Akin®

Top 10 Topics for Directors in 2019: Cybersecurity

Mar 4, 2019

Reading Time : **3 min**

Improve Disclosures and Controls

Directors should pay close attention both to cybersecurity disclosures and to internal controls related to cybersecurity vulnerabilities. In addition to publishing formal Commission-level guidance on cybersecurity disclosures and controls, the SEC has recently warned that it may consider certain cybersecurity vulnerabilities as actionable violations of federal securities laws, which require robust internal controls. In a rare Section 21(a) report, the SEC reported that companies continue to fall victims to billions of dollars in fraudulent wire transfers due to business email compromise and indicated that such failures may violate Section 13(b)(2)(B) of the Securities Exchange Act of 1934.

Be Vigilant in Supply Chain Management

With a spike in supply-chain cyber attacks, directors should ask probing questions on third-party relationships. Conducting proper due diligence, developing robust contractual security requirements and following up to ensure compliance are all critical aspects of any supply-chain relationship and, in some cases, are legally required pursuant to certain state laws (such as New York's Department of Financial Services Cybersecurity Regulation, which mandates third-party diligence compliance by March 2019).

Provide Oversight of Privacy and Security by Design

Emerging technologies have brought new risks: artificial intelligence, Internet of Things (IoT) and biometrics are changing the face of business. Directors should be forward-looking in their oversight of controls and should implement privacy and security by design into new technologies. With rigorous requirements imposed in newly passed California IoT legislation (SB 327) and Illinois's Biometric Information Privacy Act, that has more than 100 lawsuits

challenging alleged improper use of biometrics, companies will likely save money and decrease regulatory risk by anticipating privacy and security needs at the inception of any new project. Blockchain (the security technology that underlies Bitcoin) provides another emerging method to secure transactions and will likely evolve as companies adopt it more broadly.

Monitor Rapidly Changing Privacy and Cybersecurity Requirements

The patchwork of state, federal and international laws makes a challenging path forward for cybersecurity and privacy compliance for companies and their directors. In 2018, at least 35 states introduced more than 265 bills or resolutions related to cybersecurity. The California Consumer Privacy Act is arguably the most expansive, requiring covered businesses to provide General Data Protection Regulation (GDPR)-like rights to Californians and creating a narrow private right against companies that fail to implement reasonable security controls. Although not effective until 2020, it requires covered businesses to start tracking data and data practices as of January 1, 2019, to comply with a one-year look back provision. Other states, such as Colorado, Ohio, South Carolina, Connecticut and New York, have enacted privacy- and cybersecurityspecific laws and regulations affecting myriad different industries. The SEC has pursued enforcement and issued additional guidance surrounding Bitcoin. The international landscape is also evolving, with complaints to Data Protection Authorities in the European Union skyrocketing after implementation of the GDPR, including more than 1,100 complaints in a single month in the United Kingdom alone. In response, companies have banded together to seek federal legislation in the United States to preempt the patchwork of state laws, but, with contentious Senate hearings on proposed legislation, the prospects for a quick solution remain elusive.

Directors should insist on regular cybersecurity briefings. Such briefings should include updates on the adequacy of incident response plans, a review of budgets, tabletop exercises with the incident response team and a review of cybersecurity training (including statistics on phishing exercises). As cybersecurity risk issues continue to threaten companies worldwide, delegation to a committee, a CIO/CISO or a director who is a cybersecurity specialist will likely be deemed insufficient to discharge fiduciary duties.

Download Top 10 Topics for Directors: Cybersecurity in 2019.

Categories

Cybersecurity, Privacy & Data Protection | Policy & Regulation | Blockchain | Compliance | Insider Trading