The Computer & Internet Lawyer

Volume 39 ▲ Number 6 ▲ June 2022

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

SEC Proposes Rules Mandating Disclosure of Material Cybersecurity Incidents

By Cynthia Cole, Brendan Quigley, Clint Rancher and Robert Cowan

The U.S. Securities and Exchange Commission ("SEC") has proposed amendments to its rules that would enhance and standardize disclosures related to cybersecurity risks and incidents, and would expand upon cybersecurity guidance issued by the SEC in 2018. Most notably, the proposed rules would require current disclosure of material cybersecurity incidents on Form 8-K within four business days after the company determines that it has experienced a material cybersecurity incident.

The goal of the proposed amendments is to better inform investors about a company's risk management, strategy and governance, and to provide timely notification of material cybersecurity incidents.

The proposed rules are summarized below; following are key takeaways:

- The proposed rules are significant, but not a surprise. As noted above, the release follows the 2018 cybersecurity guidance, as well as the SEC's creation of a Cyber Unit in its Enforcement Division; numerous SEC enforcement actions over the last several years arising out of cyber-incidents, alleging insufficient disclosures and/or controls related to the incident; and a recent rule proposal regarding cybersecurity reporting by investment advisers and investment companies.

- As with any disclosure issue, materiality is the linchpin. Only "material" cybersecurity incidents need to be disclosed, although the proposal provides little

Cynthia Cole (cynthia.cole@bakerbotts.com), a partner at Baker Botts L.L.P., focuses her practice on corporate, strategic and technology transactions, data privacy and cybersecurity. **Brendan Quigley** (brendan.quigley@bakerbotts.com), a partner at the firm, focuses his practice on Securities and Exchange Commission and Justice Department securities and commodities enforcement matters, Foreign Corrupt Practices Act-related investigations and counseling, and matters arising under the False Claims Act, as well as commercial disputes. **Clint Rancher** (clint.rancher@bakerbotts.com), a partner at the firm, represents public and private businesses in a broad range of corporate and securities matters including in initial public offerings, public offerings and private placements of equity and debt securities, liability management transactions, mergers and acquisitions and general corporate concerns, including Securities Exchange Act reporting and corporate governance. **Robert Cowan** (robert.cowan@bakerbotts.com) is an associate at the firm.

guidance on when an incident should be considered material.

- Moreover, even when a company determines an incident is, in fact, material, it may still be faced with a series of complicated and difficult decisions. The proposal requires the filing of a Form 8-K within four business days of that determination. However, it often takes significant time to determine the scope and extent of cyber-incidents – particularly the large ones that are most likely to be material. Thus, if the proposal is adopted as proposed, sensitive disclosure issues may need to be resolved in a more compressed time frame.

- Further, the four-business-day filing deadline may lead to tension between the SEC and other parts of the government, including the cyber and intelligence arms of the Department of Justice. For example, particularly in an age of nation-state sponsored cyber-attacks, the prompt filing of a Form 8-K could provide a malicious actor with valuable, timely intelligence on the effectiveness of its cyberattack efforts.

- SEC Commissioner Hester Peirce dissented from the proposed rules, arguing that the proposal "flirts with casting us as the nation's cybersecurity command center, a role Congress did not give us" and questioned whether "securities regulators are . . . best suited to design cybersecurity programs to be effective for all companies, in all industries, across time." It will be interesting to see the extent to which these views are reflected in comments submitted during the public comment period.

- At bottom though, in light of the SEC's continued focus on cyber disclosures and controls, public company boards and management teams will need to evaluate their company's disclosure controls and procedures to confirm that they are sufficiently designed to record, process, summarize and report to investors material information related to cybersecurity risks and incidents. The proposed cybersecurity rules may prompt companies to engage cybersecurity consultants, advisers or auditors and evaluate their existing relationships with third-party digital service providers.

EXISTING CYBERSECURITY DISCLOSURE REQUIREMENTS

The SEC issued interpretive guidance in 2018 to assist companies in determining when they may be required to disclose information regarding cybersecurity risks and incidents under existing disclosure rules. Importantly, this existing guidance will remain in place regardless of whether the SEC adopts the proposed amendments described here.

REPORTING OF MATERIAL INCIDENTS ON FORM 8-K

The proposed amendments would add new Item 1.05 to Form 8-K to require that companies disclose information about a cybersecurity incident within four business days after the company determines that it has experienced a material cybersecurity incident.

Specifically, new Item 1.05 would require a company to disclose the following information about a material cybersecurity incident, to the extent the information is known at the time of the Form 8-K filing:

- When the incident was discovered and whether it is 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 registrant's operations; and

- Whether the registrant has remediated or is currently remediating the incident.

Trigger Date

The trigger for an Item 1.05 Form 8-K is the date on which a company determines that a cybersecurity incident it has experienced is material, rather than the date of discovery of the incident.

Materiality

The proposed rules provide no specific guidance on what triggers "materiality" for a cyber-incident. Instead, the proposal directs companies to the classic – and decades old – formulation of "materiality" first announced in the U.S. Supreme Court's 1976 decision *TSC Industries Inc. v. Northway Inc.*: 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."

Timing of Evaluation

The SEC emphasized that it expects companies to be "diligent in making a materiality determination." Proposed instruction 1 to Item 1.05 states that "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."

Ongoing Investigations of Cybersecurity Incidents

The SEC does not expect companies to publicly disclose specific, technical information about their planned response to an incident or their cybersecurity systems, related networks or devices, or potential system vulnerabilities in such detail as would impede the company's response or remediation of the incident. Importantly, however, an ongoing internal or external investigation would not on its own provide a basis for avoiding or delaying disclosure of a material cybersecurity incident.

No Loss of S-3 Eligibility for Untimely 8-K Filings

The proposed amendments would add Item 1.05 to the list of Form 8-K items that do not result in the loss of Form S-3 eligibility if a company fails to file in a timely manner.

Rule 10b-5 Safe Harbor

The proposed amendments would add Item 1.05 to the list of Form 8-K items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act.

Definition of Cybersecurity Incident[1]

In the proposing release, the SEC noted that the term "cybersecurity incident" should be construed broadly and provided the following non-exclusive list of examples "that may, if determined by the company to be material," trigger the proposed Item 1.05 disclosure requirement:

- An unauthorized incident that has compromised the confidentiality, integrity, or availability of an information asset (data, system, or network); or violated the registrant's security policies or procedures. Incidents may stem from the accidental exposure of data or from a deliberate attack to steal or alter data;

- An unauthorized incident that caused degradation, interruption, loss of control, damage to, or loss of operational technology systems;

- An incident in which an unauthorized party accessed, or a party exceeded authorized access, and altered, or has stolen sensitive business information, personally identifiable information, intellectual property, or information that has resulted, or may result, in a loss or liability for the registrant;

- An incident in which a malicious actor has offered to sell or has threatened to publicly disclose sensitive company data; or

- An incident in which a malicious actor has demanded payment to restore company data that was stolen or altered.

PERIODIC UPDATES TO PREVIOUSLY REPORTED INCIDENTS ON FORMS 10-Q AND 10-K

Proposed Item 106(d)(1) of Regulation S-K would require companies to disclose any material changes, additions or updates to the information required by Item 1.05 of Form 8-K on Forms 10-Q and 10-K for the period in which the material change, addition or update occurred. This would include any material information not known or disclosable at the time of the Form 8-K filing.

Proposed Item 106(d)(1) provides the following non-exclusive examples of the type of disclosures that should be provided on Forms 10-Q or 10-K, if applicable:

- Any material impact of the incident on the registrant's operations and financial condition;

- Any potential material future impacts on the registrant's operations and financial condition;

- Whether the registrant has remediated or is currently remediating the incident; and

- Any changes in the registrant's policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

Notwithstanding Proposed Item 106(d)(1), a company may need to file an amended Form 8-K (in lieu of an update on a periodic report) in situations where a previous Item 1.05 Form 8-K disclosure becomes inaccurate or materially misleading as a result of subsequent developments regarding the cybersecurity incident.

Separately, proposed Item 106(d)(2) would require disclosure of the information required by Item 1.05 of Form 8-K when a series of previously undisclosed individually immaterial cybersecurity incidents became material in the aggregate. Such incidents would need to be disclosed in the periodic report for the period in which a company has made a determination that they are material in the aggregate.

CYBERSECURITY RISK MANAGEMENT AND STRATEGY DISCLOSURES ON FORM 10-K

Proposed Item 106(b) of Regulation S-K would require companies to disclose their policies and procedures (if any) to identify and manage cybersecurity risks and threats. Specifically, proposed Item 106(b) would require disclosure, as applicable, of whether:

- The registrant has a cybersecurity risk assessment program and, if so, provide a description of such program;
- The registrant engages assessors, consultants, auditors or other third parties in connection with any cybersecurity risk assessment program;
- The registrant has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third-party service provider (including, but not limited to, those providers that have access to the registrant's customer and employee data), including whether and how cybersecurity considerations affect the selection and oversight of these providers and contractual and other mechanisms the company uses to mitigate cybersecurity risks related to these providers;
- The registrant undertakes activities to prevent, detect and minimize effects of cybersecurity incidents;
- The registrant has business continuity, contingency and recovery plans in the event of a cybersecurity incident;
- Previous cybersecurity incidents have informed changes in the registrant's governance, policies and procedures, or technologies;
- Cybersecurity-related risk and incidents have affected or are reasonably likely to affect the registrant's results of operations or financial condition and, if so, how; and
- Cybersecurity risks are considered as part of the registrant's business strategy, financial planning and capital allocation and, if so, how.

CYBERSECURITY GOVERNANCE DISCLOSURES ON FORM 10-K

Proposed Item 106(c)(1) of Regulation S-K would require disclosure of a company's cybersecurity governance, including the board's role in overseeing cybersecurity risks. Specifically, disclosure required by proposed Item 106(c)(1) would include a discussion, as applicable, of the following:

- Whether the entire board, specific board members or a board committee is responsible for the 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 or board committee considers cybersecurity risks as part of its business strategy, risk management and financial oversight.

Proposed Item 106(c)(2) would require a description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures and strategies. This description would include, but not be limited to, the following information:

- 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 or members;
- Whether the registrant has a designated a chief information security officer,[2] or someone in a comparable position, and, if so, to whom that individual reports within the registrant's organizational chart, and the relevant expertise of any such persons;
- 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 of directors or a committee of the board of directors on cybersecurity risk.

CYBERSECURITY EXPERTISE OF DIRECTORS

Proposed Item 407(j) of Regulation S-K would require that companies disclose in their annual proxy statements and Form 10-Ks the cybersecurity expertise of members of the board of directors, if any. If any member of the board has cybersecurity expertise, then the company would have to disclose the name(s) of such director(s) and provide such detail as necessary to fully describe the nature of the expertise.

Proposed Item 106(c)(2) would require a description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures and strategies.

Although the proposing release does not define "cybersecurity expertise," proposed Item 407(j) includes the following non-exclusive list of criteria that a company should consider in reaching a determination on whether a director has expertise in cybersecurity:

- Whether the director has prior work experience in cybersecurity, including, for example, prior experience as an information security officer, security policy analyst, security auditor, security architect or engineer, security operations or incident response manager or business continuity planner;
- Whether the director has obtained a certification or degree in cybersecurity; and
- Whether the director has knowledge, skills or other background in cybersecurity, including, for example, in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling or business continuity planning.

Notes

1. The SEC has proposed to define "cybersecurity incident" 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."

   The SEC has proposed to define "information systems" as "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 a registrant's information to maintain or support the registrant's operations."
2. According to the proposing release, the chief information security officer may be responsible for identifying and monitoring cybersecurity risks, communicating with senior management and the registrant's business units about acceptable risk levels, developing risk mitigation strategies and implementing a framework that protects the registrant's digital assets.