Published on *The National Law Review* https://natlawreview.com

Don’t Forget to Put SEC Cybersecurity Matters on Your Board Agenda This Fall!

Article By:

Sharon R. Klein

Yelena M. Barychev

Karen H. Shin

The U.S. Securities and Exchange Commission (“SEC”) earlier this year adopted rules requiring public companies to provide enhanced disclosure of material cybersecurity incidents, as well as cybersecurity risk management, strategy, and governance. The deadlines for providing these disclosures are fast approaching. In addition, on October 30, 2023, the SEC filed charges against SolarWinds Corp. (“SolarWinds”) and its chief information security officer (“CISO”) for fraud and internal control failures relating to allegedly known cybersecurity risks and vulnerabilities. These new SEC rules and the SEC’s complaint against SolarWinds and its CISO underscore the fact that cybersecurity is an overall business issue, not just an IT problem, which demands proactive and ongoing attention by a company’s officers and directors.

The SEC’s complaint against SolarWinds alleges that, from its October 2018 initial public offering through its December 2020 announcement that it was the target of a nearly two-year long massive cyberattack, SolarWinds and its CISO defrauded investors by overstating SolarWinds’ cybersecurity practices and understating or failing to disclose known risks. The SEC’s complaint alleges that SolarWinds and

its CISO violated the antifraud provisions of the Securities Act of 1933 and of the Securities Exchange Act of 1934, that SolarWinds violated reporting and internal controls provisions of the Exchange Act, and that the CISO aided and abetted the company's violations. In addition to seeking permanent injunctive relief, disgorgement with prejudgment interest, and civil penalties against both SolarWinds and its CISO, the complaint seeks to permanently bar the CISO from serving as an officer or director of any public company in the United States.

What Must Be Disclosed and When?

Material Cybersecurity Incidents. A cybersecurity incident[1] must be disclosed in the Current Report on Form 8-K within four business days after the company determines that the cybersecurity incident it has experienced is **material**. Foreign private issuers are also required to file Form 6-K with respect to material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders. All companies, other than smaller reporting companies, must begin complying with the incident disclosure requirements in Form 8-K and in Form 6-K beginning on **December 18, 2023**. Smaller reporting companies must begin complying with such Form 8-K disclosures on June 15, 2024.

Cybersecurity Risk Management. A company's processes to assess, identify, and manage material cybersecurity risks, management's role in such processes, and the board of directors' oversight of cybersecurity risks must be disclosed in an Annual Report on Form 10-K or Form 20-F (for foreign private issuers) **for the fiscal years ending on or after December 15, 2023**.

What to Do Now?

1. ***Companies must create appropriate disclosure controls and procedures to ensure that information regarding material cybersecurity incidents is recorded, processed, summarized, and reported within the time periods specified in Form 8-K***.

The company's disclosure controls and procedures must also ensure that information about the nature, scope, and timing of the cybersecurity incident and its material impact, or reasonably likely material impact, on the company is accumulated and communicated to the company's management to allow timely decisions regarding required Form 8-K disclosure. For example, a company should re-evaluate the composition of its disclosure committees to make sure that the company's information security officer or other representatives of the company's information technology and cybersecurity teams are part of the committee to discuss information about cybersecurity incidents and facilitate the determination of which incidents would be considered material.[2] In its SolarWinds case, the SEC has claimed that the company violated its obligation to maintain appropriate disclosure controls and procedures, with the CISO aiding and abetting such violation though his false sub-certifications and his failure to elevate or disclose to upper management certain cybersecurity incidents.

2. ***Companies should adjust, as necessary, their internal control over financial reporting***. Public companies are required to maintain an internal control over financial reporting designed to provide reasonable assurance regarding the reliability of the company's financial reporting, including reasonable assurance regarding prevention or timely detection of unauthorized use of the company's assets that could have a material effect on its financial statements. A company's software is part of its assets, and the company must design a system of internal accounting controls sufficient to provide reasonable assurance that access to such assets is permitted only in accordance with management's authorization. In SolarWinds' complaint, the SEC alleged that the CISO was aware of SolarWinds' cybersecurity risks and vulnerabilities but failed to resolve the issues or, at times, sufficiently raise them further within the company. As a result, SolarWinds allegedly could not provide reasonable assurances that its most valuable assets, including its flagship software product, were adequately protected, and its CISO allegedly aided and abetted SolarWinds' failure to devise and maintain a system

of appropriate internal controls.

3. ***Companies should finetune their cybersecurity risk management process and strategy***. Regardless of whether or not the company had a security incident, it must disclose in its annual report its processes for assessing, identifying, and managing material risks from cybersecurity threats[3] in sufficient detail for a reasonable investor to understand those processes. For example, companies may want to disclose not only whether any such processes have been integrated into the company's overall risk management system, but also whether the company engages consultants or other third parties in connection with any such processes, as well as whether the company has processes to oversee and identify risks from cybersecurity threats associated with its use of any third-party service provider. In addition, companies also need to disclose in their annual reports 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.
4. ***Companies should re-evaluate their governance related to cybersecurity matters***. Companies must describe in their annual reports the board of directors' oversight of risks from cybersecurity threats, as well as the processes by which the board or board committee is informed about such risks. In addition, companies must disclose in such annual reports the management's role in assessing and managing the company's material risks from cybersecurity threats. The SEC suggested that disclosures about the management's process may address which management positions or committees are responsible for assessing and managing cybersecurity risks, including the relevant expertise of such persons, as well as the processes by which they monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents, and who reports information about such risks to the board of directors or a committee or of the board of directors.
5. ***Companies should start developing templates of***

cybersecurity disclosures. Disclosures regarding material cybersecurity incidents and companies' risk management processes will require careful drafting. It is a delicate balance to timely disclose material information without unintentionally exposing weaknesses in a company's cybersecurity profile that could be further exploited by malicious actors. Companies should avoid sugarcoating the vulnerability of their information systems. The SEC's complaint against SolarWinds alleged that, in its filings with the SEC, SolarWinds "misled investors by disclosing only generic and hypothetical risks" at a time when the company and its CISO "knew of specific deficiencies in SolarWinds' cybersecurity practices as well as the increasingly elevated risks the company faced at the same time."

6. ***Companies should revisit their processes for managing supply chain cybersecurity risk***. In order for public companies to make disclosures mandated by the new rules, the SEC cybersecurity requirements must flow down in contracts to companies' suppliers and partners to ensure communication, transparency, and collaboration about cybersecurity risks in the supply chain. Contracts will require representations about the suppliers' cyber maturity and potentially termination of contracts in the event of a cyber incident caused by noncompliance.

---

[1] The SEC defines the term "cybersecurity incident" as 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. (See Item 106(a) of Regulation S-K)

[2] The SEC provided guidance related to materiality determinations in its final release related to cybersecurity rules and pointed out that, under U.S. securities laws, materiality "turns on how a reasonable investor would consider the incident's impact" on the company. The SEC also reminded companies that "the material impact of an incident may

encompass a range of harms, some quantitative and others qualitative," and that a "lack of quantifiable harm does not necessarily mean an incident is not material." For example, an incident that results in significant reputational harm to a company may not "cross a particular quantitative threshold, but it should nonetheless be reported if the reputational harm is material." Also, a cybersecurity incident that "results in the theft of information may not be deemed material based on quantitative financial measures alone," but it may be material given the impact "results from the scope or nature of harm to individuals, customers, or others, and therefore may need to be disclosed."

[3] The term "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. (See Item 106(a) of Regulation S-K)

National Law Review, Volume XIII, Number 312