Akin®

Top 10 Topics for Directors in 2018: Cybersecurity Threats

Dec 19, 2017

Reading Time : **4 min**

Ransomware threats shut down major multinational companies for days and have increased fourfold in the past year. SEC itself fell prey to a cyberattack, with the breach undisclosed for nearly a year. As a result, the next year will likely bring increased state and federal regulation of cybersecurity. As SEC Co-Directors of Enforcement Stephanie Avakian and Steven Peikin warned, "The greatest threat to our markets right now is the cyber threat." Boards should continue to focus on governance, crisis management and recommended best practices going forward.

Governance. Strength of governance in the risk area of cybersecurity will be a key focus in 2018. The SEC has recommended that companies designate a committee responsible for overseeing cybersecurity risk, and it has further advised that boards should have at least one cybersecurity expert or consultant. The Equifax data breach serves as a post breach governance case study. The fallout from one of the largest data breaches continues, but, so far, it has resulted in the ouster of the CEO, CIO and CISO; establishment of a special litigation committee; initiation of countless regulatory investigations, including 30+ state enforcement inquiries; investigations by the DOJ, SEC, FTC, UK Financial Conduct Authority and others; and 70+ lawsuits, including consumer class actions and securities class actions. The Equifax board has since appointed a cybersecurity expert to its board and technology committee. Ensuring that directors have properly established governance surrounding cybersecurity will be critical going forward in what is fast becoming a "bet-your-job" and "bet-the-company" risk.

Crisis management. A well-coordinated response to a cybersecurity crisis can mean the difference between being perceived as the victim of hackers or the negligent corporate wrongdoer. Although most breach notification deadlines were, at the earliest, 45 days from

discovery of the breach, companies must move much more quickly in notifying consumers and government agencies to maintain credibility. The New York Department of Financial Services (NYDFS) Cybersecurity Regulation requires notification within 72 hours for covered entities, and the National Association of Insurance Commissioners (NAIC) just passed a model law that follows suit. The NYDFS, NAIC and countless other regulations require companies to have firmly established and tailored incident response plans and to conduct tabletop scenarios to test them.

Cybersecurity and data protection abroad. The European Union's General Data Protection Regulation (GDPR) goes into force on May 25, 2018, and has significant implications for companies both in the U.S. and abroad. GDPR expands its territorial reach by applying to any company that offers goods or services or monitors the behavior of EU data subjects. It implements requirements such as requiring Data Protection Officers for certain companies; requiring Privacy by Design; imposing documentation and data minimization requirements; requiring improved consent procedures; requiring quick data breach notification; and imposing obligations on data processors, not just data controllers. Penalties for noncompliance are steep—with fines of the greater of 4% of worldwide annual revenue or EUR$20 million. The United Kingdom intends to implement a similar regulation to GDPR following its exit from the EU.

Best practices going forward. Announcing the results of the OCIE's recent exams of registered investment advisors and funds, the SEC identified consistent deficiencies by various regulated entities:

- failure to reasonably tailor policies and procedure
- failure to adhere to or enforce policies and procedures
- failure to adequately conduct system maintenance, resulting in Regulation S-P issues
- failure to remediate high-risk observations discovered through penetration tests and vulnerability scans.

The SEC recommended the following best practices, which also serve as best practices for any public company:

- maintenance of an inventory of data, information and vendors; and classification of risks, vulnerabilities, data, business consequences, and information regarding each service provider and vendor

- detailed cybersecurity-related instructions for issues such as penetration tests, security monitoring/auditing, access rights and reporting guidelines for lost, stolen or unintentionally disclosed sensitive information
- maintenance of prescriptive schedules and processes for testing data integrity and vulnerabilities, including patch management policies
- established and enforced controls for access to data and systems
- mandatory employee training at onboarding and periodically thereafter
- engaged senior management.

Calls for cybersecurity regulation following the Equifax breach have increased substantially. As the scale and scope of breaches continue to broaden, regulations will likely follow. At least 42 states have introduced more than 240 bills or resolutions related to cybersecurity in 2017, and some state regulations, such as the Illinois Biometric Information Privacy Act (which has resulted in 35 class action lawsuits in the past year alone), promise to bring increased enforcement. Improved governance and crisis management planning will make directors best prepared to respond to cybersecurity threats.

View the full report here.

Categories

Cybersecurity, Privacy & Data Protection | Investment Adviser & Fund Compliance | Policy & Regulation | Compliance

number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.