Akin®

Top 10 Topics for Directors in 2020: Cybersecurity

Mar 5, 2020

Reading Time : **4 min**

Know Your Privacy Pitfalls Under New Regulations

With the U.S. Congress' failure to pass uniform privacy and cybersecurity regulation, California's privacy law becomes, in reality, the privacy law in the United States. The CCPA creates new requirements for identifying, managing, securing, tracking, producing and deleting consumer privacy information. It also provides extensive rights to consumers to take control of their data. The CCPA is not limited to companies located in California, but rather it generally applies to most for-profit companies doing business in California. This can include simply selling to California residents.

Companies must evaluate whether they fall under the CCPA's reach and carefully structure data privacy practices to comply with the many requirements. The CCPA is not as onerous as the European Union's (EU's) General Data Protection Regulation's (GDPR's) 4 percent of worldwide revenue penalty, but it does impose penalties of $2,500 per negligent violation and $7,500 per intentional violation.

However, the likely game changer is the private cause of action: Individuals can now sue for certain data breaches where companies did not have "reasonable security," with statutory damages of $100 to $750 per incident, per consumer.

The coming year could bring copycat legislation across the country. Creative plaintiffs will certainly seek out ways to hold companies accountable for ever-changing requirements, whether they are under the Illinois Biometrics Information Privacy Act's (BIPA's) facial recognition protection, or the soon-to-be-forthcoming revised regulations related to the Children's Online Privacy Protection Act's (COPPA's) consent restrictions or other legislation.

Use Internal Controls to Stop Wire Fraud in Its Tracks

With an estimated $5.3 billion in fraud committed globally since the Federal Bureau of Investigation (FBI) began tracking in 2013, business email compromise impacts companies across the country and across all industries. The basic scheme is simple: hack into the email system, watch for planned money transfers and swap the wire instructions so that the money is wired to the hacker rather than the intended party.

The Securities and Exchange Commission (SEC) has warned that it may consider significant wire fraud a "books and records" violation of Section 13(b)(2)(b). Companies "must calibrate their internal accounting controls to the current risk environment and assess and adjust policies and procedures accordingly."

Stay Current on Cybersecurity Compliance

Just as privacy has been prioritized by legislators, cybersecurity regulations are becoming increasingly proscriptive.

- *SHIELD*. In 2019, New York enacted the Stop Hacks and Improve Electronic Data Security (SHIELD) Act. It contains a new "reasonable security requirement" that requires businesses that are not regulated by and compliant with another New York state or federal data security regime to adopt a program that includes certain very specific data security safeguards.
- *IoT*. On January 1, 2020, California's Internet of Things (IoT) law became the first in the nation to impose liability for failure to reasonably secure devices.

Global research and advisory firm Gartner estimates that more than 26 billion IoT devices relying on connectivity will be deployed by 2020. The FBI piled on by warning that hackers have been using devices to spy on employees in their own offices or homes. Directors should make sure that their company has a strong cybersecurity program, compliant with the many recently released cybersecurity regulations.

Seek Cybersecurity Insurance to Mitigate Risk

Most companies are mitigating risk by purchasing cyber and privacy insurance. But buyer beware: Directors should carefully consider whether the insurance is sufficient and provides coverage for a company's particular risks. Gaps in coverage could include:

- Lack of regulatory compliance coverage
- Absence of cyber fraud coverage

- Insufficient business disruption coverage
- No third-party coverage
- Rejection of claims based on accidental errors and omissions.

In a recent case, multinational corporation Mondelez sued its insurer for nonpayment under its cyber insurance policy because the insurer refused to pay based on the "war exclusion" after the ransomware attack was attributed to Russia. Similarly, directors should assess whether coverage exists for emerging threats, such as penalties under the CCPA or the GDPR. Directors should carefully evaluate coverage and question the sufficiency of coverage.

Establish Board Oversight on Privacy and Cybersecurity

Directors play a key oversight role in enterprise risk management, and cybersecurity and data privacy remain high-stakes risk areas for companies of all sizes and all industries. Directors must take care to properly exercise their Caremark duties—putting in place adequate internal control systems. Alternatively, they could be held liable for failing to properly monitor the company, as the Delaware Supreme Court recently found in Marchand v. Barnhill, where it allowed the matter to proceed past the directors' motion to dismiss.

Specifically, directors must be able to show that they made a good faith effort to establish appropriate reporting systems and reporting procedures that enable the board of directors to discharge its privacy and cybersecurity oversight responsibilities. Fiduciary oversight is not just a focus of derivative plaintiffs, but also a key focus of federal and state regulators.

Directors should follow a rigorous review protocol of the company's cybersecurity and privacy program that:

- Establishes clear risk management framework for cybersecurity and data privacy, ensuring proper governance, reporting and assessments
- Obtains reports on cyber and privacy risks specific to the company, considering emerging threats and risks from systemic company shifts, such as mergers and acquisitions
- Understands new and material regulations, such as the CCPA, that impact data flow and data practices
- Requires risk mitigation through a practiced incident response and effectively constructed insurance program.

Categories

Cybersecurity, Privacy & Data Protection

Compliance