WILMERHALE

Addressing Cybersecurity Oversight in Audit Committee Charters

APRIL 29, 2015

Cybersecurity continues to emerge as a key risk that is attracting the attention of regulators and boards of directors. Companies take different approaches regarding how the board fulfills its oversight duty with respect to cybersecurity/data privacy risks. KPMG's 2015 Global Audit Committee Survey reports that among United States companies, 43% assign the greatest responsibility for cybersecurity risks to the audit committee, 40% to the full board, 7% to the risk committee, 4% to the technology committee, 3% to the audit and risk or finance committee, and 3% to other committees.

A growing number of companies are revising their audit committee charters to reflect the audit committee's cybersecurity oversight responsibilities. In the course of surveying the audit committee charters of 62 S&P 500 companies, we identified 18 companies whose audit committee charters include specific duties for the oversight of privacy and data security risks. The 18 companies from the sample represent the following industries: consumer discretionary, energy, financials, health care, industrials, information technology, telecommunications services, and utilities. (See the Survey Results.)

We identified three general approaches taken by companies who refer to cybersecurity oversight in the audit committee charter: (i) a detailed section describing the audit committee's duties related to privacy and data security, (ii) a brief sentence describing the audit committee's duties related to privacy and data security, or (iii) a short clause accompanying the audit committee's general risk management duties. Companies tended to follow the latter two approaches with greater frequency.

With cybersecurity continuing to be focused on as a key risk area, boards should review their specific approach to oversight of this risk and, where applicable, should examine the role of the audit committee in coordinating with management and the entire board for assessing and responding to cybersecurity threats. In addition, companies should compare their corporate governance framework for handling cybersecurity risks with industry practices and available regulatory guidance. Financial services firms, in particular, should consider FINRA's 2015 Report on Cybersecurity Practices, which outlines a risk management approach for preventing and responding to cybersecurity threats. As cybersecurity threats continue to emerge and investors increasingly indicate they want to see evidence that the board is being proactive with respect to

overseeing management of the risk, more boards may decide to revise their audit committee charters to address the audit committee's specific responsibilities for the oversight of cybersecurity risks.

Authors

Alan J. Wilson

PARTNER

alan.wilson@wilmerhale.com

+1 202 663 6474

Jonathan Wolfman

PARTNER

Co-Chair, Corporate Governance and Disclosure Group

jonathan.wolfman@wilmerhale.com

+1 617 526 6833