WINSTON & STRAWN LLP

CLIENT ALERT

SEC Releases Enhanced Guidance on Cybersecurity Disclosure for Public Companies

MARCH 5, 2018

On February 21, 2018, the Securities and Exchange Commission ("SEC" or "Commission") unanimously approved interpretive guidance for public companies regarding disclosures of cybersecurity risks and incidents.[1] The interpretive release raises to the Commission level the previously issued guidance of the Commission's staff and highlights the focus of the Commission on cybersecurity issues under Chairman Clayton's tenure.

The interpretive release reinforces and expands the prior guidance issued by the staff of the SEC's Division of Corporation Finance in 2011, and addresses two additional topics not addressed in the staff's 2011 guidance: the importance of cybersecurity policies and procedures and the application of insider trading and selective disclosure prohibitions in the cybersecurity context.

The interpretive guidance suggests that companies should take a more expansive view of cybersecurity risks and incidents and their potential consequences beyond just disclosure considerations, including as they relate to the company's policies and procedures and reputation, and should:

- Expand disclosures to consider not only future cybersecurity risks and incidents, but also past incidents, to put the disclosures in proper context;
- Consider the materiality of information with respect to cybersecurity risks and incidents as it relates to specific disclosure requirements, as well as from a general 10b-5 anti-fraud perspective;
- Take into account cybersecurity risks and incidents in the design and evaluation of their disclosure controls and policies to ensure proper and timely disclosure of information in the company's filings;
- Take measures to restrict trading by insiders based on, or selective disclosure of, information with regard to cybersecurity events between the time of discovery and public disclosure of such events; and
- Consider and disclose, to the extent material, the role of the company's board in overseeing cybersecurity risks for the company.

Overview of Commission Guidance

Disclosures

In the interpretive release, the Commission states its belief that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack. The interpretive guidance reminds public companies that while existing disclosure requirements under the Securities Exchange Act of 1934 and the Securities Act of 1933 may not specifically refer to cybersecurity risks and incidents, a number of items would impose an obligation to disclose cybersecurity risks and incidents, depending on the company's particular circumstances, in its periodic reports (Forms 10-K, 10-Q, 8-K, 20-F and 6-K), its Securities Act registration statements and its proxy statements. In addition to risk factor disclosure, the interpretive guidance addresses potential disclosures in the MD&A, the description of the company's business, legal proceedings, financial statements and discussions of the board's role in risk oversight.

In determining their disclosure obligations regarding cybersecurity incidents and risks, the guidance suggests that companies consider, among other things, the potential materiality of any identified risk and, in the case of an incident, the impact of the incident on its operations and the importance of any compromised data to either the company or its customers. The materiality of cybersecurity risks or incidents will depend on the nature, extent and potential magnitude of the events and the range of harm that such incidents could cause, including reputational harm, financial performance impacts, customer and supplier relationship impacts and the possibility of litigation or state, federal and non-U.S. regulatory investigations or actions. The materiality analysis should consider the long-standing materiality test of assessing the probability that an event will occur and magnitude of such event in relation to the totality of the company's activities.

The guidance clarifies that companies are not required to make detailed disclosures that would compromise their own security efforts or in some way provide a roadmap to hackers for breaching their security protections. While recognizing that cybersecurity incidents may sometimes require prolonged investigations or cooperation with law enforcement, the guidance notes that an ongoing investigation alone is not sufficient grounds for delaying or avoiding disclosure of a material cybersecurity incident. The Commission expects companies to disclose material cybersecurity risks and incidents, including any related financial, legal or reputational consequences, and would expect appropriate disclosure to be made timely and sufficiently in advance of any offer or sale of securities and appropriate steps to be taken to prevent directors, officers and other insiders from trading in a company's securities until public investors have been informed about the relevant cybersecurity incident or risk. The interpretive guidance reminds companies that they may have a duty to correct or update prior disclosures if they were untrue at the time they were made or if they become materially inaccurate in light of subsequent events. In addition, companies should consider whether there is a need to revisit or refresh prior disclosure, especially during the course of investigating a cybersecurity incident.

The guidance provides some specific examples of how cybersecurity risks and incidents should be considered in assessing a company's disclosure obligations:

- In risk factor disclosure, companies may need to disclose previous or ongoing cybersecurity occurrences, as well as other past events, in order to put the discussion of cybersecurity risks in the proper context. For example, it would not be sufficient for a company that has experienced a denial-of-service incident to only disclose a risk that denial-of-service may occur. Rather, the company would need to discuss the prior incident and its consequences to provide contextual disclosure to effectively convey the cybersecurity risk to investors.
- In assessing its financial condition and results of operations in MD&A, the cost of ongoing cybersecurity efforts, the costs and other consequences of cybersecurity incidents and the risks of cybersecurity incidents, as well as other less direct costs associated with cybersecurity issues, could be relevant to a company's disclosures.
- If cybersecurity risks are material to a company's business, the company's discussion of its cybersecurity risk management program and its board engagement with management on such issues in its proxy statement would allow investors to assess how the board is discharging its risk oversight responsibility on cybersecurity matters.

Disclosure Controls and Procedures

The guidance encourages companies to adopt comprehensive policies and procedures related to cybersecurity, which should be assessed regularly for compliance. Companies should assess the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure to ensure that relevant information about cybersecurity risks and incidents is processed and timely reported to the appropriate personnel to enable senior management to make necessary disclosure decisions and certifications and to facilitate policies and procedures to prohibit insider trading on the basis of material nonpublic information about cybersecurity risks and incidents.

In designing and evaluating disclosure controls and procedures for cybersecurity risks and incidents, companies should consider whether these controls and procedures appropriately record, summarize and report information regarding cybersecurity risks and incidents required to be disclosed, and also enable the companies to identify cybersecurity risks and incidents, assess their significance, analyze their impact on the company's business and provide open communication between technical experts and disclosure advisors.

To the extent that cybersecurity risks or incidents may compromise a company's ability to record and process information that may be required to be disclosed, the interpretive guidance advises management to consider whether there are deficiencies in the disclosure controls and procedures that would make them ineffective.

Insider Trading

The interpretive guidance notes that information about a company's cybersecurity risks and incidents may be material nonpublic information. The Commission believes that it is important for companies to have well-designed policies and procedures to prohibit corporate insiders from trading on the basis of all types of material nonpublic information, including with respect to cybersecurity risks and incidents. The Commission encourages companies to consider how their insider trading policies and codes of ethics take into account and prevent trading based on material nonpublic information related to cybersecurity risks and incidents. The Commission believes that companies would be well-served to consider how to avoid any appearance of improper trading between the discovery of a cybersecurity incident and its public disclosure.

Importantly, the guidance makes clear that those prohibitions would not preclude corporate insiders from undertaking transactions pursuant to properly implemented Rule 10b5-1 plans.

Selective Disclosure and Regulation FD

The interpretive release also reminds companies that they also have disclosure obligations under Regulation FD with respect to material information relating to cybersecurity risks and incidents and that companies should not selectively disclose material nonpublic information regarding cybersecurity risks and incidents to Regulation FD enumerated persons before disclosing such information to the public. The Commission expects policies and procedures to be implemented to ensure that any required Regulation FD disclosure is timely made and otherwise in compliance with the regulation.

Conclusion

The interpretive guidance highlights the Commission's view that data management and technology have become so fundamental to business that information about cybersecurity risks and incidents may represent material information for companies operating in all industries, including public companies subject to SEC regulation, and that cybersecurity risks and incidents should be considered in the broader context of not only disclosures, but also disclosure controls and procedures, insider trading policies, selective disclosure regulations and board oversight of risk.

1 https://www.sec.gov/rules/interp/2018/33-10459.pdf

6 Min Read

Related Locations

New York

Related Topics

Securities and Exchange Commission (SEC)

Related Capabilities

Transactions

Capital Markets

Related Regions

North America

Related Professionals

Sey-Hyo Lee