DORSEY
DORSEY+WHITNEY LLP

New SEC Cybersecurity Rules Require Mandatory Disclosure

by Cam C. Hoang

On July 26, 2023, the Securities and Exchange Commission adopted new rules imposing disclosure requirements regarding cybersecurity risk management, strategy, governance and incidents. The new rules, which became effective September 5, 2023, apply to nearly all domestic SEC reporting issuers and those foreign private issuers that report on Form 20-F. Foreign private issuers that report on Form 40-F are subject only to the limited cybersecurity incident disclosure requirements.

For all affected issuers, the new disclosures regarding cybersecurity risk management, strategy and governance will be required in the annual report for fiscal years ending on or after December 15, 2023. For issuers other than smaller reporting companies, the disclosures required in connection with a cybersecurity incident will be required after December 18, 2023. Smaller reporting issuers will have an additional 180 days before they are required to comply with the cybersecurity incident reporting requirements, so after June 15, 2024. Issuers must tag the new disclosures in Inline XBRL, including by block text tagging narrative disclosures and detail tagging quantitative amounts, beginning one year after the initial compliance date for the issuer for the related disclosure requirement.

The new rules include three important definitions that are critical to the new disclosures:

- *Cybersecurity incident* means 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. The Commission advises that "cybersecurity incidents" are to be construed broadly, as cyberattacks sometimes compound over time, rather than present as a discrete event. Furthermore, an accidental occurrence may be a cybersecurity incident under the definition, even if there is no confirmed malicious activity.
- *Cybersecurity threat* means 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.

Related People

- Cam C. Hoang

Related Capabilities

- Corporate Governance & Compliance
- Privacy & Social Media

- *Information systems* means electronic information resources, owned or used by the company, 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 company's information to maintain or support the company's operations. The definition covers resources owned by third parties.

The new rules are driven by the Commission's premise that investors need more timely and consistent cybersecurity disclosure to make informed investment decisions. The Commission also cites recent significant developments in cyber-regulation. The President signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") on March 15, 2022. The centerpiece of CIRCIA is the reporting obligation placed on companies in defined critical infrastructure sectors. Once rules are adopted by the Cybersecurity & Infrastructure Security Agency ("CISA"), these companies will be required to report covered cyber incidents to CISA within 72 hours of discovery, and report ransom payments within 24 hours. Importantly, reports made to CISA pursuant to CIRCIA will remain confidential; while the information contained therein may be shared across Federal agencies for cybersecurity, investigatory, and law enforcement purposes, the information may not be disclosed publicly, except in anonymized form. We note, however, that since the relevant triggers for reporting under the CIRCIA rules will likely substantially overlap the triggers under the SEC rules, the circumstances in which cybersecurity events remain confidential are likely to be limited.

Cybersecurity Risk Management Disclosures

For domestic filers, the disclosure requirements regarding cybersecurity risk management and governance are contained in Item 106(b) and (c) of Regulation S-K. For 20-F filers, the disclosure requirements are contained in Item 16K of Form 20-F. For Canadian issuers filing on Form 40-F under the U.S.-Canada Multijurisdictional Disclosure System ("MJDS"), the new rules do not impose any new risk management or governance disclosure requirements.

The new disclosures required in an issuer's annual report cover the processes that issuers have in place to address cybersecurity risks, as well as the Board's oversight role. Specifically the new rules require an issuer to describe:

1. the registrant's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In preparing that disclosure, the rules point to a non-exclusive list of topics to consider: (i) Whether and how any such processes have been integrated into the registrant's overall risk management system or processes; (ii) Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes; and (iii) Whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.
2. 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 registrant, including its business strategy, results of operations, or financial condition and if so, how. In the final rules, the Commission removed the proposed list

of risk types (i.e., “intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk”), to foreclose any perception that the rule prescribes cybersecurity policy, but we include the list here in case it may help issuers as they develop the required disclosure.

3. the board of directors’ oversight of risks from cybersecurity threats. If applicable, identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks.
4. management’s role in assessing and managing the issuer’s material risks from cybersecurity threats. In providing such disclosure, the rules point to a non-exclusive list of topics to consider: (i) 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; (ii) the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and (iii) 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.

In response to commenters’ concerns about the proposed disclosure’s security implications and prescriptiveness, in the final rule, the Commission streamlined the disclosure elements related to risk management, strategy, and governance, and it did not adopt the requirement to disclose board cybersecurity expertise. It also clarified that certain updated incident disclosure should be filed on an amended Form 8-K instead of Forms 10-Q and 10-K for domestic issuers, and on Form 6-K instead of Form 20-F for foreign private issuers.

Cybersecurity Incident Disclosures

Domestic issuers that experience a cybersecurity incident that the issuer determines to be material, must disclose information regarding the incident on Form 8-K within four business days of determining that the incident was material. Under the rules, filings may be delayed only in very limited circumstances, including, most notably, upon a determination by the United States Attorney General that immediate disclosure would pose a substantial risk to national security or public safety.

In response to commenters’ concerns with the scope and timing of the disclosure, in the final rule, the Commission narrowed the scope of disclosure to focus primarily on the impacts rather than the details of the incident, added a limited delay for disclosures, and omitted the aggregation of immaterial incidents for materiality analyses.

The requirements, set forth in Item 1.05 of Form 8-K, require the issuer to describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the issuer, including its financial condition and results of operations.

When Form 8-K Amendments Are Required

Furthermore, the issuer must amend a prior Form 8-K to disclose any information that

was not determined or was unavailable at the time of the initial filing. The final rules do not separately create or otherwise affect an issuer's duty to update its prior statements. However, an issuer may have a duty to correct prior disclosure that they determine was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made. The Commission advises issuers to consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident.

Impact of Late Form 8-K Filing on Form S-3 Eligibility

Issuers will be glad to learn that untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility, and that the disclosure is eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act.

Determining Materiality of a Cyberincident

"Material" as used in the new rules, is consistent with the definition of "materiality" generally applied under US securities laws, namely information that a reasonable investor would consider important in making an investment decision, and information that would alter the total mix of information made available.

The issuer should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. By way of illustration, harm to an issuer's reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the issuer. Similarly, the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal Governmental authorities and non-U.S. authorities, may constitute a reasonably likely material impact on the issuer. A decision to share information with other companies or government actors does not in itself necessarily constitute a determination of materiality.

Determining Materiality "Without Unreasonable Delay"

Recognizing that a materiality determination necessitates an informed and deliberative process, Instruction 1 to Item 1.05 states that issuers must make their materiality determination "without unreasonable delay." Among the examples provided to illustrate unreasonable delay, the adopting release provides that an issuer being unable to determine the full extent of an incident because of the nature of the incident or the issuer's systems, or otherwise the need for continued investigation regarding the incident, should not delay the issuer from determining materiality.

Cybersecurity Incidents on Third-Party Systems

The Commission noted that it is not exempting issuers from providing disclosures regarding cybersecurity incidents on third-party systems they use, nor are they providing a safe harbor for information disclosed about third-party systems, because whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them, especially as issuers increasingly rely on third-party cloud services.

Issuers should disclose based on the information available to them. The final rules generally do not require that issuers conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with issuers' disclosure controls and procedures.

Delaying Cybersecurity Incident Disclosure

An issuer may delay a 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 Commission of such determination in writing. In addition, the Commission envisions that other government agencies with conflicting disclosure regimes may work with the Attorney General in seeking delayed disclosure. Initially, disclosure may be delayed for a time period specified by the Attorney General, up to 30 days following the date when the disclosure was otherwise required to be provided. The delay may be extended for an additional period of up to 30 days, and in extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days. If the Attorney General indicates that further delay is necessary, the Commission may grant such relief through an exemptive order.

Disclosures for Foreign Private Issuers

Foreign private issuers that file on Form 20-F must adhere to requirements parallel to those of domestic issuers and disclose information regarding their cybersecurity risk management, strategy and governance in Form 20-F. Both 20-F filers and 40-F filers must promptly furnish on Form 6-K information regarding a material cybersecurity incident that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders. For Canadian issuers filing on Form 40-F under MJDS, the new rules do not impose any new risk management or governance disclosure requirements, given that the MJDS generally permits eligible Canadian FPIs to use Canadian disclosure standards and documents to satisfy the Commission's registration and disclosure requirements. Such filers are already subject to the Canadian Securities Administrators' 2017 guidance on the disclosure of cybersecurity risks and incidents.

Key Takeaways

Reevaluate and update policies and processes

We anticipate that most, if not all, issuers have some level of formal processes in place to identify and respond to cybersecurity incidents. However, given that the new rules will require issuers to publicly disclose those processes, we anticipate that issuers will want to ensure their disclosed processes are within the range of best practices for their industry and that appropriate disclosure controls and procedures have been established. Further, issuers will want to ensure that the relevant members of senior management, IT and legal within their organization are informed and involved on a timely basis to ensure that critical determinations can be made, materiality can be assessed and disclosures can be prepared and reviewed in the required time periods. In our experience, it is important to articulate and memorialize the specific details of management's processes

in responding to a cybersecurity incident and, even more importantly, to ensure that policies and procedures are in fact implemented in a manner that can be audited.

A determination of materiality can be difficult in the best of circumstances. In the context of a cybersecurity incident, where all the relevant facts are not necessarily available to the issuer, it will likely often be even more challenging. Further, since the relevant inquiry is both forward-looking (i.e., a future loss that is reasonably foreseeable) and based on qualitative and quantitative factors (i.e., a reputational loss vs. a financial loss), an issuer may find it challenging to meet the requirements of the new rules without carefully defined roles and processes in place prior to the event. To facilitate compliance when a cybersecurity event occurs, issuers are well-served by undergoing exercises in which the likely types of events are identified, an assessment is made as to the appropriate response to those events, and how the company will exercise its judgment regarding the process and criteria for deterring materiality.

Cyberincident assessment and response may constitute material nonpublic information that triggers restrictions on trading by directors, officers and other employees. Insider trading policies and processes should be reviewed and tested to ensure that the issuer is prepared to identify those individuals whose trading should be restricted and to communicate those restrictions without unreasonable delay, and to plan and provide for communication regarding such events well in advance.

Equip directors and management to fulfill their duties on cybersecurity risk management

Boards and their committees should understand their role in overseeing risks from cybersecurity threats and be involved in the establishment of systems to manage these risks. There should be processes by which the board is informed about and monitors such risks on a regular basis. Agenda items may include reports from management on incident response plans and cybersecurity incidents and remediation. Likewise, management should understand their role in assessing and managing the issuer's material risks from cybersecurity threats. Tabletop exercises are essential to help boards and management prepare for future incidents.

Identify and plan for compliance with multiple agencies' disclosure regimes

Anticipating potential conflicts with regulations established under CIRCIA and from CISA, the Commission is participating in interagency working groups on cybersecurity regulatory implementation for potential modifications to Item 1.05.

For issuers subject to the Federal Communications Commission's conflicting notification rules in the event of breaches, paragraph (d) to Item 1.05 provides that such issuers may delay making a Form 8-K disclosure up to the seven business day period following notification to the U.S. Secret Service and FBI specified in the FCC rule, with written notification to the Commission.

Issuers should stay mindful of other relevant disclosure regimes, including the Department of Health and Human Service and its rule on Notification in the Case of

Breach of Unsecured Protected Health Information, as well as regulations and programs of the Department of Defense, Department of Energy, Department of Homeland Security, the Federal banking regulatory agencies, and state insurance laws.

Provide for the ability to gather information about third party information systems

Since the definition of information systems includes all systems used by the issuer, required disclosures extend to those systems owned by third parties. While the rules do not impose on issuers an obligation to perform any special inquiry of third party service providers, issuers should ensure that the agreements governing its third party relationships provide it with the ability to obtain the information necessary to make prompt assessment and disclosure of cybersecurity incidents.

Consider U.S. compliant disclosure for foreign private issuers

While 20-F filers must disclose information on cybersecurity risk management that essentially the same as domestic issuers, 40-F filers generally need only disclose a cybersecurity incident if that incident is disclosed or would be required to be disclosed in Canada. However, we anticipate that foreign issuers that are cross-listed in the United States or frequently access the US capital markets are likely to feel some pressure to adopt disclosures similar to those made by their peers in the United States. Further, since the question of whether a particular cybersecurity incident is “material” isn’t necessarily dependent on whether disclosure of the incident is mandated by a form requirement, we anticipate that issues regarding the materiality of a cybersecurity incident are likely to receive additional scrutiny in the context of the new rules in connection with cross-border registered offerings. Accordingly, we believe cross-listed foreign private issuers would be well-served to evaluate their own internal processes in order to anticipate potential changes in market practices.