Volume 2, Number 1 January–February 2024

THE JOURNAL OF FEDERAL AGENCY ACTION

fastcase FULL COURT PRESS

The Journal of Federal Agency Action

Volume 2, No. 1 | January–February 2024

THE JOURNAL OF FEDERAL AGENCY ACTION (ISSN 2834-8796 (print) / ISSN 2834-8818 (online)) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint.

For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Production Editor: Sharon D. Ray
Cover Art Design: Morgan Morrissette Wright and Sharon D. Ray

This journal's cover includes a photo of Washington D.C.'s Metro Center underground station. The Metro's distinctive coffered and vaulted ceilings were designed by Harry Weese in 1969. They are one of the United States' most iconic examples of the brutalist design style often associated with federal administrative buildings. The photographer is by XH_S on Unsplash, used with permission.

Cite this publication as:

The Journal of Federal Agency Action (Fastcase)

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF FEDERAL AGENCY ACTION, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, and anyone interested in federal agency actions.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2834-8796 (print)
ISSN 2834-8818 (online)

U.S. Securities and Exchange Commission Adopts Cybersecurity Disclosure Rules for Public Companies

David M. Lynn, Haimavathi V. Marlier, and Miriam H. Wugmeister*

In this article, the authors explain that the cybersecurity disclosure rules updated recently by the U.S. Securities and Exchange Commission (SEC) represent a significant step in the SEC's efforts to promote greater transparency regarding cybersecurity incidents.

The U.S. Securities and Exchange Commission (SEC) has adopted amendments to its rules to require disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies.[1]

Under the rule and form amendments adopted by the SEC, public companies will be required to:

- Disclose, within four business days after determining that an incident is material pursuant to new Item 1.05 of Form 8-K (subject to limited exceptions described below), any cybersecurity incident that a company experiences that is determined to be material, describing the material aspects of its:
  - Nature, scope, and timing; and
  - The impact or reasonably likely impact of the incident on the company, including on the company's financial condition and results of operations.
- Describe, on a periodic basis pursuant to new Item 106 of Regulation S-K, the company's processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, as well as 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 Journal of Federal Agency Action / January–February 2024, Vol. 2, No. 1, pp. 45–60.

ISSN 2834-8796 (print) /ISSN ISSN 2834-8818 (online).

- Describe, on a periodic basis pursuant to new Item 106 of Regulation S-K, the board's oversight of risks from cybersecurity threats; and
- Describe, on a periodic basis pursuant to new Item 106 of Regulation S-K, management's role in assessing and managing material risks from cybersecurity threats.

The SEC adopted similar disclosure requirements that will apply to foreign private issuers.

In adopting the final rules, the SEC made the following significant changes from the proposing release in response to comments:

- Narrowed the scope of the disclosure required by pursuant to Item 1.05 of Form 8-K;
- Added a limited delay for disclosures that would pose a substantial risk to national security or public safety;
- Required certain updated incident disclosure in an amended Form 8-K, rather than in Forms 10-Q and 10-K;
- Omitted a proposed requirement that contemplated periodic disclosure of aggregated immaterial cybersecurity incidents that were deemed to be material;
- Streamlined the proposed disclosure elements related to risk management, strategy, and governance; and
- Did not adopt a proposed requirement to disclose board cybersecurity expertise.

The final rules are now in effect. The compliance time frame is as follows:

- With respect to the periodic disclosures required by Item 106 of Regulation S-K, all issuers must provide such disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023;
- With respect to compliance with the current disclosure requirements for material cybersecurity incidents required by Item 1.05 of Form 8-K, all issuers (other than smaller reporting companies) must begin complying the later of 90 days after publication of the Adopting Release in the Federal Register or December 18, 2023; and
- Smaller reporting companies have an additional 180 days from the non-smaller reporting company compliance date,

so those issuers must begin complying with Item 1.05 of Form 8-K 270 days after publication of the Adopting Release in the Federal Register or June 15, 2024, whichever is later.

Key Takeaways for Public Companies

The SEC's final rules requiring disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting should prompt public companies to:

- Ensure that incident response policies and procedures provide a clear path to escalate incidents to corporate leadership and/or a disclosure committee, and that disclosure controls and procedures are in place to discern the impact that an incident may have on the company;
- Establish the framework for undertaking a materiality assessment without unreasonable delay after discovery of the incident so that decisions about whether an incident must be disclosed under SEC rules can be completed on a timely basis;
- Modify or establish disclosure controls and procedures to facilitate the reporting of material cybersecurity incidents, including the nature, scope, and timing of the incident and the impact or reasonably likely impact of the incident on the company, including on the company's financial condition and results of operations, within the four-businessday deadline contemplated by new Item 1.05 of Form 8-K, as well as any information that was not determined or was unavailable at the time of the initial Form 8K filing; and
- Prepare new disclosures for the company's annual report regarding the company's processes for the assessment, identification, and management of material risks from cybersecurity threats; 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 board's oversight of risks from cybersecurity threats; and management's role in assessing and managing material risks from cybersecurity threats.

Background

Since 2011, the SEC and its staff have been focused on disclosures that public companies make about cybersecurity risks.

On October 13, 2011, the SEC's Division of Corporation Finance issued disclosure guidance to assist public companies "in assessing what, if any, disclosures should be provided about cybersecurity matters in light of each registrant's specific facts and circumstances."[2] CF Disclosure Guidance Topic No. 2 reviewed the applicability of existing SEC disclosure requirements to cybersecurity concerns, noting that: (1) businesses increasingly focus or rely on internet communications and remote data storage; (2) risks and potential costs associated with cyber attacks and inadequate cybersecurity are increasing; and (3) as with other operational and financial risks and events, companies should, on an ongoing basis, review the adequacy of disclosure relating to cybersecurity risks and other cyber incidents.

On February 20, 2018, the SEC issued interpretive guidance, which noted that public companies should take all required actions "to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[3] The SEC noted in this guidance the importance of disclosure controls and procedures "that provide an appropriate method of discerning the impact that such matters may have on the issuer and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents." In addition, the 2018 Interpretive Release noted that "directors, officers, and other corporate insiders must not trade a public company's securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company." The SEC indicated that companies should have policies and procedures in place to: (1) guard against directors, officers, and other corporate insiders taking advantage of the period between the issuer's discovery of a cybersecurity incident and public disclosure of the incident to trade based on material nonpublic information about the incident, and (2) help ensure that the issuer makes timely disclosure of any related material nonpublic information.

In recent years, the SEC has also brought numerous enforcement actions against public companies that experienced material

cybersecurity incidents, alleging that the companies failed to adequately disclose such incidents and/or failed to have appropriate disclosure controls and procedures in place to facilitate the timely disclosure of material cybersecurity incidents. The SEC has also brought insider trading actions against individuals who traded in a company's securities while in possession of material nonpublic information regarding a material cybersecurity incident.

On March 9, 2022, the SEC proposed amendments to its rules to require real-time disclosure of material cybersecurity incidents, as well as disclosures regarding cybersecurity risk management, strategy, and governance.[4] The proposed amendments contemplated current reporting on Form 8K of material cybersecurity incidents, as well as periodic disclosures about a company's policies and procedures to identify and manage cybersecurity risks, management's role in implementing cybersecurity policies and procedures, and oversight of cybersecurity risk by the board of directors.

The SEC received over 150 comment letters in response to the Proposing Release. The SEC noted in the Adopting Release that "[the] majority of comments focused on the proposed incident disclosure requirement, although we also received substantial comment on the proposed risk management, strategy, governance, and board expertise requirements." The SEC's Investor Advisory Committee provided recommendations to the SEC, stating that the Committee supported the proposed incident disclosure requirement and proposed risk management, strategy, and governance disclosure requirements, but recommending that the SEC reconsider the proposed requirement to disclose the board of directors' cybersecurity expertise. The Committee also suggested that the SEC require companies to disclose the key factors they used to determine the materiality of a reported cybersecurity incident and suggested that the disclosures proposed for periodic reports be required in registration statements.

Current Reporting of Cybersecurity Incidents on Form 8-K

The SEC adopted new Item 1.05 of Form 8-K, titled "Material Cybersecurity Incidents." Item 1.05(a) of Form 8-K specifies that if a company experiences a cybersecurity incident that is determined by the company to be material, the company must 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. The Item 1.05 Form 8-K must be filed within four business days of determining that an incident is material, subject to limited exceptions described below. The information must be "filed," not "furnished," with the Item 1.05 Form 8-K. The required information must be tagged using Inline XBRL.

Scope of the Disclosure

In the Adopting Release, the SEC notes that the formulation in the final rule "more precisely focuses the disclosure on what the company determines is the material impact of the incident, which may vary from incident to incident," as compared to the more expansive disclosure about the incident that was contemplated by the proposed amendments. The SEC notes that the inclusion of the phrase "financial condition and results of operations" in Item 1.05(a) is not intended to be exclusive, and that companies should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. The SEC notes that, for example, harm to a company's reputation, customer or vendor relationships, or competitiveness may have a material impact on the company. Further, the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities, could constitute a reasonably likely material impact on the company.

In adopting the amendments, the SEC did not adopt, as proposed, a requirement for disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised. Further, the SEC did adopt Instruction 4 to Item 1.05, which provides that a "registrant need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident."

Some commenters raised questions concerning the application of proposed Item 1.05 of Form 8K to incidents occurring on third-party systems. In the Adopting Release, the SEC notes that it did not exempt companies from providing disclosures regarding

cybersecurity incidents on third-party systems they use, and it did not provide any safe harbor for information disclosed about third-party systems. The SEC notes that "depending on the circumstances of an incident that occurs on a third-party system, disclosure may be required by both the service provider and the customer, or by one but not the other, or by neither." The SEC indicates that the final rules "generally do not require that registrants conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants' disclosure controls and procedures," indicating that approach is consistent with the SEC's rules regarding the disclosure of information that is difficult to obtain.

Timing of the Disclosure

Consistent with the time line for reporting contemplated for most other disclosure items required to be reported on Form 8-K, a Form 8-K that is required by new Item 1.05 must be filed within four business days of determining that an incident is material, subject to limited exceptions described below.

As noted in the Adopting Release, the SEC considered comments regarding the timing of filing the Form 8-K, but determined to not establish a longer deadline, require the disclosure in periodic reports rather than in a Form 8-K, or establish a specific financial threshold as a trigger for filing Form 8-K. In a change from the proposed amendments in response to commenters' concerns, Instruction 1 to Item 1.05 of Form 8-K as adopted states: "[a] registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident," rather than indicating that the materiality determination must be made "as soon as reasonably practicable." In light of this change to the instruction, the SEC encourages companies to continue sharing information with other companies or government actors about emerging threats, noting that sharing such information may not necessarily result in an Item 1.05 disclosure obligation because a decision to share the information "does not in itself necessarily constitute a determination of materiality."

The SEC adopted two exceptions to the four-business-day deadline applicable to Item 1.05 of Form 8-K.

First, paragraph (d) of Item 1.05 indicates that if a company is subject to the Federal Communications Commission's notification rule for breaches of customer proprietary network information (CPNI),[5] the company may delay providing the disclosure required by Item 1.05 for such period that is applicable under the notification rule[6] and in no event for more than seven business days after notification required under that provision has been made, so long as the company notifies the SEC in correspondence submitted via the EDGAR system no later than the date when the disclosure required by Item 1.05 was otherwise required to be provided.

Second, paragraph (c) of Item 1.05 provides a framework for delaying the filing of an Item 1.05 Form 8-K if the U.S. 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. Paragraph (c) specifies that if the attorney general determines that disclosure required by paragraph (a) of Item 1.05 poses a substantial risk to national security or public safety, and notifies the SEC of such determination in writing, the company may delay providing the disclosure required by Item 1.05 for a time period specified by the attorney general, up to 30 days following the date when the disclosure required by Item 1.05 was otherwise required to be provided. Disclosure may be delayed for an additional period of up to 30 days if the attorney general determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing. In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the attorney general determines that disclosure continues to pose a substantial risk to national security and notifies the SEC of such determination in writing. If the attorney general indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief through exemptive orders.

The SEC notes in the Adopting Release that it consulted with the Department of Justice to establish an interagency communication process to allow for the attorney general's determination to be communicated to the SEC in a timely manner. The SEC notes that the Department of Justice will notify the affected company that communication to the SEC has been made, so that the company may delay filing its Form 8-K.

The SEC determined to not provide for any broader law enforcement exception or provide exceptions with respect to any other federal laws or regulations in the final amendments.

Antifraud Safe Harbor and Form S-3 Eligibility

The SEC adopted amendments so that the untimely filing of an Item 1.05 of Form 8-K will not result in the loss of Form S-3 eligibility. Item 1.05 is also included in the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Securities Exchange Act of 1934, as amended (Exchange Act).

Required Amendments to Item 1.05 Form 8-Ks

Instruction 2 to Item 1.05 specifies that, to the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the company must include a statement to that effect in the filing and then must file an amendment to the Form 8-K containing such information within four business days after the company, without unreasonable delay, determines such information or within four business days after such information becomes available. In light of this requirement, the SEC did not adopt a requirement to disclose updated information about an incident in a company's periodic reports. The SEC notes in the Adopting Release that "under the final rules, companies will not have to distinguish whether information regarding a material cybersecurity incident that was not determined or was unavailable at the time of the initial Form 8-K filing should be included on current reports or periodic reports, as the reporting would be in an amended Form 8-K."

Determining Materiality

The SEC affirmed in the Proposing Release that the materiality standard companies should apply in evaluating whether a Form 8-K would be triggered under Item 1.05 would be consistent with the standard set forth in the numerous cases addressing materiality in the securities laws, as well as Rule 405 under the Securities Act of

1933, as amended and Exchange Act Rule 12b-2.[7] For this purpose, information about a cybersecurity incident is considered "material" if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would have been viewed by the reasonable investor as having significantly altered the "total mix" of information made available to the investor. As part of a materiality analysis, the company should consider the indicated probability that an event will occur and the anticipated magnitude of the event in light of the totality of company activity. No single fact or occurrence is determinative as to materiality, which requires an inherently fact-specific inquiry.

The SEC has noted in its guidance that an evaluation of the materiality of a cybersecurity incident should not be based solely on a quantitative analysis of the cybersecurity incident; rather, a company must thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident (including both quantitative and qualitative factors) to determine whether the incident is material. Even if the probability of an adverse consequence from a cybersecurity incident is relatively low, when the magnitude of the loss, liability, or other harm is high, the incident may still be material.

Consistent with the SEC's guidance, the materiality of cybersecurity incidents depends on the nature, extent, and potential magnitude of the incident, particularly as those factors relate to any compromised information or the business and scope of company operations. The materiality of cybersecurity incidents also depends on the range of harm that such incidents could cause, including:

- The potential harm to the company's financial condition and results of operations;
- The potential harm to the company's relationships with customers, clients, vendors, business partners, and others;
- The potential harm to the company from a competitive standpoint;
- The potential harm to the company's reputation; and
- The possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities.

Periodic Disclosure of Cybersecurity Risk Management, Strategy, and Governance

Under a new "Item 1C. Cybersecurity" in Part I of Form 10-K, companies will be required to disclose information regarding the company's cybersecurity risk management, strategy, and governance pursuant to new Item 106 of Regulation S-K. The required information must be tagged using Inline XBRL.

As noted above, the SEC did not adopt proposed Item 106(d)(1) of Regulation S-K, which would have required companies to disclose any material changes, additions, or updates to information required to be disclosed pursuant to Item 1.05 of Form 8-K in a company's Quarterly Report on Form 10-Q or Annual Report on Form 10-K for the period in which the material change, addition, or update occurred.

The SEC also did not adopt proposed Item 106(d)(2) of Regulation S-K, which would have required disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. In the Adopting Release, the SEC notes the definition of "cybersecurity incident" that the SEC adopted extends to "a series of related unauthorized occurrences," recognizing that cybersecurity incidents sometimes compound over time, rather than present as a discrete event. The SEC indicates, "[a]ccordingly, when a company finds that it has been materially affected by what may appear as a series of related cyber intrusions, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial."

Risk Management and Strategy

The SEC adopted Item 106(b) of Regulation S-K, which provides that a company must describe the company'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 providing this disclosure, a company should address, as applicable, the following nonexclusive list of disclosure items:

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

A company must also 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 company, including its business strategy, results of operations, or financial condition, and, if so, how.

In the Adopting Release, the SEC confirms "that the purpose of the rules is, and was at proposal, to inform investors, not to influence whether and how companies manage their cybersecurity risk." To respond to commenters' concerns about security, the SEC indicates that final rules eliminate or narrow certain elements from proposed Item 106(b) of Regulation S-K.

In the final rules, the SEC did not allow Item 106(b) disclosure to be provided in the proxy statement and did not require Item 106 disclosures in registration statements as recommended by the Investor Advisory Committee. In the Adopting Release, the SEC reiterated the guidance from the 2018 Interpretive Release that "[c]ompanies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements." In the Adopting Release, the SEC notes that companies may satisfy the Item 106 disclosure requirements through incorporation by reference pursuant to Exchange Act Rule 12b-23.

Governance

The SEC adopted Item 106(c) of Regulation S-K, which provides that a company must describe the board of directors' oversight of risks from cybersecurity threats. If applicable, a company must 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.

A company must also describe management's role in assessing and managing the issuer's material risks from cybersecurity threats. In providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items:

- 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;
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors, a committee, or a subcommittee of the board of directors.

Relevant expertise of management may include, for example, prior work experience in cybersecurity, any relevant degrees or certifications, and any knowledge, skills, or other background in cybersecurity.

The SEC noted in the Adopting Release that, in the final rules, it had "streamlined Item 106(c) to require disclosure that is less granular than proposed." Significantly, the SEC also did not adopt a proposed requirement to disclose board cybersecurity expertise pursuant to Item 407 of Regulation S-K, which was opposed by many commenters. As discussed above, the final rules do include a requirement to describe the relevant expertise of members of management responsible for assessing and managing cybersecurity risks.

Definitions

The SEC adopted Item 106(a) of Regulation S-K largely as proposed, defining the terms "cybersecurity incident," "cybersecurity threat," and "information systems," as used in Item 106 of Regulation S-K and Item 1.05 of Form 8-K, as follows:

- "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;
- "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; and
- "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.

In response to comments and in light of other changes reflected in the final rules as described above, the SEC added the phrase "or a series of related unauthorized occurrences" to the "cybersecurity incident" definition, reflecting the SEC's guidance that a series of related occurrences may collectively have a material impact or reasonably likely material impact and therefore trigger a Form 8-K filing pursuant to Item 1.05, even if each individual occurrence on its own would not rise to the level of materiality. The SEC made a clarifying change to the definition of "information systems" by inserting "electronic" before "information resources," to ensure that the rules pertain only to electronic resources. The SEC also made minor revisions to the "cybersecurity threat" definition for clarity and to better align it with the "cybersecurity incident" definition.

Disclosure by Foreign Private Issuers

Foreign private issuers are not required to file Current Reports on Form 8-K, and instead must furnish on Form 6-K copies of all information that the foreign private issuer: (1) makes, or is required to make, public under the laws of its jurisdiction of incorporation; (2) files, or is required to file, under the rules of any stock exchange; or (3) otherwise distributes to its security holders. The

SEC amended General Instruction B of Form 6-K to reference material cybersecurity incidents among the items that may trigger a current report on Form 6-K. The SEC notes that, "for a cybersecurity incident to trigger a disclosure obligation on Form 6-K, the registrant must determine that the incident is material, in addition to meeting the other criteria for required submission of the Form."

The SEC amended Form 20-F to add Item 16K, which requires a foreign private issuer to include in its Annual Report on Form 20-F the same type of disclosure that the SEC requires pursuant to Item 106 of Regulation S-K.

Structured Data

The SEC requires that companies tag the information specified by Item 1.05 of Form 8-K and Item 106 of Regulation S-K in Inline XBRL in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual. These tagging requirements include block text tagging of narrative disclosures, as well as detail tagging of quantitative amounts disclosed within the narrative disclosures.

Next Steps

The final amendments adopted by the SEC represent a significant step in the SEC's efforts to promote greater transparency regarding cybersecurity incidents. With these final rules, the SEC now moves past its reliance on more general disclosure requirements and interpretive guidance by creating an entirely new disclosure regime that will apply to current disclosure of cybersecurity incidents and periodic disclosure of cybersecurity risk management, strategy, and governance. These new disclosure requirements will require companies to evaluate and adapt their disclosure controls and procedures, management processes, and governance structures around cybersecurity to prepare for the new environment of transparency in this important area.

Notes

* The authors, partners in Morrison & Foerster LLP, may be contacted at dlynn@mofo.com, hmarlier@mofo.com, and mwugmeister@mofo.com, respectively.

1. Release No. 33-11216, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (July 26, 2023) (Adopting Release), https://www.sec.gov/files/rules/final/2023/33-11216.pdf.

2. CF Disclosure Guidance: Topic No. 2—Cybersecurity (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

3. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) (2018 Interpretive Release), https://www.sec.gov/files/rules/interp/2018/33-10459.pdf.

4. Release No. 33-11038, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (Mar. 9, 2022) (the Proposing Release), https://www.sec.gov/files/rules/proposed/2022/33-11038.pdf.

5. 47 CFR 64.2011. The SEC notes in the Adopting Release that the Federal Communication Commission's rule for notification in the event of breaches of CPNI requires covered entities to notify the United States Secret Service and the Federal Bureau of Investigation no later than seven business days after reasonable determination of a CPNI breach, and further directs the entities to refrain from notifying customers or disclosing the breach publicly until seven business days have passed following the notification to the Secret Service and Federal Bureau of Investigation.

6. 47 CFR 64.2011(b)(1).

7. *See, e.g.*, TSC Industries, Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976); Basic, Inc. v. Levinson, 485 U.S. 224, 232 (1988); *and* Matrixx Initiatives, Inc. v. Siracusano, 563 U.S. 27 (2011).