CARTER LEDYARD

our resources

New Cybersecurity Disclosure Rules for Public Companies: Update

January 22, 2024

As we previously reported in July 2023, the U.S. Securities and Exchange Commission (the "**SEC**") adopted new cybersecurity disclosure rules for public companies. The new rules require issuers to promptly disclose the impacts of material cybersecurity incidents and disclose on an annual basis material information regarding cybersecurity risk management, strategy and governance.

The new Form 10-K and Form 20-F disclosures are effective beginning with annual reports for fiscal years ending on or after December 15, 2023. The new Form 8-K and Form 6-K disclosure obligations became effective December 18, 2023 (for smaller reporting companies, the new 8-K/6-K requirements will take effect on June 15, 2024.)

As the heavy annual reports season approaches, we wanted to provide this reminder and update and to point out some recent clarifications from the SEC on several matters that we had previously highlighted.

8-K/6-K Disclosures

Domestic issuers must provide the required cybersecurity incident disclosure on Form 8-K within four business days after the issuer ***determines an incident to be material***.

The deadline is *not* four business days after the incident *occurred* or is *discovered*, but when determined to be material. Nevertheless, the issuer cannot "unreasonably delay" its internal processes for determining materiality. The SEC has indicated that the materiality standard registrants should apply is consistent with that set out in the federal securities laws as well as numerous court cases addressing materiality, which is if there is a "substantial likelihood that a reasonable investor would consider it important" or if it would have "significantly altered the 'total mix' of information made available."

The required disclosure is intended to standardize the information companies disclose about a material cyber incident, and must indicate 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 issuer, including its financial condition and operations. Companies should also consider qualitative factors when assessing the materiality and impact of an incident.

For foreign private issuers ("**FPIs**"), as with other material events, this disclosure must be furnished on Form 6-K promptly after the incident is disclosed or otherwise publicized (or is required to be disclosed or publicized) in a foreign jurisdiction, to any stock exchange, or to security holders.

The National Security Dilemma

As we explained, in the final rule, the SEC provided for delayed reporting of cybersecurity incident disclosures that would pose a substantial risk to national security or public safety, contingent on a written notification by the Attorney General, who may take into consideration other Federal or other law enforcement agencies' findings.

Since then, the Department of Justice (the "**DOJ**") issued guidelines describing the process an issuer should follow to obtain a delay and the procedures the Attorney General will use to evaluate whether a delay is warranted. According to the guidelines, if believed to be applicable, issuers need to contact the FBI and convey in their report a concise description of the facts forming the basis of the issuer's belief that the cybersecurity incident disclosure required under Form 8-K or 6-K may pose a substantial risk to national security or public safety.

The SEC clarified that the mere fact that an issuer consulted with the DOJ or the FBI does not automatically mean that the incident was material, and that the determination of whether an incident is material is based on all relevant facts and circumstances surrounding the incident. Consulting with the DOJ, the FBI or any other law enforcement agency (which would appear to also include foreign agencies) before the materiality assessment is completed, is perfectly fine.

FPIs are not part of the delaying process through the DOJ which relates to the four business days' requirement of Form 8-K. Generally, while FPIs may choose to additionally follow the 8-K model, Form 6-K disclosure of a cybersecurity incident is required only if an FPI first makes (or is required to make) a home jurisdiction disclosure of a cybersecurity incident, and such information is material. For example, in the European Union, the General Data Protection Regulation (GDPR) requires disclosure of cybersecurity breaches.

Board Cybersecurity Expertise

As a reminder, in contrast to the initially proposed rules, the final rules do *not* require issuers to disclose whether any members of their board of directors have cybersecurity expertise. The final rule's disclosure requirement regarding the board focuses on describing the board's oversight of risks from cybersecurity threats, and, if applicable, identifying any relevant board committee or subcommittee and describing how the board or such committee is informed of such risks.

Cybersecurity Policies and Procedures (risk management, strategy, and governance relating to cybersecurity)

Similarly, instead of having a strict requirement to disclose the issuer's cybersecurity policies and procedures as well as certain specific details regarding those policies and procedures, the final rule focused more broadly on the issuer's cybersecurity processes and includes a non-exclusive list of disclosure items.

The SEC recognized that issuers have diverse approaches to cybersecurity, based on their particular circumstances, and that not every issuer needs formal policies and procedures. It will be interesting to compare these approaches in the upcoming annual reports, i.e., the new Item 1C to Form 10-K and Item 16K to Form 20-F, both requiring issuers to disclose certain information regarding their risk management, strategy, and governance relating to cybersecurity.

Recent Filings by Issuers

While most of the first annual reports filed to date (after December 15) have not included anything regarding these items (many have indicated "not applicable"), some issuers have already started populating these items in the following ways:

- Managing Material Risks & Integrated Overall Risk Management – description of the issuer's policies and approach to dealing with risks and engaging with experts and third parties if applicable;
- Management's Role Managing Risk and Risk Management Personnel – description of the role of the Chief Information Security Officer (CISO), the CFO or any other officers in dealing with incidents, frequency of cybersecurity risk meetings and updates;
- Monitoring Cybersecurity Incidents – description of chain of command, security measures and audits to identify potential vulnerabilities;

- Board of Directors Oversight – description of the board's role, general expertise within the board or audit committee, and the procedures regarding reporting of incidents to the board.

Conclusion

Issuers shall consult with counsel and think through carefully how to formulate the new disclosures in the Form 10-K and 20-F reports, as well as ensure that policies and controls are in place to meet the new specific disclosure obligations on Form 8-K or 6-K.

The SEC indicated it will be open to questions and discussions regarding these matters, especially in this first year following adoption and effectiveness of the new rules.

---

related professionals

Guy Ben-Ami / Partner
D 212-238-8658
benami@clm.com

Matthew D. Dunn / Partner
D 212-238-8706
mdunn@clm.com

Steven J. Glusband / Partner
D 212-238-8605
glusband@clm.com