disclosure Rules as Security Incidents Become More Frequent

In response to a significant rise in cybersecurity incidents at public companies and the SEC's view that there is inconsistent disclosure relating to such incidents, this week, the SEC adopted cybersecurity disclosure rules, with a few notable changes from the proposing release. The final rules will require a U.S. public company to disclose (1) on Form 8-K the occurrence of a material cybersecurity incident within four business days after determining that such incident is material and (2) in the Annual Report on Form 10-K, the company's risk management, strategy and governance of cybersecurity. Foreign private issuers (FPIs) are subject to similar requirements. The adopting release is available here. In this Alert, we discuss the important new rules in greater detail and provide recommendations on what to do now.

Compliance Dates

Most companies must comply with the incident disclosure requirements on Forms 8-K and 6-K (for FPIs) by the later of December 18, 2023 or 90 days after publication of the adopting release in the Federal Register. Smaller reporting companies must comply with these requirements by the later of June 15, 2024 or 270 days after publication. All companies must comply with the risk management, strategy and governance disclosure beginning with annual reports for the fiscal year ending on or after December 15, 2023. Inline XBRL is required one year after the initial compliance date for the related disclosure requirement.

Key Aspects of New Form 8-K Disclosure

- **Disclose Material Cybersecurity Incidents on Form 8-K**. Within four business days after determining that a cybersecurity incident is material, a company must disclose under new Item 1.05 of Form 8-K 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 on its financial condition or results of operations.
- **Form 8-K Trigger is Determination of Materiality**. The trigger for an Item 1.05 Form 8-K is the date on which the company determines that a cybersecurity incident that it has experienced is material, not the date the company discovers the incident.
- **No Unreasonable Delay**. *(change from proposed rule)* The materiality determination must be made by the company "without unreasonable delay" after discovery of the incident (as opposed to the proposed "as soon as reasonably practicable").

- **No Loss of Form S-3 Eligibility**. The SEC is adding Item 1.05 to the list of Form 8-K items in General Instruction I.A.3.(b) of Form S-3, so that the untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility.
- **Cybersecurity Incident is Defined Broadly**. *(change from proposed rule)* [1] The definition of "cybersecurity incident" includes "a series of related unauthorized occurrences." Thus, although the SEC did not adopt the proposed requirement that a company be required to aggregate *unrelated* incidents, *related* incidents over time – even if each incident is immaterial – could trigger an Item 1.05 8-K if, the incidents together, are quantitatively or qualitatively material. The SEC provided two examples. The first is that 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. The second is a series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially.
- **Disclosure May be Required of Third-Party Incidents.** Although the SEC recognized that companies may have reduced control over third-party systems, the final rules do not exempt companies from providing disclosures about cybersecurity incidents on third-party systems that companies use. The final rules, however, do not require additional inquiries "outside of [the company's] regular channels of communication with third-party service providers pursuant to those contracts and in accordance with [the company's] disclosure controls and procedures."
- **No Disclosure Required of Remediation**. *(change from proposed rule)* The disclosure focuses on the impact of the incident to the company rather than the details of the incident, thereby eliminating the proposed requirement of whether the company has remediated the incident. An instruction to new Item 1.05 clarifies that companies do not need to disclose specific or technical information about the planned response to the incident or its cybersecurity systems, related networks and devices or potential system vulnerabilities in such detail as would impede the company's response or remediation of the incident. However, companies may need to consider disclosing remediation efforts to address the concerns of investors, customers, supplies, employees and other stakeholders, even if not required by the rule.
- **Limited Delay Based on Substantial Risk to National Security or Public Safety**. *(change from proposed rule)* The new rules provide for a process and a limited delay if the required disclosure would pose a substantial risk to national security or public safety, contingent on a written notification by the U.S. Attorney General.[2] To accommodate companies who are subject to the Federal Communication Commission's (FCC) rule for notification in the event of breaches of customer proprietary network information, these companies may delay making an Item 1.05 Form 8-K disclosure up to the seven business day period following notification to the United States Secret Service and Federal Bureau of Investigation specified in the FCC rule. The adopting release noted, however, that the FCC recently proposed amendments to its rule, which, if adopted, would eliminate the seven-day waiting period.
- **Updates Required on Amended Form 8-K**. *(change from proposed rule)* To the extent that the information called for by Item 1.05 is not determined or is unavailable at the time of the required Form 8-K filing, the company must include a statement to this effect in the filing. Thereafter it is required to file an amendment to Form 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. This is a change from the proposed rule, which instead contemplated updates in subsequent Forms 10-Qs and 10-K. Additionally, the SEC reminded companies of their independent duty to update prior disclosures. For example, the adopting release provides an example of a duty to correct (a company later discovers contradictory information that existed at the time of the initial disclosure) and a duty to update (a statement becomes materially inaccurate after it is made and is still being relied on by reasonable investors).

Determining Materiality

The SEC emphasized that the test for materiality continues to be the seminal test as to whether "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." When assessing materiality, companies should consider qualitative and quantitative factors. The adopting release provides the following examples: harm to the company's reputation, customer or vendor relationships or competitiveness, and the possibility of litigation or regulatory investigations or actions. The SEC provided the example of a company experiencing a data breach needing to consider both the immediate fallout and any longer term effects on its operations, finances, brand perception, customer relationships, etc. as part of its materiality analysis.

Other factors we recommend considering in order to determine materiality may, depending on the facts and circumstance, include, but are not limited to:

- The number of people impacted;
- The nature of the people impacted (e.g., employees vs. customers);
- The nature of the information breached (e.g., personal identifiable information (PII) or protected health information (PHI));
- The type of impact to the company (e.g., interference with operations);
- Whether this is isolated to the company or other companies or entities also are impacted;
- The quality of the company's risk factor in its SEC filings;
- Whether the breach/ransomware is at the company or via a third party;
- How long the incident has lasted; and
- The ability of the company to remedy the incident and the timing of the remediation.

There may be additional reasons driving disclosure on a Form 8-K – for example, (1) if the company is involved in a securities offering that needs to be updated for the cybersecurity incident, (2) to control the narrative about the cyber incident, (3) to avoid selective disclosure under Regulation FD if the company wants to discuss the incident with some of its investors, and/or (4) consideration relating to the company's trading window.

Key Aspects of Risk Management and Strategy and Governance Disclosure

The following disclosures significantly expand the required discussion of cybersecurity risk management and oversight in a company's Form 10-K (new "Item 1.C. Cybersecurity" that requires the furnishing of information required by new Item 106 of Regulation S-K) or Form 20-F (new "Item 16K. Cybersecurity" of Form 20-F), as applicable.

Risk Management and Strategy. New Item 106(b) of Regulation S-K and new Item 16K of Form 20-F will require companies to describe the "process, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those pressures."[3] Specifically, Item 106(b) requires a company to address this non-exclusive list:

- 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; and
- whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

Additionally, a company will be required to describe 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 company, including its business strategy, results of operations, or financial condition and if so, how.

Governance. In addition to processes under Item 106(b), new Item 106(c) requires a description of the board of directors' oversight of risks from cybersecurity threats, and if applicable, the identification of any board committee or subcommittee responsible for such oversight (and a description of the processes by which the board of directors or such committee is informed about such risks). Item 106(c) also calls for a description of management's role in assessing and managing material risks from cybersecurity threats including the following non-exhaustive list of disclosure items:

- 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;
- whether 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.

No Requirement to Disclose Board Expertise; Management Expertise Required. *(change from proposed rule)* The final rules do not require disclosure of board members with cybersecurity expertise. However, as indicated above, companies must disclose the "relevant expertise" of management and committees responsible for assessing and managing the company's material risks from cybersecurity threats. Instruction 2 to Item 106(c) provides a non-exhaustive list of what constitutes "relevant expertise," including: prior work experience in cybersecurity; any relevant degrees or certifications; and any knowledge, skills, or other background in cybersecurity.

Applicability to Foreign Private Issuers

Disclosure must be furnished by FPIs on Form 6-K regarding material cybersecurity incidents that the company (i) makes or is required to make public under the laws of its jurisdiction of incorporation, (ii) files or is required to file under the rules of any stock exchange, or (iii) distributes or is required to distribute to its security holders.[4] Form 20-F also adds Item 16K, which requires the same type of disclosure for FPIs that will be required under Item 106 of Regulation S-K for domestic registrants discussed above.[5]

Dissenting SEC Commissioners' Perspectives

The new cybersecurity disclosure rules were adopted by a 3-2 vote with the dissenting SEC Commissioners raising several concerns with the final rules. Commissioner Peirce raised her concerns that the new strategy and governance disclosures rules potentially provide cyber hackers a "roadmap" on which to target and attack companies, and that the new Form 8-K disclosure rules potentially provide successful attackers with details of "when the company [found] out about the attack, what the company knows about it, and what the financial fallout is likely to be (i.e., how much ransom the attacker can get)." She also noted that investors may "overreact" to rushed disclosures forced to be provided without all available information, with companies potentially disclosing incidents that, with time, prove to not be material. Commissioner Uyeda voiced similar concerns, stating that "early information is often incomplete and not correct." He also flagged that "premature public disclosure of a cybersecurity incident at one company could result in uncertainty of vulnerabilities at other companies, especially if it involves a commonly used technology provider, resulting in widespread panic in the market and financial contagion."

What to Do Now?

Although the rules are not effective until the middle of December 2023, companies impacted by a cybersecurity incident should consider its materiality on the company and the company's employee and customer data, and trade secrets, and if material, should consider the new disclosure requirements summarized in this Alert as a guide to disclosure determination. Among other things, companies should:

- prepare for the accelerated reporting regime of material cybersecurity incidents by: (i) training the internal cyber incident team about the new timing and scope of the disclosure rules; (ii) reviewing the company's information flow relating to the evaluation of potentially material cybersecurity incidents; and (iii) confirming that the company's processes ensure timely escalation of cyber incidents to appropriate decision-makers.
- identify which company officers or other personnel will determine materiality of cybersecurity incidents and whether such incidents need to be disclosed or reported to regulators.
- review the company's disclosure controls and procedures around (i) the determination of materiality of cybersecurity incidents; (ii) the public disclosure of material cybersecurity incidents and (iii) the public disclosure of the company's cybersecurity processes generally; if not already previewed with the company's disclosure committee, consider adding such disclosures to the scope of the disclosure committee's duties.
- although not directly addressed by the new rules, in light of SEC comments on cybersecurity risk factors, review such risk factors to confirm that the cybersecurity risk factors acknowledge, if as is commonly the case, that breaches, threats, incidents, etc. have occurred rather than that the company is only vulnerable to such occurrences.
- review board and board committee responsibilities for overseeing material company cybersecurity risks and their intersection with company strategy; determine the frequency with which the board and board committees receive reports from the company's Chief Information Security Officer, or equivalent.
- consider the adequacy of the company's process for assessing, identifying and managing material risks from cybersecurity threats; while the SEC insists that it does not intend for the new rules to change company behaviors, companies will feel pressure to describe fulsome cybersecurity processes that have been integrated in into the company's overall risk management system or processes.
- consider whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.
- establish a process for the company to support its newly required disclosure as to 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 company, including its business strategy, results of operations, or financial condition and if so, how.
- consider the emphasis of the new rules on management expertise, management positions and management committees overseeing cybersecurity risk and the reporting process of such risks to the board of directors or a committee of the board.

* * *

Endnotes

[1] The rules include definitions of "cybersecurity incident," "cybersecurity threat," and "information systems."

[2] Companies may delay filing for up to 30 days if the U.S. Attorney General determines that the incident disclosure would pose a substantial risk to national security or public safety, which delay may be extended up to 90 days (depending on the circumstances) if the Attorney General determines disclosure continues to pose a substantial risk to national security or public safety. Beyond these delays, if the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay on a case-by-case basis. SEC Commissioner Peirce expressed skepticism that approval could be obtained from the Attorney General within the four business days, stating that it would be "quite a feat" and noting that the rule makes extensions of the delay beyond the initial 30 days difficult.

[3] As guidance, the adopting release refers to several types of risk that companies face: intellectual property theft, fraud, extortion, harm to employees or customers, violations of privacy laws and other litigation and legal risk, and reputational risk.

[4] Consistent with recent rulemaking, the SEC was not persuaded that the new rules would disproportionately burden FPIs, including those subject to potentially more stringent requirements of European Union's Market Abuse Regulations. The SEC believes "FPIs' cybersecurity incidents and risks are not any less important to investors' capital allocation than those of domestic registrants."

[5] The SEC is not amending Form 40-F, choosing instead to maintain the multijurisdictional disclosure system whereby eligible Canadian FPIs use Canadian disclosure standards and documents to satisfy SEC registration and disclosure requirements.

* * *

Authors

P.J. Himelfarb	View Bio	pj.himelfarb@weil.com	+1 202 682 7208
Lyuba Goltser	View Bio	lyuba.goltser@weil.com	+1 212 310 8048
Howard Dicker	View Bio	howard.dicker@weil.com	+1 212 310 8858
Steven Bentsianov	View Bio	steven.bentsianov@weil.com	+1 212 310 8928
Shira Barron	View Bio	shira.barron@weil.com	+1 212 310 8336

If you have questions or would like additional information, please reach out to your contact in the Public Company Advisory Group or the Privacy & Cybersecurity Group, Randi Singer or Olivia Greer.

© 2023 Weil, Gotshal & Manges LLP. All rights reserved. Quotation with attribution is permitted. This publication provides general information and should not be used or taken as legal advice for specific situations that depend on the evaluation of precise factual circumstances. The views expressed in these articles reflect those of the authors and not necessarily the views of Weil, Gotshal & Manges LLP. If you would like to add a colleague to our mailing list, please click here. If you need to change or remove your name from our mailing list, send an email to weil.alerts@weil.com.