August 2, 2023

SEC Adopts New Cybersecurity Disclosure Requirements

The SEC has adopted new disclosure requirements to enhance and standardize public company disclosures regarding cybersecurity risk management and incident reporting. Companies will be required to disclose material cybersecurity incidents within four business days on Form 8-K, and to provide annual disclosure regarding their cybersecurity governance and risk management. The final rules reflect the SEC's response to comments calling for more measured disclosure requirements, including, among other things, the elimination of the proposed requirement to disclose whether a board has cybersecurity expertise, the addition of a procedure to delay disclosure if the U.S. Attorney General determines that the disclosure would pose a substantial risk to national security or public safety and more explicit language that the disclosure is focused on material cybersecurity risks and impacts.

Companies must comply with the Form 8-K disclosure requirements starting the later of (i) 90 days after publication of the rules in the *Federal Register* and (ii) December 18, 2023; except smaller reporting companies have until the later of (i) 270 days after publication in the *Federal Register* and (ii) June 15, 2024. All companies must provide the cybersecurity governance and risk management disclosure in annual reports filed for fiscal years ending on or after December 15, 2023 (i.e., calendar-year-end companies will be required to include this in next year's Annual Report on Form 10-K). These new rules also amend Form 6-K and Form 20-F to include these new disclosure requirements.

Reporting of Material Cybersecurity Incidents on Form 8-K

New Item 1.05 of Form 8-K will require specified disclosure of material cybersecurity incidents. In response to comments, the SEC has dropped its proposal that companies provide updates on the incident in subsequent periodic reports. Instead, if any information required by Item 1.05 is not determined or unavailable at the time of the Form 8-K filing, companies must file an amendment to the Form 8-K to include such disclosure within four business days of determination or availability.

What will companies need to disclose?

Under new Item 1.05 of Form 8-K, companies must, within four business days of their determination that a "material cybersecurity incident" has occurred, file a Form 8-K describing 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.

New Item 106(a) of Regulation S-K defines a "cybersecurity incident" as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity, or availability of a company's information systems or any information residing therein." Whether a cybersecurity incident is material remains unchanged and is determined by the same principles articulated repeatedly by the courts and the SEC – namely whether there is a substantial likelihood that a reasonable investor would consider it important. Companies should consider the total mix of information, including both quantitative and qualitative factors, and that an incident may be material even if the probability of a negative consequence is low, if the potential loss or liability is large.

Companies will not be required or expected to publicly disclose specific, technical information about their planned responses to the incident or their cybersecurity systems, related networks and devices, or potential system vulnerabilities at a level of detail that could hamper their ability to respond to or remedy the incident.

When must the Form 8-K disclosure be made?
As with most other Form 8-K items, the disclosure must be made within four business days after the company determines that the cybersecurity incident is material (not the date the company learned of the incident). To ensure that companies are timely in assessing the materiality of any incidents, Instruction 1 to new Item 1.05 requires companies to make a materiality determination regarding a cybersecurity incident "without unreasonable delay." As noted above, if any information required by Item 1.05 is unavailable or not yet determined when the initial Form 8-K filing is due, the company must file an amendment to the Form 8-K to disclose that additional information within four business days of determination or availability.

Although companies may not delay disclosure pending their own investigations (even if other applicable laws would so permit), they may delay making the Item 1.05 Form 8-K filing if the Attorney General determines that the disclosure poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

Will a failure to disclose material cybersecurity events on a timely basis compromise Form S-3 eligibility?
No. A company will not lose Form S-3 eligibility if the Form 8-K filing was not made on a timely basis, though the company will need to be caught up and current at the time it files the Form S-3 Registration Statement.

Will the disclosures under new Item 1.05 of Form 8-K be eligible for the limited safe harbor from Section 10(b) or Rule 10b-5 liability for the failure to file certain Form 8-Ks?
Yes. The SEC is also amending Rules 13a-11(c) and 15d-11(c) under the Securities Exchange Act of 1934, as amended, so that disclosures made in response to new Item 1.05 will be eligible for the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act for a failure to timely file the Form 8-K. Note that disclosures made in response to Item 1.05 will be considered filed (rather than furnished) for SEC liability purposes.

Do foreign private issuers need to make similar disclosures regarding cybersecurity incidents?
Yes. The SEC is amending Form 6-K to identify material cybersecurity incidents as a filing trigger.

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

New Item 106 of Regulation S-K will require companies to describe in their Annual Reports on Form 10-K their risk management and strategy, as well as the role of their boards and management in overseeing, assessing and managing material risks from cybersecurity threats.

What will companies need to disclose about their cybersecurity risk management?
New Item 106(b) of Regulation S-K will require companies to describe their processes, if any, for assessing, identifying and managing material risks from "cybersecurity threats," defined as any "potential unauthorized occurrence on or conducted through a company's information systems that may result in, adverse effects on the confidentiality, integrity, or availability of a company's information systems or any information residing therein."

The disclosure must be in sufficient detail for a reasonable investor to understand those processes, and Item 106(b) includes the following non-exclusive list of disclosures companies should address:

- whether and how any such 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 the processes; and

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

Companies must also describe whether any risks from cybersecurity threats (including prior 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.

What will companies need to disclose about board oversight of cybersecurity risks?
New Item 106(c)(1) of Regulation S-K will require companies to describe the board's oversight of risks from cybersecurity threats, including to identify any board committee responsible for such oversight and describe the process by which the board or any committee is informed about cybersecurity risks. While the SEC's initial proposal would have required companies to identify whether any director has cybersecurity expertise, this was eliminated in the final rules.

What will companies need to disclose about management oversight of cybersecurity risks?
New Item 106(c)(2) of Regulation S-K requires companies to disclose in their Form 10-Ks the role of management in assessing and managing material risks from cybersecurity threats, including the following non-exclusive list of disclosures companies should address:

- whether and which management positions or committees are responsible for assessing and managing cybersecurity risk, and the relevant expertise of such persons in such detail as necessary to fully describe the nature of the expertise; expertise may come from prior work experience, degrees or certifications or knowledge, skills, or other background (the requirement to disclose whether the company has a designated chief information security officer was eliminated in the final rules);

- 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 of the board of directors.

Must foreign private issuers make similar disclosures regarding cybersecurity risk management, strategy and governance?
Yes. The SEC is amending Form 20-F (but not Form 40-F) to require similar disclosures by foreign private issuers.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jonathan H. Ashtor
+1-212-373-3823
jashtor@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

John P. Carlin
+1-202-223-7372
jcarlin@paulweiss.com

Christopher J. Cummings
+1-212-373-3434
ccummings@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Brian M. Janson
+1-212-373-3588
bjanson@paulweiss.com

Luke Jennings
+1-212-373-3591
ljennings@paulweiss.com

Jeh Charles Johnson
+1-212-373-3093
jjohnson@paulweiss.com

Christodoulos Kaoutzanis
+1-212-373-3445
ckaoutzanis@paulweiss.com

John C. Kennedy
+1-212-373-3025
jkennedy@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Raphael M. Russo
+1-212-373-3309
rrusso@paulweiss.com

Monica K. Thurmond
+1-212-373-3055
mthurmond@paulweiss.com

Peter Carey
+1-202-223-7485
pcarey@paulweiss.com

Anna Gressel
+1-212-373-3388
agressel@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

David K. Kessler
+1-212-373-3614
dkessler@paulweiss.com

Frances F. Mi
+1-212-373-3185
fmi@paulweiss.com

Practice Management Consultant Jane Danek contributed to this Client Memorandum.