wiley

NEWSLETTER

Lawmakers and Regulators Are Looking at Corporate Board Involvement in Privacy and Cybersecurity

June 2019

Privacy in Focus®

As legislators and regulators consider substantive proposals to regulate how companies collect, manage, and protect consumer data, and what kind of cybersecurity protections they implement, they have increasingly looked at mandating specific steps that boards of directors must take. We have previously discussed how corporate boards are advised to engage on cybersecurity issues, and companies must also pay close attention to specific legislative or regulatory requirements affecting corporate board involvement. Requirements on corporate boards continue to be proposed and adopted in piecemeal fashion – particularly in the area of cybersecurity – and it remains to be seen whether they will be adopted in any federal privacy or cyber legislation. This area continues to evolve, and below we discuss a few recent actions at the state and federal level and congressional proposals that would require explicit board oversight of privacy, cybersecurity, and data governance issues, including by requiring the establishment of senior-level positions with reporting obligations directly to the board.

State Activities

States have moved forward on adopting cybersecurity regulations on a number of fronts, and some of those moves have encompassed specific requirements for corporate boards. In particular, New York and South Carolina have taken sector-specific steps on board oversight in cybersecurity.

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Tawanna D. Lee
Consulting Counsel
202.719.4574
tdlee@wiley.law

Practice Areas

Privacy, Cyber & Data Governance

In 2017, New York's Department of Financial Services (NYDFS) issued a cybersecurity regulation designed to address cyber threats faced by the state's financial services industry. The final regulation requires financial services institutions regulated by the NYDFS to designate a chief information security officer responsible for overseeing a mandatory cybersecurity program, with a reporting requirement to the company's board of directors or equivalent governing body.[1] The annual report must include an assessment of material cybersecurity risks. New York's preeminence as an international financial hub greatly extends the reach of the NYDFS regulation.

Similarly, South Carolina took the lead in passing a cybersecurity law to address threats in the insurance industry. The South Carolina Insurance Data Security Act, effective January 1, 2019, mandates that any insurance carrier licensed in the state create a risk-based cybersecurity program with oversight by the company's board of directors.[2] Executive management must produce an annual report on material matters related to the cybersecurity program. For an insurance carrier operating in South Carolina, these kinds of requirements can have an effect on company operations that may impact cybersecurity even outside the state.

Federal Regulatory Action

Federal regulators also have begun to take action in certain areas. In February 2018, the U.S. Securities and Exchange Commission (SEC) issued updated guidance on cybersecurity disclosure obligations. Among other things, the SEC guidance provides that companies should disclose to investors how the board "engages with management on cybersecurity issues" and "discharge[es] its [cybersecurity] risk oversight responsibility." And the SEC "encourage[d] companies to adopt comprehensive policies and procedures related to cybersecurity and to assess their compliance regularly, including the sufficiency of their disclosure controls and procedures as they relate to cybersecurity disclosure."

The Federal Trade Commission (FTC) also has begun to scrutinize corporate governance with respect to cybersecurity in non-bank financial institutions. Recently, the FTC proposed revisions to its Safeguards Rule for financial institutions, modeled on the NYDFS regulations. The Safeguards Rule governs data security practices for financial institutions under the FTC's Gramm-Leach-Bliley (GLB) Act jurisdiction. The proposed revisions mirror the NYDFS mandate, requiring covered financial institutions to designate a chief information security officer with mandatory board reporting. In its Notice of Proposed Rulemaking (NPRM), the FTC has sought comment on whether a board should be required to certify compliance with the Rule.[3]

Federal Legislation

In addition to the state and federal regulatory efforts discussed above, federal lawmakers are considering whether to include board-specific requirements in crafting privacy and cybersecurity legislation. For example, in 2018, Sen. Ron Wyden (D-OR), ranking member of the Senate Finance Committee, released a discussion draft of a bill called the Consumer Data Protection Act.[4] The draft legislation aims to provide consumers with greater control over their data, and would cover companies under FTC jurisdiction that generate more than $50 million in annual revenue or store, share, or use personal information on more than 1 million consumers or

consumer devices.

The draft bill would require covered entities to designate an employee responsible for compliance with the legislation and the annual submission of data protection reports to the FTC outlining in detail the entity's compliance with the legislation's technical and security safeguards. The designated employee also must directly report to an employee acting in an executive capacity, and each report must be accompanied by written compliance certifications from the company's chief executive officer, chief privacy officer, or chief information security officer. The draft bill would levy significant civil and criminal penalties for knowing or intentionally false certifications – executives could be "fined not more than $5,000,000 or 25 percent of the largest amount of annual compensation the person received during the previous 3-year period from the covered entity, imprisoned not more than 20 years, or both."

Additionally, the House and the Senate are considering requiring publicly traded companies to disclose whether they have cybersecurity expertise in their board of directors. On March 1, a bipartisan group of Senators reintroduced the Cybersecurity Disclosure Act, S.592, followed by a House companion bill, H.R. 1731. The bills would require publicly traded companies to include in their SEC disclosures to investors information on whether any member of the company's board is a cybersecurity expert, and if not, why having this expertise on the board of directors is not necessary because of other cybersecurity steps implemented by the company.

As the legislative process plays out in this Congress, we will be continuing to watch whether proposals to impose specific board-level obligations gain traction.

Conclusion

As lawmakers and regulators continue to evaluate whether to impose additional privacy and cybersecurity requirements, it is clear that many are seeking to elevate the importance of those issues in the company by explicitly requiring board involvement or review. Companies must pay close attention to developments in this area occurring throughout government.

Wiley Rein's Cybersecurity and Data Governance team regularly helps clients manage risk and assess compliance obligations, and we assist boards of directors and senior management in discharging their responsibilities.

---

[1] 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies § 500.04(a).

[2] *See* H.B. 4655, 122nd Gen. (S.C. 2018).

[3] 16 CFR § 314 (Apr. 4, 2019).

[4] Consumer Data Protection Act, SIL18B29, 115th Cong. § 2 (2018).