HUNTON
ANDREWS KURTH

Legal Updates

SEC Finalizes Cybersecurity Disclosure Requirements

August 3, 2023

On July 26, 2023, the U.S. Securities and Exchange Commission ("SEC") adopted long-anticipated cybersecurity disclosure rules for public companies by a 3-2 party-line vote. The final rules apply both to U.S. domestic public companies as well most foreign private issuers. The new rules are effective as soon as December 18, 2023, as detailed further below.

Highlights of New Cybersecurity Rules:

- ✓ **New Item 1.05 of Form 8-K (or Form 6-K for foreign private issuers) disclosure required regarding the occurrence of material cybersecurity incidents.**
- ✓ **New Form 10-K (or Form 20-F for foreign private issuers) disclosure about corporate risk management, strategy and governance of cybersecurity risks.**
- ✗ **No quarterly disclosure requirements on Form 10-Q (though periodic amendments of Form 8-K may be required).**
- ✗ **No requirement to identify a board cybersecurity expert.**

According to the SEC, the new rules are intended to help investors better understand public companies' cybersecurity risk environment. The SEC has expressed a concern that under the current reporting regime, the cause, scope, impact and materiality of cyber incidents is subject to uneven disclosure practices across the public company ecosystem. In its proposing release for the cybersecurity disclosure rules, the SEC identified three trends that it believes underpin investors' need for more information regarding cybersecurity: (i) the increasing share of economic activity dependent on electronic systems; (ii) the rise in the prevalence of cybersecurity incidents; and (iii) the increasing cost and negative consequences of cybersecurity incidents. In the adopting release for the final rules, the SEC reinforced the growing importance of these trends, and identified the rapid expansion of the use of artificial intelligence as a recent development and exacerbating factor.

Ultimately, the SEC drafted these new disclosure rules from the perspective that "evidence suggests companies may be underreporting cybersecurity incidents" despite its more than decade long record of guidance suggesting that issuers have an obligation to disclose

material cybersecurity incidents and threats in current and periodic reports.[1] Regardless of the intent, the new rules will require companies to adopt and maintain detailed policies that address how to handle SEC reporting obligations, particularly with respect to the Form 8-K requirements in the face of an ongoing and evolving cyberattack.

New Current Reporting Requirement: Item 1.05 of Form 8-K

The new rules add Item 1.05 to Form 8-K, which requires disclosure of material cybersecurity incidents within four business days from the determination of materiality.

> ***Item 1.05 Material Cybersecurity Incidents.***
>
> *(a) If the registrant experiences a cybersecurity incident that is determined by the registrant to be material, describe the material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the registrant, including its financial condition and results of operations.*

Despite its brevity, this new language under Item 1.05(a) of Form 8-K leaves a variety of open questions and the potential for confusion and inconsistent disclosure as companies wrestle with these novel disclosure requirements.

What triggers the four-day disclosure clock?

The new disclosure is required within four business days after a company makes a determination that a cybersecurity incident is material. Instruction 1 to new Item 1.05 clarifies that "[a] registrant's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident." In its adopting release, the SEC highlighted its elimination of the "as soon as practicable" requirement in its proposed rule with the more favorable "without unreasonable delay" requirement in the final version, which it did to avoid registrant's rushing to make disclosure without sufficient information.

> "We believe the revised language should alleviate this unintended consequence, while providing registrants notice that, ***though the determination need not be rushed prematurely, it also cannot be unreasonably delayed to avoid timely disclosure.***"

However, the SEC is clear that determining the full extent of an incident is not a reasonable delay if the facts known at the time are sufficient to determine its overall materiality. Other examples of unreasonable delays include (i) delays in scheduling board meetings required to make a materiality determination or (ii) changing internal policies to delay incident severity assessments or other reporting mechanisms to management. Drawing an important distinction, the SEC explicitly states that a registrant's "decision to share information with other companies or government does not in itself necessarily constitute a determination or materiality." The SEC encourages companies to share information with stakeholders about emerging threats without that act of information sharing being a trigger for Item 1.05 disclosure in the absence of a comprehensive determination of materiality.

Ultimately, adhering to normal internal policies and disclosure controls and procedures will suffice to demonstrate good faith compliance, which underscores the fundamental importance for having such policies and procedures in place that specifically address cybersecurity incidents.

Given the complexity for determining the exact trigger for this new requirement, the SEC determined that the untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility for issuers conducting short-form securities offerings.

What is the materiality threshold?

In its adopting release, the SEC makes clear that the traditional concepts of materiality apply in the context of a cybersecurity incident just like any other. Quoting well-trodden caselaw, the SEC emphasizes that the analysis as to materiality of a cybersecurity incident depends on whether "there is a substantial likelihood that a reasonable investor would consider it important" in making an investment decision, or if it would significantly alter the "total mix of information made available." Referring back to its proposing release, the SEC instructs that "'[a] materiality analysis is not a mechanical exercise'" and not solely quantitative, but rather should take into consideration "'all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors.'"

> "Importantly, we remind registrants, ... that '[d]oubts as to the critical nature' of the relevant information 'will be commonplace' and should 'be resolved in favor of those the statute is designed to protect,' namely investors."

This analysis applies to both the identification of the event as a trigger, and also the scope of the disclosure provided under Item 1.05 once a company determines a material cybersecurity incident has occurred. The SEC's intent is that this disclosure focus on the facts a company determines are the material impact of an incident, and should not be excluded to impacts on the financial condition or results of operation. Providing a non-exhaustive list, the release flags the following as potential material impacts to a company: harm to a company's reputation; harm to customer or vendor relationships; negative impact on competitiveness; the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal governmental authorities and non-U.S. authorities.

What is a "Cybersecurity Incident"?

Pursuant to new Item 106(a) of Regulation S-K (discussed in greater detail below), "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 therein."

This new defined term hinges on the identification of an event that "jeopardizes" a registrant's IT systems. While the word "jeopardize" is used in other cybersecurity regimes and is incorporated into the definition of cyber incident in the Cyber Incident Reporting for Critical Infrastructure Act, it does not appear regularly in the SEC's existing regulations or disclosure forms. By its simple

dictionary definition, an event that jeopardizes a registrant's IT systems is one that exposes that system to danger or risk. Based on the virtually nonexistent use of the word "jeopardize" elsewhere in Regulation S-K, the SEC would likely expect issuers to adopt a similarly broad understanding that does not require damage, merely the threat of damage.[2] Coupled with the fact that the adopting release for the new rules emphasizes that the term "cybersecurity incident" in the final rules is to be "construed broadly," we think the SEC will take the broadest view of the term "jeopardize."[3]

Notably, an element of the proposed rules that would have required companies to aggregate individually immaterial events for purposes of determining whether a cybersecurity incident has occurred has been eliminated in the final rules in favor of the final definition's use of the term "series of related unauthorized occurrences." This new language, however, introduces another potential unintended consequence – do companies need to implement disclosure controls processes designed to identify a "series of related unauthorized occurrences" that rise to the level of materiality in the aggregate? And if so, how "related" must the immaterial occurrences be and over what time period must they occur to be considered material in the aggregate?

What information is required in the Form 8-K?

Companies should include material information about material cybersecurity incidents under Item 1.05, including material aspects of the nature, scope, and timing of the incident, and the material impact or reasonably likely material impact on the company. In response to comments, the SEC determined that a company 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 its response or remediation of the incident. Additionally, the SEC did not adopt the proposed requirement for disclosure regarding the incident's remediation status, whether it is ongoing, and whether data were compromised. Still, such information may be material depending on the specific facts and circumstances. Moreover, the final rules do not include any exemption for providing disclosures regarding cybersecurity incidents on third-party systems, nor do the final rules include any safe harbor for information disclosed about third-party systems.

"The 8-K disclosures, which are unprecedented in nature, could then tell successful attackers when the company finds out about the attack, what the company knows about it, and what the financial fallout is likely to be (i.e., how much ransom the attacker can get). The requirement to file an amended 8-K when new information comes in will provide the attacker regular updates on the company's progress. The 8-K disclosures also will signal to other would-be attackers an opportune time to attack." – Commissioner Hester Peirce

Critics of these rules point out that even without disclosing highly technical information regarding remediation and the compromised information, the disclosure nonetheless serves to provide a major advantage to bad actors in the middle of an ongoing cyberattack. Commissioner Hester Peirce, in her statement in opposition, describes the dangers of this disclosure, which require careful and thoughtful drafting to avoid unintentionally assisting the efforts of an ongoing threat. Companies will need to designate time and resources to thinking strategically about how to comply with these new SEC rules while also maintaining the integrity of their remediation efforts during an ongoing cybersecurity crisis.

What happens if the known facts change after the first Form 8-K?

Instruction 2 to Item 1.05 advises 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, a company must include a statement to this effect in the initial Form 8-K. Then, a company must file an amendment to its Form 8-K filing under Item 1.05 containing such missing information within four business days after the company, without unreasonable delay, determines such information or within four business days after such information becomes available. This new requirement is intended to take the place of the quarterly Form 10-Q reporting requirement featured in the proposed version of the rules, and may necessitate multiple amendments over time to the original Form 8-K filing.

Given the incredible speed with which facts and circumstances develop in the midst of a material cybersecurity breach, the practical reality of this requirement to update in real-time seems like an unwanted challenge during an already difficult situation. Companies should consider the four-day clock as a tool to aggregate as much new information as possible that may be reportable before filing an amendment to the initial Form 8-K disclosure. Companies also have an obligation to avoid misleading disclosure, which could prove a daunting task against the competing requirement to comply with these new rules. Subsequent disclosures will also need to be thoughtfully crafted to avoid providing any timely updates to the bad actors responsible for an ongoing or future attack.

Can companies postpone disclosure for confidentiality, security or other important reasons?

In response to concerns from commenters, the final rules include a narrow law enforcement exemption for disclosures that would pose a substantial risk to national security or public safety. Specifically, disclosure on Form 8-K may be delayed for 30 days if the U.S. Attorney General provides written notification to the SEC that national security or public safety would be impaired substantially by immediate disclosure. The rules also lay out procedures by which the Attorney General may extend the delay for additional periods of time. Under questioning from SEC Commissioner Peirce at the open meeting, the SEC staff revealed that the SEC and Department of Justice ("DOJ") have developed an interagency communication process to facilitate this exemption, and DOJ will notify affected public companies directly if they are subject to the delay. The SEC's adopting release also discusses this protocol, but there are not many practical details provided regarding how exactly companies should engage DOJ for an exemption, if at all. It remains to be seen how this exemption will work in practice, and whether affected companies will have sufficient time during the four-business day window to avail themselves of the delay.[4] We are not optimistic that the DOJ will frequently invoke this exemption.

Delaying disclosure requires written confirmation from DOJ that that ***national security or public safety would be impaired substantially by immediate disclosure.***

Given these uncertainties, companies would be well-advised to make progress on both requesting an exemption from DOJ and preparing the required disclosures in order to comply with the new rules within four business days. This added burden further emphasizes the additional time and resources companies must be prepared to spend complying with the new SEC rules while managing a cybersecurity incident.

Additionally, the final rules further provide a limited reporting delay for telecommunications carriers subject to the cybersecurity reporting requirements of 47 CFR 64.2011.[5] The SEC also clarified in its adopting release that the delay to protect national security or public safety is separate from Exchange Act Rule 0-6, which exists separately from the new rules and permits the omission of information that has been classified by an appropriate department or agency of the Federal government for the protection of the interest of national defense or foreign policy. Rule 0-6 is not frequently invoked in practice, but it is possible that it may gain new life in light of the Form 8-K reporting requirement.

What is the corresponding impact on Form 6-K?

Foreign private issuers have an existing obligation to disclose material information on Form 6-K that they disclose offshore, on a stock exchange or to their securityholders. For foreign private issuers, the new rules amend Form 6-K to add material "cybersecurity incident" to the list in General Instruction B of information required to be furnished on Form 6-K. Arguably, the new rules do not change the existing requirement to report on material home country events, which could already include cybersecurity matters. In practice, this requirement removes any doubt and will obligate foreign private issuers to report on material cybersecurity incidents they make or are required to disclose in a foreign jurisdiction to any stock exchange or to securityholders.

New Periodic Reporting Requirement: Item 106 of Regulation S-K

The final rules create a new Item 106 to Regulation S-K concerning cybersecurity risk management, strategy and governance. Each of the components in Item 106 must be disclosed annually in a domestic public company's Form 10-K, even if otherwise disclosed in the proxy statement. The final rules also create an analogous annual reporting requirement for foreign private issuers filing Form 20-F. To avoid repetition, we summarize the Form 10-K requirements below, which apply mutatis mutandis to Form 20-F. We note that the SEC did not amend Form 40-F for Canadian foreign private issuers reporting under the multi-jurisdictional disclosure system; affected Canadian issuers would still be required to make disclosure to the extent required under Canadian provincial requirements.

How detailed are the required disclosures regarding cybersecurity risk management and strategy?

The SEC's intent in adopting Item 106(b) is to require registrants to provide more consistent and informative disclosure regarding cybersecurity risk management and strategy in their annual reports, not to require disclosure of information that could jeopardize a company's security.

> *Item 106. Cybersecurity.*
> ...
> *(b) Risk Management and Strategy.*
> *(1) Describe the registrant'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. ...*

The SEC limited the scope of the final language adopted in Item 106(b) in response to concerns that detailed public disclosure of the methods and capabilities a company uses to defend against cyberattacks "has the potential to advantage threat actors." For example, the SEC substituted the term "processes" for "policies and procedures" to avoid mandatory disclosure of operational details that could aid bad actors.

Item 106 provides a nonexclusive list of topics companies should address in describing their risk management processes, including: (i) whether and how any such processes have been integrated into the company's overall risk management system or processes; (ii) whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and (iii) whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

The SEC emphasized that although the required disclosure asks companies to disclose whether they rely on third-parties for any part of their cybersecurity, companies need not name the service providers or describe the scope of services being provided. Additionally, the SEC is not requiring disclosure of any quantifiable metrics used by companies to assess risks.

> "We still expect the disclosure to allow investors to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place, with sufficient detail for investors to understand the registrant's cybersecurity risk profile."

Under Item 106(b)(2), companies must also disclose whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how.

How is the disclosure regarding the board's role in cybersecurity risk oversight different from existing disclosure requirements?

New Item 106(c)(1) requires companies to "[d]escribe the board of directors' oversight of risks from cybersecurity threats," and, if applicable, "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks." Arguably, this is an existing SEC disclosure requirement under Item 407(h) of Regulation S-K, as highlighted in the SEC's 2018 guidance regarding cybersecurity disclosures.[6] The SEC, however, is taking the position that its new requirement under Item 106(c)(1) is distinct in scope compared with Item 407(h)'s requirements,

which it views as more general. In responding to comments, the SEC eliminated much of the granular disclosure initial found in its proposed rules, which if maintained, would have more clearly identified the new Item 106(c)(1) disclosure as distinct from existing disclosure requirements. Regardless, the streamlined disclosure required by the final rule is somewhat more company-friendly than the proposed rules. Companies are not required to disclose any particular board expertise in relation to cybersecurity, a change from the rule proposal, or whether the board considers cybersecurity as part of its business strategy, risk management and financial oversight. There is no obligation in the final rules to identify a board cybersecurity expert.

> Existing Item 407(h) "requires description of the board's leadership structure and administration of risk oversight generally," while new Item 106(c)(1) "requires detail of the board's oversight of specific cybersecurity risk."

What new information must companies disclose regarding management's role managing and assessing cybersecurity risk?

Item 106(c)(2) requires companies to describe "management's role in assessing and managing the registrant's material risks from cybersecurity threats." The SEC continued its trend of streamlining the final required disclosure in response to criticism in public comments on the proposed rules. In providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items: (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 necessary to fully describe the nature of the expertise; (ii) the 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.

The SEC commented that these elements "are limited to disclosure that we believe balances investors' needs to understand a registrant's governance of risks from cybersecurity threats in sufficient detail to inform an investment or voting decision with concerns that the proposal could inadvertently pressure registrants to adopt specific or inflexible cybersecurity-risk governance practices or organizational structures."

Compliance Dates and Practical Advice

Compliance Dates. The Form 8-K and 6-K reporting requirement will take effect for cyber incidents occurring on or after December 18, 2023, though smaller reporting companies will have a delay until June 15, 2024. These dates may slip further if there is any undue delay in publishing the final rules in the Federal Register. The annual reporting requirement on Form 10-K or 20-F will take effect for fiscal years ending on or after December 15, 2023. Thus, annual reports published in 2024 will generally require the inclusion of the new Item 106 disclosure.

Review Governance Documents. Given the increased disclosure regarding the board's and management's roles in cybersecurity oversight, companies should review their governance documents to confirm they accurately reflect the allocation of responsibility in practice. Policies and guidelines should align with practice, which should all align with disclosure.

Update Incident Response Plans. As discussed, incident response will potentially become more complicated as the additional burdens of timely complying with the new Form 8-K requirements add additional complexity to delicate fact patterns. The speed with which a company determines the materiality of a cybersecurity incident and files the required disclosure should be carefully managed to avoid mistakes. The new rules serve as a new enforcement playground for the SEC to use the benefit of hindsight to scrutinize a company's decisions in the very early stages of managing a cybersecurity incident. Well documented disclosure controls policies and intentional documentation of the record as events unfold will demonstrate good faith on a company's behalf.

Adapt to Evolving Disclosure. As with any new reporting requirements, the first year will consist of companies wrestling with the new disclosure with variety in terms of detail and scope. As practice progresses, the market practice will conform and eventually this disclosure will become more consistent among similarly situated companies. As issuers work through those growing pains, however, they may need to update disclosure controls and procedures to capture and refresh all of the new required disclosures and ensure their periodic disclosures under Item 106 accurately reflect their practices.

[1] It is worth noting that in its 2018 "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," the SEC encouraged issuers to disclose material cybersecurity incidents on Form 8-K and throughout periodic reports. While these rules codify that encouragement and guidance, the SEC has long held and expectation that material cyber security incidents should be reported as responsive disclosures to a variety of existing requirements.

[2] The only other use of the word "jeopardize" (and its variations) in Regulation S-K is in Instruction 6 to Item 504 regarding the disclosure of the use of proceeds, in which the SEC exempts certain disclosures regarding acquisitions when such disclosure would "jeopardize" the transaction. In reviewing comments letters addressing this Instruction 6 to Item 504, the SEC appears to take at face value a registrant's withholding of information regarding the use of proceeds simply by stating that such disclosure would "jeopardize" the potential acquisition and therefore do not appear to be any notable examples of the SEC rejecting this response by a registrant, indicating that it takes a fairly broad approach to its understanding of the term "jeopardize."

[3] In her statement in opposition, Commissioner Hester Peirce posed a number of critical questions, including, "'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?"

[4] In response to comments asking for delays in the reporting requirements during ongoing investigations by federal agencies and non-Federal law enforcement agencies, the SEC responded by acknowledging that "the rule does not preclude any such agency from requesting that the Attorney General determine that the disclosure poses a substantial risk to national security or public safety and communicate that determination to the Commission. However, we believe that designating a single law enforcement agency as the Commission's point of contact on such delays is critical to ensuring that the rule is administrable."

[5] The FCC's rule for notification in the event of breaches of CPNI requires covered entities to notify the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI") 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 USSS and FBI. To accommodate registrants who are subject to this rule and may as a result face conflicting disclosure timelines, the SEC added paragraph (d) to Item 1.05 providing that such registrants may delay making a Form 8-K disclosure up to the seven business day period following notification to the USSS and FBI specified in the FCC rule, with written notification to the SEC.

[6] In its 2018 "Commission Statement and Guidance on Public Company Cybersecurity Disclosures," the SEC said, "Item 407(h) of Regulation S-K and Item 7 of Schedule 14A require a company to disclose the extent of its board of directors' role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board's leadership structure. The Commission has previously said that 'disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company.' A company must include a description of how the board administers its risk oversight function. To the extent cybersecurity risks are material to a company's business, we believe this discussion should include the nature of the board's role in overseeing the management of that risk."

HUNTON
ANDREWS KURTH

Related People

Mayme Donohue
Partner
+1 804 787 8021
mdonohue@HuntonAK.com

Scott H. Kimpel
Partner
+1 202 955 1524
skimpel@HuntonAK.com

Susan S. Failla
Partner
+1 212 309 1238
sfailla@HuntonAK.com

Lisa J. Sotto
Partner
+1 212 309 1223
lsotto@HuntonAK.com

Aaron P. Simpson
Partner
+1 212 309 1126
asimpson@HuntonAK.com

HUNTON
ANDREWS KURTH

Brittany M. Bacon
Partner
+1 212 309 1361
bbacon@HuntonAK.com

Michael La Marca
Partner
+1 212 309 1116
mlamarca@HuntonAK.com

Adam H. Solomon
Partner
+1 212 309 1327
asolomon@HuntonAK.com

Related Services

Capital Markets and Securities

Sustainability

Privacy and Cybersecurity

‘34 Act Reporting and Related Matters

Real Estate Sustainability

Media Contact

Lisa Franz
Director of Public Relations

Jeremy Heallen
Public Relations Senior Manager
mediarelations@HuntonAK.com