

Client Alert

July 2014

SEC Provides Guidance to Directors of Public Companies

Chair Mary Jo White of the Securities and Exchange Commission (the “SEC” or “Commission”) recently delivered a speech at the Twentieth Annual Stanford Directors’ College entitled [“A Few Things Directors Should Know About the SEC”](#). Also, Commissioner Luis Aguilar recently attended the “Cyber Risks and the Boardroom” conference at the New York Stock Exchange, where he delivered comments about the boards of directors in cybersecurity and data breaches.

Directors and corporate counsel at public companies should be aware of the views of these important regulators. The key take-aways from these speeches are below.

Chair White on “A Few Things Directors Should Know About the SEC”

Directors are Gatekeepers

- *The SEC views directors as “gatekeepers.”* Both investors and the SEC rely on boards to prevent, detect, and stop violations of the federal securities laws.
- *Boards must establish corporate culture.*
 - “[I]t is essential for directors to establish expectations for senior management and the company as a whole, and exercise appropriate oversight to ensure that those expectations are met. It is up to directors, along with senior management under the purview of the board, to set the all-important ‘tone at the top’ for the entire company.”
 - Chair White conveyed her position that boards should clearly convey that they stand for “good corporate governance” and “rigorous compliance” to create a strong corporate culture that permeates an organization.
 - Boards must select a chief executive officer who “ ‘gets it,’ in terms of understanding the importance of tone at the top and a strong corporate culture.”
 - The SEC believes that “[d]eficient corporate cultures are often the cause of the most egregious securities law violations.”
- *To be effective, directors must learn and be engaged.* Chair White, who has previously served as a director and audit committee member of a public company, advised that a director “must understand your company’s business model and the associated risks, its financial condition, its industry and its competitors. You must pay attention to what senior managers say, but also listen for the things they are not saying. You have to know what is going on in your company’s industry, but also the broader market. You need to know what your company’s competitors are doing and what your shareholders are thinking.” She even suggested that directors might consider meeting with their regulators.
- *Directors should listen to shareholders.* “Many institutional shareholders have unique insights on industry dynamics, competitive challenges and how macroeconomic events are shaping the environment for your company.” Directors should also consider the voting results from their shareholder meetings.

- *The potential for individual liability is small.* Recent SEC enforcement actions, when viewed in context, “should not strike fear in the heart of a conscientious, diligent director.”

Self-Reporting

- *Whether to self-report.* When discovery of wrongdoing does not require a public disclosure, the board of directors must still make an important decision on whether to self-report the violation. The decision whether to cooperate should be made early in the investigation.
- *The substance of cooperation is important.* When a company self-reports, it should focus on the “tone and substance of the early communications” with the SEC, which communications “are critical in establishing the tenor of [the SEC’s] investigations and how the staff and the Commission will view [the company’s] cooperation in the final stages of an investigation.” For example, Chair White advised that “[h]olding back information, perhaps out of a desire to keep options open as the investigation develops, can, in fact, foreclose the opportunity for cooperation credit.” The board of directors, she continued, has a responsibility for overseeing the manner in which the company cooperates. In addition, “[c]ooperation means more than complying with our subpoenas for documents and testimony — the law requires you to do that. If you want your company to get credit for cooperation ... then sincere and thorough partnering with the Division of Enforcement to uncover all the facts is required.”
- *Companies that decide to self-report should be decisive.* “Make it clear from the outset that the board’s expectation is that any internal investigation will search for misconduct wherever and however high up it occurred; that the company will act promptly and report real-time to the Enforcement staff on any misconduct uncovered; and that the company will hold its responsible employees to account.”

Whistleblowers Under the New SEC Rules

- *New rules have not displaced internal reporting.* Following enactment of the new SEC whistleblower rules under the Dodd-Frank Wall Street Reform and Consumer Protection Act (the “Dodd-Frank Act”), the SEC finds that many in-house whistleblowers have first reported the issue internally at their companies.
- *Protection against retaliation.* The SEC has authority under the Dodd-Frank Act to pursue companies who retaliate against whistleblowers. The SEC recently brought its first enforcement action for retaliation under the new rules.
- *Take whistleblowers seriously.* Boards should take whistleblowers seriously, even if prior “tips” have proven to be false.

Commissioner Aguilar on “Board of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus”

In this speech, Commissioner Aguilar advised directors to focus on the need for increased oversight of cyber-related risks and encouraged boards to take a more active role in managing these risks. In light of the significant cyberattacks occurring with greater frequency, and evidence that companies of all sizes are readily susceptible to such attacks, Commissioner Aguilar emphasized that ensuring the adequacy of a company’s cybersecurity measures is a critical part of a board of directors’ risk oversight responsibilities. He noted how quickly the need for cybersecurity has grown and cautioned “boards that choose to ignore, or minimize the importance of cybersecurity oversight responsibility, do so at their own peril.” Commissioner Aguilar advised that, at a minimum, boards should work with management to assess the company’s corporate policies to gauge how they match up to the guidelines in the Framework for Improving Critical Infrastructure Cybersecurity, released by the National Institute of Standards and Technology in February 2014.

Board of Directors' Duty of Oversight with Respect to Cybersecurity

Cyber-risk is part of the board of directors' overall risk oversight responsibilities. Public company directors have a duty of oversight, which requires that they attempt in good faith to assure that a corporate information and reporting system and internal controls exist, which the board concludes is adequate. Boards of directors must also consider important risks to the enterprise. Although the board's risk oversight function may be delegated to a committee, Commissioner Aguilar warned that an audit committee might not have the expertise, support, or skills necessary to add oversight of a company's cyber-risk management to its agenda. He suggested creating a separate enterprise risk committee on the board and focusing on adequacy of resources and overall support provided to company executives responsible for risk management. Commissioner Aguilar stated that while there are "various mechanisms that boards can employ to close the gap in addressing cybersecurity concerns ... boards need to be proactive in doing so."

Directors need to proactively address the risks associated with cyberattacks. Commissioner Aguilar also highlighted the need for boards to "take seriously their responsibility to ensure that management has implemented effective risk management protocols." In his comments, Commissioner Aguilar also referred to the recent data breach at Target Corporation ("Target") and the fact that a leading proxy advisory firm had recommended against the election of seven of the ten Target directors who served on the Audit Committee or the Corporate Responsibility Committee at the time of the data breach. Commissioner Aguilar stated that the proxy advisory firm "urg[ed] the ouster of most of the Target Corporation directors because of the perceived 'failure ... to ensure appropriate management of these risks.'" The quality of director oversight was also a key issue identified by The Conference Board Task Force on Corporate/Investor Engagement in its reports released in March 2014.

Contact

Steven M. Haas
shaas@hunton.com

© 2014 Hunton & Williams LLP. Attorney advertising materials. These materials have been prepared for informational purposes only and are not legal advice. This information is not intended to create an attorney-client or similar relationship. Please do not send us confidential information. Past successes cannot be an assurance of future success. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials.