Akin®

Boards of Directors Charged with Cybersecurity Risk Management by SEC Commissioner

Jun 20, 2014

Reading Time : **2 min**

To address these concerns, Commissioner Aguilar outlined the role of boards of directors in monitoring cybersecurity risk management. Directors owe a fiduciary duty to their shareholders and have a significant role in overseeing the risk management of the Company. Post-financial crisis, the Commission emphasized the board's role in overseeing risk management, without mandating any particular structure. Instead, the Commission noted that "risk oversight is a key competence of the board" and 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." *See Proxy Disclosure Enhancements, SEC Rel. No. 33-9089 (Dec. 16, 2009), 74 Fed. Reg. 68334*.

Commissioner Aguilar then focused on what the boards of directors can and should be doing to oversee cyber-risk, including:

- reviewing the cybersecurity framework issued by the National Institute of Standards and Technology ("NIST")
- considering structural changes to the board to focus on cyber-risk management
- creating and defining internal roles and responsibilities focused on cyber-risk
- preparing for a cyber-attack and resulting fallout.

NIST was the starting point suggested by Commissioner Aguilar. See *NIST Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014) (the "NIST Cybersecurity*

Framework"). He indicated that directors should review the framework and evaluate how company-wide cybersecurity policies match up with the framework.

Recognizing that not all directors have the technical expertise to evaluate the NIST framework, Commissioner Aguilar noted that companies may consider mandatory cyber-risk education for directors or nominate an adequate representation of directors with a "good understanding of information technology issues that pose risks to the company." Alternatively, companies may consider establishing an enterprise risk committee, similar to that mandated for financial institutions by Dodd-Frank. "Such committees can foster a 'big picture' approach to company-wide risk that not only may result in improved risk reporting and monitoring for both management and the board, but also can provide a greater focus—at the board level—on the adequacy of resources and overall support provided to company executives responsible for risk management."

Companies should also consider hiring a full-time privacy or security officer or "at a minimum" have a "clear understanding of who at the company has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber-risk management practices."

The SEC appears to be setting a customized standard for board preparedness: "boards should put time and resources into making sure that management has developed a well-constructed and deliberate response plan that is consistent with best practices for a company in the same industry." Companies must be prepared to respond "within hours, if not minutes, of a cyber-event to detect the cyber-event, analyze the event, prevent further damage from being done, and prepare a response to the event." Commissioner Aguilar emphasizes that this should include the decision on whether and how to disclose a cyber-attack internally and externally to customers and investors. See *CF Disclosure Guidance: Topic No. 2*. He concluded, "Although different companies may choose different paths, ultimately, the goal is the same: to prepare the company for the inevitable cyber-attack and the resulting fallout from such an event."

Categories

Capital Markets | Special Situations | Cybersecurity, Privacy & Data Protection | Compliance