Corporate Governance in Insurance: Maintaining a Culture of Compliance with New and Developing Cybersecurity Requirements



By Fred E. Karlinsky, Richard J. Fidei, Christian Brito

Cybersecurity has emerged over the past several years as one of if not the greatest concerns to the insurance industry, with multiple high-profile data breaches of insurance companies and other entities demonstrating the potential scope of the issue. The growing threat has prompted both the insurance industry and regulators to devote vast resources to cybersecurity preparedness. Overseeing the development and maintenance of protocols to effectively manage cybersecurity threats and satisfy applicable reporting requirements has become a critical corporate governance and compliance issue for insurance companies across the United States.

Maintaining an insurer's cybersecurity program and ensuring that the company complies with all legal and regulatory reporting requirements is becoming increasingly difficult.

Maintaining an insurer's cybersecurity program and ensuring that the company complies with all legal and regulatory reporting requirements is becoming increasingly difficult. In recent years, state legislatures and insurance regulatory agencies have implemented a myriad of cybersecurity legal and regulatory standards making it difficult for insurers to stay abreast of developing changes. Ultimately, ensuring compliance with new cybersecurity standards is an issue that must be addressed at the top and boards must ensure that their organizations not only comply with current standards, but that they are also prepared to comply with new and evolving standards that are being adopted across the country.

The New York Cybersecurity Regulations

The New York Department of Financial Services took the lead on establishing new cybersecurity standards applicable to banks, insurance companies, and other financial institutions when it adopted cybersecurity regulations that went into effect on March 1, 2017 (the New York Cyber Regulation). Specifically, the New York Cyber Regulation applies to "covered entities," which include any person operating under or required to operate under a license, registration, charter, or similar authorization under New York's Banking, Insurance, or Financial Services Laws.

According to NYDFS Superintendent Maria Vullo, the key goal in developing the New York Cyber Regulation was to adopt flexible standards to permit companies to assess their risks and adopt an appropriate cybersecurity program. This risk-based approach is favored by the industry over a more rigid standards-based approach. There are also some fixed standards, such as regular reporting requirements and a requirement that cybersecurity personnel regularly attend training sessions. With certain exceptions, entities covered by the regulation must periodically conduct and document a risk assessment, and certify each year to the Superintendent of Financial Services that they are in compliance with the regulation. The first certification was due by February of 2018.

Insurers should be aware of the New York Cyber Regulation, regardless of whether they operate in New York, because, as is explained further below, it has set the tone for the development of future laws and regulations that are being developed by legislatures and insurance departments across the country.

The NAIC Insurance Data Security Model Law

The National Association of Insurance Commissioners (NAIC) followed in New York's footsteps in 2017 when it approved the Insurance Data Security Model Law (the Model Law), which creates standards for data security and for the investigation of and notification to the insurance commissioner of certain cybersecurity events. The Model Law requires that covered licensees develop cybersecurity programs, conduct cybersecurity testing, and develop

This article first appeared in the Winter 2019 issue of *The Demotech Difference*, a publication of Demotech, Inc., www.demotech.com

incident response plans for breach notification procedures. While the two are not identical, the Model Law is similar to the New York Cyber Regulation and adopts many of the same concepts and terminology. Despite certain differences between the two, the drafters of the Model Law included a drafting note indicating that a company that is in compliance with the New York Cyber Regulation is also in compliance with the Model Law.

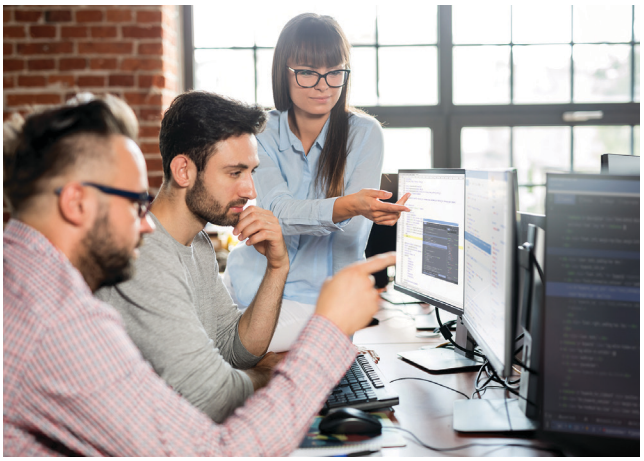
As indicated above, the Model Law applies to "licensees," which include any individual or entity (other than nongovernment agencies) operating, or required to operate, under a license, registration, or other authorization under the insurance laws of a state. Excluded from that definition are purchasing groups and risk retention groups chartered and licensed in another state as well as assuming insurers domiciled in another jurisdiction. The Model Law establishes a framework for licensees to protect the security of nonpublic information and information systems through the development of information security programs based on the insurer's risk assessment. The information security program must be designed to mitigate identified risk and must include administrative, technical, and physical safeguards for the protection of nonpublic information and information systems.

The Model Law also requires that the board of directors or a board committee is responsible for the development, implementation, and maintenance of the information security program. Moreover, the board or committee must prepare a written report, at least annually, summarizing the overall status of the information security program, the insurer's compliance with the Model Law, and other material matters, including cybersecurity events, violations of the information security program, and recommendations for changes. This requirement is significant because it creates affirmative obligations for the board and makes the board responsible for cybersecurity from a governance perspective.

As with other NAIC model laws, the Model Law will have a significant impact on the manner in which states regulate matters related to its subject matter, regardless of whether states fully implement all of its requirements. Although most states have yet to adopt the Model Law, many experts believe it eventually will become the law in the majority of United States jurisdictions. Insurance company boards should not wait until the Model Law is adopted in their backyards, but should instead immediately begin overseeing the development of information security programs by their organizations and ensure that they comply with the Model Act's requirements now.

The South Carolina Data Security Act

South Carolina became the first state to adopt the Model Law in May of 2018. The South Carolina Data Security Act (the South Carolina Act) will become effective January 1, 2019 and is nearly identical to the Model Law. Like the



REDPIXEL.PL/shutterstock.com

Model Law, the South Carolina Act requires that licensed insurers implement a comprehensive written information security program based on self-conducted, mandatory risk assessment. Insurers licensed in South Carolina must submit an annual statement to the Director certifying they are in compliance with the Act and also establish incident response plans and comply with certain reporting and response requirements in the event of a cybersecurity event. Importantly, the South Carolina Act establishes minimum requirements for a licensee's board of directors regarding the board's oversight of the licensee's information security program.

As part of the risk management process required by the South Carolina Act, insurers must evaluate whether to implement certain security measures, including implementing authentication protocols and access controls on the company's information systems, restricting access of nonpublic information, encryption of information, and conducting regular testing of its cybersecurity systems to identify actual and attempted attacks or intrusions.

Like the Model Act, the South Carolina Act differs to some extent from the New York Cybersecurity Regulations. However, unlike the Model Act, the South Carolina Cyber Act did not include the NAIC drafter's note related to compliance with the New York Cybersecurity Regulation. Indeed, it is unclear whether South Carolina will consider companies that are compliant with the New York Cyber Regulation to be compliant with the South Carolina Cyber Act. Thus, even companies that are already in compliance with the New York Cybersecurity Regulation must closely monitor developments related to the South Carolina Act if they are currently doing business in South Carolina, or wish to do business there in the future.

Conclusion

Rather than being compelled to act through regulatory action or litigation, boards should be proactive and create company-wide cybersecurity protocols that regularly test the company's cybersecurity systems, train its employees in cyber risk management, establish a data breach response and

reporting plan, and manage relationships with third-party service providers. Implementing important corporate governance mechanisms aimed at securing the company's data management and IT systems will help the board mitigate cyber risk and potential liability. Importantly, maintaining oversight over a robust cybersecurity program can help achieve a culture of compliance in light of new and evolving regulatory requirements.

Cybersecurity will continue to be a major issue affecting all companies, but it is a particular concern for companies like insurers that collect and store massive amounts of sensitive policyholder data. Insurance company directors may be exposed to legal liability if they fail to implement and oversee cybersecurity protocols in their respective organizations. Policyholders and shareholders who have been injured as a result of breaches will seek to hold the board responsible for the breaches. Regulators will continue to take action against companies that do not adequately protect their consumer data. Regulators will also continue to create regulations imposing cybersecurity requirements on directors and their companies. Effective corporate governance is the key to ensuring compliance with those regulations, satisfying the board's duty of care, and avoiding the severe consequences of a data breach.

Fred E. Karlinsky is Co-Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Fred has over twenty years of experience representing the interests of insurers, reinsurers, health plans, managing general agencies, brokers, third-party administrators, claims companies and other insurance entities on their regulatory, transactional, corporate and governmental affairs matters. He is experienced in the formation, licensure and capitalization of insurers, business expansion activities, regulatory examinations, reinsurance and alternate risk transfer mechanisms and many other operational and regulatory issues. Recognized as one of the top insurance lawyers by Chambers and Partners, Fred's extensive knowledge of insurance compliance matters and insurance related legislative and regulatory initiatives is applicable nationally and internationally. Fred can be reached at 954.768.8278 or karlinskyf@gtlaw.com.

Rich J. Fidei focuses his practice on national insurance regulatory and compliance matters as well as insurance transactional matters. He represents a wide variety of insurance entities, including insurance companies, health plans, reinsurers, producers and other insurance-related entities, in connection with regulatory, corporate, compliance and transactional issues. Rich is experienced in the formation, licensure and capitalization of insurers, business expansion activities, financial and market conduct examinations, reinsurance and alternate risk transfer mechanisms, product filings, as well as many other operational issues applicable to insurance entities. Rich can be reached at 954.768.8286 or fideir@gtlaw.com.

Christian Brito is a practice group attorney in Greenberg Traurig's Insurance Regulatory and Transactions Practice Group in Fort Lauderdale. He focuses his practice on national insurance regulatory and compliance matters. Christian represents a wide variety of insurance entities, including insurance companies, reinsurers, managing general agencies, brokers, third-party administrators, claims companies, and other insurance-related entities in connection with regulatory, transactional, corporate, and governmental affairs matters. Christian advises clients on operational, regulatory, and compliance issues, including start-up initiatives, product filings, licensure and corporate governance assessments, business expansion initiatives, and financial and market conduct examinations.

Christian received a Juris Doctor from The Pennsylvania State University Dickinson School of Law and a Bachelor of Arts from Florida International University. He is admitted to practice in Florida and Pennsylvania. He can be reached at britoc@gtlaw.com.