No. 2023-04
Updated 19 September 2024

Technical Line

A closer look at the SEC's new rules on cybersecurity disclosures

In this issue:

What you need to know

- Registrants will have to disclose information about a material cybersecurity incident on Form 8-K within four business days of determining it is material, with a delay only when the US Attorney General concludes that disclosure would pose a substantial risk to national security or public safety.
- The rules require nearly all registrants that file periodic reports with the SEC, including SRCs and FPIs, to describe the processes they use to assess, identify and manage cybersecurity risks, as well as the board's oversight of them and management's role in assessing and managing them.
- Financial reporting, cybersecurity, legal and other professionals likely will be involved in preparing the new disclosures and implementing processes for incident reporting, including the disclosure controls and procedures related to gathering the information and performing materiality analyses of cybersecurity incidents, among other things.
- The SEC staff has said it will focus on registrants' compliance with the new cybersecurity rules. Registrants should carefully consider the SEC staff's C&DIs and statements as they prepare disclosures.

Overview

The rules **adopted** by the Securities and Exchange Commission (SEC or Commission) are intended to enhance and standardize disclosures by requiring registrants to timely report on cybersecurity incidents on Forms 8-K and 6-K and make disclosures about their cybersecurity risk management, strategy and governance in annual reports on Forms 10-K and 20-F.

Building a better working world

The SEC acknowledged that an ever-increasing share of economic activity is dependent on electronic systems, and disruptions to those systems can have significant effects on registrants. The SEC also said that investors and other capital market participants need more timely and reliable information about the impacts of material cybersecurity incidents. The rules are intended to make sure that registrants disclose material cybersecurity information and provide investors with more consistent, comparable and decision-useful information.

The rules codify many of the concepts in the interpretive guidance on cybersecurity that the SEC issued in 2018 (the 2018 Interpretive Release[1]) and in the 2011 Division of Corporation Finance (DCF) staff guidance[2] on cybersecurity disclosures. The 2018 Interpretive Release and the 2011 DCF staff guidance didn't require specific, prescriptive disclosures related to cybersecurity.

Instead, the 2011 DCF staff guidance states that registrants should consider the risk associated with cybersecurity breaches when disclosing material matters in their registration statements and periodic reports. The staff guidance referred registrants to their reporting obligations under Regulation S-K, including risk factors, legal proceedings, business description and management's discussion and analysis of financial condition and results of operations (MD&A), among other reporting and disclosure requirements.

As cybersecurity risks evolved, the SEC issued the 2018 Interpretive Release that went beyond the 2011 DCF staff guidance and addressed the importance of corporate governance, the application of disclosure controls and procedures to cybersecurity risks. The 2018 Interpretive Release stated that registrants should consider incident reporting on Form 8-K and Form 6-K and also addressed whether registrants should consider restrictions on insider trading in the period of time following a breach but prior to disclosure.

The SEC said because disclosure practices among registrants vary, it adopted the new rules to require more prescriptive disclosures about cybersecurity incidents and risk management and governance. Registrants nonetheless should consider the guidance in the 2018 Interpretive Release and the 2011 DCF staff guidance related to risk factors, legal proceedings and MD&A, among other areas, when preparing periodic reports and registration statements.

The rules apply to nearly all registrants that are required to file periodic reports (e.g., Form 10-K, Form 20-F) with the SEC, including smaller reporting companies (SRCs) and foreign private issuers (FPIs). The rules do not amend Form 40-F, and therefore, they don't apply to Canadian FPIs under the multijurisdictional disclosure system (MJDS).

This publication includes an appendix with a disclosure checklist that summarizes the requirements for cybersecurity incidents and cybersecurity risk management, strategy and governance, as well as those for FPIs.

Incident disclosures

Form 8-K reporting requirement

The rules amend Form 8-K to add Item 1.05, which requires domestic registrants to disclose a material cybersecurity incident within four business days[3] of determining that the incident is material. Item 1.05 requires registrants to disclose the following information about a material incident on Form 8-K:

- Material aspects, including the nature, scope and timing of the incident
- The material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations

If any of the above information cannot be determined or is not available at the time of the initial Form 8-K filing, the registrant should include a statement to that effect.

The SEC staff has clarified that if a registrant voluntarily discloses a cybersecurity incident that is not required to be reported under Item 1.05 (e.g., a cybersecurity incident for which the registrant has either not made a materiality determination or has determined is not material), it should be disclosed under a different item of Form 8-K (e.g., Item 8.01, Other Events).[4] If the incident is subsequently determined to be material, an Item 1.05 is required to be filed within four business days of that determination.

In response to feedback on the proposal, the rule requires the incident disclosures to primarily focus on the material impacts of the incident rather than the details about the incident. The SEC staff believes this information is available within four business days of a registrant determining that an incident is material, since the information likely would have been required to perform the registrant's materiality determination (see Materiality section below).

For example, most registrants' materiality analyses will include consideration of the financial impact due to a cybersecurity incident, and therefore, information regarding the incident's impact on the registrant's financial condition and results of operations will likely have already been developed when Item 1.05 is triggered. If any required information is not determined or is unavailable at the time a registrant prepares the initial Form 8-K, the registrant must file an amended Form 8-K containing such information within four business days after it determines such information or the information becomes available.

While a registrant is only required to include information required under Item 1.05 that is not determined or available at the time the initial Form 8-K is filed and does not have an obligation to update its prior disclosures in the amended Form 8-K, it may have a duty to correct prior disclosure when it determines that the information previously disclosed was untrue (or omitted a material fact) at the time the disclosure was made.

For example, a registrant may have a duty to correct prior disclosure if it subsequently discovers contradictory information that existed at the time of the initial disclosure. It also may have a duty to update disclosure that becomes materially inaccurate after the disclosure is made.

Instruction 4 to Item 1.05 also affirms that a registrant is not expected to publicly disclose detailed technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities that would impede its response or remediation of the incident.

The SEC staff has said that Item 1.05 does not prohibit a registrant from privately discussing a material cybersecurity incident with other parties or from providing information about the incident to such parties beyond what was disclosed in Item 1.05.[5] Those parties may include commercial counterparties (e.g., vendors, customers, other companies that may be affected by the same incident). The SEC staff said a registrant can privately share information regarding a material cybersecurity incident beyond what is disclosed in Item 1.05 without implicating Regulation FD.

Materiality

Timing of assessment

Companies must have sufficient disclosure controls and procedures to make their materiality determinations without unreasonable delay. Accordingly, the SEC did not establish any bright lines or deadlines for materiality determinations in the final rules.

The SEC stated in the adopting release that adhering to normal internal practices and disclosure controls and procedures will suffice to demonstrate good faith compliance with the "without unreasonable delay" provision. However, if a registrant revised its existing incident response

policies and procedures, changed the criteria required to report an incident to management or committees, or introduced other steps to delay the materiality determination or disclosure, that would constitute an unreasonable delay.

Definition of materiality

The rules state that what constitutes materiality for purposes of determining whether an incident must be reported in a Form 8-K is consistent with the Supreme Court's definition of materiality. Information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision, or if it would have "significantly altered the 'total mix' of information made available."[6] The analysis for materiality of cybersecurity incidents is the same as the materiality analysis for other securities laws purposes, including for satisfying other Form 8-K reporting obligations.

For incidents that impact key systems and information (i.e., a company would have difficulty operating without the system or information) and incidents involving unauthorized access to or exfiltration of large quantities of important data, a registrant may not have complete information about the incident but may know enough about the impact to conclude on its materiality.

To assess materiality, registrants need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances.

Registrants need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances of the cybersecurity incident, including quantitative and qualitative factors. Judgment will be involved in making these materiality determinations.

For example, if a registrant experiences a data breach, it should consider both the immediate impact and any longer-term effects on its operations, finances, brand perception and customer relationships. Given the fact-specific nature of the materiality determination, the same incident that affects multiple registrants may not become reportable at the same time, and it may be reportable for some registrants but not others. That is, the materiality determination will be based on the individual registrant and incident.

The SEC staff issued Compliance and Disclosure Interpretations (C&DIs)[7] on incidents involving ransomware attacks that result in a disruption in operations or the exfiltration of data. The C&DIs clarify, among other things:

- Making a ransomware payment does not relieve a registrant of the requirement to determine the materiality of an incident (and disclose the incident when required)
- A registrant cannot necessarily conclude an incident is not material based only on the size of the ransomware payment or whether the registrant holds an insurance policy that covers cybersecurity incidents and is reimbursed for some or all of the ransomware payment
- Disclosure may be required about a series of ransomware attacks over time, either by a single threat actor or by multiple threat actors, even if the registrant determines that each incident is immaterial individually

How we see it

In performing materiality assessments, registrants should consider the nature of the data that may have been compromised when considering the effects of a cybersecurity incident on its financial condition and operations. For example, they should consider whether the incident involved information privacy, proprietary data loss, cyber extortion or data related to business interruption or network security, among other things.

The rules note that registrants should consider quantitative factors to assess materiality in the context of the financial statements, including considering SEC staff guidance on materiality (e.g., Staff Accounting Bulletin 99). Similarly, they should consider the impact of a cybersecurity incident on revenues and expenses, among other financial statement line items.

The required disclosures for a material cybersecurity incident are not limited to only the material impacts on a registrant's financial condition and results of operations. In assessing the material impact of an incident, the registrant should consider quantitative factors in addition to qualitative factors, including harm to an entity's brand or reputation, customer or vendor relationships, and competitiveness. Registrants should also consider the possibility of litigation or regulatory investigations or actions, including regulatory actions by state or federal government authorities and non-US authorities. Registrants may also want to consider data theft, asset loss, intellectual property loss, reputational damage or business value loss in assessing materiality.

While a registrant isn't required to disclose the incident's remediation status and whether remediation is ongoing, this information may be required when assessing the materiality of an incident.

How we see it

Although the rules formalize the timing and specify the content and location of the cybersecurity incident disclosure, the use of materiality as the threshold for providing disclosure about cyber incidents is no different than the use of materiality in other areas of securities laws.

Materiality assessments in the context of cybersecurity incidents are often complex, and registrants of all sizes may struggle to perform them. Many registrants have established cross-disciplinary disclosure committees that consider the materiality of information, and they should be involved in these assessments, along with cybersecurity specialists and external securities counsel.

Delay in incident reporting

A registrant may delay disclosure of a material cybersecurity incident for up to 30 days only if the US Attorney General determines that disclosure poses a substantial risk to national security or public safety and notifies the SEC of such determination in writing. The delay may be extended for an additional period of up to 30 days if the US Attorney General determines that disclosure continues to pose a substantial risk. In extraordinary circumstances, if the US Attorney General determines that disclosure continues to pose a substantial, critical risk to national security or public safety, disclosure may be delayed for a final additional period of up to 60 days.[8] Beyond this delay, if the US Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief through an exemptive order.

When a registrant wants to request a delay of the disclosure of a cybersecurity incident on Form 8-K, they must first work with the Federal Bureau of Investigation (FBI), which will then submit the request to the Department of Justice (DOJ). The FBI issued a **notice** in December 2023 with guidance for SEC registrants who want to delay reporting an incident on Form 8-K. The DOJ also issued **guidelines** for SEC registrants to follow when requesting that the US Attorney General authorize a delay for reporting the incident under Item 1.05.

The SEC staff has published C&DIs[9] that clarify the filing deadlines that apply when a registrant requests that the US Attorney General determine that disclosing the incident on Form 8-K could pose a substantial risk to national or public safety.

Definition of cybersecurity incident

The rules define a cybersecurity incident as an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information system that jeopardizes the confidentiality, integrity or availability of a registrant's information systems or any information residing there.[10]

The SEC decided not to require registrants to report incidents that are individually immaterial but are material in the aggregate, as it had proposed, based on feedback that such a provision would have been challenging to implement. However, the rules expand the definition of "cybersecurity incident" to include "a series of related unauthorized occurrences," which reflects the fact that cyber attacks sometimes occur over time.

The rules say that the definition of "cybersecurity incident" is intended to be broad, and the Form 8-K requirement may be triggered even if the material impact to the registrant is caused by a series of individually immaterial related cyber attacks.

Examples of related unauthorized occurrences include: (1) the same malicious actor engages in a number of small but continuous cyber attacks related in time (e.g., occurred the same day) and form (e.g., ransomware attacks) against the same registrant, which are collectively either quantitatively or qualitatively material, and (2) a series of related attacks from multiple actors exploit the same vulnerability and collectively impede the registrant's business materially.

How we see it

Registrants may find the requirement to report a series of related unauthorized occurrences challenging because the rule does not define "related." For example, registrants may need to develop a process to track individually immaterial related incidents over an undefined time period and identify controls over that process to make sure they are reporting all cybersecurity incidents subject to the rule.

If a registrant concludes that an incident is immaterial, it should have processes and controls in place to confirm that the immaterial incident is not related to prior incidents.

The adopting release also includes an example of an "accidental occurrence." For instance, if a registrant's customer data is accidentally exposed, allowing unauthorized access to such data, the data breach would constitute a cybersecurity incident requiring a materiality analysis to determine whether disclosure under Item 1.05 of Form 8-K is required.

Incident reporting related to third-party systems

Depending on the circumstances, registrants may be required to disclose a material cybersecurity incident that occurs on a third-party system that they use, and both the service provider and the registrant may be required to provide the Form 8-K incident disclosures. In determining how to make these disclosures and what to include, registrants generally are not required to conduct additional inquiries outside of their normal process and communication with their third-party service providers and in accordance with their disclosure controls and procedures. That is, registrants may have reduced visibility into third-party service providers' systems but should disclose information that is known or reasonably available to them.

How we see it

Although the rules do not require registrants to conduct additional procedures outside of their normal process and communication with their third-party provider, they may want to consider how they communicate with third-party service providers (i.e., what information about incidents they receive and when) in light of the new rule and establish appropriate protocols. Registrants should also consider whether their third-party providers are nonpublic entities and how they may be gathering data for incident reporting since they aren't subject to reporting under the final rule.

Limited safe harbor

A registrant must meet certain requirements to use a Form S-3, including timely filing reports as required under the Exchange Act (e.g., Form 10-K and certain Form 8-K items) during the 12 months before filing the registration statement. The rules clarify that that the untimely filing of Item 1.05 of Form 8-K will not result in a registrant losing its Form S-3 filing eligibility.

The rules also amended Rules 13a-11(c) and 15d-11(c) under the Exchange Act to provide for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act for the new Item 1.05 of Form 8-K.

The rules require disclosures under Item 1.05 of Form 8-K to be "filed" rather than "furnished" for Exchange Act liability purposes.

Registrants are not required to disclose the name of the third parties used to assess, identify and manage their risks from cybersecurity threats or the services provided.

Risk management, strategy and governance disclosures

The rules also add Item 106 to Regulation S-K to require registrants to disclose their cybersecurity risk management, strategy and governance in their annual reports on Form 10-K but not in their registration or proxy statements.

Risk management and strategy

Item 106(b) requires registrants to disclose their processes, if any, to assess, identify and manage material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. The rule provides the following list of potential disclosure items:

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

A registrant must disclose 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 its business strategy, results of operations or financial condition and, if so, how.

A registrant is not required to disclose the name of any third-party service provider used or a description of its services because this information could expose cybersecurity vulnerabilities, but the registrant may elect to do so.

Although the SEC used the term "processes" instead of "policies and procedures" in the rules to avoid providing detailed operating disclosures to bad actors, registrants should disclose additional information as necessary based on their facts and circumstances such that a reasonable investor can understand their cybersecurity processes and practices. This may

include whether the registrant has a risk assessment program in place and sufficient detail for investors to understand the registrant's cybersecurity risk profile. Registrants are only required to describe these processes if they relate to material cybersecurity risks.

Examples of risks from cybersecurity threats that a registrant may face and that may be material include intellectual property theft, fraud, extortion, harm to employees or customers, violation of privacy laws, and other legal risk and reputational risk.

Governance

Board oversight of cybersecurity risk

The rules also add Item 106(c)(1) to Regulation S-K to require disclosure of the board's role in overseeing risks from cybersecurity threats. A registrant must identify any board committee or subcommittee that oversees cybersecurity risks, if applicable, and describe the processes by which the committee is informed about such risks.

Although the rules do not require registrants to disclose the frequency of the board's or committee's discussions on cybersecurity, registrants could include this information when describing the processes by which their board or relevant committee is informed about cybersecurity risks.

Registrants may find that Item 407(h) of Regulation S-K, which requires the description of the board's leadership structure and administration of risk oversight, overlaps with the disclosure requirements under Item 106(c)(1) related to the board's oversight of specific cybersecurity risk. If the disclosures are duplicative, a registrant may incorporate this information by reference.

How we see it

Because registrants will be required to disclose the board's role in overseeing risks from cybersecurity threats, management should be prepared to respond to questions from the board about cybersecurity risk management and processes and controls related to determining the impact of a cybersecurity incident and the time it takes to do so.

Management's role in assessing and managing cybersecurity risk

The rules also add Item 106(c)(2) to require disclosures about management's role in assessing and managing material risks from cybersecurity threats. At a minimum, companies should consider disclosing:

- Whether and which management positions or committees are responsible for assessing and managing cybersecurity risk and their relevant expertise in such detail as is necessary to fully describe the nature of the expertise
- The processes by which management is informed about and monitors the prevention, detection, mitigation and remediation of cybersecurity incidents
- Whether management reports information about such risks to the board of directors or a board committee or subcommittee

The SEC did not adopt the proposed requirement to disclose board members' cybersecurity expertise. The SEC staff believes effective cybersecurity processes are designed and administered at the management level, and the board can effectively oversee management's efforts without specific subject-matter expertise. If a registrant has determined that board-level expertise is a necessary part of its cybersecurity risk management, it should provide the disclosure under Item 106.

How we see it

Registrants may need to identify and disclose in their annual reports management's relevant expertise to assess and manage material risk from cybersecurity threats.

Reporting requirements for foreign private issuers

The rules require FPIs to provide disclosures on Form 6-K about material cybersecurity incidents and on Form 20-F about cybersecurity risk management, strategy and governance, comparable to those required by domestic registrants.

Incident disclosures

The rules amend Form 6-K to include a "material cybersecurity incident" as an event that could trigger a disclosure obligation. As such, FPIs that are subject to Form 6-K filing requirements, including Canadian FPIs under the MJDS,[11] are required to furnish information about a material cybersecurity incident promptly on Form 6-K if the information is (1) distributed to stockholders or to a national exchange (if the information is made public by that exchange) or (2) required to be made public under the registrant's domestic laws.

Risk management, strategy and governance disclosures

The rules add Item 16K on Form 20-F to require FPIs to provide cybersecurity management, strategy and governance disclosures comparable to those required by domestic registrants, as discussed above.

The rule did not amend Form 40-F, and therefore, the risk management, strategy and governance disclosures don't apply to Canadian FPIs under the MJDS.

Transition and other considerations

Transition

All domestic registrants must provide the disclosures under Item 106 of Regulation S-K, and FPIs must comply with the comparable requirements in Form 20-F, beginning with annual reports for fiscal years ending on or after 15 December 2023.

All registrants other than SRCs were required to disclose a material cybersecurity incident on Form 8-K or Form 6-K starting on 18 December 2023. SRCs were required to comply with Form 8-K[12] disclosure requirements starting on 15 June 2024.

XBRL requirements

The rules require all registrants to tag cybersecurity disclosures as discussed above in Inline eXtensible Business Reporting Language (Inline XBRL) beginning one year after the initial compliance date for the related disclosure requirements. For example:

- For Item 106 of Regulation S-K, all registrants must begin tagging responsive disclosure in Inline XBRL beginning with annual reports for fiscal years ending on or after 15 December 2024.
- For Item 1.05 of Form 8-K and Form 6-K, all registrants must begin tagging responsive disclosure in Inline XBRL beginning on 18 December 2024.

Next steps

The SEC staff has stated that it will focus on cybersecurity disclosures in the future, with an initial focus on registrants' compliance with the new rules. Registrants should carefully consider the C&DIs and staff statements as they prepare the disclosures.

Endnotes:

1 ***Commission Statement and Guidance on Public Company Cybersecurity Disclosures***, 26 February 2018. See our publication, **SEC Reporting Update — SEC issues guidance on cybersecurity**, for more details about the interpretive guidance.

2 ***CF Disclosure Guidance: Topic No. 2: Cybersecurity***, 13 October 2011.

3 Unless otherwise specified, a Form 8-K report is required to be filed or furnished within four business days after the occurrence of a reportable event as required in the Form, including an acquisition or disposition of assets or changes in the registrant's certifying accountant.

4 ***Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents***, 21 May 2024.

5 ***Selective Disclosure of Information Regarding Cybersecurity Incidents***, 20 June 2024.

6 *TSC Indus. v. Northway*, 426 U.S. 438, 449 (1976); *Matrixx Initiatives v. Siracusano*, 563 U.S. 27, 38-40 (2011); *Basic,* 485 U.S. at 240. See also the definition of "material" in 17 CFR 230.405 (Securities Act Rule 405); 17 CFR 240.12b-2 (Exchange Act Rule 12b-2).

7 See Item 1.05 Material Cybersecurity Incidents C&DIs 104B.05 through 09 at **SEC.gov | Exchange Act Form 8-K**.

8 The 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 of 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.

9 See Item 1.05 Material Cybersecurity Incidents C&DIs 104B.01 through 04 at **SEC.gov | Exchange Act Form 8-K**.

10 ***Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure***, July 2023.

11 **Financial Reporting Manual Section 16210.1.**

12 Any FPI is eligible to qualify as an SRC. However, to take advantage of the disclosure relief as an SRC, an FPI must use domestic forms (e.g., Form 8-K, not Form 6-K) and file financial statements prepared using US GAAP on Form 10-K, not Form 20-F.

Appendix: Disclosure checklist

Incident disclosures		
Disclosure location	**Disclosure requirement**	**SEC guidance**
Form 8-K — Item 1.05. Material Cybersecurity Incidents*	Within four business days of determining a cybersecurity incident is material, registrants must disclose: ▸ The material aspects of the nature, scope and timing of the incident ▸ The material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations If any of the above information cannot be determined or is not available at the time of the initial filing, the registrant should include a statement to that effect. Registrants must make their materiality determination without unreasonable delay. A registrant may delay reporting a cyber incident on Form 8-K if the US Attorney General determines that the disclosure would pose substantial risk to national security or public safety and notifies the Commission of such determination in writing before the form deadline. * *If the registrant has determined the incident is not material, or has not yet made a materiality determination, the Staff has clarified that the incident should be disclosed under a different item of Form 8-K (e.g., Item 8.01, Other Events).*	Item 1.05 of Form 8-K
Form 8-K/A — Item 1.05. Material Cybersecurity Incidents	If information was omitted from the original Form 8-K filing, registrants must file an amendment to the filing under Item 1.05 containing such information within four business days after such information is determined to be or becomes available.	Item 1.05 of Form 8-K
Risk management, strategy and governance disclosures		
Disclosure location	**Disclosure requirement**	**SEC guidance**
Form 10-K, Part I, Item 1C. Cybersecurity	Registrants must describe their processes, if any, for assessing, identifying and managing material risks from cybersecurity threats, including: ▸ Whether and how such 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 such processes ▸ Whether the registrant has processes in place to oversee and identify material risks from cybersecurity threats related to its use of third-party service providers	Item 106(b)(1) of Regulation S-K
	Registrants must describe 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.	Item 106(b)(2) of Regulation S-K
	Registrants must describe the board of directors' oversight of risks from cybersecurity threats, including, as applicable: ▸ Any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats ▸ Describe the processes by which the board or subcommittee is informed about such risks	Item 106(c)(1) of Regulation S-K

	Registrants must describe management's role in assessing and managing the registrant's material risks from cybersecurity threats, including, as applicable: ▸ Whether and which of the certain management positions or committees are responsible for assessing and managing cybersecurity risk and the relevant expertise ▸ The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents ▸ Whether such persons or committees report information about such risks to the board of directors or a committee of the board of directors	Item 106(c)(2) of Regulation S-K
Foreign private issuers		
Disclosure location	**Disclosure requirement**	**Disclosure location**
Form 6-K	Registrants must furnish information on material cybersecurity incidents promptly on Form 6-K if the information is (1) distributed to stockholders or to a national exchange (if the information is made public by that exchange) or (2) required to be made public under the registrant's domestic laws.	Instruction B of Form 6-K
Annual reports on Form 20-F, Part II, Item 16K	See the respective risk management, strategy and governance disclosures section for domestic registrants above.	Item 16K of Form 20-F