BCLP. Client Intelligent

BCLPSecCorpGov.com

SEC PROPOSES NEW CYBERSECURITY DISCLOSURE REQUIREMENTS

Mar 09, 2022

On March 9, 2022, the SEC proposed new requirements for reporting of material cybersecurity incidents in 8-Ks and periodic reports as well as disclosure of board and management roles with respect to cybersecurity and of cybersecurity policies and procedures.

Commissioner Pierce dissented, expressing concern that the proposal "flirts with casting [the SEC] as the nation's cybersecurity command center" without the necessary expertise. She believes the disclosure requirements may have the effect of substantively changing corporate practices with respect to the design of cybersecurity programs.

The public comment period will remain open until the later of May 9, 2022 or 30 days following publication of the proposing release in the Federal Register.

Background

The SEC observed that cybersecurity incidents have increased and become more significant, and that such threats "pose an ongoing and escalating risk to public companies, investors, and market participants." It believes that investors would benefit from more timely and consistent disclosure about material incidents, in light of their potential impact on companies and the economy.

As discussed in our February 26, 2018 client alert, the SEC issued interpretative guidance on cybersecurity matters, as well as related insider trading and Regulation FD considerations, in 2011 and 2018. After conducting a review of company filings since then, the SEC believes disclosure practices have been inconsistent and inadequate – with many incidents reported in the media but not in company filings or, if disclosed, with different levels of specificity or prominence.

Recommended actions

Although these rules are only in the proposal stage, companies should consider the implications in the event of their adoption, and begin to take preparatory steps, including:

- Developing controls and procedures for reporting material cybersecurity incidents that are included in and align with the broader incident response program

- Evaluating risk management and strategies with respect to cybersecurity threats, including the factors listed below
- Evaluating board and management roles with respect to cybersecurity
- Considering cybersecurity expertise as part of board skill matrix analyses

Reporting of cybersecurity incidents

The SEC is proposing to:

Amend Form 8-K – New Item 1.05 would require reporting about cybersecurity incidents within four business days after the company determines that it has experienced a material cybersecurity incident, including (to the extent known at the time):

- 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 operations; and
- whether the company has remediated or is currently remediating the incident.

The SEC would not expect a company to disclose specific, technical information about its planned response to the incident or its information systems or potential vulnerabilities in such detail as would impede its response or remediation of the incident.

To address any concern that a company may delay making such a determination to avoid a disclosure obligation, Instruction 1 to proposed Item 1.05 states: "a registrant shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident."

Definition of cybersecurity incident – New Item 1.06 of Regulation S-K would define a 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 believes the term should be broadly construed and may result from an accidental exposure of data, a deliberate action or activity to gain unauthorized access to systems or to steal or alter data, or other system compromises or data breaches.

Materiality Determination. The release provides a list of examples of incidents that may be deemed material for purposes of Form 8-K. (See page 24.) The SEC stated that in evaluating materiality:

> "[Companies] would need to thoroughly and objectively evaluate the total mix of information, taking into consideration all relevant facts and circumstances surrounding the cybersecurity incident, including both quantitative and qualitative factors, to determine whether the incident is material. Even if the probability of an adverse consequence is relatively low, if the magnitude of the loss or liability is high, the incident may still be material; materiality 'depends on the significance the reasonable investor would place on' the information."

No Delay for Ongoing Investigations. Although recognizing that a delay in reporting might help law enforcement apprehend criminals and prevent future incidents, the SEC believes "the importance of timely disclosure of cybersecurity incidents for investors would justify not providing for a reporting delay" – even if state law would permit such a delay in the notification of state agencies.

No Impact on Form S-3 Eligibility. Late filing of Item 1.05 8-Ks would not result in loss of Form S-3 or Form SF-3 eligibility. Item 1.05 would similarly be included in the list of items eligible for a limited safe harbor from liability under Section 10(b) or Rule 10b-5 pursuant to Rules 13a-11(c) and 15d-11(c).

Amend Form 6-K – to add cybersecurity incidents as a reporting topic.

Amended Periodic Reports – New Item 106 of Regulation S-K and amended Form 20-F would require companies to provide (1) updated disclosure relating to previously disclosed cybersecurity incidents and (2) disclosure, to the extent known to management, when a series of previously undisclosed individually immaterial cybersecurity incidents has become material in the aggregate.

The proposed rules includes examples of the type of disclosure that should be provided, if applicable:

- any material impact of the incident on operations and financial condition;
- any potential material future impacts on operations and financial condition;
- whether the company has remediated or is currently remediating the incident; and
- any changes in policies and procedures as a result of the cybersecurity incident, and how the incident may have informed such changes.

In cases where such incidents become material in the aggregate, companies would

need 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 operations and actions; and
- whether the company has remediated or is currently remediating the incidents.

Cybersecurity risk management, strategy and governance disclosure

The SEC is proposing to require standardized disclosure of cybersecurity risk management, strategy and governance. New Item 106 of Regulation S-K and Item 16J of Form 20-F would require disclosure of:

Risk management and strategy – policies and procedures, if any, for the identification and management of risks from cybersecurity threats, including whether the company considers cybersecurity as part of its business strategy, financial planning and capital allocation

- Risks and threats include operational risk, intellectual property threat, fraud, extortion, harm to employees or customers, violation of privacy laws and other litigation and legal risk, and reputational risk
- To the extent applicable, disclosure would include whether:
  - the company has a cybersecurity risk assessment program and, if so, a description of such program;
  - the company engages assessors, consultants, auditors, or other third parties in connection with such program;
  - the company has policies and procedures to oversee and identify the cybersecurity risks associated with its use of any third party service provider (including with respect to 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 company undertakes activities to prevent, detect, and minimize effects of cybersecurity incidents and, if so, a description of the types of such activities;
  - the company has business continuity, contingency, and recovery plans in the event of a cybersecurity incident;
  - previous cybersecurity incidents have informed changes in governance, policies and procedures, or technologies;
  - cybersecurity related risk and incidents have affected or are reasonably likely to affect strategy, business model, results of operations or financial condition and if so, how; and

- cybersecurity risks are considered as part of business strategy, financial planning, and capital allocation and if so, how.

Governance disclosure – board oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the company's cybersecurity policies, procedures, and strategies

Disclosure of board oversight – would include:

- 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.

Disclosure of management's role – would include:

- 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 company has a designated chief information security officer, or someone in a comparable position, and if so, to whom that individual reports within the 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.

Board expertise – amended Item 407 of Regulation S-K and Form 20-F would require disclosure in annual reports and certain proxy filings if any member of the board of directors has expertise in cybersecurity, including the name(s) of any such director(s) and any detail necessary to fully describe the nature of the expertise.

Inline XBRL required

The SEC proposes to require that cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).

RELATED PRACTICE AREAS

- Securities & Corporate Governance

MEET THE TEAM

R. Randall Wang

St. Louis

randy.wang@bclplaw.com
+1 314 259 2149

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.

© 2024 Bryan Cave Leighton Paisner LLP.