The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2017
PHILADELPHIA, TUESDAY, AUGUST 29, 2017 VOL 256 • NO. 41 An ALM Publication

INSURANCE LAW

5 Things Insurers' GCs and Their Boards Must Know for Cybersecurity

BY JOSHUA A. MOONEY AND RICHARD BORDEN
Special to the Legal

Cyberregulation and the meaning of reasonable cybersecurity measures are changing rapidly. Insurance companies are in the red zone for new regulatory schemes and heightening expectations of duties of care that are well beyond the responsibility of a company's CIO. In January, the New York State Department of Financial Services (NYDFS) promulgated 23 NYCRR 500, a first-of-its-kind cyberregulation that requires companies to conduct assessments of their information systems and affirmatively build cybersecurity policies and programs based on those assessments. This includes creating oversight committees of senior officers, reliable chains of communication, and internal reports to educate appropriate decision-makers. The regulation also requires companies to make determinations as to the materiality of risks and events that may implicate other reporting obligations, such as SEC reporting requirements of public entities. The approach outlined in the NYDFS regulation is catching on. Recent NAIC Insurance Data Security Model Law drafts (drafts four and five) are based on the regulation and incorporate many of the same requirements. So is pending legislation in other states.

Simply put, the regulation and other legislation to come will require insurance companies, brokers, and soon their lawyers, to change their management and corporate culture toward cybersecurity or face certain liability. For those insurers that conduct business in New York and have not yet


MOONEY


BORDEN

As the co-chair of White and William's cyber law and data protection group, **JOSHUA A. MOONEY** *guides corporate clients in assessing cyberrisks and responding to cybersecurity incidents, including data collection and breaches, identifying exposures, complying with state and federal notification requirements.*

RICHARD BORDEN *is the chief privacy officer of the firm. He is at the forefront of cybersecurity and privacy issues and focuses his practice on big data governance and the Internet of Things, cybersecurity risk management, and technology sourcing and transactions.*

> *"The regulation and other legislation to come will require insurance companies, brokers, and soon their lawyers, to change their management and corporate culture toward cybersecurity or face certain liability.*

taken action, time is running out. Here are five things that every insurance carrier, its general counsel and its board of directors should know about these new cybersecurity regulations.

• Yes, Aug. 28. Any insurer or broker who operates under a license, accreditation, or similar authorization under New York's Banking Law, the Insurance Law, or the Financial Services Law must comply with significant portions of the NYDFS regulation by Aug. 28. There is no safe harbor or time extension. The requirements include implementing and maintaining a written cybersecurity policy, implementing a cybersecurity program designed to protect the confidentiality, integrity and availability of the company's "information systems," appointing a "qualified individual" as a chief information security officer (CISO), instituting access privileges utilization of cybersecurity personnel (either in-house or through a third-party service provider), and implementation of a written incident response plan designed to promptly respond to and recover from any cybersecurity event. Assessments must include any subsidiary or affiliate of the insurer that may have access to the insurer's "information systems" or stored "nonpublic information."

By Sept. 27, any company seeking exemption from the regulation must file a notice of exemption. Because the regulation is intended to protect what NYDFS views as critical infrastructure, exemptions are very limited and only apply to companies employing 10 persons (including independent contractors) or fewer, or have less than $5 million in gross annual revenue or $10 million in total assets. Even exempt companies still must conduct a risk assessment, implement cybersecurity policy and program and institute access privileges.

The establishment of cybersecurity policies and a cybersecurity program is complex, and the manner in which they must be built makes the NYDFS regulation revolutionary. Most companies have established cyberpolicies and procedures, and then conduct a risk assessment against those policies and procedures. NYDFS requires the opposite because the cybersecurity policies and program must be based on the assessment.

Insurers first must tackle information governance issues by categorizing and inventorying "nonpublic information" housed on their "information systems" and the information systems of their affiliates, subsidiaries and vendors. Because the regulation's definition for nonpublic information goes beyond personally identifying information (PII) or personal health information (PHI) to include "business related information" the loss or disclosure of which would "cause a material adverse impact" to the company, an insurer's past data classifications or inventories (to the extent done) may be outdated. Effectively, information systems themselves must be categorized to determine criticality to operations. After conducting an appropriate inventory, each insurer must develop criteria and protocol presumptions to conduct an overall risk assessment. Only after these steps are taken, may a company begin to construct, or revise, its cybersecurity policies and program in compliance with the regulation.

• Liability starts at the top. The NYDFS regulation is modeled after *Sarbanes Oxley*. Thus, a company's board of directors or senior officer may be held liable for noncompliance because they are responsible for personally certifying the insurer's compliance with the regulation. The NYDFS regulation requires that each "covered entity," which may be numerous companies with a particular insurance carrier, certify compliance with the regulation's requirements through a designated form to be signed by either the chairman of the company's board of directors, or by a suitable "senior officer" (typically, the CEO). By Feb. 15, 2018, all companies are required to submit their first annual certification. Insurance companies and other regulated entities must maintain all data and records supporting its certification of compliance for five years. To the extent that a company has identified a system or process in its cybersecurity policies or programs that requires material improvement, the company must document the identification of the deficiency and any remedial steps undertaken to implement those improvements. The NAIC current draft model law, however, does not require personal certification like the NYDFS regulation.

• Compliance is not a one-time event. Compliance is an ever-

ongoing function. The goal of the regulation is for each insurance company to eliminate systemic risk through a living and breathing, comprehensive cybersecurity program. The regulation also requires insurers to maintain constant vigilance. Thus, periodic reports and cyber risk assessments, including penetration and vulnerability testing, are required. By March 1, 2018, the company's appointed CISO must have begun providing annual reports about the company's cyberrisks to the board of directors. Every insurer also must be engaged in periodic risk assessments, and have implemented multi-factor authentication and appropriate employee training to mitigate cyberrisk. (For many of these activities, insurers will be well-served to use outside cybercounsel to coordinate these actions and help maintain privilege.) By Sept. 3, 2018, companies must maintain technically challenging audit trails, encrypt nonpublic data (whether in transit or at rest), and have appropriate data destruction polices.

• Notice requirements can be onerous. The NYDFS regulation defines a "cyberevent" as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system." The regulation requires insurers to report "as promptly as possible but in no event later than 72 hours" after the determination of a cyberevent that either triggers a notice requirement to a government body, self-regulatory agency or other supervisory body, or that has "a reasonable likelihood of materially harming any material part of" the company's normal operations. Thus, notice requirements even apply to "unsuccessful" attacks, but only ones that the company determines are material. The NYDFS interprets the latter provision to include any cyberevent that involves material harm to a consumer. Notice to consumers, however, is governed by state or federal data breach notification laws.

NYDFS recently clarified the extent to which insurers and other companies must report unsuccessful attacks to the Department. NYDFS acknowledged that the notice requirement is "intended to facilitate information sharing about serious events" and to assist NYDFS's "overall supervision of the financial services industries." Thus, the department recognized that "most unsuccessful attacks will not be reportable," and that the regulation only "seeks the reporting of those unsuccessful attacks that, in the considered judgment of the covered entity, are sufficiently serious to raise a concern."

• These cybersecurity requirements will trickle-down. In an economic environment where conformity often equates to economic efficiency, vendors including law firms should expect insurer clients to demand that they comply with these same standards and safeguards. By March 1, 2019, insurers, including companies otherwise exempt from some portions of the regulation, must develop "minimum cybersecurity practices" required to be met by vendors in order for them to do business with insurance company. The insurance company must also have a policy and procedures to assess and evaluate the cybersecurity measures of each vendor and service provider to ensure that the "minimum cybersecurity practices" are employed. Third-party contracts also must include rep and warranty provisions addressing a vendor's cybersecurity programs and policies. The contracts also must contain what the regulation calls "contractual protections," which undoubtedly are indemnity provisions, risk-transfer, and likely the procurement of cyberinsurance. The difficulty involved in implementing these policies and procedures is the reason that it has the longest implementation period. The difficulty in defining the minimum practices may drive significant vendor consolidation to those companies willing and able to meet stringent requirements, including accepting liability if they breach the agreement.

Developing a cybersecurity compliance program, and the timing of developing processes and procedures to carry out that program, is more difficult than what a straight read of NYDFS regulation suggests. It is a highly complex and intense project interdependent upon its inner components. Yet, establishing appropriate cybersecurity policies and programs can be done. For insurance carriers, it must be done. •