Proskauer

SEC Issues Updated Guidance on Public Company Cybersecurity Disclosures

March 5, 2018

On February 21, 2018, the Securities and Exchange Commission (SEC) issued an interpretive Commission Statement and Guidance on Public Company Cybersecurity Disclosures (the "Guidance") to assist public companies in meeting their cybersecurity disclosure requirements under the federal securities laws.[i] The Guidance notes that, as reliance on networked systems and the Internet have increased, so too have the risks and frequency of cybersecurity incidents, and companies have no choice but to incur the considerable costs of addressing information security risks, particularly in the wake of a cybersecurity incident. Examples of such costs include IT costs, employee training, remediation expenses, litigation, agency investigations and enforcement actions, reputational harm and damage to long-term shareholder value.

Within this context, the Guidance instructs public companies to:

- inform investors of material cybersecurity risks and incidents, and the related actual or potential costs and consequences, in compliance with the federal securities laws;
- implement comprehensive disclosure controls and procedures to enable companies to make accurate and timely cybersecurity disclosures; and
- guard against insider trading risks and selective disclosures in the context of cybersecurity incidents.

This latest Guidance builds on prior guidance issued by the SEC's Division of Corporation Finance in October 2011, offering an SEC-level endorsement and expansion of those views and highlighting the SEC's continued attention to cybersecurity risks. The Guidance goes further than the 2011 guidance because (i) it is issued directly by the SEC, rather than the staff, and (ii) it squarely addresses disclosure controls and procedures and restrictions against insider trading and selective disclosures in the cybersecurity context. That said, the Guidance tracks the substance of the 2011 guidance closely, without imposing new or unexpected standards on public companies. However, statements made by Commissioner Kara M. Stein and Commissioner Robert J. Jackson Jr., among others, regarding the Guidance suggest that SEC rule-making or other stronger actions on cybersecurity could be on the horizon.

Disclosure Obligations

According to the SEC, it is "critical" for public companies to disclose material cybersecurity risks and incidents, and the related potential or actual costs and consequences, in registration statements and periodic and current reports. These disclosure requirements may impact: (i) risk factors, (ii) management's discussion and analysis of financial condition and results of operations (MD&A), (iii) description of business, (iv) legal proceedings, (v) financial statement disclosures and (vi) board's role in risk oversight.

The SEC emphasizes that cybersecurity disclosures should be specific and tailored to each company, avoiding generic or boilerplate language. However, the SEC stresses that the Guidance should not be interpreted to require disclosures so specific or technical that they provide a "roadmap" for cyberattackers to exploit vulnerabilities or that could otherwise compromise the company's cybersecurity efforts.

In determining the materiality of cybersecurity risks and incidents, companies should take into account the following factors, among others:

- the nature, extent and potential magnitude of the cybersecurity risk or incident;

- the potential range and degree of harm that may stem from the cybersecurity risk or incident, including financial, legal and reputational consequences;

- the importance and scope of the information comprised by a cybersecurity incident; and

- the actual or potential impact of a cybersecurity incident on the company's operations.

Such disclosures must be made on a timely and ongoing basis. In particular, the SEC states that a company may be required to disclose a material cybersecurity incident before internal or external investigations of the incident have been completed. Moreover, companies may have a duty to correct or update certain prior disclosures for accuracy and completeness – for example, where new or different information has come to light in the course of investigating a previously disclosed cybersecurity incident.

The SEC cautions against material omissions in this context, and considers omitted information to be material "if there is a substantial likelihood that a reasonable investor would consider the information important in making an investment decision or that disclosure of the omitted information would have been viewed by the reasonable investor as having significantly altered the total mix of information available."

Disclosure Controls and Procedures

The SEC emphasizes the "crucial" nature of comprehensive internal controls and procedures that enable companies to comply with cybersecurity disclosure requirements in the appropriate timeframe. Such controls and procedures should be designed to ensure that adequate information is reported internally to the right employees to enable senior management to make timely and sound decisions about disclosing cybersecurity risks and incidents. For example, such controls and procedures should:

- require employees to appropriately record, process, summarize and report up the corporate ladder any information related to cybersecurity risks and incidents that is potentially required to be disclosed in public filings;

- enable open communications between technical experts and disclosure advisors; and

- provide an appropriate method of discerning the potential impact and materiality of cybersecurity matters to the company and its business, financial condition and operations.

The SEC states that the requirements for disclosure decisions and certifications by senior management also apply to cybersecurity risk disclosure controls and procedures. Under these requirements, management must evaluate and make certifications regarding the design and effectiveness of disclosure controls and procedures, and companies must disclose the conclusions regarding their effectiveness as well.

In this context, companies should regularly assess the scope and effectiveness of the cybersecurity disclosure controls and procedures they have in place and, as needed, adopt and implement more comprehensive controls and procedures to address any deficiencies.

Safeguards Against Insider Trading and Selective Disclosure

Through the Guidance, the SEC reminds companies of risks related to insider trading and selective disclosure in the context of cybersecurity. Information about a company's cybersecurity risks and incidents may be "material nonpublic information" within the meaning of federal restrictions on insider trading or selective disclosures under Regulation FD.

If a company learns of a cybersecurity incident or risk that may be material to its investors, the SEC expects the company to take steps to prevent directors, officers and other corporate insiders aware of these matters from trading the company's securities until investors have been appropriately informed about the incident or risk. The SEC suggests that companies adopt appropriate insider trading policies and procedures that address these circumstances, which may include insider trading restrictions while companies are investigating and assessing cybersecurity incidents and similar protections to avoid the appearance of improper trading prior to public disclosure of an incident.

Similarly, the SEC advises that companies should not disclose any material nonpublic information related to its cybersecurity risks and incidents to Regulation FD enumerated persons until it has publicly disclosed the same information.

---

[i] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures*, Release Nos. 33-10459; 34-82746.

Related Professionals

- **Laura E. Goldsmith**
  Partner