Cooley

FTC Expects Board-Level Cybersecurity Oversight

May 14, 2021

Federal Trade Commission (FTC) staff published a blog post that highlights increased cybersecurity threats and emphasizes the key role corporate boards play in a successful cybersecurity program: "Corporate boards: don't underestimate your role in data security oversight." Boards that are not actively considering cybersecurity risks should take notice.

The FTC's post contains five recommendations:

1. Make data security a priority.

Boards are ultimately responsible for data security. According to the FTC, "data security begins with the Board of Directors, not the IT Department." Boards should set high expectations regarding data security, build a team of stakeholders from throughout the organization, establish formal board-level oversight and hold regular security briefings. While there is no one-size-fits-all approach, a board-level cybersecurity committee or subcommittee can be an effective way to foster board engagement.

2. Understand your company's cybersecurity risks.

Board members should demonstrate a sophisticated grasp of the data security challenges their organization faces. While a board does not need to manage day-to-day operational security of the company, they should set priorities and allocate appropriate resources to manage cybersecurity risks. Board members should be in active dialogue with cybersecurity leaders within the organization (again, this can occur via a board cybersecurity committee or subcommittee).

3. Don't confuse legal compliance with effective cybersecurity.

To have an effective cybersecurity program, boards cannot view cybersecurity as a formulaic, check-the-box exercise. Cybersecurity threats are quickly evolving, and every company's risk profile is unique. Boards should have regular, in-depth conversations about the adequacy of their company's cybersecurity policies and procedures.

4. Preparation is key.

Even the best preventative measures sometimes fail – indeed, boards should probably assume that they will fail. It is critical for boards to ensure the company invests in robust incident response plans with clear escalation guidelines, including board notification where appropriate. It is increasingly difficult to prevent and respond to security incidents. When one occurs, every minute counts.

5. Learn from mistakes.

Boards should not only learn from their own cybersecurity challenges but also analyze challenges faced by competitor organizations. Industries can face similar vulnerabilities, and this review may lead to the discovery of latent, undetected incidents or potential incidents. Periodic, independent third-party assessments are an effective way to track progress and identify risks. Third party assessors are often essential partners in preventing and responding to a cyberattack.

Board engagement with cybersecurity issues does not occur in a vacuum. The risks to company and customer data are real, and in the event of a breach, regulatory enforcement is a distinct possibility. FTC challenges to allegedly deceptive or unfair data security practices led to recent settlements with SkyMed International and Tapplock. In its complaint against SkyMed, the FTC alleged the company failed to take reasonable steps to secure sensitive consumer information by, among other practices, not securing databases with customer information and failing to assess risks through network monitoring and penetration testing. In its complaint against Tapplock, the FTC alleged the company failed to take reasonable precautions such as implementing written data security standards, policies, procedures or practices, or implementing adequate privacy and security guidance or training for relevant employees.

In addition to tracking Securities and Exchange Commission (SEC) guidance on cybersecurity risks, boards should take notice and incorporate the FTC's guidance and lessons learned from recent FTC settlements into their cybersecurity committees or other oversight mechanisms.

Cooley regularly advises corporate boards and companies on the strategic management of cybersecurity risks. Our cyber/data/privacy team is also available to assist with FTC and SEC guidance on cybersecurity.

Key Contacts

Tiana Demas	tdemas@cooley.com +1 212 479 6560
Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018
Christian Lee San Francisco	christian.lee@cooley.com +1 415 693 2143
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090