THE REVIEW OF
BANKING & FINANCIAL SERVICES
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 40 No. 9 September 2024

BOARD OVERSIGHT OF CYBERSECURITY MATTERS

As companies increasingly rely on information systems and digital networks to carry out their daily operations, cybersecurity incidents and their responses have grown more frequent, complex, and consequential. And just as the stakes have grown for companies that find themselves confronted with a cybersecurity incident, they have grown for the boards of directors overseeing the response. We offer below key considerations and best practices for boards seeking to mitigate the threat presented by cybersecurity incidents, as well as how to best approach disclosure decisions and obligations as they arise. We also summarize the current regulatory landscape and provide insights into trends in cybersecurity enforcement evinced through recent SEC actions. Rather than maintaining a reactive posture, boards can and should feel empowered in proactively mitigating and managing cybersecurity risk.

By A. Kristina Littman and Erik Holmvik *

Cybersecurity threats, with their increasing frequency, complexity, and consequence, have presented boards of directors and issuers[1] with difficult oversight demands and disclosure decisions. New rules from the U.S. Securities and Exchange Commission, while establishing clear expectations for boards with respect to certain cybersecurity issues and disclosure topics, have ultimately raised the stakes and introduced fresh uncertainties.

For boards of directors, the stakes and importance of effective oversight couldn't be higher. Cybersecurity incidents carry a plethora of potential costs — many of them significant — among many other negative consequences. These costs and consequences include disruptions in service, loss of proprietary or customer information, reputational damage, litigation and regulatory enforcement actions, increased insurance premiums, and remediation costs, to name a few. As time goes on and cybersecurity threats continue to mount, the demands placed on boards will almost certainly only increase. However, there are a number of tools available to the savvy board to shore up both their respective issuer's preventative measures, as well as crafting an effective and efficient incident response.

In this article, we break down the SEC's new cybersecurity rules and the impact they had on issuers' disclosures during this first affected reporting cycle, examine a few recent high-profile SEC enforcement actions and related litigation, and end with a discussion of several actionable takeaways.

[1] As that term is defined at 15 USC §78c(a)(8).

* *A. KRISTINA LITTMAN is a partner at Willkie Farr & Gallagher LLP's Washington, DC office and ERIK HOLMVIK is an associate in the same office. Their e-mail addresses are aklittman@willkie.com.and eholmvik@willkie.com.*