March 16, 2022

# SEC Issues Proposed Rules on Public Company Cybersecurity Disclosures

**Attorneys**
Kevin J. Angle
Paul M. Kinsella
Edward R. McNicholas
Marc Rotter
Marko S. Zatylny

On March 9, 2022, the Securities and Exchange Commission ("SEC") proposed updates to its disclosure rules intended to "enhance and standardize" public company disclosure regarding cybersecurity risk management, strategy, governance, and incident reporting (the "Proposed Rules").[1] The Proposed Rules may require issuers to update their disclosure controls and procedures, in particular with respect to determining the materiality of cybersecurity events and providing prompt disclosure.

The Proposed Rules build on a body of pre-existing SEC guidance regarding cybersecurity disclosures. In 2011, the Division of Corporation Finance issued interpretive guidance regarding disclosure obligations relating to cybersecurity risks and cyber incidents. The SEC followed up that guidance with a 2018 statement on cybersecurity disclosure addressing, among other things, the materiality of incidents, updates to risk factors, and board risk oversight. If adopted, the proposed rules make many of these recommendations express requirements, while adding additional clarity and detail regarding cybersecurity risks and practices that must be reported. While the proposed rules are focused on disclosure, if adopted, they may lead issuers to enhance cybersecurity risk management and oversight, as well as to add directors with expertise in cybersecurity.

The Proposed Rules would require the following:

*Public Reporting of Cybersecurity Incidents*

The SEC would amend Form 8-K to add a new 8-K trigger (proposed Item 1.05) for cybersecurity incidents[2] that are material to the issuer.[3] Like other disclosure required by Form 8-K, an issuer would be required to file the Form 8-K within four business days after a triggering event. This is substantially shorter than notification periods under most state data breach notification laws (typically, "without unreasonable delay" or within periods ranging from 30 to 60 days). SEC guidance already indicates that public companies should disclose material cybersecurity incidents in both voluntary disclosures and periodic reports. The Proposed Rules codify that guidance and generally accelerate the timing of required disclosure. The SEC makes clear (as it has before) that the same standard of materiality applies for cybersecurity incidents as generally applies under the Securities and Exchange Act (i.e., 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" to the investor).[4] Both quantitative and qualitative factors should be considered.

Notably, the trigger for disclosure is when the registrant determines the incident is *material*, not when the registrant discovered the unauthorized access or other security event. In practice, the two may prove difficult to distinguish. Proposed Instruction 1 to Item 1.05 would provide that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." The SEC states that requests from law enforcement to delay public disclosure of material cybersecurity incidents would not justify delayed reporting. Similarly, provisions that allow for delay in reporting under other regulatory regimes, such as state law, would not

[1] See Release No. 33-11038 (Mar. 9, 2022) (the "Proposing Release").
[2] Defined as "an unauthorized occurrence 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."
[3] As proposed, failure to timely file an Item 1.05 Form 8-K would not make an issuer ineligible to use Form S-3.
[4] Proposing Release at 23 (quoting *TSC Industries v. Northway*, 426 U.S. 438, 449 (1976)).

provide a basis for delayed reporting on Form 8-K. Early involvement of counsel, therefore, would be key to ensuring prompt disclosure.

Determining materiality in the midst of an incident can prove challenging. New and sometimes different information may become available rapidly, and company IT specialists and others involved in the response typically are stretched thin with the demands of the response. Advance preparation and established procedures may prove critical to ensuring company counsel receives the information necessary to assess disclosure obligations. Issuers also may need to consider updating disclosure controls to ensure that a robust process exists for the timely reporting of cybersecurity incidents to the disclosure committee or other relevant body, with sufficient resources to facilitate that reporting.

As to the details of the disclosure, Item 1.05 would require disclosure of the following facts, to the extent known at the time of the filing: (1) when the incident was discovered and whether it is ongoing; (2) the nature and scope of the incident; (3) whether data was stolen or otherwise altered, accessed or used for an unauthorized purpose; (4) the effect of the incident on the registrant's operations; and (5) whether the registrant has remediated or is currently remediating the incident. Many of these facts may be difficult to ascertain for some time following discovery of an incident, as facts may take time to develop. Often, assessments of breaches and their implications evolve rapidly in a non-linear manner. Companies, consequently, must carefully consider and hedge disclosure in the early stages of an incident to avoid subsequent allegations that the early disclosure was misleading.

*Cybersecurity Incidents in Periodic Reports*

The SEC proposes amendments to Form 10-Q and Form 10-K that would require updates to disclosure of cybersecurity incidents. Proposed Item 106(d)(1) of Regulation S-K would require that annual and quarterly reports include "material changes, additions, or updates" with respect to cybersecurity incidents previously reported under Item 1.05 of Form 8-K. Proposed Item 106(d)(1) includes a non-exclusive list of items that should be addressed if applicable, including material impacts and potential impacts on the issuer, remediation efforts and any changes in policies resulting from the incident. Additionally, proposed Item 106(d)(2) of Regulation S-K would require issuers to disclose cybersecurity incidents that are individually immaterial but in the aggregate, material.

*Risk Management, Strategy and Governance*

The SEC proposes adding Item 106(b) and (c) to Regulation S-K to require registrants to disclose risk management programs and strategies for addressing cybersecurity risks, along with information regarding the registrant's related governance structure. Specifically, Item 106(b) of Regulation S-K would require disclosure of whether:

- the registrant has a cybersecurity risk assessment program, and, if so, the registrant should provide a description of the program;
- the registrant engages assessors, consultants, auditors or other third parties in connection with the program;
- the registrant has policies and procedures to oversee and identify the cybersecurity risks associated with the use of third-party service providers;
- the registrant undertakes activities to prevent, detect, and minimize the effects of cybersecurity incidents;
- the registrant has business continuity and recovery plans;
- previous cybersecurity incidents have informed changes in the registrant's cybersecurity program;
- cybersecurity risks or incidents have affected or are likely to affect the registrant's results of operations or financial condition; and
- cybersecurity risks are considered as part of the registrant's overall business strategy, and if so, how.

Each of these disclosures would require a registrant to provide details about its existing cybersecurity program, well beyond current, typical risk factor disclosures. Companies that do not have such policies and procedures in place should consider implementing them, whether or not these proposals are adopted. Such measures are generally part of a robust cybersecurity program. Disclosures regarding the involvement of third parties like assessors and auditors in the risk management program may also increase the benefit of involving third parties in risk assessments, penetration tests, or certifying to controls such as in a SOC 2 Type II report.

Proposed Item 106(c) would require disclosure regarding the role of management and the board in overseeing cybersecurity. Such disclosure would include information about who within the board and management is responsible for oversight of cybersecurity risks and how the board and management are informed of cybersecurity risks. Similar to other recent cybersecurity regulations, such as the FTC's recent updates to its Safeguards Rule and the New York Department of Financial Services' Cybersecurity Regulation (23 NYCRR 500), the Proposed Rules highlight the potential value of a single chief information security officer (CISO) with relevant experience and clear reporting lines to senior management and the board.

*Board Cybersecurity Expertise*

Finally, the SEC proposes amending Item 407 of Regulation S-K to require that issuers identify any director who has expertise in cybersecurity and identify the nature of that expertise. The proposed amendments to Item 407 include several safe harbors to make clear that identifying a director as having expertise in cybersecurity does not impose additional federal securities law duties or liabilities on that director or relieve other directors of any of their federal securities law obligations.

The proposed amendments would not require an issuer that does not have a director with cybersecurity expertise to make an affirmative statement that it does not have such a director or explain why it does not have such a director. That contrasts with the disclosure requirements for audit committee financial experts, which require such statements.

*Looking Ahead*

The Proposed Rules are not final, and companies and others will have an opportunity to comment. The SEC requests comments on, among other things:

- Whether the proposed disclosures could have the unintentional effect of putting registrants at additional risk of future incidents;
- Whether the four-day filing deadline provides sufficient time for registrants to prepare disclosures;
- Whether the proposed disclosure obligations create conflicts with other federal and state notification regimes;
- Whether notification about the use of third parties in assessing risk constitutes useful disclosure;
- Whether reporting requirements should not apply to certain categories of registrants, such as smaller reporting companies; and
- Whether registrants that do not have a person with cybersecurity expertise on its board of directors should be required to affirmatively state that fact.

The comment period for the Proposed Rules is open until the later of May 9, 2022 or 30 days after publication in the Federal Register, and significant public comments are likely.

* * *

If you would like to learn more about the issues in this Alert, please contact your usual Ropes & Gray attorney contacts.