SEC CYBERSECURITY RULES: A SNAPSHOT

APRIL 2025

This Snapshot summarizes the SEC's cybersecurity rules and related SEC staff guidance.

OVERVIEW

The SEC's cybersecurity rules (the "rules") require registrants to disclose material cybersecurity incidents in Form 8-K. The rules also require annual disclosures about a registrant's policies and procedures to identify and manage:

- Cybersecurity risk
- The board's oversight of risks from cybersecurity threats
- Management's role in assessing and managing material risks from cybersecurity threats

The rules apply to virtually all registrants, except for asset-backed issuers and Canadian issuers in the Multi-Jurisdictional Disclosure System.

SEC Reference

Regulation S-K, Item 106

Item 1.05 of Form 8-K

Item 16K of Form 20-F

ANNUAL DISCLOSURES

Item 106 of Regulation S-K ("S-K") and Item 16K of Form 20-F ("Item 16K") requires a registrant to disclose information about its cybersecurity risk management, strategy, and governance in sufficient detail for a reasonable investor to understand. Although S-K Item 106 and Item 16K only apply to annual reports on Forms 10-K and 20-F, registrants should consider the materiality of cybersecurity risks and incidents when preparing disclosures in connection with registration statements.

REQUIREMENT	REGISTRANTS MUST DESCRIBE:	REGISTRANTS MUST, AT A MINIMUM, ADDRESS:
Risk Management and Strategy Item 106(b)	▶ Their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats ▶ Whether any risks from cybersecurity threats have materially affected (or	▶ Whether and how they have integrated cybersecurity processes into their overall risk management process ▶ Whether they engage third parties in connection with such processes

REQUIREMENT	REGISTRANTS MUST DESCRIBE:	REGISTRANTS MUST, AT A MINIMUM, ADDRESS:
	are reasonably likely to materially affect) their business strategy, results of operations, or financial conditions	▶ Whether they have processes to oversee and identify material risks from cybersecurity threats associated with third-party service providers ▶ Any other information necessary for a reasonable investor to understand their cybersecurity processes
Governance Item 106(c)	▶ The board's oversight of risks from cybersecurity threats and any board committee or subcommittee responsible for the oversight of these risks and the related processes by which such committee is informed about the risks ▶ Management's role in assessing and managing material risks from cybersecurity threats	▶ Whether and which management positions or committees are responsible for assessing and managing cybersecurity risks and Management's relevant expertise ▶ How management or committees are informed about and monitor cybersecurity incidents ▶ Whether such information is reported to the board or board committee

At the 2024 AICPA & CIMA Conference on Current SEC and PCAOB Developments ("2024 Conference"), the SEC staff addressed its observations on the annual risk management, strategy, and governance disclosures required by S-K Item 106, noting that:

- If a registrant has a process for identifying, assessing, and managing significant cybersecurity risks, the disclosure should clearly describe this process to inform investors. Merely stating that a process exists is not enough. The disclosure should also cover any processes associated with third-party service providers used by the registrant.
- If a group is responsible for assessing and managing cybersecurity risks, the expertise of each individual should be described, rather than focusing on a single individual or the group in total. This ensures that investors have a clear understanding of the collective expertise within the organization, and the impact to the registrant if the composition of the group changes.

INCIDENT DISCLOSURES

Definitions in S-K Item 106

- **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 System**: 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.

Item 1.05 of Form 8-K ("Item 1.05") requires a registrant to disclose a cybersecurity incident within four business days from the date it determines the incident(s) to be material, unless the U.S. Attorney General ("Attorney General")

notifies the SEC that such disclosure poses a substantial risk to national security or public safety.[1] While the materiality determination may occur upon the same date or after the incident's discovery, it must be made without "unreasonable delay." Foreign private issuers (FPIs) must make similar disclosures on Form 6-K.

The materiality evaluation for a cybersecurity incident is consistent with the evaluation of any other event or risk that a registrant may face. That is, an incident is material if "there is substantial likelihood that a reasonable shareholder would consider it important" or if it would have "significantly altered the 'total mix' of information made available" from the perspective of a reasonable investor. The materiality determination may require considerable judgment as registrants must consider all relevant facts and circumstances, including both quantitative and qualitative factors.

When required, the registrant must disclose the material:

- Aspects of the scope, nature, and timing of the cybersecurity incident[2]
- Impact or reasonably likely material impact on the registrant's financial condition and results of operations

If the registrant does not have the information required to make these disclosures at the time of filing, it must include a statement to that effect and file an amended Form 8-K within four business days after the information becomes available. The rule does not require a registrant to update information about the incident in its Form 8-K, Form 10-Q or Form 10-K (or Form 20-F). However, a registrant has a duty to update when it determines prior disclosure was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made or becomes materially inaccurate after it is made.

Disclosures made in Item 1.05 are eligible for the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act.

BDO INSIGHT: ROBUST PROCESSES AND CONTROLS ARE NEEDED TO ADDRESS CYBERSECURITY DISCLOSURE REQUIREMENTS

The definition of a cybersecurity incident includes "a series of related unauthorized occurrences" to reflect that cyberattacks can compound over time, rather than occurring at a point in time. In the adopting release for the rules, the SEC gave the following examples:

- The same malicious actor engages in small but continuous cyberattacks against the registrant and collectively, they are material.
- A series of related attacks from multiple actors attack the same vulnerability and collectively, impede the registrant's business in a material way.

Evaluating whether a series of related unauthorized occurrences are collectively material to the registrant may require the application of professional judgment, based on the facts and circumstances.

Moreover, the definition of an information system includes resources "used by" the registrant. Accordingly, the registrant must determine whether it is required to report cybersecurity incidents that occur on third-party systems used by the registrant.

Registrants must have processes and controls in place to evaluate such events for disclosure.

After the adoption of the rules in 2023, the SEC staff has released guidance on incident disclosures to assist registrants with their implementation and interpretation of the disclosure requirements.

Voluntary Disclosure of Cybersecurity Incidents

In May 2024, the SEC staff issued a **statement** clarifying that registrants who voluntarily disclose cybersecurity incidents in Form 8-K should not do so under Item 1.05, as it may confuse investors. Registrants that voluntarily disclose cybersecurity incidents may do so under a different item in Form 8-K, such as Item 8.01 ("Item 8.01"). The SEC staff believes the distinction between disclosing a material cybersecurity incident under Item 1.05 and voluntarily disclosing under another item, such as Item 8.01, allows investors to make better investing and voting decisions related to material cybersecurity incidents.

[1] The initial delay period of up to 30 days may be extended by the U.S. Attorney General up to a total of 90 days after which the SEC will consider additional requests for delay and potential relief through exemptive order.

[2] Specific or technical information about the registrant's cybersecurity system, planned response to the incident, or potential system vulnerabilities is not required.

The following details the SEC staff's statement on disclosing material and other cybersecurity incidents:

CYBERSECURITY INCIDENT DETERMINATION	IS DISCLOSURE REQUIRED IN FORM 8-K?
MATERIAL	Yes. Registrants must disclose material cybersecurity incidents under Item 1.05 within four business days from the date they determine the incident(s) to be material.
MATERIALITY ASSESSMENT INCOMPLETE	No. Registrants that voluntarily disclose cybersecurity incidents in Form 8-K should do so under another item, such as Item 8.01, and not Item 1.05. Registrants that later determine an incident is material must disclose the incident under Item 1.05 within four business days of the date they determine the incident is material. Registrants may refer to their previous disclosures about the incident, but additional disclosure may be necessary to comply with the requirements under Item 1.05.
IMMATERIAL	No. Registrants that voluntarily disclose cybersecurity incidents in Form 8-K should do so under another item, such as Item 8.01, not Item 1.05.

The SEC staff stated that the intent of this clarification is not to deter registrants from voluntarily reporting cybersecurity incidents, but rather to help investors more readily distinguish between material and other cybersecurity incidents.

Additionally, the SEC staff reminded registrants that determining the materiality of a cybersecurity incident involves an assessment of both quantitative and qualitative factors and must be made without unreasonable delay. At the 2024 Conference, the SEC staff shared its observation that cybersecurity incident disclosures often emphasize quantitative factors, indicating that the incident did not materially affect the registrant's operations or financial condition. However, the assessment of an incident's materiality should also include qualitative factors, such as reputational damage and the impact on customer relationships.

Cybersecurity Incidents Involving Ransomware

SEC STAFF GUIDANCE

C&DIs 104B.05 through 104B.09

The SEC staff's C&DIs provide guidance on the materiality assessment and disclosure requirements under various scenarios involving ransomware attacks:

C&DI	GUIDANCE
If the ransomware payment occurs before the registrant makes a materiality determination, does the registrant need to assess whether the incident is material?	Yes. The registrant must assess the materiality of the incident, even though the incident is resolved (that is, the resolution of the incident does not alleviate the registrant's obligation to determine the materiality of the incident). If material, the registrant must report the incident under Item 1.05 within four business days from the date it determined the incident is material.
If the registrant determines the incident is material, but the ransomware payment is made before filing Item 1.05, does the registrant need to disclose the incident?	Yes. The registrant must report the incident under Item 1.05 within four business days from the date it determined the incident is material. The resolution of the incident does not exempt the registrant from disclosure under Item 1.05.
If under its insurance policy, the registrant is reimbursed for all (or most) of the ransomware payment made, is the incident immaterial?	Not necessarily. The registrant may not conclude the incident is immaterial based solely on the fact that all or a substantial portion of the ransomware payment was reimbursed under its insurance policy. When determining whether the incident is material, the registrant must consider all relevant facts and circumstances, including both quantitative and qualitative factors. For example, the registrant may consider an increase in the cost and availability of future insurance policies that cover cybersecurity incidents.
If the ransomware payment is a small dollar amount, is the incident immaterial?	Not necessarily. The registrant may not conclude the incident is immaterial based solely on the quantitative harm to the registrant (for example, the small amount paid). Qualitative factors, such as reputational harm, must also be considered.

The definition of a cybersecurity incident includes "a series of related unauthorized occurrences" as cyberattacks sometimes compound over time, rather than at a point in time. The C&DIs also remind registrants who have experienced multiple individually immaterial cybersecurity incidents that disclosure under Item 1.05 is required if the incidents are related and collectively material.

Requests to Delay Disclosure of Material Cybersecurity Incidents

SEC STAFF GUIDANCE

C&DIs 104B.01 through 104B.04

Registrants may delay disclosing a material cybersecurity incident when the Attorney General) notifies the SEC in writing that such disclosure poses a substantial risk to national security or public safety.[3] The SEC staff's C&DIs address the timeline to disclose material cybersecurity incidents when registrants request to delay disclosure in the interest of national security or public safety.[4] The guidance is as follows:

[3] Item 1.05(c) of Form 8-K.

[4] The DOJ released **guidance** that registrants should follow to obtain a delay, which includes information about the Attorney General's process to determine whether a delay is appropriate.

SCENARIO	FORM 8-K FILING DUE DATE
The Attorney General does not respond to the registrant's request or declines to make a determination.	Within four business days from the date the registrant determined the cybersecurity incident is material
The Attorney General notifies the SEC in writing that such disclosure poses a substantial risk to national security or public safety, and: ▶ The registrant requests an additional delay, but the Attorney General does not respond to the request or declines to make a determination. ▶ During the delay period, the Attorney General notifies the registrant and SEC that disclosure no longer poses a substantial risk to national security or public safety.	Within four business days from the date: ▶ The delay period ends ▶ The Attorney General notifies the registrant and SEC

The SEC staff also indicated that consulting with the U.S. Department of Justice ("DOJ") regarding the availability of a delay in reporting does not indicate that the registrant has concluded the incident is material. Accordingly, a registrant may consult with the DOJ or other national securities agencies before its materiality assessment is complete.

Contacts

TIMOTHY KVIZ
National Managing Principal, SEC Services
703-245-8685 / tkviz@bdo.com

PAULA HAMRIC
Professional Practice Principal, SEC Services
312-616-3947 / phamric@bdo.com

BRANDON LANDAS
Professional Practice Principal, SEC Services
312-233-1887 / blandas@bdo.com

MEGHAN DEPP
Professional Practice Principal, SEC Services
248-688-3368 / mdepp@bdo.com

Material discussed in this publication is meant to provide general information and should not be acted on without professional advice tailored to your needs.