February 22, 2018

SEC Releases New Guidance on Cybersecurity Disclosures and Controls

Yesterday, in keeping with a heightened governmental focus on cybersecurity, as exemplified by the Justice Department's formation of a new Cyber-Digital Task Force earlier this week, the Securities and Exchange Commission announced new guidance on cybersecurity disclosures by public companies (the "Guidance").

Much of the Guidance tracks 2011 interpretive guidance from the SEC's Division of Corporation Finance and retains a focus on "material" cyber risks and incidents. However, the expanded details and heightened pressure to disclose indicated in the Guidance, along with its issuance by the Commission itself, signal that the SEC expects public companies to consider more detailed disclosure of cyber risks and incidents, and to maintain "comprehensive" policies and procedures in this area. The SEC is also encouraging, though not requiring, forward-leaning approaches, such as with respect to disclosures about the company's cyber risk management programs and the engagement of the board of directors with management on cybersecurity issues. SEC Chairman Jay Clayton has also directed SEC staff to monitor corporate cyber disclosures.

The majority of the Guidance focuses on "reinforcing and expanding upon" the 2011 interpretive guidance, advising public companies to evaluate the materiality of cyber risks and incidents and make necessary disclosures in a timely fashion, while warning that the SEC is watching closely. As in the 2011 document, yesterday's Guidance notes that cyber disclosures should be non-generic and tailored to a company's particular circumstances, and may be required in sections of public filings addressing Risk Factors, MD&A, Description of Business, Legal Proceedings and Financial Statement Disclosures. While this portion of the Guidance provides a primer on the scope and nature of adequate cybersecurity disclosures, it is unlikely to trigger significant changes to corporate practice by companies that have already incorporated cybersecurity concerns into their disclosure reviews.

However, as Chairman Clayton emphasized in his accompanying statement, the Commission's Guidance delves into some new areas – particularly, board oversight, disclosure controls and procedures, insider trading and selective disclosures. *First*, the Guidance advises that public companies should disclose the role of boards of directors in cyber risk management, at least where cyber risks are material to a company's business. Given the grave threat posed by cyber risks,

most boards are likely already engaged in some form of cyber risk oversight, but the call for more public disclosure may prompt consideration of whether to deepen or sharpen that engagement.

Second, the Guidance encourages companies to have controls that ensure important cyber risk and incident information is elevated to senior management and enable informed disclosure decisions. Upping the ante, the Guidance advises that required executive certifications regarding the design and effectiveness of disclosure controls include controls governing relevant cyber risk disclosures.

Third, the Guidance reminds companies that cyber risks and incidents may constitute material non-public information implicating insider trading laws and Regulation FD. Chairman Clayton's statement urges companies "to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives." Companies should accordingly evaluate their insider trading policies to ensure they operate effectively in the wake of cyber incidents, including by ensuring that consideration is given in any specific situation whether to restrict trading by insiders before public disclosure. As highlighted in the Guidance, executive trading prior to disclosure of significant cyber incidents may invite scrutiny and second-guessing, even where legal requirements are met. Further, companies should carefully consider how disclosures of cyber incidents to affected individuals or transaction partners as part of due diligence align with disclosures made publicly to investors.

The Guidance reflects the SEC's increased attention to cybersecurity and concerns that investors may be inadequately informed about the growing risks. But as recently appointed SEC Commissioner Robert Jackson stated in "reluctantly" supporting the Guidance as a "first step," it largely "reiterates years-old staff-level views on this issue," a view shared by Commissioner Kara Stein. The Guidance's greatest impact may well flow not from the specific disclosures discussed, but from promoting increased board oversight and senior management attention to cybersecurity-related policies and procedures.

John F. Savarese
David A. Katz
Wayne M. Carlin
David B. Anders
Sabastian V. Niles
Marshall L. Miller
Jonathan Siegel