BCLP. Client Intelligent

BCLPSecCorpGov.com

DIVIDED SEC ADOPTS CONTROVERSIAL CYBERSECURITY DISCLOSURE REQUIREMENTS

Jul 27, 2023

A divided SEC on July 26, 2023 approved new requirements for reporting of material cybersecurity incidents in real-time current reports on Form 8-K or 6-K and disclosure of cybersecurity risk management, strategy and governance in annual reports on Form 10-K or 20-F.

EXECUTIVE SUMMARY

New Form 8-K Item 1.05 requires companies to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations.

The filing is due four business days after the determination of materiality but may be delayed if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and so notifies the SEC in writing.

New S-K Item 106 requires companies to include in annual reports on Form 10-K or 20-F descriptions of their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company.

Item 106 also requires companies to describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

COMPLIANCE DATES

For annual disclosures of risk management and governance, all companies must provide such disclosures beginning with Form 10-Ks or 20-Fs for fiscal years ending on or after December 15, 2023.

For incident disclosures, all companies – except for smaller reporting companies (SRCs) – must begin complying in Form 8-Ks or 6-Ks on the later of 90 days after the date of publication of the new rules in the Federal Register or December 18, 2023. SRCs will have an additional 180 days and must begin complying on the later of 270 days from the effective date of the rules or June 15, 2024.

For data tagging, all companies must begin tagging the new disclosures using Inline XBRL beginning one year after initial compliance with the related disclosure requirement.

RECOMMENDED ACTIONS

With as little as five months to get ready, companies should begin to take preparatory steps now, including:

- Update/implement and test regularly cybersecurity policies to include guidance on determining materiality in the context of a security incident and to identify (and engage under privilege) responsible parties, including third parties (e.g., external legal counsel, forensics providers)
- Update/develop controls and procedures for reporting material cybersecurity incidents, , including identification of contacts to collect and evaluate required information to conduct materiality determinations
  - Review arrangements with third-party providers, taking into account the SEC's guidance regarding Rule 12b-21, which provides that information need only be disclosed insofar as it is known or reasonably available to the company
- Evaluate risk management and strategies with respect to cybersecurity threats
  - Consider any national security, public safety or classification issues and develop plans, as needed, for coordination with governmental agencies, including possible need for requests for delays in 8-K reporting
- Evaluate board and management roles and management expertise with respect to cybersecurity, as well as any third parties
- Review and formalize, if necessary, board or committee procedures for oversight of cybersecurity
- Prepare frameworks for draft forms of disclosures in response to the new rules

CHANGES FROM PROPOSED RULES

As discussed in our March 2022 post, the SEC proposed new cybersecurity rules early last year. In response to comments, the SEC softened the final rules by:

- Revising the 8-K Item 1.05 requirements relating to the determination of materiality:
  - The determination will need to include not only the material impact of the incident, but also its "reasonably likely material impact"
  - Replacing the proposed "aggregation of immaterial incidents" test with requirement to report "a series of related unauthorized occurrences" determined to be material
- Permitting delay in an 8-K filing in cases of national security or public safety determinations by the United States Attorney General
  - Concerns of other federal agencies or non-federal law enforcement will need to be conveyed to and effected through the US AG
- Reducing required 8-K disclosures to focus primarily on the effects rather than the details of the incident
- Eliminating the obligation to update 8-K incident disclosures in periodic reports, but instead requiring amendments to the 8-K to disclose previously omitted or unavailable information
- Reducing requirements in annual reports for disclosure of cybersecurity risk management and strategy
- Eliminating the obligation to disclose board-level cybersecurity expertise, but requiring disclosure of management expertise

Among the comments for which the SEC declined to make changes:

- "Furnishing" 8-Ks, instead of filing
- Longer 8-K delays to allow for investigation and completion of remediation efforts
- Exclusions for cybersecurity incidents on third-party systems used by companies
- Exceptions for incidents covered by notification requirements of other federal agencies

DISSENTING COMMISSIONERS

Commissioners Peirce and Uyeda issued strong dissents, believing the majority failed to explain why the new rules are needed, in light of existing SEC guidance, or to address the weaknesses in the economic analysis of estimated costs of the new rules. Additionally, Peirce believes:

- The overly prescriptive disclosure requirements have the potential to help bad actors by providing a roadmap for attacks, while diverting company resources better spent on

combatting or responding to threats

- The law enforcement exception for delayed 8-K filings is too narrow, and could be difficult to obtain within the four business day window

Uyeda also objects to the new rules because:

- They elevate cybersecurity risks above others that may be even more material to particular companies.
- They require disclosure of "reasonably likely material impacts, thereby introducing a forward-looking disclosure requirement in 8-Ks and amendments for the first time

REAL-TIME REPORTING OF CYBERSECURITY INCIDENTS – 8-K ITEM 1.05 AND 6-K

New 8-K Item 1.05 requires companies to disclose any cybersecurity incident they determine to be material and describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the company, including its financial condition and results of operations. Form 6-K will require foreign private issuers to furnish information on material cybersecurity incidents that they make or are required to make public or otherwise disclose in a foreign jurisdiction to any stock exchange or to security holders.

The SEC believes the "streamlined" requirements should allow companies to have the information required to be disclosed as part of their normal disclosure controls and procedures. To the extent any required information is not determined or is unavailable at the time of the required filing, Instruction 2 directs companies to include a statement to that effect in the 8-K and then file an amended 8-K containing such information within four business days after the company – "without unreasonable delay" – determines such information or within four business days after such information becomes available.

Form 6-K is being amended to add cybersecurity incidents as a reporting topic for FPIs.

Determination of materiality by company as trigger

In response to comments, the trigger for disclosure is the determination by the company of the materiality of the incident. However, instructions make clear that the company must determine the materiality of an incident without unreasonable delay following discovery and, if the incident is determined material, file the 8-K within four business days of such determination.

The SEC changed the timing as originally proposed from "as soon as reasonably practicable" to "without unreasonable delay" to address possible concern that some companies may delay making a determination to avoid a disclosure obligation.

The SEC declined to provide a new definition of materiality for cybersecurity purposes.

Delay permitted in case of national security or public safety determination by US AG

The disclosure may be delayed for a time period of up to 30 days, with a possible extension of up to 30 additional days and, in extraordinary circumstances, a final extension of up to 60 days, if the United States Attorney General determines that immediate disclosure would pose a substantial risk to national security or public safety and, in each case, notifies the SEC of such determination in writing.

If the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief through possible exemptive orders.

Although a number of commentators recommended that other federal agencies and non-Federal law enforcement agencies also be authorized to trigger delays, the SEC believes that having a single point of contact "is critical to ensuring that the rule is administrable." Further, it noted that the other agencies can ask the Attorney General to take action on their behalf.

The delay provision for substantial risk to national security or public safety is separate from Exchange Act Rule 0-6, which provides for the omission of classified information.

Content of disclosure – effects, not details, of incident

In response to comments, the final rule focuses disclosure primarily on the effects rather than the details of the incident, noting that "the disclosure of certain details required by proposed Item 1.05 could exacerbate security threats, both for the registrants' systems and for systems in the same industry or beyond, and could chill threat information sharing within industries."

Qualitative factors. The SEC notes that "financial condition and results of operations" are not exclusive forms of "material impact" and companies should consider qualitative factors, such as:

- Harm to a company's reputation, customer or vendor relationships, or competitiveness
- The possibility of litigation or regulatory investigations or actions, including regulatory actions by state and federal governmental authorities and non-U.S. authorities

Availability of information. The SEC believes that even though a company may not have complete information about the incident, it may know enough to determine whether the incident was material. As a result, it believes "a company being unable to determine the full extent of an incident because of the nature of the incident or the company's systems, or otherwise the need for continued investigation regarding the incident, should not delay the company from determining materiality."

It acknowledged that, on occasion, an incident may initially appear material but later developments reveal otherwise. However, it believes "the alternative of delaying disclosure beyond the four

business day period after a materiality determination has the potential to lead to far more mispricing and will negatively impact investors making investment and voting decisions without the benefit of knowing that there is a material cybersecurity incident."

Remediation efforts; compromised data. The SEC is not requiring disclosure of an incident's remediation status, whether it is ongoing or whether data were compromised. However, it notes that companies may need to address "data theft, asset loss, intellectual property loss, reputational damage, or business value loss . . . as part of their materiality analyses."

No exception for third party systems. The SEC rejected requests for an exemption for cybersecurity incidents on third-party systems used by companies. In its view, the materiality of an incident is unrelated to the location or ownership of the relevant IT system. Although companies may have limited insight to third party systems, the SEC notes that the new rules generally do not require that companies "conduct additional inquiries outside of their regular channels of communication with third-party service providers pursuant to those contracts and in accordance with registrants' disclosure controls and procedures," consistent with Rule 12b-21, which provides that information need only be disclosed insofar as it is known or reasonably available to the company.

Exclusion of technical information. Instruction 4 will provide that a company "need not disclose specific or 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 [its] response or remediation of the incident."

Sharing information with agencies, etc. The SEC notes that "a decision to share information with other companies or government actors does not in itself necessarily constitute a determination of materiality."

Required amendments for incomplete information in lieu of updates in periodic reports

Companies must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial

Form 8-K filing. The filing is due within four business days after, without unreasonable delay, determining such information or within four business days after such information becomes available.

The SEC explained that the new rules do not require updated reporting for *all* new information – only information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial 8-K filing. Otherwise, the new rules do not separately create or otherwise affect a company's duties to update or correct under existing case law.

No conflict with other laws; accommodation for FCC notification rule

In response to comments, the SEC conducted a review of other federal laws and regulations for potential conflicts with the new rule. It identified only one issue – the FCC's notification rule for breaches of customer proprietary network information ("CPNI") – which itself is the subject of proposed amendments that may eliminate the conflict. To accommodate the FCC's current requirements, paragraph (d) to Item 1.05 provides that companies subject to that rule may delay making a Form 8-K disclosure up to the seven business day period in the FCC rule following notification to the US Secret Service and FBI, with written notification to the SEC.

Broad definition of cybersecurity incident

Largely as proposed, new Item 1.06 of Regulation S-K defines a cybersecurity incident as "an unauthorized occurrence, or a series of related unauthorized occurrences, 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.

In a change from the proposed rules (and in place of a proposed "aggregation" requirement), it extended the definition to "a series of related unauthorized occurrences." As a result, Item 1.05 may be triggered even if the material impact or reasonably likely material impact could be parceled among the multiple intrusions to render each by itself immaterial, such as:

- The same malicious actor engages in a number of smaller but continuous cyberattacks related in time and form against the same company and collectively, they are either quantitatively or qualitatively material
- A series of related attacks from multiple actors exploiting the same vulnerability and collectively impeding the company's business materially.

Over the objections of some commenters, the SEC explained that it:

- Retained the term "owned or used by" because, as discussed above, it believes the materiality of a cybersecurity incident is contingent neither on where the relevant electronic systems reside nor on who owns them, but rather on the impact to the company.
- Retained the term "jeopardizes," in part because the effects of an incident may be foreseeable even if no actual harm has yet occurred, and because 8-K reporting is ultimately dependent on a materiality determination.

No impact on Form S-3 eligibility

As proposed, late filing of Item 1.05 8-Ks will not result in loss of Form S-3 or Form SF-3 eligibility. Item 1.05 will 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).

The SEC declined to allow companies to "furnish" 1.05 8-Ks in order to "help promote the accuracy and reliability of such disclosures" for investors.

ANNUAL DISCLOSURE OF CYBERSECURITY RISK MANAGEMENT, STRATEGY AND GOVERNANCE

New Item 106 of Regulation S-K and amended Form 20-Fs require companies to describe in their annual reports:

- their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats
- whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company
- the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats

The SEC believes it softened the rules from those proposed so as to "avoid levels of detail that may go beyond information that is material to investors and address commenters' concerns that those details could increase a company's vulnerability to cyberattack." In particular, it:

- Substituted the term "processes" for the proposed "policies and procedures" to avoid requiring disclosure of sensitive operational details
- Added a materiality qualifier to the proposed requirement to disclose "risks from cybersecurity threats," and removed the proposed list of risk types (i.e., "intellectual property theft; fraud; extortion; harm to employees or customers; violation of privacy laws and other litigation and legal risk; and reputational risk"), to avoid perception that the rule prescribes cybersecurity policy
- Dropped proposed paragraphs (4) (prevention and detection activities), (5) (continuity and recovery plans), and (6) (previous incidents)
- Revised proposed paragraph (3) to require only high-level disclosure regarding third-party service providers

Risk management and strategy

As revised, Item 106(b) now requires companies disclose (together with any other information needed for a reasonable investor to understand the cybersecurity processes):

- Whether and how the described cybersecurity processes in Item 106(b) have been integrated into the company's overall risk management system or processes
- Whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes
  - The SEC believes investors should know the level of a company's in-house versus outsourced cybersecurity capacity. However, it indicated that neither the names nor a description of services provided by third parties is required.
- Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider

In addition, companies should include a description of "[w]hether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition and if so, how."

Cybersecurity governance

In response to comments, the SEC "streamlined" Item 106(c) to require less detail. As revised, companies must "[d]escribe the board's oversight of risks from cybersecurity threats," and, if applicable, "identify any board committee or subcommittee responsible" for such oversight "and describe the processes by which the board or such committee is informed about such risks."

Among the changes from the proposal, the SEC:

- Eliminated proposed Item 106(c)(1)(iii), which had covered whether and how the board integrates cybersecurity into its business strategy, risk management and financial oversight
- Eliminated the proposed Item 106(c)(1)(ii) requirement to disclose "the frequency of [the board or committee's] discussions" on cybersecurity, although noting frequency may still be implicated by descriptions of governance processes
- Modified Item 106(c)(2) to add a materiality qualifier, to make clear that companies must "[d]escribe management's role in assessing and managing the [company's] *material* risks from cybersecurity threats" (emphasis added). The non-exclusive list of elements for consideration include:
  - Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members 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, detection, mitigation, and remediation of cybersecurity incidents; and
- Whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors

Instructions to Item 106 provide that relevant expertise of management may include prior work experience, relevant degrees or certifications and any knowledge, skills, or other background in cybersecurity.

In addition, the SEC did not adopt the proposed requirement in Item 407(j) regarding board-level cybersecurity expertise. It was "persuaded that effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters."

RELATED PRACTICE AREAS

- Securities & Corporate Governance
- Data Privacy & Security

MEET THE TEAM

R. Randall Wang

St. Louis

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

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

William L. Cole

St. Louis

bill.cole@bclplaw.com
+1 314 259 2711