“The most pressing issue in corporate governance today…”

Date : 23-05-2018

…is risk from cyber threats. On March 15, SEC Commissioner Robert Jackson Jr. dubbed cyber threats “the most pressing issue in corporate governance today”. His speech built on an earlier SEC statement providing guidance for proper disclosure of cybersecurity incidents. This announcement was motivated by the trend toward insufficient disclosure of data breaches as exemplified by the Equifax management team. In his speech, Jackson went further. He stated that regulators should provide more definitive guidance to directors in three areas relative to cybersecurity: disclosure, insider trading, and internal controls. He’s right.

Today almost every company is, in some sense, a technology company. The winners will be those who leverage technology to create competitive advantage by delivering better goods and services, reducing costs, and delivering value to new customers. This journey has a cost in that it leads to greater exposure to cyber risks inherent in new cloud, mobile, and IoT platforms. The winners will be those leaders to leverage technology to drive growth while at the same time managing the technology risk associated with these investments.

Jackson’s speech should motivate all board directors to raise their game with regard to their firm’s cybersecurity governance. Yes, we can expect more stringent requirements from regulators. Further, we can expect to be held to higher standards of cyber hygiene by our investors, customers, and stakeholders. Consequently, all board members should improve their cyber fluency. However, cyber requires specific skills and experience. There are three actions all boards should consider:

- Add or develop at least one director with the requisite technical and business skills.
- Add a technology or cybersecurity committee to focus on this risk. Work closely with management to ensure the adequacy of your cyber risk management program. Provide a regular forum for discussion with the full board.
- Implement a ‘cyber blueprint’ which guides board directors and management on their respective priorities, objectives, and metrics.

An effective ‘cyber blueprint’ establishes clear spheres of responsibility. Management owns the creation of the operational plans which includes prioritizing risks, implementing controls, and measuring success against relevant frameworks. The board needs to lead in areas of assessing culture and key personnel, integration into overall corporate strategy, and, of course, assurance of proper disclosures and insider actions. Both management and boards should understand the impact external factors (policy, regulation, world events) have on their specific profile. Finally, similar to audit committee practices, develop close partnerships with advisors who will test your cyber program and help keep the firm abreast of issues.

For many, cybersecurity is the most pressing issue in both corporate governance and technology-focused value creation. Give it the time and attention it deserves and implement a ‘cyber blueprint’ to ensure management and the board are working effectively to navigate these waters.

- Jim Pflaging