BEST'S REVIEW
www.bestreview.com May 2018

Insight

Regulatory/Law

A Cresting Wave

State cybersecurity requirements for insurers and producers will follow the lead of the NAIC and the N.Y. Department of Financial Services.

The NAIC adopted its Insurance Data Security Model Law in October 2017, establishing insurance industry standards for information and systems security. Rhode Island and South Carolina recently proposed legislation tracking the model. Other states will follow, contributing to a wave of cybersecurity requirements affecting the insurance industry.

The model's terminology, concepts and technical requirements track the New York DFS Cybersecurity Regulation. Despite differences, licensees subject to both laws based on the model and the DFS regulation can look to a drafter's note in the model stating compliance with the DFS regulation is deemed to be compliance with the model.

Licensees include individuals and nongovernmental entities licensed, authorized or registered (or required to be) under state insurance laws. Therefore, the model applies to virtually any insurance industry participant, except purchasing groups and risk retention groups chartered in another state, and foreign assuming insurers.

The model exempts from the requirement for a written information security program (WISP) licensees with under 10 employees, agents, representatives and designees covered by another licensee's WISP, and licensees compliant with HIPAA requirements. They must, however, comply with requirements for cybersecurity events.

As further relief for small businesses, WISP requirements consider the licensee's size and complexity, the nature and scope of its activities, and the sensitivity of its information.

By
Theodore P. Augustinos

Compliance with the New York model is deemed to be in compliance with the NAIC model.

The WISP must protect information systems, defined to include operating and control systems beyond most businesses' current cybersecurity focus. WISPs pursue objectives for security and confidentiality of nonpublic information and security of information systems; protection against threats and hazards to security and integrity of, and unauthorized access to or use of, information and systems; and record retention and destruction.

WISPs must address the following elements.

- **Risk assessment** to identify threats, and assess potential damage and sufficiency of safeguards.
- **Risk management** to mitigate identified risks, determine which of 11 security measures are appropriate, and implement such measures. Cybersecurity is included in enterprise risk management. The board of directors must exercise oversight of cybersecurity, and receive annual reporting.
- **Third-party service providers** are subject to due diligence, and cybersecurity requirements must be imposed, where vendors have access to information and systems.
- **Program adjustments** are made to keep up with, and adjust to, changes in technology, information, threats, business relationships and systems.
- **Incident response plan** in writing, addressing seven specified areas.
- **Certification** by domestic insurers to the commissioner annually on compliance with WISP requirements.

Licensees must investigate and report cybersecurity events, providing required information. These requirements differ from the DFS regulation and existing state breach notification requirements. Also, reinsurers must notify insurers, and insurers must notify producers, of certain cybersecurity events. BR

Best's Review contributor **Theodore P. Augustinos** is a partner of Locke Lord LLP, where he serves on the steering committee of the firm's Privacy & Cybersecurity Practice Group and leads its New York Department of Financial Services Cybersecurity Initiative. He can be reached at *ted.augustinos@lockelord.com*.