SEC Guidance Affirms Need for Board Oversight of Cybersecurity Risks

As cyberattacks increase in frequency and severity, effective oversight by a company’s board of directors is key.

By David M. Lisi, David M. Furbush

TAKEAWAYS

どころ️ A company should disclose the extent of its board of directors’ role in overseeing cybersecurity risks.

どころ️ Over one-fifth of directors are dissatisfied with the quality of cyber-risk information provided to the board by management.

どころ️ Directors should satisfy themselves that procedures are adequate to identify cybersecurity risks and incidents, assess their impact, and ensure timely disclosure of such events.

02.28.18

In a prior client alert, we stated that “In light of evolving rules and jurisprudence concerning public companies’ duties around a data breach or other cyber incident, the board should work with professional service providers, such as its counsel, to perform a thorough review of the company’s cybersecurity policies, processes, vulnerabilities and protections.”

On February 21, 2018, the SEC released its “Commission Statement and Guidance on Public Company Cybersecurity Disclosures” in which, among other things, it affirms the need for board oversight of cybersecurity risks.

According to the statement, SEC regulations “require a company to disclose the extent of its board of directors’ role in the risk oversight of the company, such as how the board administers its oversight function and the effect this has on the board’s leadership structure.” The Commission has previously said that “disclosure about the board’s involvement in the oversight of the risk management process should
provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company.” The statement continues, “we believe disclosures regarding a company’s cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.”

The statement also emphasizes the need for “comprehensive policies and procedures related to cybersecurity,” including procedures to ensure that risks and incidents are reported “up the corporate ladder” when appropriate. Procedures should include procedures for identifying cybersecurity risks and incidents and assessing their impact, appropriate and timely disclosure of such events, correction or updating of prior statements if needed, and protections against insider trading when aware of undisclosed cybersecurity events or their expected consequences.

In a recent survey of its members, the National Association of Corporate Directors found that less than half (49 percent) are confident or very confident in the ability of management to address cyber risk, and more than one-fifth of directors (22 percent) expressed dissatisfaction with the quality of cyber-risk information provided to the board by management. In light of the increasing frequency and severity of cyberattacks, the increased public frustration with poor protection of personal information and delayed or incomplete reporting of data breaches, and the increased emphasis this issue is now receiving from lawmakers and regulators, these statistics should be seen as unacceptable.

Our prior client alert sought to offer constructive guidance on how boards can exercise effective oversight in this important area, and to either gain confidence in management’s ability to manage cyber-risks or implement improvements where needed.

*A version of this alert was originally published as a guest post in the* D&O Diary.

For additional information on cybersecurity matters, please visit Pillsbury’s Cybersecurity and the Law website.