BEST'S REVIEW
www.bestreview.com November 2017

Regulatory/Law

Forward Vision

New York's cybersecurity regulation imposes a series of deadlines.

New York's cybersecurity regulation that went into effect in March has far reaching implications. The first transition date for implementation of several requirements of the state's Department of Financial Services regulation has passed, the NAIC has revised its draft model cybersecurity law to track the DFS requirements, and Colorado has proposed similar requirements for the securities industry. What should covered entities, including insurance companies and producers, and many others licensed in New York, be doing now?

By the first transition date of Aug. 28, covered entities had to meet several of the new requirements.

Sept. 27 was the deadline for filing a Notice of Exemption, and Feb. 15, 2018, is the deadline for filing the first annual compliance certificate. Covered entities need to identify the appropriate person to execute and file the compliance certificate, and to address any internal requirements for due diligence and documentation to support it.

The next transition date, March 1, 2018, is around the corner. By this date, each covered entity will be required to complete its first required risk assessment under written policies and procedures, and document its findings. In addition, each covered entity, unless subject to one of the limited exemptions, must fulfill the following requirements:

- Chief information security officer's annual written report to the board of directors on the company's cybersecurity risks and program.
- Continuously monitor, or conduct periodic penetration testing and vulnerability assessments.
- Multifactor or risk-based authentication.
- Cybersecurity awareness training for all personnel.

The remaining requirements have a transition date of Sept. 3, 2018, except the requirement for third-party service provider security, which is March 1, 2019. The requirements with the transition date next September include limitations on data retention, which applies to all covered entities, and the following, which do not apply to covered entities that are subject to the limited exemptions:

- Audit trail able to recreate material financial transactions and to detect and respond to certain cybersecurity events.
- Policies for security of applications within tech environment.
- Monitor activities of authorized users.
- Satisfy encryption requirements.

And then we still are not done. First, the NY DFS cybersecurity regulation requires periodic risk assessments, penetration testing and vulnerability assessments, monitoring and training of employees, reports to boards of directors, filings of compliance certificates, and notices of certain cybersecurity events.

Second, given that several required policies are based on the periodic risk assessment, they must be updated from time to time.

Third, similar requirements will certainly be imposed by other jurisdictions, and, if existing breach notification requirements are any indication, these new requirements may require state-specific attention by covered entities. Finally, rather than just tick a box on regulatory compliance, covered entities should continually monitor both the ever-changing-threat environment, and the rapid development of defensive technologies and techniques, including emerging insurance coverages, to help address these risks. BR

By
Theodore P. Augustinos

Covered entities should continually assess and respond to both the ever-changing-threat environment, and the rapid development of defensive technologies and techniques.

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*.