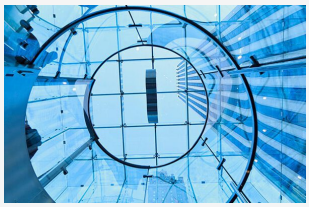
OSLER

SEC's new mandatory cybersecurity disclosure rules and implications for Canadian issuers



AUGUST 21, 2023 12 MIN READ

Related Expertise

- Corporate Governance
- Privacy and Data Management
- Risk Management and Crisis Response

Authors: Andrew MacDougall, Jason Comerford

On July 26, 2023, the United States Securities and Exchange Commission (SEC) adopted final rules requiring disclosure [PDF] by public companies of cybersecurity incidents, risk management and governance. The new rules apply to most U.S. domestic issuers, as well as foreign private issuers reporting on Form 20-F (FPIs), but do not apply to Canadian issuers reporting on Form 40-F under the U.S.–Canada Multijurisdictional Disclosure System (MJDS).

U.S. domestic issuers must disclose material cybersecurity incidents on Form 8-K within four business days of determining that the incident is material, and must describe their cybersecurity risk management, strategy and governance practices annually. FPIs must promptly disclose material cybersecurity incidents on Form 6-K that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders, and must describe their cybersecurity risk management, strategy and governance practices in their Form 20-F annually.

The rules' approach to the timely reporting of material cybersecurity incidents will likely influence the timely disclosure practices of Canadian issuers over time and their application of Multilateral Staff Notice 51-347 – *Disclosure of cyber security risks and incidents* [PDF], which was released by the Canadian Securities Administrators (CSA) in January 2017.

Overview

The SEC's adoption of the new mandatory disclosure requirements was prompted by its perception that despite the substantial increase in cybersecurity incidents over time, there has been a tendency for companies to underreport them, as well as inconsistent approaches to cybersecurity disclosures. The SEC had issued prior guidance on cybersecurity reporting in 2011 and 2018 [PDF]. However, the SEC stated its belief that the prior guidance had not been sufficiently effective in enhancing cybersecurity disclosure practices and that adoption of a mandatory requirement was necessary to enable investors to locate, interpret and analyze the necessary information.

These new rules apply to all U.S. domestic issuers and FPIs, but expressly do not apply to asset-backed security issuers and Canadian issuers that file annual reports with the SEC on MJDS Form 40-F. While MJDS issuers are not subject to the rules, the new requirement for timely reporting of material cybersecurity incidents will likely influence timely disclosure practices for MJDS issuers under Canadian securities laws.

In the final rules, the SEC provides guidance on how issuers should make materiality determinations in determining when a material cybersecurity incident has occurred. If the new rules are seen as improving the quality and timeliness of disclosure on cybersecurity matters for U.S. securities law purposes, they will likely influence the approach to making materiality determinations for Canadian securities law purposes. A key difference between the U.S. and Canadian approaches is that the SEC mandates the filing of a Form 8-K within four business days of determining that the cybersecurity incident is material, whereas under Canadian securities law and stock exchange requirements a press release is required to be issued forthwith upon determining that the cyber breach is material.

Summary of the new disclosure requirements

Document	Disclosure required
Incident reporting	
Current reports on Form 8-K	U.S. domestic issuers must disclose on Form 8-K any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its (i) nature, scope and timing and (ii) impact or reasonably likely impact. While the Form 8-K must be filed within four business days of determining an incident was material, the filing may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. The four-business-day deadline must be met even if some of the information required to be disclosed was not determined or was unavailable at the time of the Form 8-K filing. An amended Form 8-K must be filed once that information has been determined or becomes available.
Current reports on Form 6-K	FPIs must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange or to security holders.
Annual report disclosure	
Annual report on Form 10-K	
Cybersecurity risk disclosure	U.S. domestic issuers must describe their processes, if any, for the assessment, identification and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations or financial condition.
Cybersecurity governance	U.S. domestic issuers must describe (i) the board's oversight of risks from cybersecurity threats and (ii) management's role in assessing and managing material risks from cybersecurity threats.
Annual report on Form 20-F	FPIs must describe (i) the board's oversight of risks from cybersecurity threats and (ii) management's role in assessing and managing material risks from cybersecurity threats.

Disclosure of material cybersecurity incidents

The new rules require reporting material cybersecurity incidents on Form 8-K or Form 6-K, as applicable. A "cybersecurity incident" is defined as an "unauthorized occurrence or 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 the final release, the SEC clarified that "accidental" occurrences are to be considered "unauthorized".

The SEC also stated that there may be cases, even if uncommon, where the jeopardy caused by a cybersecurity incident materially affects the company, even if the incident has not yet caused actual harm. Finally, the SEC clarified that the issuer's information systems include third-party systems used by the issuer, such as cloud storage services.

Timing for disclosure

When a cybersecurity incident has been discovered, the issuer must evaluate whether the incident is material based on how a reasonable investor would consider the incident's impact on the issuer. Materiality determinations must be made by Form 8-K filers "without unreasonable delay"; however, in the final release the SEC states that materiality determinations are not required to be on the same day as the incident is discovered. If the cybersecurity incident is found to be material, disclosure on Form 8-K is due within four business days of the determination. However, if the U.S. Attorney General determines that disclosure of the incident would pose a substantial risk to national security or public safety, the issuer may delay filing the Form 8-K for a time period specified by the U.S. Attorney General, up to 30 days, which can be extended for an additional 60 days in extraordinary circumstances where the U.S. Attorney General determines that disclosure continues to pose a substantial risk to national security.

The SEC states in the final release that materiality is to be determined consistent with determining materiality for securities law purposes generally — i.e., whether there is substantial likelihood that a reasonable shareholder would consider it important in making an investment decision or if it would significantly alter the total mix of information available. The SEC notes that materiality is a fact-specific analysis and a cybersecurity incident that affects multiple issuers may be reportable for some of them and not others, or may not be reportable at the same time. The SEC noted that a series of related cyber attacks, each by itself immaterial, could collectively become material.

Content of disclosure

New Item 1.05 of Form 8-K will require issuers to describe the material aspects of the nature, scope and timing of the cybersecurity incident, and the material impact or reasonably likely material impact on the issuer, including its financial condition and results of operations. The SEC noted that the inclusion of the reference to "financial condition and results of operations" is not exclusive and that issuers should consider qualitative factors alongside quantitative factors, such as customer and vendor relationships, reputation, competitiveness or the potential for litigation. To address concerns that issuers should not be required to provide information that would be useful to cybersecurity threat actors, the SEC added an instruction to Item 1.05 stating that it is not necessary to disclose specific or technical information about the issuer's planned response to the incident or its cybersecurity systems, related networks and devices or potential system vulnerabilities in such detail as would impede the issuer's response or remediation of the incident.

If any of the required information is unavailable or indeterminate at the time of the Form 8-K filing, the issuer must file an updated disclosure on an amended Form 8-K within four business days after the information becomes available.

While issuers are not required to disclose the incident's remediation status, whether it is ongoing, whether data was compromised or specific information about the issuer's planned response, the final release notes that issuers may choose to provide such information on a voluntary basis as part of their disclosure.

Where the cybersecurity incident occurs in a third-party system used by the issuer, the rules mandate disclosure of only the information accessible to the issuer, with no obligation to conduct additional inquiries.

Material cybersecurity incident disclosure is afforded a limited safe harbour from liability under section 10(b) of the *Securities Exchange Act of 1934* and Rule 10b-5 thereunder, and an

untimely filing required under Item 1.05 of Form 8-K will not result in loss of Form S-3 short-form registration statement eligibility.

Implications for Canadian issuers

The assessment of materiality for 8-K reporting purposes is generally aligned with, and the SEC's release may serve as an additional reference resource for, the assessment to be made by a Canadian issuer for purposes of determining whether a material change report is required to be filed under Canadian securities laws and the guidance set out in CSA Multilateral Staff Notice 51-347. However, under Canadian securities laws a press release must be issued and filed forthwith upon determining that the cybersecurity incident is material, and there is no safe harbour protection under Canadian securities laws for the disclosure provided.

Annual disclosure of cybersecurity risk management, strategy and governance

The new rules also require annual disclosure by issuers in Form 10-K or Form 20-F, as applicable, regarding their cybersecurity risk management, strategy and governance.

With respect to risk management and strategy disclosure, the issuer is required to describe

1. the issuer's processes, if any, for the assessment, identification and management of material risks from cybersecurity threats
2. whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations or financial condition

The processes must be described in sufficient detail for a reasonable investor to understand, while staying within the bounds of information that is material to investors. Issuers will be required to describe whether and how their cybersecurity processes have been integrated into their overall risk management system or processes and whether the issuer has processes to oversee and identify material risks from cybersecurity threats associated with their use of any third-party service provider.

In addition, to enable investors to understand the level of cybersecurity capacity that is outsourced by the issuer, the issuer must also disclose whether assessors, consultants, auditors or other third parties are engaged in connection with their cybersecurity processes. U.S. domestic issuers are required to describe their risk oversight practices generally in their proxy statement, which they may do by incorporating by reference the cybersecurity disclosure provided in the issuer's Form 10-K.

With respect to cybersecurity governance, issuers must describe

1. the board's oversight of risks from cybersecurity threats, including, if applicable, the identification of any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and the process by which the board or that committee is informed about such risks
2. management's role in assessing and managing material risks from cybersecurity threats, including, as applicable

1. whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of those persons or members in such detail as necessary to fully describe the nature of the expertise (such as prior work experience in cybersecurity; any relevant degrees or certifications; or any knowledge, skills or other background in cybersecurity)
2. the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents
3. 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 a reversal from its proposed rules, the SEC chose not to require specific disclosure of board members' cybersecurity expertise, noting that cybersecurity processes are predominantly designed and administered at the management level.

Compliance dates

The final rules are effective September 5, 2023. Disclosures complying with Regulation S-K, Item 106 (i.e., disclosure by U.S. domestic issuers of risk management, strategy and governance) and Item 16K of Form 20-F (covering disclosure by FPIs of the same topics) must be included in annual reports for fiscal years ending on or after December 15, 2023. Incident disclosures under Item 1.05 of Form 8-K and in Form 6-K will be required starting on December 18, 2023, except smaller reporting companies, who will be given an additional 180 days to comply with the requirement, starting on June 15, 2024.

Recommended steps for Canadian issuers

The vast majority of Canadian issuers that are cross-listed to a U.S. stock exchange will be filing under MJDS or will otherwise qualify as FPIs and so will not be subject to the prescribed requirements for cybersecurity incident reporting under Form 8-K within four business days of determining that a material cybersecurity incident has occurred. Instead, they will be required to promptly report on Form 6-K material cybersecurity incidents publicly disclosed in Canada pursuant to applicable Canadian disclosure standards. Canadian securities laws require disclosure by press release of the nature and substance of the cybersecurity incident promptly on determining that the cybersecurity incident is a material change (or on determining it is a material fact if they are subject to timely disclosure obligations under stock exchange listing rules), and such disclosure may not need to address all the elements prescribed under Form 8-K.

Given the significant increase in regulator and investor scrutiny of timely and decision-useful information about cybersecurity incidents, all Canadian issuers are advised to take steps now to help ensure that they are meeting applicable legal requirements and the expectations of capital markets participants, such as

- reviewing their existing disclosure controls and procedures to ensure that cybersecurity incidents can be communicated quickly to appropriate personnel who can make materiality determinations and disclosure decisions, such as senior management and legal counsel. There should be a clear process through which the IT team can promptly bring potentially material cybersecurity incidents to the attention of the senior management and the legal team.

- closely monitoring the cybersecurity defenses and incident response readiness of third-party vendors at the engagement stage and on an ongoing basis through periodic audits. Issuers should have direct and timely communication processes in place with their third-party vendors mapping out the prompt assessment and disclosure of material cybersecurity incidents.
- ensuring that the board of directors and management have comprehensive training with respect to cybersecurity incidents and clearly understand potential disclosure obligations. Also consider adding questions to directors and officers questionnaires relating to their cybersecurity expertise.
- considering creation of a cybersecurity committee of the board, ideally composed of members with cybersecurity expertise and periodic updated training, tasked with specific oversight of cybersecurity matters.
- scheduling regular cybersecurity updates on board agendas, which include review of current analysis from management about areas of risk, areas of updating and improvement, systems readiness, cybersecurity incidents and remediation.
- actively updating cybersecurity programs, implementing incident response plans, conducting simulated incident response exercises, requiring periodic employee training and reinforcing company-wide a focus on close attention to good cybersecurity hygiene, such as use of complex passwords and multifactor authentication and awareness of phishing and other forms of cyber attacks.