O'Melveny | Public Company Advisory

Complying with the SEC's New Cybersecurity Reporting Requirements

The Securities and Exchange Commission (SEC) adopted new rules in 2023 to enhance and standardize disclosures regarding cybersecurity processes and cybersecurity incidents by public companies. The new rules require current disclosure of material cybersecurity incidents and annual disclosure regarding cybersecurity risk management, strategy and governance. The new requirements build on prior SEC and SEC staff guidance addressing cybersecurity matters.

New Current Reporting Requirements

Item 1.05 of Form 8-K for events ***on or after December 18, 2023***[1,2]

Content of Disclosure

- Item 1.05 of Form 8-K requires registrants to disclose, to the extent known at the time of the Form 8-K filing:
  - the material aspects of the nature, scope and timing of the incident, and
  - the material impact or reasonably likely material impact of the incident, including to the registrant's financial condition and results of operations.
- A registrant is not required to include specific or technical information about its planned response or potential system vulnerabilities in such detail as would impede the incident response or remediation (Instruction 4 to Item 1.05).
- A Form 8-K amendment must be filed to provide any required information that is not determined or is unavailable at the time of the initial 8-K filing.

Materiality Trigger

- Item 1.05 disclosure must be filed within 4 business days after the registrant determines that a cybersecurity incident it has experienced is ***material***.
- In many cases, the registrant will be unable to determine materiality the same day the incident is discovered.
- Materiality determinations must be made ***"without unreasonable delay"*** after discovery of a cybersecurity incident (Instruction 1 to Item 1.05). As stated in the SEC adopting release, "adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance."

Determining Materiality

- Information is material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the "total mix" of information available.
- Any doubts about materiality should be resolved in favor of disclosure.
- The materiality analysis should evaluate the total mix of information and consider all relevant facts and circumstances, including both qualitative and quantitative factors. Example factors include:
  - Financial impact
  - Nature and scope of incident / access to systems and data
  - Duration of incident / outages
  - Costs for response and remediation
  - Harm to reputation, customer or vendor relations or competitiveness
  - Litigation / regulatory actions

Filed, Not Furnished

- Item 1.05 of Form 8-K will be deemed "filed" with the SEC (versus "furnished").
- Similar to other 8-K items requiring materiality determinations, an untimely Item 1.05 8-K will not impair S-3 eligibility and will have limited safe harbor protection from liability under Section 10(b) and Rule 10b-5 under the Exchange Act.

Form 8-K due *four business days* after determination of a *material* cybersecurity incident

Third Party Systems

Item 1.05 disclosure is also required for cybersecurity incidents involving information resources used by the registrant, even if they are not owned by the registrant (i.e., third-party systems). If material, disclosure is required based on information available to the registrant.

National Security Exception

- In limited instances, the 8-K may be delayed if the U.S. Attorney General gives the SEC written notice that *disclosure* would pose substantial risk to national security or public safety.
- The Attorney General may consider other Federal or law enforcement agencies' findings.
- Initial delay limited to up to 30 days, with possible delay of another 30 days and, in exceptional cases, up to final 60 days.
- DOJ Guidelines and FBI Guidance outline delay request process.
- SEC staff Form 8-K CDIs (Section 104B) address interplay with 8-K reporting.

Inline XBRL Tagging

Inline XBRL tagging of Item 1.05 disclosure is required beginning one year after the initial compliance date.

KEY TERMS

See the next page for definitions of key terms.

[1] **Note**: Smaller reporting companies have an extended compliance date of June 15, 2024.
[2] **Note**: For foreign private issuers, Form 6-K now provides that material cybersecurity incidents are events that may trigger a Form 6-K.

New Annual Reporting Requirements

Part I, Item 1C of Form 10-K for ***fiscal years ending on or after December 15, 2023***[3]

Risk Management and Strategy

- New Item 106(b) of Regulation S-K requires a description of the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats. Disclosure must be in sufficient detail for a reasonable investor to understand the registrant's processes.
- The following non-exclusive list of items should be addressed in the disclosure:
  - whether *and how* the registrant's processes have been integrated into its overall risk management system or processes,
  - whether the registrant engages assessors, consultants, auditors or other third parties in connection with its processes (a registrant is not required to name such persons or describe the services they provide), and
  - whether the registrant has processes to oversee and identify material cybersecurity risks associated with use of third-party service providers.
- Registrants must also describe whether any risks from cybersecurity threats, including resulting from 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. If so, the disclosure must also explain *how*.

Board Governance

- New Item 106(c) requires a description of the board of directors' process for overseeing risks from cybersecurity threats.
- The disclosure must identify the board committee or subcommittee, if any, responsible for the cybersecurity risk oversight, and describe the process by which the board or the applicable committee is informed about the risks.

Management Governance

- New Item 106(c) also requires a description of management's role in assessing and managing the registrant's material risks from cybersecurity threats.
- The following is a non-exclusive list of disclosure items that should be addressed:
  - whether and which management positions or committees are responsible for assessing and managing cybersecurity risks,
  - the relevant expertise of the management positions or committees in such detail to fully describe the nature of their expertise,
    - for example, prior work experience in cybersecurity, relevant degrees or certifications, skills or other background in cybersecurity
  - the processes by which the management positions or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents, and
  - whether the management positions or committees report information about the material risks from cybersecurity threats to the board of directors or a committee or subcommittee of the board of directors.

KEY TERMS

Cybersecurity Incident:
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.

Cybersecurity Threat:
Any potential unauthorized occurrence on or conducted through a registrant's information systems that may result in adverse effects on the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein.

Information Systems:
Electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

Inline XBRL Tagging

Inline XBRL tagging of disclosure is required beginning one year after the initial compliance date.

Key Contacts

Shelly Heyduk, *Partner*
+1 949 823 7968
sheyduk@omm.com

Robert Plesnarski, *Partner*
+1 202 383 5149
rplesnarski@omm.com

Michelle Earley, *Partner*
+1 737 261 8629
mearley@omm.com

Randall W. Edwards, *Partner*
+1 415 984 8716
redwards@omm.com

Sid Mody, *Partner*
+1 945 221 1645
smody@omm.com

Scott Pink, *Special Counsel*
+1 650 473 2629
spink@omm.com

[3] **Note:** The SEC adopted parallel disclosure requirements for foreign private issuers in Form 20-F.