Articles + Publications | July 31, 2023

SEC Adopts Final Cybersecurity Rules — Requires Companies to Focus on Their Security and Disclosure Plans

WRITTEN BY

Heather M. Ducat | James Koenig | David I. Meyers | Sadia Mirza | Kim Phan | Betty Linkenauger Segaar | Karla Ballesteros | Jason L. Langford | Connor Nechodom

On July 26, the Securities and Exchange Commission (SEC) adopted, by a 3-2 margin, a final rule to require more immediate disclosure of material cybersecurity incidents by public companies. In addition, the final rule requires annual disclosure of material information regarding a public company's cybersecurity risk management strategy and cybersecurity governance.

In approving the final rule, SEC Chairman Gary Gensler stated that the final rule will provide investors with more consistent, comparable, and decision-useful tools for analyzing disclosures about cybersecurity incidents. The reality is that the final rule requires public companies to make difficult real-time decisions about whether a cybersecurity incident requires disclosure, all while in the middle of responding to and addressing the actual incident. When a cybersecurity incident inescapably happens, the right information must be reported up the chain to those making disclosure decisions. Public companies should consider identifying gaps in reporting structures and increasing collaboration among security teams and legal counsel.

Compliance Deadlines

The final rule becomes effective 30 days after publication in the *Federal Register*. The new disclosures will need to be incorporated into Form 10-K and Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023. The new disclosures will need to be incorporated into Form 8-K and Form 6-K beginning December 18, 2023. Smaller reporting companies will have an additional 180 days before they must begin providing the Form 8-K disclosures. All public companies must tag disclosures required under the final rule with iXBRL beginning one year after initial compliance with the related disclosure requirement.

Material Cybersecurity Incidents Must be Disclosed on Current Reports on Form 8-K

The final rule adds a new disclosure requirement to Item 1.05 of Form 8-K that will require public companies to disclose any "cybersecurity incident"[1] determined to be material. The Form 8-K must be filed within four business days of a public company's materiality determination. That is, a public company is not required to make the cybersecurity disclosures within four business days of the discovery of a cybersecurity incident, but within four business days of the date that the company determines that the cybersecurity incident is material. In assessing materiality, the final rule adopted the long-accepted definition of "materiality" from *TSC Industries, Inc. v. Northway, Inc.* 426 U.S. 438 (1976), *i.e.*, something 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." A company must make this determination without "unreasonable delay after discovery of the incident." The Item 1.05 disclosure must describe (1) the material aspects of the cybersecurity incident, including the nature, scope, and timing of the incident; and (2) the material impact, or reasonably likely material impact, of the cybersecurity incident on the company, including its impact on its financial condition and results of operations.

The new Form 8-K disclosure requirement encompasses disclosure of material incidents that occur on a public company's third-party systems (such as cloud-hosted systems). While acknowledging that public companies will have less visibility into third-party systems, the SEC stressed that public companies should make their disclosure based on the information available to them. The final rule generally does not require public companies to conduct additional inquiries outside of their regular channels of communication with third-party service providers.

In response to public comments, the SEC made several significant changes from the proposed rules (described here). To balance the most common criticisms of the proposed Item 1.05 requirements reported during the comment process concerning the scope and timing of the disclosure, the final rule narrowed the information required to be disclosed. As adopted, the final rule does not require disclosure of: (1) the incident's remediation status; and (2) information about the company's planned response to the incident, its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail that would impede the company's response. As such, the final rule attempts to focus disclosures on the material impact of a cybersecurity incident rather than requiring extensive details about the incident itself, which critics argued could be misused by malicious actors. The SEC noted, however, that it was not persuaded that it should forgo requiring disclosure of the existence of an incident while it is ongoing. As to concerns with timing of the disclosure, the SEC stated that by reducing required disclosures to information "focused on an incident's basic identifying details and its material impact or reasonably likely material impact" public companies should have all the information necessary to make the disclosure.

Additionally, the final rule provides for a limited delay of the Form 8-K disclosure for cybersecurity events that could pose a "substantial risk to national security or public safety." However, a company's ability to earn this relief requires the intervention of the U.S. attorney general. If a public company persuades the attorney general that the required disclosure would pose a substantial risk to national security or public safety, disclosure may be delayed for 30 days following the date when the disclosure was otherwise required to be provided. The attorney general must notify the SEC of such determination in writing. After the initial delay notification period, the attorney general may recommend, subject to the SEC's discretion, additional delays of up to 60 days if disclosure would still pose a substantial risk to national security or public safety. Beyond that, additional requests for delay may be considered through exemptive orders. To facilitate such communications, the SEC noted that it consulted with the Department of Justice to establish an interagency communication process – but details on how this process would work were absent in the final rule.

Finally, as proposed, the late disclosure of an Item 1.05 Form 8-K would not result in a loss of S-3 eligibility.

Updates with a Form 8-K Amendment

In a significant change from the proposed rule, the SEC did not require updates to cybersecurity incidents

previously reported under Item 1.05 of Form 8-K be reported in periodic reports. Instead, public companies must make such updates through an amended Item 1.05 disclosure on Form 8-K. The instructions to Item 1.05 of Form 8-K will require a public company to identify any information required by Item 1.05 that was not determinable or was unavailable at the time of the required filing. When such information becomes available, the company must file an amended Form 8-K within four business days. The SEC specifically noted that the final rule does not require an amended Form 8-K for all new information, but only for that information required by Item 1.05 of Form 8-K that was unavailable at the time the initial Form 8-K was required. The final rule does not separately create or otherwise affect a company's duty to update its prior statements.

Practical Guidance

Security teams and legal counsel should collaborate to determine whether an incident is material. This will challenge companies to balance timely disclosure with accurate disclosure. No incidents are equal in size and nature; what may seem like a material incident can later be deemed immaterial and vice versa. Companies should ensure incident response plans account for consistent communication flows among key stakeholders. It does not matter how robust a security response plan is if the information does not make its way to those making disclosure decisions or if it is not reported in time.

Whether an incident is material also does not solely depend on a financial threshold. A public company should consider harm to such company's reputation, customer or vendor relationships, competitiveness, or the possibility of litigation or a regulatory investigation, from state, federal, and non-U.S. authorities when determining whether disclosure is required.

Once a company determines a cybersecurity event has occurred, it must make a materiality determination without "unreasonable delay." While public companies should generally be experienced in applying the *TSC v. Northway* materiality standard, many companies may not be comfortable applying these standards to a cybersecurity incident.

A company should not delay filing a Form 8-K once the cybersecurity event is deemed material even if material information is "undetermined or unavailable" at the time of the initial Form 8-K filing. The instructions to Item 1.05 of Form 8-K specifically envision this scenario and permit amendments to the Form 8-K to be filed as such material information becomes known. A company should also correct any prior disclosures made under Item 1.05 of Form 8-K that such company later determines were untrue at the time they were made or become materially inaccurate after they were made.

Public companies should also consider whether a series of cybersecurity incidents, taken as a whole, cross the materiality threshold, rather than failing to disclose the incidents because each incident was determined to be immaterial.

Annual Disclosure Obligations

The final rule also amends Form 10-K and adds new Item 106 to Regulation S-K to require updated cybersecurity disclosure in Form 10-Ks concerning how public companies manage and govern for cybersecurity risks.

The amendment to Form 10-K adds new Item 1C. Cybersecurity to Part I of Form 10-K, which will require the disclosures mandated by Item 106 of Regulation S-K. New Regulation S-K Item 106(b) will require public companies to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. It will also require a public company to describe whether any risks from cybersecurity incidents have, or are reasonably likely to, materially affect such company, including its business strategy, results of operations, or financial condition. The final rule limits the level of detail required to be disclosed regarding a public company's internal processes to information that is material to investors in order address concerns that requiring additional detail could increase a public company's vulnerability to cyberattack. In addition to adding a materiality qualifier to the required disclosures, the final rule also reduces the amount of granular disclosure required by the proposed rules.

New Regulation S-K Item 106(c) will require public companies to describe the board's oversight of risk from cybersecurity threats, identify a board committee or subcommittee responsible for such oversight, if any, and describe the processes by which the board or such committee or subcommittee is informed about such risks. Item 106(c) will also require disclosures describing management's role in assessing and managing material risks from cybersecurity threats, including identifying which management positions and committees are involved, the processes undertaken, and how management reports cybersecurity risks to the board. Similar to its approach to Item 106(b), the SEC reduced the disclosures required from those in proposed Item 106(c), added materiality qualifiers, and adopted a relatively less granular approach.

The final rule does not require public companies to disclose (as proposed): (1) whether and how the board integrates cybersecurity into its business strategy, risk management, and financial oversight; or (2) the frequency of discussions on cybersecurity. The final rule also did not adopt the proposal to require disclosure about the cybersecurity expertise, if any, of a public company's board members.

Practical Guidance

Item 106 – and the final rule as a whole – make it clear that cybersecurity threats are no longer just an IT problem. Boards will be required to oversee the collaborative efforts to protect against and respond to cyber threats. What has traditionally been a reactive process will slowly shift to a proactive collaboration among various key stakeholders.

Security teams and legal counsel will again need to work together to draft the disclosure to ensure the information is accurate, relevant, and necessary. Companies responding to cybersecurity incidents face the difficult task of managing incident response efforts while maintaining attorney-client privilege protections. As with forensic reports, disclosures should be factual and avoid speculations or opinions. While a company may want to minimize the impact of the incident, companies that fail to be forthcoming with information can face probes and potential penalties from the SEC for misleading investors. This means companies should create and/or tailor incident response plans to be effective in providing guidance on how to identify and respond to red flags. These response plans should be consistently tested and reviewed to keep up with the evolving threats. Again, these disclosures will require collaboration from multiple key stakeholders.

Public companies are not required to disclose formally adopted cybersecurity policies and procedures, which could lead to the disclosure of operational details that could be weaponized by cyber criminals. Rather, a public

company can still comply with the newly adopted Items 106(b) and (c) of Regulation S-K by focusing disclosures generally on its risk assessment and putting a governance program in place and discussing how such programs have evolved given changes in the company's material cybersecurity risks.

Public companies should consider the following when describing management's role in assessing and managing material risks from cybersecurity threats:

- Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of those individuals in enough detail to fully describe the nature of the expertise;

- How 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 or a committee or subcommittee of the board.

Additionally, although the frequency of discussion on cybersecurity is not an express requirement under Item 106(c)(1), a public company should consider whether a discussion of frequency should be included in its description of how the board or relevant committee is informed about cybersecurity risks.

Application to Foreign Private Issuers

The final rule is applicable to foreign private issuers (FPIs) and modifies Forms 20-F and 6-K to require disclosures concerning material cybersecurity incidents similar to those required by public companies using domestic filing forms. The final rule amends Part II of Form 20-F by adding Item 16K, which has language identical to that in new Regulation S-K Item 106. Form 6-K was modified by amending General Instruction B to include material cybersecurity incidents among the items triggering a Form 6-K filing.

The SEC, however, declined to require Canadian FPIs utilizing the Multi-Jurisdiction Disclosure System (MJDS) to make the annual disclosure requirements enumerated in Regulation S-K Item 106 (and added to Form 20-F) when filing annual reports on Form 40-F. Given that such filers are already subject to the Canadian Securities Administrator's 2017 guidance on the disclosure of cybersecurity incidents and that the MJDS generally permits such filers to use Canadian disclosure standards and documents, the SEC did not find a reason to adopt prescriptive cybersecurity disclosure requirements for 40-F filers.

Structured Data Requirements

The SEC adopted the Structured Data Requirements as proposed, which requires public companies to tag the information specified by new Item 1.05 of Form 8-K and new Items 106(b) and (c) of Regulation S-K with Inline XBRL (iXBRL) in accordance with Rule 405 of Regulation S-T and the EDGAR Filer Manual.

Criticism of the Rule

In dissenting from the final rule, Commissioner Hester Peirce delivered an excoriating critique listing a series of question and open interpretative issues that the final rule does not address. Commissioner Mark Uyeda also dissented from the adoption of the final rule and criticized it as elevating cybersecurity disclosures above other risks and issues that may be more material to investors.

Peirce raised concerns with the SEC's expansive view of its authority as expressed in the final rule, warning that it "reads like a test run for future overly prescriptive, overly costly disclosure rules covering a never-ending list of hot topics." In her view, the expansive view of the SEC's authority manifests itself in three ways throughout the final rule. First, the rejection of financial materiality as the touchstone for disclosures, causing the granular disclosures the final rule requires to "seem designed to better meet the needs of would-be hackers" rather than investors. Second, the required governance disclosures read like a compliance checklist that would have the SEC managing public companies' cybersecurity and will "drive companies to spend resources on compliance with our rules and conformity with other companies' disclosed practices, instead of on combatting cyber threats as they see fit." Finally, Peirce was concerned with the SEC's refusal to consider other cybersecurity rules and a failure to "defer to other government agencies with overarching mandates to protect national security, public safety, and critical infrastructure." In a similar vein, she noted that getting the necessary approval from the U.S. attorney general — within four days — to use the national security or public safety exemption "will be quite a feat."

Additionally, Peirce worried that the final rule's prescriptive approach will impose considerable costs on investors, arguing that a more flexible, principles-based approach would be a better way to protect investors. Her views on these costs can also be broken down into three categories. First are the direct compliance costs that public companies will face in complying with the final rule — a matter the final rule admits it is generally unable to quantify. In this compliant, she was joined by Uyeda, who found the SEC's determination that the final rule was not a "major rule" under the Small Business Regulatory Enforcement Act, completely uncredible, as the comments suggested that compliance costs could be well in excess of $100 million. Second, Peirce warned that the disclosures will aid cyber criminals by handing them a roadmap of which companies to target and how to attack. And third, she worried that disclosures might "mislead otherwise uninformed investors without first-hand knowledge of cyber attacking" while "the fast timeline for disclosing cyber incidents could lead to disclosures that are tentative and unclear, resulting in false positives and mispricing in the market."

In closing her dissent, Peirce raised several questions that registrants will have to wrestle with as they begin to prepare the disclosures required under the final rule, including:

- Whether public companies will have to develop new systems to track immaterial cybersecurity incidents given that the definition of "cybersecurity incident" includes "an unauthorized occurrence, or a series of related unauthorized occurrences."

- Given that "related" is not defined, how will a company determine whether to aggregate occurrences for purposes of determining whether to file a Form 8-K?

- "Cybersecurity incident" is defined to include anything that "jeopardizes" information systems. Under this definition, a cybersecurity incident could occur whenever information is merely at risk even if not actually stolen. Won't companies have difficulty tracking cybersecurity incidents, so broadly defined?

- Will public companies become less nimble in updating their cyber policies and procedures because they would have to simultaneously change their regulatory filings?

Uyeda also criticized the final rule for elevating cybersecurity disclosures above other risks and issues that may be more material to investors. Uyeda worried that the final rule, by neglecting financial materiality standards, advances an overly prescriptive standard without a meaningful discussion as to why there should be an increased focus on cybersecurity risks, as compared to other risks that potentially could have a greater material impact on a public company. He also lamented that the final rule "breaks new ground" in mandating real-time, forward-looking disclosure by requiring companies to assess a cybersecurity incident's material impact while the incident is ongoing.

Five Things Companies Subject to the new SEC Cyber Requirements Have to Do Now (or at least before December 2023):

1. **Update Incident Response Plans** to Add New SEC Disclosure Process, including definitions and timing triggering notification that balance transparency, accuracy and maintaining level privilege.

2. **Develop Template Annual Reporting (Form 10-K and new Item 1C) and Periodic Reporting (8-K) Templates** just like companies develop template regulatory, HR, consumer and B2B breach notification notices.

3. **Have Legal/General Counsels and CISOs Collaborate**, including around identifying and conducting assessment around a cybersecurity framework for the organization and corresponding key controls (e.g., CIS-18, NIST Cybersecurity Framework and ISO 27001)

4. **Global Companies Identify Exceptions for Foreign Public Issues Covered under Local Country Laws**, including Canadian Foreign Public Issuers utilizing the Multi-Jurisdiction Disclosure System (MJDS) utilizing Form 20-F when filing annual reports on Form 40-F.

5. **Develop Data Classification Policies to Help Support Calculation of Materiality** including the Business Criticality and Regulatory Impact) of the Breach of Theft of Business Crown Jewels.

Contact your Troutman Pepper attorney or any of the authors of this article if you need more information or assistance in compliance with the final rule.

---

[1] A "cybersecurity incident" is defined as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardize the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein."

RELATED INDUSTRIES + PRACTICES

- Capital Markets
- Corporate
- Corporate Governance
- Data + Privacy
- Privacy + Cyber