King & Spalding
Client Alert

MARCH 16, 2022

SEC Proposes Rules Enhancing Cybersecurity Disclosures

For more information, contact:

Zachary L. Cochran
+1 404 572 3518
zcochran@kslaw.com

Zachary J. Davis
+1 404 572 2770
zdavis@kslaw.com

Elizabeth Morgan
+1 212 556 2351
emorgan@kslaw.com

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309
Tel: +1 404 572 4600

New York
1185 Avenue of the Americas
New York, New York 10036
Tel: +1 212 556 2100

On March 9, 2022, the Securities and Exchange Commission (SEC) proposed rules intended to enhance and standardize public company disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting.[1] The proposed rules accomplish these objectives through specific, mandated disclosure requirements applicable to all companies in a manner designed to enhance comparability across issuers and industries. If adopted, the proposed rules would supplement existing SEC guidance on cybersecurity disclosure requirements for public companies.[2] Comments on the proposed rules are due by the later of May 9, 2022 and the date 30 days after publication of the proposed rules in the Federal Register.

Disclosure Concerning Cybersecurity Incidents

Form 8-K Disclosure of Material Cybersecurity Incidents

In its proposing release, the SEC stated that cybersecurity incident disclosure was inconsistent notwithstanding the SEC's existing guidance. In particular, the SEC noted that some incidents were reported in the media but were not disclosed by the affected companies in their periodic filings and that the nature of disclosures, when made, varied widely.[3]

To create a uniform expectation regarding the timing and substance of required disclosures, the proposed rules would create a new Item 1.05 to Form 8-K requiring disclosure within four business days after a company experiences a "cybersecurity incident" that the company determines is material.[4] As proposed, Item 1.05 requires disclosure of the following:

- When the incident was discovered and if it remains ongoing;
- A brief description of the nature and scope of the incident;
- Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose;
- The effect of the incident on the company's operations; and
- Whether the company has remediated or is remediating the incident.

The disclosure obligation in Item 1.05 is triggered by the company's determination that a material cybersecurity incident has occurred, not simply the occurrence of any cybersecurity incident. To address any concern that companies may delay making a materiality determination to avoid disclosure, Item 1.05 instructs companies to "make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident." Due to the need to make this materiality determination during a rapidly developing situation, the proposed rules also (1) specify that failure to timely file an Item 1.05 Form 8-K would not adversely impact Form S-3 eligibility and (2) extend the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Securities Exchange Act of 1934 to cover Item 1.05 Form 8-K filings.

While tying the disclosure trigger to materiality provides flexibility for companies to properly assess the magnitude of an incident before the four-day disclosure clock begins to run, assessing materiality amid an ongoing cybersecurity incident and related investigation will undoubtedly be challenging. Companies will need robust procedures in place to ensure that information security officials with knowledge of the details and significance of an incident promptly communicate with officers responsible for disclosure decisions, so that information and context can be escalated quickly to facilitate an accurate materiality determination. Companies will want to avoid prematurely disclosing an incident that is ultimately not significant once fulsome facts and circumstances are known following investigation. However, Item 1.05 does not permit disclosure to be delayed while an investigation is completed.

The proposing release also makes clear that, even though some state laws permit companies to delay notifying regulatory bodies of a cybersecurity incident to allow law enforcement to covertly pursue the attackers, Item 1.05 does not authorize a delay in disclosing material incidents based on that same rationale. So, once a company has made an assessment that an incident or series of incidents is material, it must make disclosure on Form 8-K within four business days, regardless of whether there is an ongoing law enforcement investigation and whether law enforcement authorities would prefer that the company not publicly announce the incident.

The proposing release provides guidance on how to determine materiality when assessing whether a Form 8-K is triggered by looking to existing case law standards. Specifically, the release cites, among other things, the standard from *TSC Industries, Inc. v. Northway* that information would be considered material if there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision, or if it would significantly alter the "total mix" of available information. The proposing release goes on to note that materiality should be based on an analysis of all quantitative and qualitative factors relevant to a particular cybersecurity incident, not just a quantitative analysis of the incident's impact or a risk assessment of adverse consequences from failing to disclose. The proposing release also provides the following non-exhaustive examples of what the SEC considers material:

- An unauthorized incident that compromised confidentiality, integrity, or availability of an information asset, or violated the company's security policies or procedures (can be accidental or deliberate attack);
- An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology system;
- An unauthorized party accessed or exceeded authorized access and altered or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted in a loss or liability for the company;
- An incident where a malicious actor has offered to sell or threatened to disclose sensitive company data; and
- An incident where a malicious actor has demanded payment to restore data that was stolen or altered.

We expect the timing of materiality and disclosure assessments will continue to be closely scrutinized by the SEC's Enforcement Division in any investigation resulting from a cybersecurity incident.

Notwithstanding this framework, some may believe that a materiality standard provides too much flexibility. To that end, the proposing release requests comments on whether the appropriate disclosure standard should be any cybersecurity incident.

Periodic Reporting of Updates Concerning Material Cybersecurity Incidents

The proposed rules would amend Forms 10-K and 10-Q to require disclosure of any material updates regarding any previously disclosed cybersecurity incidents, including information regarding (1) any material effect (or potential material future impacts) on the company's operations and financial condition, (2) whether the company has remediated or is remediating the incident, and (3) any changes in the company's policies and procedures as a result of the cybersecurity incident, and how the incident informed those changes. Notwithstanding this updated disclosure, the proposing release highlights situations where a company is also required to update its original Item 1.05 disclosure by amending the original Form 8-K filing, such as "where [the] disclosure becomes inaccurate or materially misleading as a result of subsequent developments . . . For example, if the impact of the incident is determined after the initial Item 1.05 Form 8-K filing to be significantly more severe than previously disclosed. . . ."[5]

In addition, the proposed rules require disclosure in Form 10-K and Form 10-Q filings if a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. It will be challenging for companies to assess whether a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate. The proposing release gives only one example of this type of scenario—where a malicious actor engages in a number of smaller but continuous cyber-attacks related in time and form against the same company. This lone example does not provide much guidance on *how* companies would determine that the individually immaterial incidents had become material in the aggregate or what other scenarios could result in a similar determination.

Disclosure Concerning Cybersecurity Risk Management, Strategy and Governance

Similar to the approach taken with cybersecurity incidents, the proposed rules seek to create a uniform expectation regarding the substance of cybersecurity disclosures as they relate to risk management, strategy and governance. As noted above, these new disclosure requirements would supplement, not replace, the SEC's existing guidance with respect to cybersecurity disclosure requirements under existing SEC rules, such as disclosures as part of company risk factors and MD&A, and the SEC's existing rules around the establishment of disclosure controls sufficient to ensure the timely reporting of material information and decision-making related to cybersecurity matters.

Disclosure of Cybersecurity Risk Management and Strategy

The proposed rules would create a new Item 106 of Regulation S-K, which requires each company to disclose information about its cybersecurity risk management and strategy as part of its Form 10-K. In particular, the new Item 106 requires each company to describe its policies and procedures to identify and manage cybersecurity threats, including whether:

- The company has a cybersecurity risk assessment program, and if so, to describe the program;
- The company engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- The company has policies and procedures to oversee and identify cybersecurity risks associated with its use of any third-party service provider, and if so, to describe these policies and procedures, including whether

and how cybersecurity considerations affect the selection and oversight of these service providers and contractual and other mechanisms used to mitigate cybersecurity risks;

- The company undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents, and if so, to describe the types of activities undertaken;
- The company has business continuity, contingency and recovery plans addressing a cybersecurity incident;
- Previous cybersecurity incidents have informed changes in the company's governance, policies and procedures, or technologies;
- Cybersecurity-related risks and previous cybersecurity-related incidents have affected or are reasonably likely to affect the company's strategy, business model, results of operations or financial condition, and if so, how; and
- Cybersecurity risks are considered as part of the company's strategy, financial planning, and capital allocation, and if so, how.

Disclosure of Cybersecurity Governance

Proposed Item 106 also requires companies to describe management's role in assessing and managing cybersecurity risks and in implementing cybersecurity policies, procedures, and strategies. In particular, Item 106 would require disclosure of the following, among other matters:

- Whether certain management positions or committees are responsible for measuring and managing cybersecurity risk, specifically the prevention, mitigation, detection, and remediation of cybersecurity incidents, and the relevant expertise of such persons;
- Whether the company has a designated chief information security officer, or a comparable position, and if so, to whom that individual reports within the company's organizational structure, and the relevant expertise of any such person;
- The processes by which such persons or committees are informed about and monitor the prevention, mitigation, detection, and remediation of cybersecurity incidents; and
- Whether and how frequently such persons or committees report to the board on cybersecurity risks.

At the board level, proposed Item 106 requires disclosure regarding the board's oversight of cybersecurity risk, including:

- Which board members or committees are responsible for oversight of cybersecurity risks;
- The processes by which the board is informed about cybersecurity risks, and the frequency of its discussions on this topic; and
- Whether and how the board considers cybersecurity risks as part of its business strategy, risk management, and financial oversight.

In a requirement analogous to that for audit committee financial experts, the proposed rules would amend Item 407 of Regulation S-K to require registrants to disclose which, if any, directors have cybersecurity expertise, as well as information on the nature of this expertise and how it was obtained (*e.g.*, prior work experience as an information security officer, or a certification or degree in cybersecurity).

Other Changes in the Proposed Rules

In addition to the changes discussed above, the proposed rules would also (1) amend Forms 6-K and 20-F to make disclosure requirements applicable to foreign private issuers generally consistent with those applicable to U.S. issuers and (2) require that disclosures mandated by the proposed rules be presented in inline XBRL format.

Initial Takeaways

Although the proposed rules appear to be a logical extension of the SEC's earlier guidance on cybersecurity disclosure, several of the new requirements will be challenging for companies to implement and maintain. In addition, for many companies, the proposed governance and oversight disclosures will likely force a re-evaluation of existing practices and disclosures. It will be interesting to see what comments are submitted and what, if any, changes the SEC makes to the final promulgated rules. The debate will continue about the risks and rewards of increased disclosure of cybersecurity risks and incidents. The proposing release acknowledged one of the primary criticisms of increased disclosure—that it will make companies more vulnerable by providing a roadmap for attackers showing which companies are more vulnerable and where they are vulnerable. In an attempt to address this, the release noted that under the proposed rules, a company would not have to disclose "specific, 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."[6] It remains to be seen whether this limitation will reduce the risks of increased disclosure.

[1] The proposed rules are available here ("Proposing Release"), and the SEC's accompanying press release and fact sheet are available here and here, respectively.
[2] *See* CF Disclosure Guidance: Topic No. 2- Cybersecurity (Oct. 13, 2011) available here, and Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166] available here.
[3] *See* Proposing Release at 16 (stating that while "some companies provide a materiality analysis, disclose the estimated costs of an incident, discuss their engagement of cybersecurity professionals, and/or explain the remedial steps they have taken or are taking in response to a cybersecurity incident, . . . others do not provide such disclosure or provide much less detail").
[4] The term "cybersecurity incident" is defined broadly for these purposes as any "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." The term "information systems" is likewise broadly defined by the proposed rules.
[5] Proposing Release at 33, FN 69.
[6] Proposing Release at 29.