BCLP. Client Intelligent

BCLPSecCorpGov.com

SEC SCHEDULES VOTE ON PROPOSED CYBERSECURITY DISCLOSURE RULES; ENFORCEMENT DIRECTOR SPEAKS ON CYBER RESILIENCY

Jul 20, 2023

The SEC has scheduled a public meeting for July 26, 2023 to, among other things, "consider whether to adopt rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incidents by public companies." The proposed rules issued in March 2022 generated substantial public comment.

At the Financial Times Cyber Resilience Summit in late June, Director of the SEC Division of Enforcement Gurbir Grewal commented on the SEC's approach to cybersecurity issues. He began by discussing the importance of cybersecurity in public companies and noted that more than a third of executives reported that their organization's accounting and financial data was targeted by cyber adversaries last year. As markets grow increasingly complex and global, cybersecurity measures become more and more essential. Grewal commented that because of the increased risk, cybersecurity is imperative to maintaining the integrity of the securities markets and the economy in its entirety.

Although Grewal did not comment on the SEC's proposed cybersecurity disclosure rules scheduled for consideration on July 26, he shared five principles set forth below that are meant to "guide the work" that the SEC is doing to "ensure that registrants take their cybersecurity and disclosure obligations seriously."

1. **Investors are also victims.** "When there are cyber attacks on publicly traded companies and other market participants, we consider the investing public to also be potential victims of those incidents…[O]ur goal is to prevent additional victimization by ensuring that investors receive timely and accurate required disclosures…[I]f you wait too long to make the necessary disclosures, you risk creating additional victims."

2. **Actually implement cybersecurity policies.** "[F]irms need to have real policies that work in the real world, and then they need to actually implement them; having generic "check the box" cybersecurity policies simply doesn't cut it… [S]ome firms have just been paying lip service to these requirements."

3. **Constant vigilance is required.** "[R]egistrants [must] regularly review and update all relevant cybersecurity policies to keep up with constantly evolving threats…[R]egistrants and the professionals that counsel them would be well-served by reviewing the Commission's enforcement actions and public orders on these topics."

4. **Report to the right people.** "When a cyber incident does happen, the right information must be reported up the chain to those making disclosure decisions. If they don't get the right information, it doesn't matter how robust your disclosure policies are."

5. **Avoid "gamesmanship" in disclosure decisions.** "[W]e have zero tolerance for gamesmanship around the disclosure decision. Here, I am talking about those instances where folks are more concerned about reputational damage than about coming clean with shareholders and the customers whose data is at risk…If you have a material event, or think you might, comply with your disclosure obligations and come and talk to us sooner rather than later – not in six months after you finish your internal investigation. You can always complete that after meeting your disclosure obligations, if any, and reaching out to us."

Additionally, Grewal noted, as a broad principle, that firms that "meaningfully cooperate" with the SEC during cybersecurity investigations, including self-reporting, will benefit. These benefits could include reduced penalties or no penalties. A transcript of Grewal's remarks is posted on the SEC's website.

RELATED CAPABILITIES

- Securities & Corporate Governance

MEET THE TEAM

Eliot W. Robinson

Atlanta

eliot.robinson@bclplaw.com
+1 404 572 6785

William L. Cole

St. Louis

bill.cole@bclplaw.com
+1 314 259 2711
