FEDERAL TRADE COMMISSION
PROTECTING AMERICA’S CONSUMERS

Corporate boards: Don’t underestimate your role in data security oversight

Share This Page

Jared Ho
Apr 28, 2021

TAGS: Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Data Security | Gramm-Leach-Bliley Act

For businesses in the middle of a global pandemic, there’s no such thing as “business as usual.” The percentage of Americans working remotely has grown substantially, now reportedly up to 33% of the U.S. workforce. Accompanying that seismic shift have been increased security threats to data, with one analysis reporting that over 36 billion online records were exposed in the first half of 2020 alone. Consumers whose lives have been upended by identity theft are paying close attention to how corporations are responding. But is the typical corporate Board of Directors giving data security the attention it deserves?

In addition to the significant costs to consumers, data breaches, network intrusions, and looming cyber threats can open up a firm to substantial financial costs, reputational hits, and legal liability. The FTC has continued to challenge allegedly deceptive or unfair conduct related to companies’ data security practices. A few recent examples include settlements with SkyMed International, Tapplock, and Zoom. We’re also in the process of reviewing some data security rules for industry, including the Health Breach Notification Rule and the Gramm-Leach-Bliley Safeguards Rule.

Against that backdrop, it’s essential for corporate boards to do what they can to ensure that consumer and employee data is protected. The good news is that according to a recent study, 60% of directors surveyed said they plan to improve their cybersecurity oversight role over the next year. What would that look like for a typical corporation? FTC staff has five common-sense recommendations for conscientious directors.

Make data security a priority.

Contrary to popular belief, data security begins with the Board of Directors, not the IT Department. A corporate board that prioritizes data security can set the tone throughout an organization by instilling a culture of security, establishing strong security expectations, and breaking down internal silos to facilitate technical and strategic collaboration. While there’s no one-size-fits-all formula, here are strategies some companies have implemented to make security a priority.

> **Build a team of stakeholders from across your organization.** Despite a 2018 study that found that 89% of CEOs treat cybersecurity as an IT function, experience suggests that cyber risk management is a “whole business” issue. A sound data security program should incorporate stakeholders from business, legal, and technology departments across the company – both high-level executives and operational experts. Of course, many committees include the Chief Information Officers and the Chief Information Security Officer, but other

companies promote practical synergies by also including executives who bring a different perspective to the issues – for example, the CEO, CFO, or General Counsel. A broad and diverse range of voices can provide the board with cross-cutting information about cyber risks and solutions.

Establish board-level oversight. Some corporate boards delegate their cyber risk oversight duties to an audit committee. Others have a stand-alone cybersecurity committee at the board level. Irrespective of how an organization structures its cyber risk oversight duties, the key takeaway is that cyber risks should be a priority within the board room. Board-level oversight helps to ensure that cybersecurity threats, defenses, and responses have the attention of those at upper echelons and get the resources needed to do the job right.

Hold regular security briefings. When it comes to security, board members need to be in the know, but research suggests many of them are out of the loop. A 2012 survey found that fewer than 40% of corporate boards regularly received reports about privacy and security risks and 26% rarely or never got that information. According to another study, only 12% of boards frequently received cyber threat briefings. A survey of public companies conducted six years later in 2018 didn’t suggest much progress. Only 37% of board members said they felt “confident” or “very confident” that their company was properly secured against cyberattack. Of course, cybersecurity isn’t a one-and-done proposition. It’s a dynamic process that requires board members to be informed, engaged, and updated. Regular briefings prepare boards to carry out their oversight responsibility, navigate the security landscape, and prioritize threats to the company.

Understand the cybersecurity risks and challenges your company

faces.

A strong data security program starts at the top. While it might not be the board’s role to manage day-to-day security operations, it is their job to set priorities and allocate the resources necessary to ensure effective security. Board members need to talk the talk and walk the walk. They should demonstrate a sophisticated grasp of the data security challenges their company faces and act in a way that sets the tone for the entire organization.

Don’t confuse legal compliance with security.

In 2019, the FTC held a series of hearings on consumer protection and technology in the 21st century. One common theme was that compliance doesn’t necessarily translate into good security. Cybersecurity threats are constantly and rapidly evolving. A strong data security program should never be reduced to a “check the box” approach geared toward meeting compliance obligations and requirements. Instead, boards should ensure that their security programs are tailored to their companies’ unique needs, priorities, technology, and data. Boards should ask tough questions about whether their policies and procedures effectively address their company’s security risks and whether actual security practices effectively address the threats they face. That no-holds-barred conversation might include fundamental questions like:

> What kind of data are we keeping and why? And where are we keeping it?
>
> Are our policies and procedures adequate to protect our data?
>
> Are our actual security practices in line with our policies and our public-facing statements?
>
> Are our security investments and expenditures in line with our security risks and threats?

It’s more than just prevention.

A strong data security program ensures that a company is undertaking reasonable precautions to protect its network and consumers’ personal information from intruders. However, no data security program is perfect and no program can guarantee that a company will be protected from attack or a data breach. If nothing else, recent breaches have demonstrated the importance of both a strong data security program *and* a robust incident response plan. In responding to a security incident, time is often of the essence. Every minute that employees spend attempting to flag down key executives and focus their attention on what’s happened is time taken away from the critical tasks of stanching the damage to data and implementing an appropriate response. In contrast, an effective security program ensures that when it’s appropriate, a security incident can be swiftly elevated to the appropriate level. In addition, building organizational resilience into your security program can help your company sustain operations while responding to a security incident.

Learn from mistakes.

If your company has had the misfortune of experiencing a data breach, take the opportunity to learn from the incident and improve your program. Companies often require periodic independent third-party assessments to establish a baseline against which future progress can be measured and – in the event of a security incident – to determine how a breach occurred. Of course, learning from other companies’ mistakes can be just as valuable (and substantially less painful). There are certainly no shortage of data breaches and many likely involve competitors or other parties in similar lines of business. Boards should take the opportunity to understand the cybersecurity risks related to their industry and learn from their company’s own mistakes as well as the mistakes of others.

The FTC Business Center has data security resources for companies of any size and in any sector.

ftc.gov