BLANKROME

Privacy, Security & Data Protection

MARCH 24, 2022 • NO. 1

SEC Proposes New Cybersecurity Rules

The Securities and Exchange Commission ("SEC") has proposed rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and cybersecurity incident reporting by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934 ("registrants"). The rules, proposed on March 9, 2022, build on the interpretative guidance provided by the SEC in 2011 and 2018 and require registrants to report material cybersecurity incidents and to provide updates about previously reported cybersecurity incidents in their periodic reports, as well as to disclose (i) their policies and procedures to identify and manage cybersecurity risks; (ii) management's role in implementing cybersecurity policies and procedures; (iii) the board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk management. The proposed rules are open for public comment, which should be received on or before 30 days after the date of the proposed rules' publication in the Federal Register or May 9, 2022, whichever is later.

REPORTING ON FORM 8-K

The proposed rules seek to amend Form 8-K to add Item 1.05 to require registrants to disclose information about a cybersecurity incident within four business days after the registrant determines that it has experienced a material cybersecurity incident. "Cybersecurity incident" is 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."

Examples of material cybersecurity incidents include:

- 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.

The proposed rules require a registrant to disclose the following information about a material cybersecurity incident in Item 1.05 of Form 8-K, 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.

Unlike state breach notification laws that generally provide for a delay in notifying affected individuals of data breaches where law enforcement determines the notification will impede a civil or criminal investigation, the proposed rules do not provide for such a reporting delay.

For foreign private issuers ("FPIs") the proposed rules require furnishing Form 6-K to report material cybersecurity incidents.

The proposed rules also seek to amend General Instruction I.A.3.(b) of Form S-3 to provide that an untimely filing of a Form 8-K under Item 1.05 would not result in loss of eligibility to offer securities on Form S-3, nor would such a failure be deemed a violation of the antifraud provisions of Rule 10b-5.

DISCLOSURE ABOUT CYBERSECURITY INCIDENTS IN PERIODIC REPORTS

Proposed Item 106(d)(1) of Regulation S-K requires registrants to provide updates on one or more cybersecurity incidents previously disclosed in Form 8-K and disclose any material changes, additions, or other updates regarding such incidents in a Form 10-Q or Form 10-K for the quarter (the fourth quarter, for Form 10-K), in which such change, addition, or update occurred.

Examples of the type of disclosure that should be provided include:

- Any material effect 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.

Under Proposed Item 106(d)(2) of Regulation S-K, the registrant should provide the following disclosure in Forms 10-Q and 10-K, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate:

- A general description of 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 effect of such incidents on the registrant's operations; and
- Whether the registrant has remediated or is currently remediating the incidents.

DISCLOSURE OF A REGISTRANT'S RISK MANAGEMENT, STRATEGY, AND GOVERNANCE REGARDING CYBERSECURITY RISKS

The proposed rules seek to amend Form 10-K to require disclosure regarding a registrant's policies and procedures, if any, for identifying and managing cybersecurity risks; a registrant's cybersecurity governance, including the board of directors' oversight role regarding cybersecurity risks; and management's role and relevant expertise in assessing and managing cybersecurity related risks and implementing related policies, procedures, and strategies.

More specifically, proposed Item 106(b) of Regulation S-K would require disclosure of whether:

- The registrant has a cybersecurity risk assessment program and if so, 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 service 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 service providers, and contractual and other mechanisms the registrant uses to mitigate cybersecurity risks related to these service 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 risks and previous incidents have affected or are reasonably likely to affect the registrant's strategy, business model, 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.

Proposed Item 106(c)(1) requires disclosure of the board of directors' oversight role regarding cybersecurity risks, including 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) requires a description of management's role in assessing and managing cybersecurity-related risks and in implementing the registrant's cybersecurity policies, procedures, and strategies, including 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;

- Whether the registrant has designated a 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;

- 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.

DISCLOSURE REGARDING THE BOARD OF DIRECTORS' CYBERSECURITY EXPERTISE

Proposed Item 407(j) of Regulation S-K requires disclosure about the cybersecurity expertise of members of the board of directors of the registrant, if any. If any member of the board has cybersecurity expertise, the registrant would have to disclose the name(s) of any such director(s) and provide such detail as necessary to fully describe the nature of the expertise. Such disclosure would be required in a registrant's proxy or information statement when action is to be taken with respect to the election of directors and in its Form 10-K (or incorporated by reference into Form 10-K from the proxy statement or information statement).

Proposed Item 407(j) does not define "cybersecurity expertise" but does provide a non-exclusive list of criteria that a registrant should consider in determining whether a director has cybersecurity expertise:

- 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.

Proposed Item 407(j)(2) states that a person who is determined to have expertise in cybersecurity will not be deemed an expert for any purpose, including, without limitation, for purposes of Section 11 of the Securities Act of 1933, as a result of being designated or identified as a director with cybersecurity expertise. This safe harbor is intended to clarify that Item 407(j) would not impose on such person any duties, obligations, or liability that are greater than the duties, obligations, and liability imposed on such person as a member of the board of directors in the absence of such designation or identification.

DISCLOSURE BY FPIS IN ANNUAL REPORTS

The proposed rules seek to amend Form 20-F to require FPIs to provide the same type of cybersecurity disclosures in their annual reports as those the proposed rules require of domestic registrants under Items 106 and 407(j) of Regulation S-K. One difference is that while domestic registrants would be required to include the proposed Item 407(j) disclosure about board expertise in both their annual reports and proxy or information statements (or incorporate it by reference into annual reports), FPIs are not subject to SEC rules for proxy or information statement filings and thus, would only be required to include this disclosure in their annual reports.

For additional information or assistance, contact Sharon Klein, Yelena Barychev, Karen Shin, or a member of Blank Rome's Privacy, Security & Data Protection or Corporate Governance groups.

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

Yelena M. Barychev
215.569.5737 | yelena.barychev@blankrome.com

Karen H. Shin
949.812.6012 | karen.shin@blankrome.com