LATHAM & WATKINS LLP

Boardroom Perspectives™

June 1, 2018 | 2329

5 Key Takeaways on Cybersecurity

What directors really need to know about the SEC guidance that has generated so much chatter.

Jennifer C. Archie and Serrin Turner

With so much boardroom attention on cybersecurity, directors continue to focus on the Securities and Exchange Commission (SEC) guidance issued earlier this year and its implications. The guidance adds specific expectations for disclosure controls and incident response procedures, and reiterates prior guidance on disclosure of material cybersecurity risks and incidents.

This issue of *Boardroom Perspectives* outlines five steps for companies to consider in response to the SEC guidance.

1. Disclose the board's role in managing cybersecurity risk

The SEC expects public company boards to sharpen their attention on the "increasingly important area" of cybersecurity risk, and expects to see evidence of that in companies' filings. Companies should discuss "the nature of the board's role" in overseeing cybersecurity risk management so that investors can "assess how a board of directors is discharging its risk oversight" in this area.

Companies may consider updating their proxy statement disclosures to discuss relevant lines of reporting to the board (*e.g.*, whether the company has a Chief Information Officer or Chief Information Security Officer who reports to the board), whether the board has cybersecurity experience, and any other factors relating to how the board oversees cybersecurity risk. The board may delegate cybersecurity risk management to a board committee, typically the audit or risk committee, and the committee's charter may be updated to reflect these responsibilities.

2. Include disclosure review in incident response procedures

The SEC expects response protocols for cybersecurity incidents to include steps for escalating information and evaluating public disclosure and reporting obligations. Public companies must maintain effective disclosure controls to identify incidents when they occur, analyze their business impact, and determine whether incidents require public disclosure. The Chief Executive Officer and Chief Financial Officer must evaluate the effectiveness of the company's disclosure controls and personally certify their conclusions in each periodic report. As a result, the SEC expects cyber response protocols to address public reporting obligations rather than isolating the response function with IT personnel.

Companies may review incident response policies to ensure their full integration with disclosure controls. This would include a process for assessing the severity of a cybersecurity incident, escalating the matter to senior management if appropriate, and involving disclosure experts to determine whether SEC disclosure is required. Incident response plans often include protocols for submitting internal reports of cybersecurity incidents, implementing external communications plans, and assessing the need to impose trading restrictions on company personnel.

3. Mitigate insider trading risks after cybersecurity incidents

The SEC has increased its focus on instances of insider trading during an ongoing cyber incident. Cyber risks and incidents may constitute material nonpublic information, and the new guidance directs companies to "consider whether and when it may be appropriate to implement restrictions on insider trading." The guidance also recommends precautions to avoid Regulation FD violations, by adopting "policies and procedures to ensure that any disclosures of material nonpublic information related to cybersecurity risks and incidents are not made selectively."

Companies may wish to consider updating their insider trading policies and imposing trading restrictions if warranted. Companies may use non-disclosure agreements or appropriate confidentiality language in engagement letters to ensure Regulation FD compliance.

4. Disclose material incidents promptly

The SEC's new guidance reiterates the need to disclose promptly any cybersecurity incidents that are material to investors. While recognizing that "a company may require time to discern the implications of a cybersecurity incident," the SEC warns that "an ongoing internal or external investigation — which often can be lengthy — would not on its own provide a basis for avoiding disclosures." The guidance adds that a company should consider updating its disclosures if further investigation reveals new and material information about the incident.

Companies may not delay disclosure of material information solely because an investigation is continuing. Disclosure will be appropriate once a cybersecurity incident is known to be sufficiently serious to be material to investors. Disclosure should not occur prematurely (*e.g.*, during initial fact-finding or while an uncertain situation remains fluid). However, limited information might affect only the scope of disclosure, not whether disclosure can occur.

5. Avoid generic disclosure

SEC comment letters have repeatedly emphasized, and the new guidance underscores, that companies' disclosures should contain sufficient detail to enable investors to evaluate material cybersecurity risks. Cybersecurity disclosures need provide a roadmap to specific vulnerabilities. However, companies may need to disclose past cybersecurity incidents, including their costs and consequences, "to place discussions of these risks in the appropriate context," according to the guidance.

Companies may avoid generic cybersecurity disclosures by tailoring their disclosures to the specific business, reputational, and legal risks they face from cybersecurity threats. This may take into account the types of data and systems on which they rely and the regulatory environment in which the company operates. Companies may consider disclosure of past incidents to inform investors about the nature of these incidents and the risks they present.

Jennifer C. Archie
jennifer.archie@lw.com
+1.202.637.2205
Washington, D.C.

Serrin A. Turner
serrin.turner@lw.com
+1.212.906.1330
New York

You Might Also Be Interested In

Resources for Boards

Latham Global IPO Guide 2018

Boardroom Perspectives: 5 Steps Towards a Workplace Without Sexual Misconduct

Boardroom Perspectives: 3 Steps FPI Directors Can Take to Oversee Related-Party Transactions

Boardroom Perspectives: How Directors Can Use Sustainability to Drive Value

Boardroom Perspectives™ is a periodic series from Latham's Public Company Representation Practice.

CONTACTS
Richard Butterwick, London
Ryan J. Maierson, Houston
Joel H. Trotter, Washington, D.C.

Unsubscribe and Contact Information

If you wish to update your contact details or customize the information you receive from Latham & Watkins, please visit https://www.sites.lwcommunicate.com/5/178/forms-english/subscribe.asp to subscribe to our client mailings. To ensure delivery into your inbox, please add LathamMail@lw.com to your e-mail address book. If you wish to be removed from our distribution, please click this link, unsubscribe@lw.com, or reply to this message with "Unsubscribe" in the subject line.