Deloitte.

Heads Up | Volume 30, Issue 13
July 30, 2023

In This Issue

SEC Issues New Requirements for Cybersecurity Disclosures

Background

On July 26, 2023, the SEC issued a final rule[1] that requires registrants to provide enhanced and standardized disclosures regarding "cybersecurity risk management, strategy, governance, and incidents." The final rule addresses concerns over investor access to timely and consistent information related to cybersecurity as a result of the widespread use of digital technologies and artificial intelligence, the shift to hybrid work environments, the rise in the use of crypto assets, and the increase in illicit profits from ransomware and stolen data, all of which continue to escalate cybersecurity risk and its related cost to registrants and investors.

The SEC has monitored registrants' disclosure practices as cybersecurity risk has evolved. In 2011 and 2018, the SEC issued interpretive guidance[2] that did not create any new disclosure obligations; instead, the guidance presented the SEC's views on how its existing rules should be interpreted in connection with cybersecurity threats and incidents.[3] The interpretive guidance discussed the impact of cybersecurity risks and incidents on disclosure requirements for risk factors, MD&A, and the financial statements and expanded the SEC's interpretive guidance on cybersecurity policies and controls, most notably those related to cybersecurity escalation procedures and the application of insider trading prohibitions. Further, the guidance addressed the importance of avoiding selective disclosure as well as considering the role of the board of directors in risk oversight. See Deloitte's February 23, 2018, *Heads Up* for more details about the interpretive guidance.

[1] SEC Final Rule Release No. 33-11216, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure*.
[2] CF Disclosure Guidance Topic No. 2, "Cybersecurity," and SEC Interpretive Release No. 33-10459, *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*.
[3] The SEC also issued an investigative report on October 16, 2018, in which it cautioned companies to consider cybersecurity threats when they are implementing their internal accounting controls. See Deloitte's October 30, 2018, *Heads Up* for more information.

By contrast, the final rule establishes new requirements related to:

- Material cybersecurity incidents, which would need to be disclosed on Form 8-K within four business days of their being deemed material. A registrant may delay filing the Form 8-K if the U.S. Attorney General "determines immediate disclosure would pose a substantial risk to national security or public safety."
- Annual disclosures in Form 10-K pertaining to (1) cybersecurity risk management and strategy, (2) "management's role in assessing and managing material risks from cybersecurity threats," and (3) "the board of directors' oversight of cybersecurity risks."
- The presentation of disclosures in Inline eXtensible Business Reporting Language (Inline XBRL).

All types of periodic SEC filers are affected by the final rule, including domestic registrants, foreign private issuers (FPIs),[4] smaller reporting companies, and emerging growth companies.

Changes From the Proposed Rule

The final rule incorporates certain key changes from the proposed rule,[5] including:

- Narrowing the scope of the cyber incident disclosures and adding a limited delay for disclosures that would pose a substantial risk to national security or public safety.
- Requiring registrants to use an amended Form 8-K instead of Forms 10-Q and 10-K to update incident disclosures.
- Omitting the aggregation of immaterial incidents for disclosure in Forms 10-Q and 10-K; however, a series of related unauthorized occurrences may prompt a requirement to provide disclosures on Form 8-K.
- Streamlining the proposed disclosure elements related to risk management, strategy, and governance with a focus on processes as opposed to specific policies and procedures.
- Removing the proposed requirement to disclose cybersecurity expertise of the board of directors.
- Adding transition provisions for disclosing material cyber incidents on Form 8-K and for providing annual cybersecurity risk management, strategy, and governance disclosures.

Initial Reporting of Material Cybersecurity Incidents

The final rule amends Form 8-K to add Item 1.05, "Material Cybersecurity Incidents," which requires a registrant to file a Form 8-K to disclose a material cybersecurity incident within **four business days** from the date on which the registrant determines that the incident is considered material to the registrant. Item 1.05 defines a cybersecurity incident as "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." In addition, the final rule broadly defines "information systems" to encompass resources owned or used by the registrant (e.g., cloud-based or hosted systems) and will require issuers to consider incidents occurring both internally and within third-party service providers. A cybersecurity incident could occur accidentally or because of a deliberate attack.

[4] The final rule amends Forms 20-F and 6-K to require FPIs to provide disclosures that are generally consistent with those discussed herein for domestic registrants. Specifically, FPIs must disclose in their annual Form 20-F the board's oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats. The final rule also requires FPIs to furnish on Form 6-K information on material cybersecurity incidents that they disclose or publicize in a foreign jurisdiction to any stock exchange or security holders.

[5] SEC Proposed Rule Release No. 33-11038, *Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure.*

Connecting the Dots

Although the final rule includes examples of cybersecurity incidents, a registrant will need to use judgment to determine whether "any information" residing in its information system has been jeopardized. Such judgment will vary on the basis of factors such as the complexity of the registrant's information, the importance of the information to its operations, and the nature and extent of the information. Further, the final rule notes that "the definition [of cybersecurity incident] is not self-executing; rather it is operationalized by Item 1.05, which is conditioned on the incident having been material to the registrant."

Further, given that the definition of a cybersecurity incident extends to "'a series of related unauthorized occurrences,'" a registrant will still have to consider whether to aggregate related cyber incidents. For example, aggregation would be expected when, collectively, the following incidents are material: (1) incidents in which the same malicious actor engages in a number of smaller, continuous attacks against the same company or (2) there are related attacks from multiple actors exploiting the same vulnerability. Thus, a registrant may need to consider establishing processes for, among other things, (1) inventorying *related* immaterial incidents, (2) updating the inventoried incidents as changes occur, (3) continually updating its assessment of the aggregate materiality of such *related* incidents, and (4) retaining any information necessary for providing disclosures in case they are ultimately required. Registrants may want to consider whether their current cybersecurity monitoring infrastructure is designed to accommodate this type of assessment and reporting.

Under Form 8-K, Item 1.05, a registrant must disclose the following information about the cybersecurity incident if known at the time of the filing:

- "[T]he material aspects of the nature, scope, and timing of the incident."
- "[T]he material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations."[6]

The registrant must also provide disclosures if any of the above required information is not determined or is unavailable at the time of the filing. A registrant would need to seek to obtain such information without unreasonable delay and file an amended Form 8-K containing the information within four business days of when the information is determined or becomes available. An amended Form 8-K may similarly be required if the registrant subsequently determines that information previously provided is inaccurate or materially misleading.

The instructions to Item 1.05 further explain that a registrant is not required to include specific or technical information in its disclosures that could affect its incident response or remediation or reveal potential system vulnerabilities.

Connecting the Dots

To maintain eligibility to use Form S-3 or Form SF-3, registrants are required to be "timely filers"; that is, they must file Forms 8-K, 10-Q, and 10-K by their respective due dates. However, the final rule excludes from the scope of this requirement the failure to file a Form 8-K on a timely basis as a result of a material cybersecurity incident (i.e., the failure to file Form 8-K in accordance with Item 1.05 on time related to a material cybersecurity incident will not affect a registrant's Form S-3 or Form SF-3 eligibility).

[6] Note that the final rule's inclusion of "financial condition and results of operations" is not exclusive, and companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.

Materiality Assessment of Cybersecurity Incidents

A Form 8-K must be filed when a cyber incident is determined to be material. The final rule acknowledges that, in many cases, a registrant may not be able to determine the materiality of an incident on the same day it is discovered. While there is no specific deadline by which a registrant must determine whether an event is material, it must make its materiality determinations "without unreasonable delay." Examples of an unreasonable delay include intentionally deferring committee meetings to determine materiality beyond the time it typically takes to convene such meetings (if the determination of materiality is made by committee), altering existing incident response policies to extend deadlines, or changing the criteria related to reporting the incident to management or the committee.

When assessing materiality, a registrant must be objective and consider all relevant quantitative and qualitative factors. The final rule indicates that the definition of "materiality" is consistent with that established by the U.S. Supreme Court in multiple cases, including *TSC Industries, Inc. v. Northway, Inc.* (426 U.S. 438, 449 (1976)); *Basic, Inc. v. Levinson* (485 U.S. 224, 232 (1988)); and *Matrixx Initiatives, Inc. v. Siracusano* (563 U.S. 27 (2011)). Quoting *TSC Industries, Inc. v. Northway, Inc.*, the SEC notes in the final rule that "information is material if (1) 'there is a substantial likelihood that a reasonable shareholder would consider it important' in making an investment decision" or (2) disclosure of the information would have been viewed by the reasonable investor as having "'significantly altered the 'total mix' of information made available.'" Therefore, a lack of significant quantifiable harm does not necessarily mean that an incident is not material.

Factors to consider in the assessment of materiality include, but are not limited to, the probability of an adverse outcome; the potential significance of the loss; and the nature and extent of harm to individuals, customers, vendor relationships, and the registrant's reputation and competitiveness. The possibility of litigation or regulatory investigations may also affect materiality assessments. In a manner consistent with the SEC's 2018 interpretive guidance, "companies generally weigh, among other things, the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company's operations."

The materiality of the impact of a cybersecurity incident to a registrant does not depend on whether the registrant owns the relevant systems. Therefore, a registrant is not exempt from disclosing cybersecurity incidents on third-party systems. However, a registrant is not required to name third parties or describe the services provided by them.

Connecting the Dots

In some circumstances, it may be particularly challenging for a registrant to determine the materiality of a cyber incident, and it may need to use significant judgment when doing so. For example, if the registrant uses, but does not own, third-party resources, it may be difficult for the registrant to obtain the information it needs to make a materiality determination related to an incident involving such resources. This could be especially difficult if a third-party resource also uses outside service providers. However, as noted above, registrants are not exempt from disclosing third-party cyber events, nor is there a safe harbor for information disclosed about third-party systems. The SEC observed that the final rule generally does "not require that registrants conduct additional inquires outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants' disclosure controls and procedures." Registrants may wish to consider the design of their disclosure controls and procedures related to their communication processes with third-party service providers.

Temporary Delay of Disclosure as a Result of Concerns of National Security or Public Safety

Registrants may delay the filing of Form 8-K if it is determined by the U.S. Attorney General that such disclosure poses a substantial risk to national security or public safety. Registrants must notify the SEC of such determination in writing for each of the following delays:[7]

Initial delay	Up to 30 days after the date on which the registrant was otherwise required to provide the disclosure
Secondary delay	Extended for an additional period of up to 30 days
Final additional delay (extraordinary circumstances)	Extended for an additional period of up to 60 days
SEC exemptive order	If the U.S. Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief in an SEC exemptive order

Connecting the Dots

The final rule notes that the SEC has established an interagency communication process with the Department of Justice to facilitate the U.S. Attorney General's determination of national security risk. The Department of Justice will notify the respective registrant that communication to the SEC has been made so that a registrant may delay its Form 8-K filing. Registrants may want to consider developing a process as part of their cyber response framework that takes into account the required procedures to obtain this delay, if needed.

Risk Management, Strategy, and Governance

The final rule adds Item 106, "Cybersecurity," to Regulation S-K. Disclosure required by Item 106 is to be provided in Part I of Form 10-K in Item 1C, "Cybersecurity."

Risk Management and Strategy

Item 106(b)(1) requires a registrant to include a comprehensive disclosure of its processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats including:

- "Whether and how the described cybersecurity processes . . . have been integrated into the registrant's overall risk management system or processes;
- Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and
- Whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider."

The list above is not all-inclusive, and registrants should consider disclosing "whatever information is necessary . . . for a reasonable investor to understand their cybersecurity processes."

Registrants must also explain whether any risks from cybersecurity threats, including those resulting from previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant's business strategy, results of operations, or financial condition and, if so, how.

[7] The final rule notes that "[t]he delay provision for substantial risk to national security or public safety is separate from Exchange Act Rule 0-6, which provides for the omission of information that has been classified by an appropriate department or agency of the Federal government for the protection of the interest of national defense or foreign policy. 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."

Connecting the Dots

The final rule streamlines certain disclosures set forth in the proposed rule. However, registrants will need to consider how they describe their processes to avoid giving bad actors a "road map" to potential vulnerabilities in their processes or associated information systems. Given the relatively short implementation period, registrants may consider drafting these disclosures in advance of the upcoming 10-K reporting season to allow sufficient time for their review.

Governance

The SEC observed in the final rule that disclosing cybersecurity risk governance from the perspective of management and the board of directors allows investors to understand how leadership oversees and implements its cybersecurity processes.

Disclosure of the Board's Roles and Responsibilities

Item 106(c)(1) requires a registrant to provide specific disclosures about the oversight of cybersecurity risk by its board of directors, including:

- A description of the board's oversight of risks from cybersecurity threats.
- Identification of any board committee or subcommittee responsible for oversight of risk from cybersecurity threats (if applicable).
- A description of the processes by which the board or such committee is informed of risk from cybersecurity threats.

Connecting the Dots

The requirement to disclose the frequency of discussions between the board or committees and management about cybersecurity was eliminated in the final rule. Nevertheless, a registrant may include a discussion of such frequency in its descriptions of the process by which its board or relevant committee is informed of cybersecurity risks.

Disclosure of Management's Responsibilities

Item 106(c)(2) requires a registrant to disclose how management assesses and responds to material risks from cybersecurity threats, including, but not limited to:

- "Whether and which management positions or committees are responsible for assessing and managing such risks, and [their relevant expertise]."
- "The processes by which such persons or committees [monitor cybersecurity incidents]."
- Whether and how management reports cybersecurity information "to the board of directors or a committee or subcommittee of the board of directors."

Connecting the Dots

When disclosing relevant expertise of management, registrants may want to consider the examples in Item 106(c), Instruction 2. Such examples address prior work experience in cybersecurity; any relevant degrees or certifications; and any knowledge, skills, or other background in cybersecurity.

Transition Provisions

The final rule is effective 30 days after its publication in the *Federal Register* and includes the following transition provisions:

Disclosures will be required in:[8]	
Form 8-K, Item 1.05, "Material Cybersecurity Incidents"	*For all registrants other than smaller reporting companies* — The later of 90 days after the date of publication in the *Federal Register* or December 18, 2023. *For smaller reporting companies* — The later of 270 days from the effective date of the rules or June 15, 2024.
Regulation S-K, Item 106 (in Form 10-K, Item 1C, "Cybersecurity")	Beginning with annual reports for fiscal years ending on or after December 15, 2023.

Additional Cybersecurity Rulemaking

In February 2022, the SEC issued a proposed rule[9] that would require advisers and funds to adhere to cybersecurity policies and procedures, disclose cybersecurity risks and significant cybersecurity incidents in their brochures and registration statements, and enhance recordkeeping requirements of cybersecurity-related information. The SEC's rulemaking agenda also includes multiple other proposed rules related to cybersecurity considerations for broker-dealers, clearing agencies, major security-based swap participants, the Municipal Securities Rulemaking Board, national securities associations, national securities exchanges, security-based swap data repositories, security-based swap dealers, and transfer agents.

Other Resources

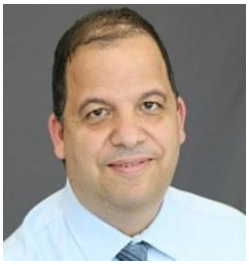
In addition to those discussed previously, resources such as the following publications may help companies assess their approach to cyber risk, governance, and related disclosures:

- Deloitte's *On the Audit Committee's Agenda — 2023: The Year of the Risk-Centric Agenda*, which highlights areas of focus for audit committees, including cybersecurity risk oversight.
- *Audit Committee Practices Report: Priorities and Committee Composition*, a collaborative effort between Deloitte's Center for Board Effectiveness and the Center for Audit Quality, which includes a survey of audit committee priorities and composition, including observations related to the audit committee's role in cybersecurity oversight.

Contacts

Lior Kalev
Partner,
Head of Cyber Center

lkalev@deloitte.co.il



Ram Nasi
Senior Consultant,
Cyber Risk Services,
IL Cyber Center
Ransi@deloitte.co.il

[8] Adoption dates applicable to FPIs for disclosures in Form 6-K are consistent with Form 8-K, Item 1.05, and disclosures in Form 20-F are consistent with Item 106.

[9] SEC Proposed Rule Release No. 33-11028, *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies.*

Dbriefs for Financial Executives

We invite you to participate in Dbriefs, Deloitte's live webcasts that give you valuable insights into important developments affecting your business. Topics covered in the Dbriefs for Financial Executives series include financial reporting, tax accounting, business strategy, governance, and risk. Dbriefs also provide a convenient and flexible way to earn CPE credit — right at your desk.

Subscriptions

To subscribe to Dbriefs, or to receive accounting publications issued by Deloitte's Accounting and Reporting Services Department, please register at My.Deloitte.com.

The Deloitte Accounting Research Tool

Put a wealth of information at your fingertips. The Deloitte Accounting Research Tool (DART) is a comprehensive online library of accounting and financial disclosure literature. It contains material from the FASB, EITF, AICPA, PCAOB, and SEC, in addition to Deloitte's own accounting manuals and other interpretive guidance and publications.

Updated every business day, DART has an intuitive design and navigation system that, together with its powerful search and personalization features, enable users to quickly locate information anytime, from any device and any browser. While much of the content on DART is available at no cost, subscribers have access to premium content, such as Deloitte's *FASB Accounting Standards Codification Manual*. DART subscribers and others can also subscribe to *Weekly Accounting Roundup*, which provides links to recent news articles, publications, and other additions to DART. For more information, or to sign up for a free 30-day trial of premium DART content, visit dart.deloitte.com.