Wolters Kluwer

Strategic Perspectives | Cybersecurity Policy Report

SEC Cybersecurity Disclosure Rules Take Effect: What Public Companies Need to Know

By Tony Foley, Senior Legal Analyst, Wolters Kluwer Legal and Regulatory U.S.

On September 5, 2023, new cybersecurity disclosure rules adopted by the Securities and Exchange Commission officially took effect, subjecting all public companies to new requirements around cybersecurity incident disclosure, risk management, and governance. Chief among them, the SEC will require material incidents to be disclosed on Form 8-K, the SEC's current event reporting form, within 4 days, with very narrow exceptions.

Although many companies have voluntarily provided cybersecurity incident information in their periodic reports, the new rules create a significant compliance burden for public companies regulated by the SEC. An important goal of the new rules is to provide consistency in reporting to make the information provided more useful for investors.

This Strategic Perspective provides an overview of the new rules and the obligations they impose, as well as key takeaways for public companies to consider as they prepare to comply.

What are the new reporting requirements?

The new requirements, which Exchange Act reporting companies must comply with beginning in December (with a six-month grace period for specified smaller reporting companies), relate to disclosures of cybersecurity incidents, as well as the disclosure of information on companies' processes for managing risks, as detailed below.

Cyberincident reporting: The rules provide for a new Item 1.05 in Form 8-K in which regulated companies must disclose any cybersecurity incident that they determine to be material "without unreasonable delay" but in all cases within four business days of making a materiality determination.

[For those of you, like the author, whose knowledge of securities extends to having them in my 401(k) portfolio and lying awake worrying about them, Form 8-K is the form that regulated companies must file with the SEC to announce major events that shareholders should know about.]

A highly limited exception to the requirement is provided where the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety. In addition, companies must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial filing. It's important to note, however, that the rules do not require companies to provide updated information regarding a previously reported incident in subsequent Form 10-K or 10-Q filings, as was contemplated in an earlier stage of the rulemaking process.

Cybersecurity risk management: Revised Regulation S-K Item 106(b) requires companies to describe their processes for the assessment, identification, and management of material risks from cybersecurity risks, and describe whether any such risks have materially affected or are reasonably likely to affect their business strategy, results of operations, or financial condition.

[Again, for the non-securities experts in the crowd, Regulation S-K is the SEC rule that specifies how reporting companies should disclose non-financial statement information in their filings, including periodic reports. The required cybersecurity risk management disclosures are made on Form 10-K, the annual report required to be filed by domestic companies.]

Cybersecurity governance: Revised Regulation S-K Item 106(c) requires a registrant to describe its Board's oversight of cybersecurity risks and management's role in assessing and managing such risks on its annual Form 10-K. However, a requirement in the proposed rule that would have required disclosures in annual reports regarding the level of cybersecurity expertise possessed by Board members did not make its way into the final rule.

Provisions applicable to FPIs: With respect to foreign private investors (FPIs), the new rules provide that they furnish information on Form 6-K (which such companies must file to provide information that must be made public in their country or origin) on material cybersecurity incidents that they disclose in a foreign jurisdiction, to any stock exchange or to security holders. In addition, FPIs must describe their boards' oversight of risks from cybersecurity threats and their managements' role in assessing

and managing material risks from cyber threats on Form 20-F, the annual report required to be filed by FPIs.

What key definitions apply to the new rules?

The reporting requirements outlined above apply to a "cybersecurity incident," which is expansively defined as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that compromises the confidentiality, integrity or availability of a registrant's information systems or any information residing therein." The SEC noted in the documentation for the final rule that, to broaden the construction of the term, it added "a series of related unauthorized occurrences" to the definition to clarify that cyberattacks may compound over time, rather than present as a discrete event. Accordingly, a series of events that individually may not present as material in nature may collectively trigger a reporting requirement on Item 1.05 of Form 8-K.

"Information systems" are defined as "electronic information resources, owned or used by the registrant, 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 registrant's information to maintain or support the registrant's operations."

What's a "material" cybersecurity incident?

The SEC's definition of "materiality" for purposes of its general registration requirements is contained in 17 CFR §230.405 (Rule 405) and the standard is further articulated in the accounting literature and, in the securities fraud context, in court cases and Supreme Court opinions. Rule 405 provides that;

> The term *material,* when used to qualify a requirement for the furnishing of information as to any subject, limits the information required to those matters to which there is a substantial likelihood that a reasonable investor would attach importance in determining whether to purchase the security registered.

Given the breadth of the reporting requirements, one may be inclined to assume that the rules would provide a granular definition of "materiality" as it relates to cybersecurity incidents. However, that is not the case; in fact, the final rule takes pains to explain the agency's decision NOT to do so, saying that the SEC expects that registrants will apply materiality considerations in a similar fashion as they would for any other risk or event. "Carving out a cybersecurity-specific materiality definition would mark a significant departure from current practice, and would not be consistent with the intent of the final rules," the SEC said on page 80 of the final rule. "Accordingly, we reiterate, consistent with the standard set out in the cases addressing materiality in the securities laws, that 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 also declined to define "cybersecurity," given the broad understanding of the term, the fact that the cybersecurity industry has not itself settled on an exact definition, and the rapidly evolving legal landscape.

So how do companies navigate this uncertainty? Danette Edwards, Partner and Co-Chair of the Securities Enforcement Defense practice at Katten Muchin Rosenman LLP, suggests that robust disclosure controls and procedures will help registrants with their assessment of materiality. "Some things a company might consider when making this determination include what and how much information was stolen, the expected consequences of the incident, whether the incident damaged the company's internal controls, and the range of legal consequences and reputational risks."

Ms. Edwards also cites the lack of a quantitative trigger in the new rules as something registrants should consider. "Companies can refer to the US Supreme Court cases *Basic Inc. v. Levinson* and *TSC Industries, Inc. v. Northway, Inc.* for the basic definition of materiality, including whether a reasonable investor would view a fact as having altered the total mix of available information," she said. "The impacts of a cyber incident can become clearer over time, and this may alter a company's original materiality evaluation, prompting new or corrective disclosures. We will likely see more corrective disclosures in the future."

What pitfalls should regulated entities look out for?

Prior planning prevents poor performance. The timing requirements under the reporting rules may prove to be particularly dicey for companies. It can be hard enough to make sure that periodic reports are accurate and complete under normal circumstances, and requiring a company to properly capture all required information regarding a cybersecurity incident, in four days, in a chaotic situation that may be having business impacts far beyond those posed by the new rule, will just increase the degree of difficulty. Companies that have made compliance preparations and have established response protocols prior to an incident stand a much better chance of fulfilling their reporting requirements successfully.

Don't panic. The four-day window is a challenging bar to clear, but a small but significant change in the rules from their proposed to final forms should assist companies who are grappling with defining materiality. In the proposed version, a company's materiality determination, which triggers the four-day deadline, was required to be made "as soon as reasonably practicable" after discovery of a cybersecurity incident. Based on concerns raised by commenters that this standard could pressure companies to draw conclusions about incidents with insufficient evidence, the SEC modified the language in the final rule to state that the materiality determination be made "without unreasonable delay." The change was designed to alleviate companies' concerns regarding undue pressure to make a determination, allowing them to be somewhat more deliberative in the process, while also providing them notice that, in the SEC's words, "though the determination need not be rushed prematurely, it also cannot be unreasonably delayed in an effort to avoid timely disclosure."

Periodic reporting will require policy review, training. Particularly for companies that have not already been including information on their cyber policies in their periodic reports, it is critical to begin to review their existing cybersecurity risk assessment and governance policies right away. Specific issues of concern include making sure that the Board, management and cyber personnel are briefed on the new requirements, as well as evaluating current risk management mechanisms to ensure that they are sufficient to support the additional reporting requirements in the final rule.

Ms. Edwards told WK that the SEC's prior statement and guidance on cyber reporting from 2018, which reinforced and expanded on guidance issued by the agency's Division of Corporation Finance issued in 2011, should be useful for companies as they prepare for their compliance obligations. "Hopefully, companies heeded the Commission's earlier messages, and will not be starting from scratch when seeking to comply with the new rules," she said.

Brace for additional enforcement activity. Companies can expect the SEC to carefully review filings under the new rules to assess whether they have properly reported a cybersecurity incident. Agency enforcement will likely help define the concept of materiality in this context, but companies need to be cognizant of the uncertainty of the materiality determination and be prepared to justify their determinations (or lack thereof). It's also likely that, with respect to the new risk management and governance rules, the SEC will ask companies how they have determined key indicators like the strategies employed by their Boards and management to manage these issues.

Ms. Edwards predicts that government enforcement actions and private litigation centered around alleged inadequate statements to investors, inadequate disclosure controls, and theft of personal information are unlikely to abate. "More incidents will lead to more disclosures for enforcers and private litigants to scrutinize," she said. "And of course, now that there are new SEC rules, it would be reasonable to expect additional SEC enforcement actions targeting instances of non-compliance with the new rules."

Other compliance strategies. One good way for businesses to streamline their reporting on risk management and governance is to begin to implement processes and policies in line with recognized industry standards like the Privacy and Cybersecurity Frameworks established by the National Institute of Standards and Technology (NIST), which will likely comport with the new reporting requirements. In addition, considering that many companies use third-party service providers to manage some or all of their cybersecurity protocols, they might want to consider developing mechanisms to document the activities of such providers so that this information can be properly captured in required periodic reports. Finally, companies should consider creating a checklist that outlines the new requirements, the information to be provided, the forms to be used, and any relevant deadlines.

Compliance dates. The compliance dates of the rules vary by the type of disclosure and size of registrant.

Type of Disclosure	Registrant Type	Compliance Date
Annual Form 10-K and Form 20-F cybersecurity disclosures	All registrants, including Smaller Reporting Companies (SRCs)	Fiscal years ending on or after December 15, 2023
Material cybersecurity incident disclosure on Form 8-K and Form 6-K	Registrants that are not SRCs	December 18, 2023
Material cybersecurity incident disclosure on Form 8-K and Form 6-K	SRCs	June 15, 2024
Structured data requirements (Inline XBRL tagging) for cybersecurity disclosures in Form 10-K and Form 20-F	All registrants (including SRCs)	Fiscal years ending on or after December 15, 2024
Structured data requirements (Inline XBRL tagging) for material cybersecurity incident disclosures in Form 8-K and Form 6-K	All registrants (including SRCs)	December 18, 2024