LEGAL UPDATES

PUBLISHED: AUGUST 15, 2023

SEC Heightens Issuers' Cybersecurity Disclosure Requirements

Services

Artificial Intelligence

Securities & Corporate Governance

Professionals

STEVEN R. BARRETT
CHATTANOOGA:
423.757.5905
STEVE.BARRETT@
HUSCHBLACKWELL.COM

ROBERT J. JOSEPH
CHICAGO:
312.526.1536
ROBERT.JOSEPH@
HUSCHBLACKWELL.COM

ANDREW SPECTOR
BOSTON:
617.598.6700
ANDREW.SPECTOR@
HUSCHBLACKWELL.COM

BRIAN WETZSTEIN
CHATTANOOGA:
423.266.5500
BRIAN.WETZSTEIN@
HUSCHBLACKWELL.COM

On July 26, 2023, the U.S. Securities and Exchange Commission (SEC) adopted final rules regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies. The final rules require registrants to (i) report on Form 8-K under a new Item 1.05 any material cybersecurity incident and (ii) disclose on Form 10-K under new Item 106 of Reg. S-K the registrant's cybersecurity risk management and strategy, the registrant's governance practices related to cybersecurity issues, and the material impacts of cybersecurity threats and previous cybersecurity incidents. In explaining its rationale for the new rules, the SEC's adopting release noted (a) inconsistent timing, content, and location of current disclosures on cybersecurity risks and incidents; (b) the increasing prevalence of cybersecurity incidents and attacks (as well as the significant impact such attacks may have on a company); and (c) the potential of recent developments in artificial intelligence to exacerbate cybersecurity threats. The SEC also cited academic studies suggesting that, overall, companies may be underreporting cybersecurity incidents.

Current reports required under new Item 1.05 of Form 8-K

Substance of the disclosure

Once a registrant determines that a material cybersecurity incident has occurred, it must describe (1) the material aspects of the nature, scope, and timing of the incident and (2) the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations. *Instruction* 4 to Item 1.05 clarifies that companies do not need to disclose specific or technical information about the company's planned response to the incident or its cybersecurity systems in such detail as would impede the company's response or remediation of the incident. The SEC noted that it believes the adopted standard "more precisely focuses the disclosure on

what the company determines is the material impact of the incident, which may vary from incident to incident," rather than on requiring disclosure of details regarding the incident itself.

If an incident is ongoing, the disclosure need not include details such as whether data were stolen and the status of any remediation efforts, although the SEC noted that disclosure regarding those items may be required if they are material.

In the event that information required to be disclosed under Item 1.05 of Form 8-K is not determined or is unavailable at the time of the required filing, companies must note the missing information in the initial disclosure and file an amendment to Form 8-K within four business days after such information is determined or becomes available.

There is no specific requirement to provide updated information concerning a cybersecurity incident, either in a Form 8-K or in a company's periodic reports; however, the SEC noted in the adopting release that companies may have a duty to correct prior disclosure that they determine was untrue at the time it was made or a duty to update disclosure that becomes materially inaccurate after it was made.

The SEC did not exempt registrants from providing disclosures regarding cybersecurity incidents on third-party systems they use; however, consistent with SEC rules regarding disclosure of information that is difficult to obtain (see Securities Act Rule 409 and Exchange Act Rule 12b-21), the final rules "generally do not require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers." Therefore, to the extent that information regarding third-party systems is available to a registrant or could be obtained without unreasonable effort or expense (e.g., pursuant to contractual rights), it appears that registrants would be required to disclose that information.

Materiality

The final rules require a registrant to disclose any cybersecurity incident determined to be material. For these purposes, a "cybersecurity incident" means 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 on such information systems.

The SEC declined to use a quantifiable materiality trigger for Item 1.05, stating that some cybersecurity incidents may be material yet not cross a particular financial or other quantitative threshold. The adopting release highlighted that the definition of a "cybersecurity incident" is intended to be construed broadly — potentially including an accidental exposure of data involving no "bad actor" — and may include "a series of related unauthorized occurrences." As a result, while the

SEC dropped its proposal to *require* aggregation of individually immaterial incidents in making a materiality analysis, it still noted that Item 1.05 could be triggered by a series of related immaterial occurrences that are determined by a registrant to be material in the aggregate.

The SEC also emphasized that the material impact of an incident may encompass a range of harms, some quantitative and others qualitative, and that a lack of quantifiable harm does not necessarily mean an incident is not material. By way of example, the SEC noted that a cybersecurity incident involving the theft of information may be deemed immaterial based on quantitative financial measures alone, but may become material — and therefore require disclosure — due to the impact on the registrant of the scope or nature of resulting harm to individuals, customers, or others. The SEC also noted that an incident that results in "significant reputational harm" may not be readily quantifiable and therefore may not cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material.

The SEC stressed its intention that the materiality standard registrants should utilize for these purposes is consistent with the general materiality standard under the securities laws—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." The SEC further stated that "doubts as to the critical nature" of the relevant information should be "resolved in favor of those the statute is designed to protect," namely investors. The adopting release also emphasized that the rule's inclusion of "financial condition and results of operations" is not exclusive, and that companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident.

Timing of the disclosure

The SEC stated that, as a result of its focus on materiality for purposes of triggering Item 1.05 disclosures, registrants will have to file an 8-K within four business days after the company determines that it has experienced a material cybersecurity event (rather than tying disclosure to the date of discovery of the incident itself). The adopting release also expressed the SEC's opinion that, in the majority of cases, the registrant will likely be unable to determine materiality the same day the incident is discovered, and that "disclosure becoming due less than a week after discovery should be uncommon." Instead, the SEC expects that registrants will continue to develop information after discovery until it is sufficient to facilitate a materiality analysis. The SEC also observed that, since these disclosure requirements focus on an incident's basic identifying details and its material impact or reasonably likely material impact, registrants should have developed a sufficient amount of such information to support the initial Item 1.05 disclosures as part of conducting their required materiality determination.

Exceptions or delay in disclosure/national security/FCC

The SEC rejected comments arguing that disclosure should be delayed until companies mitigate, contain, remediate, or otherwise diminish the harm resulting from a cybersecurity incident. In doing so, the SEC stressed its belief that Item 1.05 does not require disclosure of the types of details that have the potential to be exploited by threat actors, as the disclosure is intended to focus on the incident's material impact or reasonably likely material impact on the registrant.

However, a registrant may delay making an Item 1.05 Form 8-K filing if the United States attorney general determines that immediate disclosure would pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. Initially, disclosure may be delayed for a time period specified by the United States attorney general of up to 30 days following the date when the disclosure was otherwise required to be provided. The delay may be extended for additional periods in certain circumstances. The Department of Justice will notify the affected registrant that communication to the SEC has been made, so the registrant may delay filing its Form 8-K.

In addition to the permitted delay in filing in connection with national security, companies that are subject to the Federal Communications Commission's (FCC) notification rule for breaches of customer proprietary network information (CPNI) may delay making the Form 8-K disclosure up to seven business days following notification to the U.S. Secret Service and the Federal Bureau of Investigation, as specified by the FCC rule, subject to written notification to the SEC via a non-public Correspondence filing on EDGAR.

Other timing-related issues

The SEC declined to require periodic reporting of material cybersecurity incidents on Forms 10-Q and 10-K in lieu of adding a new Form 8-K requirement, arguing that such an approach may result in significant variance as to when investors learn of material cybersecurity incidents.

The instructions to Item 1.05 state that companies must make their materiality determinations "without unreasonable delay." The SEC noted that a materiality determination before a registrant has sufficient information is problematic for both registrants and investors, as a materiality determination necessitates an informed and deliberative process; however, the SEC also stated that a materiality determination cannot be unreasonably delayed in an effort to avoid timely disclosure. A registrant may not delay a determination of materiality solely due to the need for continued investigation regarding the incident. The SEC also warned that actions such as intentionally delaying a board meeting necessary to determine materiality or revising incident procedures to support a delayed materiality determination would constitute an unreasonable delay.

The SEC's adopting release also sought to assure registrants that they could (and should) continue normal practices of sharing information with other companies or government actors about emerging

cybersecurity threats without necessarily triggering Item 1.05 disclosure obligations. The SEC emphasized that Item 1.05 disclosure is only triggered once a company has developed information regarding an incident sufficient to make a materiality determination, and noted a decision to share information with other companies or government actors does not in itself constitute a determination of materiality. A registrant may alert similarly situated companies as well as government actors immediately after discovering an incident and before determining materiality, so long as it does not unreasonably delay its internal processes for assessing the materiality of the incident for disclosure purposes.

Limited safe harbors and S-3 eligibility

The untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility. The SEC noted that the consequences of the loss of Form S-3 eligibility would be unduly severe given the circumstances that will surround Item 1.05 disclosures. Similarly, new Item 1.05 of Form 8-K will be eligible for a limited safe harbor from liability under Section 10(b) and Rule 10b-5 under the Exchange Act. This accords with the view the SEC articulated in 2004 that the safe harbor is appropriate if the triggering event for the Form 8-K requires management to make a rapid materiality determination.

Form 10-K disclosures required under new Item 106 of Reg. S-K

The final rules amend Form 10-K to require registrants to add detailed disclosures describing their governance and risk management with respect to cybersecurity risks, including board oversight of cybersecurity risks. These rules represent a significant expansion of the disclosures previously required by SEC rules and expand on the SEC's previously issued interpretive guidance from 2011 and 2018.

Specifically, new Item 106(b) of Reg. S-K requires in each annual report on Form 10-K a description of the registrant’s processes for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. This description should address: (i) whether and how the described cybersecurity 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 material risks from cybersecurity threats associated with its use of any third-party service providers.

Item 106(b) also requires a registrant to disclose whether, and if so how, any risks from cybersecurity threats or previous cybersecurity incidents have materially affected or are reasonably likely to materially affect the registrant. This disclosure must address any material effects on the registrant including effects on its business strategy, results of operations, or financial condition.

New Item 106(c) requires in the Form 10-K a governance-related discussion of the registrant's oversight of cybersecurity risks at both the board and management levels. This must include a discussion of the extent to which the registrant's board of directors oversees risks from cybersecurity threats and, if applicable, the identity of any board committee or subcommittee responsible for such oversight. The discussion should include the internal processes by which the board or committee is informed and manages such risks. In a notable departure from the proposed rules, the final rules will not require disclosure as to whether and how the board integrates cybersecurity into its business strategy, risk management, and financial oversight function; the frequency of board discussions on cybersecurity; and whether directors have expertise in cybersecurity. The adopting release nevertheless noted that, depending on context, some registrants' descriptions of the processes by which their board or relevant committee is informed about cybersecurity risks may include the frequency of board or committee discussions.

Item 106(c) also requires a discussion of management's role in assessing and managing the registrant's material risks from cybersecurity threats. This discussion should address: (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 is necessary to fully describe the nature of the expertise; (ii) the internal 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.

Impact on Foreign Private Issuers (FPIs)

The new rules enhance required cybersecurity disclosures for FPIs as follows:

While less prescriptive than the requirements of new Item 1.05 of Form 8-K, the SEC amended *General Instruction* B to Form 6-K to require FPIs to furnish on that form any information concerning "material cybersecurity incidents" that they either (i) make or are required to make public pursuant to the law of their home jurisdiction, (ii) file or are required to file with any stock exchange on which their securities are traded (which was made public by that exchange) or (iii) otherwise distribute or are required to distribute to their security holders.

A new Item 16K was added to Part II of Form 20-F which will require FPIs who file annual reports on that form to provide essentially the same information required by new Item 106 of Reg. S-K in Form 10-K annual reports for domestic issuers.

The SEC noted that it did not amend Form 40-F, choosing instead to maintain the multijurisdictional disclosure system (MJDS) whereby eligible Canadian FPIs use Canadian disclosure standards and documents to satisfy SEC registration and disclosure requirements.

Compliance dates for the final rules

These new rules are effective September 5, 2023. For all registrants other than smaller reporting companies, the compliance date for cybersecurity incident disclosures under new Item 1.05 of Form 8-K and in Form 6-K is December 18, 2023. For smaller reporting companies, the compliance date is June 15, 2024.

All registrants must provide the new disclosures required under new Item 106 of Reg. S-K and Item 16K of Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023. This means calendar-year reporting companies must comply with the new rules in their upcoming annual reports.

All registrants must tag disclosures required under the final rules in Inline XBRL beginning one year after initial compliance with the related disclosure requirement. Therefore, for the annual report disclosures, companies must begin tagging in Inline XBRL starting with annual reports for fiscal years ending on or after December 15, 2024, and for Form 8-K disclosures, companies must begin tagging responsive disclosure starting with annual reports for fiscal years ending on or after December 18, 2024.

What this means to you

In light of these upcoming disclosure requirements, companies should carefully review and consider the current state of their cybersecurity and risk management systems, including consideration of any appropriate updates. This should include an examination of any recent changes in their technology infrastructure that may impact the risk of cybersecurity incidents, changes in the general cybersecurity threat landscape, and the impact of any recent cybersecurity incidents.

Companies should also ensure that their disclosure controls and procedures are sufficient to allow timely disclosure of cybersecurity incidents within four business days of the materiality determination required by Item 1.05 of Form 8-K (as opposed to 30-plus-day windows afforded by most state laws) and have a team in place to conduct real-time analysis of cybersecurity incidents to avoid delaying their materiality determinations. It is also important to note that, depending on the facts and circumstances surrounding a particular incident, disclosure within four business days of a company's materiality determination may likely precede the date otherwise required for data breach notices to individuals (and potentially affected business partners, customers, and clients) and state attorney

general notices. Accordingly, there may be some cases in which a company might want to accelerate these other disclosures—but only to the extent practicable—to coordinate with their Form 8-K filing.

Companies should (1) review and test their procedures for responding to cybersecurity incidents and amend or supplement them if needed to address the procedures and attendant documentation contemplated under the new reporting requirements and (2) confirm that their disclosure controls and procedures provide for effective communication between the cybersecurity team, the legal team supporting cybersecurity, and the disclosure committee and legal team supporting SEC filings, as well as for appropriate interaction with the board of directors or a responsible committee or subcommittee of the board. This process should include when and how to raise significant or material incidents with senior management and/or the board.

Companies should also confirm that their disclosure controls and procedures reflect the considerations discussed in the final rule's adopting release for assessing materiality, including inputs to consider potential reputational harm and damage to customer and vendor relationships. Companies should plan to carefully document both their materiality analysis and the reasonableness of the time that it takes to assess materiality. At the same time, since many incident response investigations are conducted under attorney-client and work product privileges, disclosure of material aspects of the incident could potentially undermine the confidentiality associated with investigating the incident. Related updates to a company's disclosure controls and procedures should take into account protection of these privileges, to the extent feasible. Unfortunately, heightened litigation risk may be an unavoidable byproduct of these new Form 8-K disclosures, since providing details concerning the expected impacts of an incident prior to the completion of a forensic investigation and data mining efforts has the potential to expose a company to premature litigation before it has a complete picture of the cybersecurity incident.

Companies should perform mock incident sessions with their cybersecurity incident response team at least annually to ensure familiarity with the incident response plan and to identify and address any inefficiencies. The SEC has recently brought enforcement actions against companies for inadequate disclosure controls and procedures involving cybersecurity incidents in which there was a breakdown in communication between the IT and financial reporting functions, leading to inaccurate disclosures to investors. Clear processes and chains of command will be necessary in order to ensure coordination and that neither activity is impeded by the other. In addition, companies should evaluate the adequacy and formality of their existing cybersecurity policies and procedures, to ensure that their cybersecurity programs are generally comparable with those of competitors, as the strength of companies' cybersecurity protocols could be a factor weighed by investors.

While the final rule did not impose new insider trading procedures relating to cybersecurity incidents, companies should continue to carefully assess that topic during the course of their response to a

cybersecurity incident and consider whether and when to employ event-specific blackouts to suspend any purchases or sales of company securities by the company and by insiders.

In the event of a cybersecurity incident at a third-party vendor, public companies may have difficulty obtaining timely information or obtaining sufficient details to make a materiality determination or disclose all the information required by Item 1.05 of Form 8-K. Companies should ensure they have effective communication protocols in place with third-party service providers to facilitate timely assessment and disclosure. To reduce some of this risk, public companies (and companies considering becoming public companies) may want to reassess the cybersecurity and data privacy risks associated with their vendor management programs. This may include conducting due diligence reviews and cybersecurity audits, strengthening contractual provisions to ensure access to third-party information needed to support timely and detailed cyber incident reporting, or even reconsidering the mix of internal and outsourced information technology systems. Companies should be aware of the need to describe their engagement of third parties in connection with the risk management process, any processes to oversee and identify risks associated with the use of third-party service providers, and the division of responsibility for oversight of cybersecurity risks between the board and management.

Companies should also evaluate their existing cybersecurity risk oversight at the board and management level and consider whether any improvements are needed, such as delegating tasks to a designated board committee or subcommittee, scheduling additional cybersecurity updates on board agendas, increasing the amount of time spent keeping the board informed concerning the company's strategies and tactics to address cybersecurity threats, and strengthening processes for timely communications regarding these issues between management and board members.

Regarding the new cybersecurity risk management and strategy disclosures required in Form 10-K, companies should be able to answer the following questions clearly to meet the requirements of the final rules:

Are our company's processes for assessing, identifying, and managing material risks from cybersecurity threats sufficiently well developed to support required disclosures for each of the elements identified in Item 106 of Reg. S-K and to help shield the company from potential "antifraud" liability related to such disclosures in actions brought by either the SEC or private litigants?

Are our company's policies and procedures updated regularly and are they followed/enforced effectively?

How do we monitor the effectiveness of our cybersecurity risk mitigation activities and controls?

Are our management processes for assessing and managing material risks from cybersecurity threats and related management communications to the board in support of the directors' oversight role sufficiently well developed to support the governance-related disclosures required by Item 106(c) of Reg. S-K?

Companies also should review their existing risk factor and proxy statement discussions of cybersecurity issues when drafting these new Form 10-K disclosures, to maintain consistency with past statements and assess how those disclosures may need to be enhanced or revised going forward. Similarly, companies should consider whether any new details disclosed in response to Item 106 should be incorporated into future proxy statement disclosures regarding cybersecurity oversight and governance.

Contact us

Husch Blackwell's Securities & Corporate Governance team will continue to monitor these changes and their implications. Should you have any questions, please do not hesitate to contact Steve Barrett, Bob Joseph, Andrew Spector, Brian Wetzstein, Robert Fritsche, or your Husch Blackwell attorney.