Checklist: Form 10-K Disclosure — Cybersecurity

By TheCorporateCounsel.net

1. **The SEC's 2023 Cybersecurity Disclosure Rules:** In July 2023, the SEC adopted rule and form changes regarding cybersecurity reporting by public companies. Specifically, under a new "Item 1C. Cybersecurity" in Part I of Form 10-K, the new rules require companies to disclose information regarding cybersecurity risk management, strategy and governance pursuant to new Item 106 of Regulation S-K. The required information must be tagged using Inline XBRL (beginning one year after the initial compliance date).

   Item 106(b) of Regulation S-K requires a company to describe its processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing this disclosure, a company should address, as applicable, the following nonexclusive list of disclosure items:

   - Whether and how any such processes 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; and
   - Whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

   Under these new requirements, a company must also describe 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, including its business strategy, results of operations or financial condition, and, if so, how.

   Per Item 106(a) of Regulation S-K:

   - A "cybersecurity threat" means any potential unauthorized occurrence on or conducted through a company's information systems that may result in adverse effects on the confidentiality, integrity or availability of a company's information systems or any information residing therein;

- A "cybersecurity incident" means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a company's information systems that jeopardizes the confidentiality, integrity or availability of a company's information systems or any information residing therein; and

- "Information systems" means electronic information resources, owned or used by the company, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of the company's information to maintain or support the company's operations.

Item 106(c) of Regulation S-K provides that a company must describe the board of directors' oversight of risks from cybersecurity threats in the Form 10-K. If applicable, a company must identify any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the processes by which the board or such committee is informed about such risks. A company must also describe management's role in assessing and managing the company's material risks from cybersecurity threats. In providing such disclosure, a company should address, as applicable, the following nonexclusive list of disclosure items:

- 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, a committee or a subcommittee of the board of directors.

Relevant expertise of management may include, for example, prior work experience in cybersecurity, any relevant degrees or certifications, and any knowledge, skills or other background in cybersecurity (this disclosure appears to contemplate disclosure about positions, rather than specifically identifying individuals by name).

While not a Form 10-K disclosure requirement, note that the rules also added a new Form 8-K triggering event in Item 1.05 that requires companies to disclose (with limited exceptions), any cybersecurity incident that a company experiences that is determined to be material within four business days after such materiality determination.

The final rules are effective September 5, 2023. All companies must provide the disclosures newly required by Item 106 of Regulation S-K beginning with annual reports for fiscal years ending on or after December 15, 2023.

2. **SEC Disclosure Guidance:** In October 2011, SEC Staff issued disclosure guidance for cybersecurity risks and cyber incidents in the form of CF Disclosure Guidance: Topic No.2 "Cybersecurity." The SEC also issued a "Statement & Guidance on Cybersecurity Disclosures" in February 2018. The guidance didn't create new disclosure obligations, but it emphasizes that existing disclosure requirements must be applied to the cybersecurity arena.

   In December 2019, Corp Fin issued CF Disclosure Guidance: Topic No. 8 that provides guidance on disclosure obligations that companies should consider regarding intellectual property and technology risks that may occur when they have international operations. The guidance says that it may be particularly applicable when international jurisdictions don't have comparable levels of protection of corporate proprietary information such as intellectual property, trademarks, trade secrets, know-how and customer information and records.

   While certain aspects of the prior interpretive guidance have now been incorporated into SEC's rules (in particular, the construct for current reporting on Form 8-K), companies still must consider that guidance in determining what to disclose under items that were not amended with this latest rulemaking effort, including those items discussed below. As always, material information about cybersecurity risks and cyber incidents is required to be disclosed when necessary in order to make other required disclosures, in light of the particular circumstances, not misleading.

   - **Risk Factors:** Companies should disclose the risk of cyber incidents if the issues are "among the most significant factors that make an investment in the company speculative or risky." Cybersecurity risk disclosures must adequately describe the nature of the material risks and specify how each risk affects the company, and particular care must be taken to avoid characterizing a risk as hypothetical if it has in fact occurred (including in

connection with reviewing risk factors each quarter to determine if updates are needed since the 10-K disclosure).

- **Legal Proceedings:** If the company is involved in a material pending legal proceeding that involves a cyber incident, it should disclose information about the litigation in accordance with Item 103 of Regulation S-K.

- **MD&A:** Companies should address cybersecurity risks and cyber incidents in their MD&A if the costs of ongoing cybersecurity efforts or the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend or uncertainty that is reasonably likely to have a material favorable or unfavorable impact on net sales or revenues or income from continuing operations or reasonably likely to cause reported financial information not to be necessarily indicative of future operating results or of future financial condition.

- **Financial Statements:** The guidance addresses a number of situations in which cybersecurity risks and cyber incidents could impact financial statement disclosures — depending on the nature and severity of the actual or potential incident. And, the SEC expects companies to consider the impact of cyber incidents on each of their reportable segments.

- **Disclosure Controls and Procedures:** A cyber incident may affect the company's conclusion about the effectiveness of its disclosure controls and procedures, and thus the associated Item 307 of Regulation S-K disclosure.

See our "Risk Factors Disclosure," "MD&A," "Materiality" and "Legal Proceedings Disclosure" handbooks posted on TheCorporateCounsel.net.

3. **Disclosure Considerations:** Based on the SEC Staff's discussion of particular situations that may give rise to disclosure in one or more areas of a filing, consider these factors in determining whether and to what extent disclosure may be warranted:

   - Prior cyber incidents
   - Severity and frequency of prior incidents
   - Probability of occurrence of cyber incidents

- Quantitative and qualitative magnitude of potential cyber incidents
- Potential costs and other consequences resulting from cyber incidents, including reputational risk
- Costs associated with maintaining cybersecurity protections — *e.g.*, insurance coverage or payments to service providers
- Adequacy of preventative actions taken to reduce cybersecurity risks in the context of the company's industry (including insurance coverage limits as compared to potential costs)
- Risks to company's cybersecurity processes, practices, etc., including known threatened attacks
- Risks of outsourced functions that have material cybersecurity risks, and how the company addresses those risks
- Cyber incidents the company experienced that are individually — or in the aggregate — material, including a description of costs and other consequences (if a material attack has occurred, simply discussing risks of an attack without disclosure of the occurrence is likely inadequate)
  - Note that, in connection with the cybersecurity rules, the Commission omitted from the final rules a proposed requirement that contemplated periodic disclosure of aggregated immaterial cybersecurity incidents that were deemed to be material, while adopting a definition of "cybersecurity incident" that extends to "a series of related unauthorized occurrences," recognizing that cybersecurity incidents sometimes compound over time, rather than present as a discrete event
- Risks related to cyber incidents that may remain undetected for an extended period
- Pending legal proceedings, regulatory investigations and remediation costs involving cyber incidents
- Existing or pending laws and regulations that may affect cybersecurity requirements and costs for the company

- Cyber incidents that impact the company's ability to record, process, summarize and report information required to be disclosed in its filings such that the disclosure controls and procedures may be ineffective

- Any other relevant information

4. **Topic of SEC Scrutiny:** Even prior to the final 2023 cybersecurity disclosure rules, the SEC has made cybersecurity risk a top disclosure priority. The SEC has sent numerous comment letters about the adequacy of their disclosures — most commonly in relation to Risk Factors and/or MD&A. Here's one example:

> "We note your disclosure that an unauthorized party was able to gain access to your computer network 'in a prior fiscal year.' So that an investor is better able to understand the materiality of this cybersecurity incident, please revise your disclosure to identify when the cyber incident occurred and describe any material costs or consequences to you as a result of the incident. Please also further describe your cyber security insurance policy, including any material limits on coverage."

The Staff has repeatedly indicated that companies should avoid boilerplate cybersecurity disclosures and instead should include such information as:

- Aspects of the business that are subject to risks,

- Updates for new information, and

- Cost estimates — if possible and material

So, companies shouldn't state that there is a hypothetical risk of a cybersecurity breach after the occurrence of an actual cyberattack. Rather, they should disclose that they have experienced security breaches or attacks. However, this doesn't mean that disclosures need to be so detailed that they constitute a "roadmap" that would further expose a company to cyberattacks.

In addition, Corp Fin Staff may monitor information outside a company's filings (for example, provided in regulatory or contractual notices) and ask why certain cyber incidents are not disclosed. And a company may be asked to confirm that it has disclosed the occurrence of material cyber incidents. Annual reports on comment letters are available in our "SEC Comment Process" Practice Area on TheCorporateCounsel.net.

5. **Disclosure Becoming More Common:** In addition to the SEC's emphasis on this topic, companies have become more reliant on cloud-based technology and high-profile breaches have proliferated.

   According to benchmarking surveys available in the "Risk Factors" and "Cybersecurity" practice areas on TheCorporateCounsel.net, nearly all companies now cite cybersecurity as a risk factor — particularly large companies and organizations in the financial services, health care and real estate sectors. Here are some other takeaways:

   - Companies that discuss cyber risks often cite financial exposure, reputational and operational disruptions
   - Many companies indicate that third-party vendors increase their vulnerability
   - Companies also site the increased level of sophistication and volume of attacks — which make it more difficult to predict the impact of a future breach — and describe the intersection with their commitment to data privacy

6. **Impact of Other Disclosure Requirements:** Most companies that experience a data breach will have to comply with notice and/or disclosure requirements under applicable state and foreign laws. All 50 states have data breach notification laws. The EU's Market Abuse Regulation applies to U.S. companies with debt, equity or other securities admitted to trading on EU-regulated markets, multilateral trading facilities or EU-organized trading facilities.

   The GDPR applies to U.S. companies with an operational or jurisdictional presence in the EU — and some states have adopted or are considering similar regulations. Companies may also be subject to contractual arrangements that require disclosure.

   Companies that provide regulatory or contractual notices should consider whether their shareholders will be able to access that information. That would weigh in favor of disclosing the event to all shareholders in an SEC filing, unless it's clearly immaterial. One reason for this is FD compliance — required state law notices are usually publicly available, and can provide savvy investors and analysts with leg up unless efforts are made to disseminate the information more broadly.

As the risks associated with cybersecurity and number and magnitude of cyber incidents have increased, the need for prevention, mitigation and response measures has also increased. See our separate checklists on "Cybersecurity — Incident Response Planning" and "Risk Management — Cybersecurity."

Learn more in the "Cybersecurity" Practice Area on TheCorporateCounsel.net.