A Matter of Time: States Adopt New Cybersecurity Requirements

Large data breaches impacting millions regularly make news headlines; and, increasingly, small businesses are becoming frequent targets of cyberattacks. In response, states across the country are beginning to introduce laws and regulations requiring entities to implement security measures to proactively protect against a data breach.

In a 2017 study on small- and medium-sized U.S. businesses (companies with fewer than 1,000 employees), the Ponemon Institute found that 61% of such businesses had experienced a cyber-attack in the past 12 months. Even more concerning, USA Today reports that nearly 90% of small- and medium-sized businesses in the U.S. don’t use any data protection at all for company and customer information. These statistics show that many businesses, especially small ones, are not prepared for today’s cybersecurity threats.

The latest state-level cybersecurity regulations

Signed into law May 3, 2018, and effective January 1, 2019, the South Carolina Insurance Data Security Act is the latest instance of state-level cybersecurity regulation. Under the law, insurers, agents, and other licensed entities authorized to operate under South Carolina’s insurance laws will be subject to a set of requirements designed to protect their companies and their consumers from a data breach. Entities will have until July 1, 2019, to develop, implement, and maintain a comprehensive written information security program. The development of such a program to comply with these laws is likely to be a significant undertaking for any entity. A poorly implemented plan is more likely to result in a data breach, increasing a company’s notification and investigation requirements.

Background on current trends in state-level cybersecurity laws

South Carolina’s law follows in the steps of the New York State Department of Financial Services (DFS) Cybersecurity Requirements of Financial Services regulation. Issued March 1, 2017, the DFS regulation was designed to promote the protection of customer information, as well as the information technology systems of DFS-regulated entities. South Carolina’s law became the first based on the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (NAIC Model Law). The NAIC Model Law provides a framework for insurance organizations to create and operate cybersecurity programs. New York’s cybersecurity law shares many common requirements with the NAIC Model Law.
The current cybersecurity regulation landscape consists of a patchwork of varying regulations across all 50 states, making compliance inconsistent and challenging for companies operating in multiple states. Although the NAIC Model Law is only applicable to entities licensed under state insurance regulators, it represents an attempt to enact consistent policies across multiple states. As such, South Carolina’s enactment is at the forefront of a movement toward consistent cybersecurity laws. As more states impose cybersecurity laws, they are likely to follow the NAIC Model Law and New York’s regulation.

What these laws require

The South Carolina law and the New York regulation share many common requirements for preventing, and responding to, cybersecurity incidents, and are among the first state laws to place an emphasis on security. Currently, most state laws focus on a response to a data breach.

Under these new laws, businesses are required to implement written information security programs designed to protect their information system. A program must be able to protect the information system’s security and the confidentiality of nonpublic information contained therein. To implement such a program, an entity will need to conduct a risk assessment to determine any potential threats. The results of the assessment will inform the creation of program policies and procedures customized to the size and complexity of the entity.

Both regulations include these key information security program elements:

- Baseline levels of data security, including encryption of nonpublic information, and access controls (including multi-factor) to protect against unauthorized access.
- Regular penetration testing to identify weaknesses in the information system.
- Creation and implementation of procedures and plans to monitor for, detect, and respond to cyberattack incidents.
- Development of disaster recovery plans, including measures to respond to environmental hazards or technological failures.
- Personnel training that reflects relevant cybersecurity risks.
- Due diligence over third-party service providers during selection, when conducting risk assessment, while designing an information security program, and in requiring third parties to implement cybersecurity measures.

Each of these requirements, and others, must be implemented in a manner consistent with the entity’s risk assessment. As a result, each entity must create personalized plans and procedures customized to address the specific risks it is facing.

Management involvement beyond passive oversight of the information security program is a major tenet required by both laws. The laws place responsibilities on company leadership for maintaining a cybersecurity program that meets the above requirements, and ensures annual certification. The New York regulation requires each entity to designate a Chief Information Security Officer (CISO) who is responsible for overseeing and implementing the cybersecurity program. The CISO must report to the board of directors, at least annually, on the status and effectiveness of the cybersecurity program.

Once a year, the board of directors or senior officer must certify to the DFS that the entity is in compliance with the regulation’s requirements. Similarly, the South Carolina law places responsibility on the board of directors to develop, implement, and maintain the entity’s information security program. Annually, the company must certify to the South Carolina Department of Insurance that it is in compliance with the law’s requirements. Both laws require the entity to maintain documents
supporting the certification for five years.

In addition to annual certification requirements, both laws require notification when a “cybersecurity event” has occurred. The New York regulation defines a “cybersecurity event” as any attempt—even if unsuccessful—to gain unauthorized access to, disrupt, or misuse the information system or information stored on the system. The South Carolina law excludes from its cybersecurity event definition unsuccessful attempts and unauthorized access to data that was not used and has been returned or destroyed. Cybersecurity events meeting certain minimum requirements under the laws require notification to the head of the state’s respective insurance regulatory agency within 72 hours of learning the event has occurred. The entity suffering the cybersecurity event must conduct an investigation and provide a multitude of information about what transpired.

**To whom do these laws apply**

Under the South Carolina law, a “licensee”—a “person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of [South Carolina]”—is subject to the law’s requirements. Exclusions exist for a licensee that is: 1) covered by the information security program of another licensee, or 2) subject to HIPAA regulations.

Under the New York regulation, generally, any entity operating or required to operate under a license, registration, charter, certificate, permit, accreditation, or similar authorization under the DFS is required to comply with the regulation. This applies to banks, insurers, and other financial service companies doing business in New York. Certain entities, including those with fewer than 10 employees, are exempt from the requirements of both states. The New York regulation also has exemptions for businesses that do not meet certain gross revenue or total asset requirements.

**Upcoming trends in cybersecurity regulation**

Following South Carolina’s example, Rhode Island has introduced a cybersecurity law based on the NAIC Model Law. Nevada and Vermont have already enacted similar laws covering the financial service industry. And, if South Carolina offers any indication, as more and more states implement similar laws, licensees may have as few as 14 months from the date the law is enacted to implement an information security program. Given the significant amount of work that goes into such a program, licensees may find themselves scrambling when their home state passes similar regulations. The best approach, to both avoid an expensive data breach and prepare for future regulation, is to stay ahead of the upcoming wave of cybersecurity regulation and start developing an information security program now.

© 2018 PYA

*No portion of this article may be used or duplicated by any person or entity for any purpose without the express written permission of PYA.*