Davis Polk

Commissioner Aguilar Urges Boards to Ensure Oversight of Cybersecurity Risks

June 12, 2014 | Client Update | 2-minute read

The recent announcement that ISS has recommended against the election of the board of directors of Target because of the perceived failure to provide appropriate management of cyber-risk should "put directors on notice to proactively address the risks associated with cyber-attacks," according to Commissioner Luis Aguilar in a **recent speech**.

Commissioner Aguilar discussed what boards should do to ensure that their organizations are appropriately considering and addressing cyber-risk, as there can be little doubt that cyber-risk, and a company's cybersecurity measures, must be considered as part of a board's overall risk oversight. He warned that boards that choose to ignore or minimize the importance of cybersecurity oversight responsibility do so at their own peril, in light of the litigation risk. According to data he cited, evidence suggests that boards are not spending enough time on, or devoting sufficient corporate resources to, key oversight activities such as reviewing annual budgets for privacy and IT security programs, assigning roles and responsibilities for privacy and security, and receiving regular reports on breaches and IT risks.

Commissioner Aguilar strongly recommended that companies consider the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology in February 2014, which is intended to provide companies with a set of industry standards and best practices for managing their cybersecurity risks. As some have suggested that it will become a baseline for best practices by companies, the Commissioner believes that boards should work with management to assess their corporate policies against the guidelines.

In addition, since many boards lack expertise, directors may need "mandatory cyber-risk education" or members with an understanding of information technology issues. Another possibility is to create a separate enterprise risk committee. Boards must also confirm that companies have appropriate risk personnel, who would provide regular reports to the board, such as a full-time chief information security officer. Even without a dedicated individual, boards should have a clear understanding of who has primary responsibility for cybersecurity risk management at the company.

Since the speed with which the company must respond to a cyber-attack distinguishes it from other crises, Commissioner Aguilar encouraged boards to ensure that management has developed a well-constructed and deliberate response plan, including whether and how the cyber-attack needs to be disclosed internally and externally.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Ning Chiu
+1 212 450 4908
ning.chiu@davispolk.com
