March 14, 2022

SEC Proposes New Cybersecurity Disclosure Requirements

The SEC has proposed new disclosure requirements (available here) to enhance and standardize public company disclosures regarding cybersecurity risk management and incident reporting. The proposed amendments would require companies to disclose material cybersecurity incidents within four business days on Form 8-K, and provide any necessary updates in their subsequent periodic reports on Form 10-Q and 10-K. In addition, companies would be required to provide annual disclosure regarding their policies and procedures to identify and manage cybersecurity risks, their board's oversight of cybersecurity risk (and the cybersecurity expertise of any members of the board) and management's role and expertise in assessing and managing cybersecurity risk and implementing cybersecurity policies and procedures.

Reporting of Material Cybersecurity Incidents

To address the concern that cybersecurity incidents are not being reported on a timely basis, or are underreported, the SEC is proposing amending Form 8-K to add new Item 1.05 which would set out reporting requirements related to material cybersecurity incidents. In addition, the SEC is proposing amending Regulation S-K to add new Item 106, which would require registrants to update any such Form 8-K disclosures in their periodic reports.

What is a cybersecurity incident?

Under proposed new Item 106(a) of Regulation S-K, a "cybersecurity incident" would be defined to mean "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."

What is a "material" cybersecurity incident?

In the proposing release, the SEC confirmed that the determination of whether a cybersecurity incident is material should be guided by the same materiality principles articulated repeatedly by the courts and the SEC – namely whether there is a substantial likelihood that a reasonable investor would consider it important. In making this determination, the SEC reminded registrants that they need to consider the total mix of information, including both quantitative and qualitative factors, and that an incident may be material even if the probability of a negative consequence is low, if the potential loss or liability is large. Materiality must be assessed on an incident by incident basis, as well as on an aggregate basis, to determine whether a series of minor incidents has become material in the aggregate and must be disclosed in the registrant's periodic reports.

The proposing release identified the following examples of potentially material cybersecurity incidents (note this is not an exhaustive list):

- 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.

What would registrants need to disclose?
Proposed new Item 1.05 would require registrants to disclose, within four business days of their determination that a material cybersecurity incident has occurred, the following information (to the extent known at the time of the 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.

Registrants would not be required or expected to publicly disclose specific, technical information about their planned responses to the incident or their cybersecurity systems, related networks and devices, or potential system vulnerabilities at a level of detail that could hamper their ability to respond to or remedy the incident.

When would the disclosure need to be made?
The disclosure would be required to be made within 4 business days after the registrant determines that the cybersecurity incident is material (not the date the registrant learned of the incident). In order to ensure that registrants are timely in assessing the materiality of any incidents for the purposes of their disclosure obligations, Instruction 1 to proposed new Item 1.05 would require registrants to "make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."

Proposed new Item 1.05 would not permit registrants to delay their disclosures pending their investigations (even if other applicable laws would permit them to delay such reporting).

Would a failure to disclose material cybersecurity events on a timely basis compromise S-3 eligibility?
No. Under the proposed rules, a registrant would not lose S-3 eligibility if their Form 8-K filing was not made on a timely basis (the registrant would need to be caught up and current at the time it files the Form S-3 Registration Statement).

What if there has been a change in the information regarding a cybersecurity incident disclosed on Form 8-K?
Under proposed new Item 106(d)(1) of Regulation S-K, registrants would be required to disclose any material changes, additions, or updates to the information required to be disclosed on Form 8-K in their periodic reports for the quarter in which such change, addition or update occurred.

Proposed new Item 106(d)(1) provides the following examples of disclosures that should be provided, if applicable (note, this is not an exhaustive list):

- 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.

What if a registrant has experienced a series of minor cybersecurity incidents?
Under proposed new Item 106(d)(2) of Regulation S-K, registrants would be required to disclose that a series of previously unreported cybersecurity incidents has become material in the aggregate in the periodic report for the quarter in which such determination is made. As a result, registrants will need to evaluate incidents on an individual and ongoing aggregate basis to assess materiality. If a series of incidents is determined to be material, registrants would be required to disclose:

- when the incidents were discovered and whether they are ongoing;
- a brief description of the nature and scope of such incidents; whether any data was stolen or altered;
- the impact of such incidents on the registrant's operations and the registrant's actions; and
- whether the registrant has remediated or is currently remediating the incidents.

Would the disclosures under proposed new Item 1.05 of Form 8-K be eligible for the limited safe harbor from Section 10(b) or Rule 10b-5 liability for the failure to file certain Form 8-Ks?
Yes. The SEC has proposed amending Rules 13a-11(c) and 15d-11(c) under the Exchange Act of 1934, as amended, so that disclosures made in response to proposed new Item 1.05 would be eligible for the limited safe harbor from liability under Section 10(b) or Rule 10b-5 under the Exchange Act for a failure to timely file the Form 8-K.

Do foreign private issuers need to make similar disclosures regarding cybersecurity incidents?
Yes. The SEC has proposed amending Form 6-K to identify material cybersecurity incidents as a filing trigger. Material updates regarding previously disclosed incidents would also need to be provided on Form 6-K. In addition, the SEC has proposed amendments to Form 20-F that would require foreign private issuers to disclose on an annual basis information regarding any previously undisclosed material cybersecurity incidents that have occurred during the reporting period. The SEC is not proposing any changes to Form 40-F.

Disclosure of Risk Management, Strategy and Governance Regarding Cybersecurity Risks

In order to elicit more consistent and informative disclosure, the SEC has proposed new Item 106 of Regulation S-K, which would require registrants to describe in their Annual Reports on Form 10-K their risk management and strategy, as well as the role of their boards and management in overseeing, and assessing and managing these risks.

What would registrants be required to disclose about their cybersecurity risk management?
Under proposed new Item 106(b) of Regulation S-K, registrants would need to disclose their policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including, but not limited to: operational risk (i.e., disruption of business operations); intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk. Specifically, registrants would need to disclose whether:

- they have a cybersecurity risk assessment program and if so, provide a description of such program;
- they engage assessors, consultants, auditors, or other third parties in connection with any cybersecurity risk assessment program;

- they have 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;

- they undertake activities to prevent, detect, and minimize effects of cybersecurity incidents;

- they have 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.

What would registrants need to disclose about the board oversight of cybersecurity risks?
Under proposed new Item 106(c)(1) of Regulation S-K, registrants would be required to include the following disclosures regarding their board's cybersecurity oversight, as applicable:

- 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.

In addition, registrants would need to identify in their Form 10-K or proxy statement whether any director has expertise in cybersecurity, and to describe that expertise. Proposed new Item 407(j) of Regulation S-K identifies a number of factors that registrants should consider when evaluating the cybersecurity expertise of their board members, including prior work experience, degrees or certification, or other knowledge, skills or background. Any board director so designated would not be deemed an expert under securities laws. The duties, obligations or liability of other members of the board would not change as a result of designating one (or more) directors as cybersecurity experts.

What would registrants need to disclose about management oversight of cybersecurity risks?
Under proposed new Item 106(c)(2) of Regulation S-K, in their Form 10-K, registrants would be required to describe the role of management in assessing and managing cybersecurity-related risks and implementing cybersecurity policies, procedures and strategies. This disclosure should include at least the following:

- 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 in such detail as necessary to fully describe the nature of the expertise (expertise may come from prior work experience, degrees or certifications or knowledge, skills, or other background);

- whether the registrant has a designated chief information security officer, 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 in such detail as necessary to fully describe the nature of the expertise;

- 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.

Do foreign private issuers need to make similar disclosures regarding cybersecurity risk management, strategy and governance?
Yes. The SEC has proposed amending Form 20-F to require similar disclosures by foreign private issuers. The SEC is not proposing any such prescriptive disclosure requirements for Form 40-F filers.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

Jonathan H. Ashtor
+1-212-373-3823
jashtor@paulweiss.com

H. Christopher Boehning
+1-212-373-3061
cboehning@paulweiss.com

Christopher J. Cummings
+1-212-373-3434
ccummings@paulweiss.com

David S. Huntington
+1-212-373-3124
dhuntington@paulweiss.com

Brian M. Janson
+1-212-373-3588
bjanson@paulweiss.com

John C. Kennedy
+1-212-373-3025
jkennedy@paulweiss.com

Raphael M. Russo
+1-212-373-3309
rrusso@paulweiss.com

Jeannie S. Rhee
+1-202-223-7466
jrhee@paulweiss.com

Tracey A. Zaccone
+1-212-373-3085
tzaccone@paulweiss.com

Steven C. Herzog
+1-212-373-3317
sherzog@paulweiss.com

Practice Management Consultant Jane Danek contributed to this Client Memorandum.