Published on *The National Law Review* https://natlawreview.com

Is Your Board Cyber-Ready? Leadership Steps to Support Corporate Cybersecurity

Article By:

Jason C. Gavejian

Alison Jacobs Wice

Trisana N. Spence

The growing concern around cyberthreats for companies across the nation is reflected in the increasingly crowded legislative landscape that provides guidance to organizations, employers, employees, consumers, and investors. As part of that landscape, enterprises — both public and private — operate under an unprecedented level of scrutiny. Last month, new SEC requirements went into effect for public enterprises. Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (the “Rule”). The Rule not only requires public enterprises to report cyber breaches within only four days, but it also requires annual disclosure of material information regarding cybersecurity risk management, strategy, and governance and other periodic disclosures about the enterprise’s processes for assessing, identifying, and managing material cybersecurity risks, management’s role in assessing and managing material cybersecurity risks, and the board of directors’ oversight of cybersecurity risks.

This Rule adds yet another layer to the complicated issues of managing cybersecurity risks, but strong corporate governance equips companies to address them efficiently and accurately. The best practices for public companies that must comply with the SEC's Rule also guide advice for private entities for managing cybersecurity risks. Key components of the SEC's Rule shine a light on ***action items*** for preventing, navigating, and responding to cyberthreats through **strong board governance and engagement**, including:

1. Identify cybersecurity risks as a required disclosure to the organization's Board;
2. Ensure the Board understands that it is responsible for oversight of the organization's cyber security program;
3. Provide the Board with "decision-useful" information relative to cyber risks;
4. Train leadership on the necessity of reporting actual and potential cybersecurity incidents and risks to the Organization's Board;
5. Create a cybersecurity breach response plan enforced by the Board;
6. Perform stress tests of the cybersecurity breach plan, with Board participation; and
7. Leadership and the Board should engage with the Organization's IT/ Data Governance Teams to ensure best practices are being followed, including ensuring employees are trained on cybersecurity risks.

National Law Review, Volume XIII, Number 285

Source URL:https://natlawreview.com/article/your-board-cyber-ready-leadership-steps-support-corporate-cybersecurity