SEC Issues New Interpretive Guidance on Public Company Cybersecurity Disclosures

March 6, 2018 Matthew Fry

PRACTICES Corporate, Capital Markets and Securities, Corporate Governance

On February 21, 2018, the Securities and Exchange Commission (the "SEC") issued interpretive guidance to assist public companies in preparing disclosures concerning cybersecurity risks and incidents. Without creating new disclosure requirements, this guidance reinforces and expands upon the previous guidance released by the SEC's Division of Corporation Finance in 2011,[1] which clarified how companies should consider cybersecurity matters within existing disclosure requirements. In short, the SEC believes it is critical for public companies to timely inform investors about material cybersecurity risks and incidents, and that these risks should be disclosed even if a company has not been the target of a cyber-attack. The new guidance also addresses the importance of cybersecurity policies and procedures within the contexts of a company's disclosure controls and procedures and financial reporting and control systems, and emphasizes the application of insider trading prohibitions in the cybersecurity context.

View a copy of the 2018 interpretive guidance.

Disclosure of Cybersecurity Risks and Incidents

The new guidance does not create new disclosure requirements, and the SEC was careful to say that it does not expect companies to disclose cybersecurity risks in such detail that the disclosures compromise their cybersecurity efforts. However, the guidance reiterates that, within existing disclosure requirements, the SEC expects companies to disclose cybersecurity risks and incidents that are material to investors, including the accompanying financial, legal, or reputational consequences. Disclosure should be tailored to a company's specific cybersecurity risks and incidents, providing relevant and useful information to investors.

While the SEC recognized that an ongoing investigation of a cybersecurity incident may affect the scope and timing of its disclosure, it noted that an ongoing internal or external investigation would not on its own provide the basis for avoiding disclosure that a material incident has occurred.[2] The SEC also stressed that disclosures of material cybersecurity risks and incidents should be made timely and sufficiently in advance of companies' offers and sales of securities, and that companies should take steps to prevent directors and officers, as well as other insiders with knowledge of material cybersecurity incidents or risks, from trading until investors have been appropriately informed.

Largely tracking the 2011 guidance, the SEC provided insight reinforcing and expanding upon how existing disclosure requirements may apply to cybersecurity risks and incidents:

Risk Factors. A company should disclose the risks associated with cybersecurity and cybersecurity incidents if they are among the factors that make an investment in the company's securities speculative or risky. To place risk factor disclosure in context, the SEC stated that companies may need to include disclosure of previous or ongoing cybersecurity incidents.

© 2026 Haynes Boone

The SEC also provided a list of factors that would be helpful to consider in the evaluation of cybersecurity risk factor disclosure, including the following:

- Severity and frequency of historical incidents
- Probability of the occurrence and potential magnitude of incidents
- Adequacy of preventative actions taken
- Whether the nature of the company's business exposes the company to risks and consequences
- Costs of maintaining protection against incidents, including insurance coverage
- Existing or pending laws and regulations that may affect company requirements or costs relating to cybersecurity
- Litigation, regulatory investigation, and remediation costs

Management's Discussion and Analysis of Financial Condition and Results of Operations. Item 303 of Regulation S-K requires companies to disclose material factors affecting their financial results or condition as well as known events, trends and uncertainties that are reasonably likely to have a material effect on their results, liquidity or financial condition. The costs and consequences of ongoing cybersecurity efforts (such as system enhancements or remediation), cybersecurity incidents, and potential incidents, among other matters, should be considered in such analysis. The SEC expects companies to consider these and other impacts of cybersecurity issues on a segment-level basis.

Description of Business. Any material impact cybersecurity incidents or risks have on the company's products, services, relationships with customers or suppliers or competitive condition should be disclosed to investors.

Legal Proceedings. As with any other litigation, material pending legal proceedings concerning cybersecurity incidents should be discussed if the company or a subsidiary is a party.

Financial Statement Disclosures. The SEC expects that financial reporting and control systems be designed to provide reasonable assurance that any information about the range and magnitude of financial impacts that cybersecurity issues may have would be incorporated into financial statements in a timely manner.

Board Risk Oversight. Companies are required to include a discussion in proxy statements concerning the administration of their boards' risk oversight function. To the extent that cybersecurity risks and incidents are material to a company's business, the SEC expects this discussion to include the nature of board oversight in managing cybersecurity risks and incidents.

Cybersecurity Policies and Procedures

Disclosure Controls and Procedures. Companies are required to design and maintain disclosure controls and procedures, and senior management must evaluate their effectiveness and deliver related certifications on a quarterly basis. The guidance encourages companies to adopt comprehensive cybersecurity policies and procedures and to confirm the sufficiency of their

© 2026 Haynes Boone

disclosure controls and procedures in relation to cybersecurity risks and incidents required to be disclosed in filings. The SEC stated that evaluations of the effectiveness of disclosure controls and procedures and Sarbanes-Oxley certifications should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact.

Insider Trading. Information about a company's cybersecurity risks and incidents could constitute material nonpublic information. Companies are encouraged to consider how their codes of ethics and insider trading policies take into account cybersecurity risks and incidents to prevent insider trading. The SEC also cautioned that companies should consider if, and at what time, it would be appropriate to implement trading restrictions on insiders while investigations of significant cybersecurity incidents are ongoing.

Implications

We believe that the SEC's reinforcement of recent staff guidance through the issuance of the interpretive release is indicative of the importance of cybersecurity matters to the SEC. In light of this focus, companies should revisit their disclosures concerning cybersecurity risks and incidents for consistency with the guidance and confirm that their cybersecurity disclosures are up to date. Companies should also confirm that their disclosure controls and procedures, including cybersecurity incident response plans, are designed to adequately identify cybersecurity incidents and assess their impact, and that information concerning cybersecurity incidents is timely communicated to persons responsible for administering insider trading policies.

If you have any questions about this topic, please contact a member of our Capital Markets and Securities Practice Group.

---

[1] CF Disclosure Guidance: Topic No. 2 – Cybersecurity (Oct. 13, 2011).

[2] In footnote 2 of the interpretive guidance release, the SEC cited the definition of the term "cybersecurity incident" from the U.S. Computer Emergency Readiness Team's website as being "[a]n occurrence that actually or potentially results in adverse consequences to … an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences."

© 2026 Haynes Boone