



Alerts

FTC Lessons Learned: Corporate Board Oversight

May 6, 2021

Hinshaw Privacy & Cyber Bytes

The Business Alert

On April 28, 2021, the FTC issued a business alert reminding corporate boards to make data security a priority and to advocate implementing a top-down approach to the issue. The alert warns: “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 Business Alert suggests that data security begins with corporate Board of Directors instead of the IT Department.

The Recommendations

FTC staff offered five “common-sense recommendations for conscientious directors.”

1. **Make data security a priority.** This includes building a team of stakeholders from across the organization and holding regular security briefings.
2. **Understand cybersecurity risks and challenges facing the company.** Board members should set priorities and allocate necessary resources.
3. **Don’t confuse legal compliance with security.** The alert cautioned against adopting a “check the box” approach in favor of a security program that is narrowly tailored to the company’s unique circumstances.
4. **It’s more than just prevention.** An effective security program should be enhanced with a “robust incident response plan.”
5. **Learn from mistakes, both internally and externally.**

The Takeaways

The FTC staff recommendation that board members “talk the talk and walk the walk” is the key takeaway. This effort includes having tough conversations 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?

Service Areas

Privacy, Security & Artificial Intelligence



- Are our security investments and expenditures in line with our security risks and threats?