Regulating Insurers' CYBERSECURITY

By Karrie Hyatt

In the wake of increasingly high-profile cyber security attacks, regulatory bodies are looking to inact compulsory comprehensive cybersecurity risk management programs to emphasize data security and streamline what happens after a cyber attack. Earlier this year, the New York Department of Financial Security (NYDFS) began requiring cybersecurity programs for financial companies, including banks and insurers. The National Association of Insurance Commissioners' (NAIC) Cybersecurity (EX) Working Group is currently working on a model law to help state insurance departments regulate this growing concern.

So far, 2017 has seen a number of high-profile cyber security events. Experts agree that cyber crime is only going to get worse as people and companies become even more technology dependent. While many of the best-known events in the first half of 2017 were ransomware attacks—an attack where malware is used to take over another computer system or network and then hold its

data hostage—any type of cybercrime can have the potential to expose nonpublic information. By their very nature, insurance companies maintain a vast amount of private information for the individuals and companies they insure which makes them a significant target for a cyber security event.

Concerned for the potential cyber exposures insurers face, state regulators and those in the industry are looking for ways to prevent and counteract any attacks. Appeals have even been made to the federal government to create uniform regulation for insurers and other financial institutions. In late July, the U.S. House Committee on Small Business met with business owners and insurance representatives about the lack of uptake of cyber liability insurance by small- to medium-sized companies.

Insurance representatives took the opportunity to speak about standardizing cyber security regulation nationwide. While nearly every state has its own version of how data breaches are to be reported, this is burdensome to the industry. If regulatory processes were uniform it would help reduce insurance costs so small businesses could take better of the products available on the market.

NYDFS 23 NYCRR 500

In February of this year, NYDFS posted to the New York state register new requirements regarding cybersecurity for all NYDFS-regulated entities—including banks, insurance companies, and other financial institutions. The requirements went into effect on March 1 and affected companies need to file a Certification of Compliance with NYDFS' Cybersecurity Regulations office on an annual basis starting next February. Exempted are companies with fewer than ten employees, have less than $5 million in gross revenue, or less than $10 million in year-end total assets.

Regulation 23 NYCRR 500 emphasizes data security ahead of post-attack and reporting procedures and is quite broad in its scope. The new regulations focus on:

- Cybersecurity Program and Policy
- Risk Assessment, Penetration Testing and Vulnerability Assessments, and Audit trail
- Chief Information Security Officer, Personnel, Accesses, and Training
- Encryption of Nonpublic Information, Multi-Factor Authentication, and Limitations on Data Retention
- Third Party Service Provider Security Policy
- Incident Response Plan and Notices to Superintendent

As required, each entity must have a specially designed cybersecurity program and cybersecurity policy that includes written policies that will protect "confidentiality, integrity, and availability" of the entity's information systems. Entities must conduct periodic risk assessments of the company's information systems to inform cybersecurity programs and policies as well as monitoring and testing of the cybersecurity program and maintaining an audit trail of at least five years.

Financial entities will need to appoint a qualified Chief Information Security Officer to enforce cybersecurity policies and hire appropriate cybersecurity personnel. Companies must also limit accesses to nonpublic information and provide cybersecurity awareness training. Firms need to have controls to protect nonpublic information including encryption and multi-factor or risk-based authentication and must have policies and procedures for the secure disposal of certain nonpublic information.

Companies need to have written policies and procedures in place that identify risks involving third party services providers, including cybersecurity practices that those providers must meet, as well as due diligence processes and periodic assessments in place.

Finally, firms must have a written incident response plan that will allow them to promptly address any cybersecurity event both internally and externally as well as immediately notifying the NYDFS.

The NYDFS was very clear that risk retention groups (RRGs) would not be subject to this regulation. RRGs, while operating across state jurisdictions, are by law only to be regulated by their state of domicile. While many RRGs operate in the state of New York, there are no RRGs domiciled there.

NAIC Insurance Data Security Law

In 2015, the NAIC formed Cybersecurity (EX) Working Group as a subgroup to the Executive (EX) Committee to monitor developments in the area of cybersecurity and insurance companies. Since that time the subcommittee has been working to create a model law to help guide state insurance regulators with cybersecurity concerns. The first draft of the Insurance Data Security Law was released in early 2016 and has been undergoing a drafting process since then.

During the drafting process, in its sixth iteration at the beginning of August, parties outside NAIC members that have been active in commenting range from the American Bankers Association to Blue Cross Blue Shield Association to the National Association of Professional Insurance Agents.

The prevailing endorsement among the commenters has been the Working Group's efforts to streamline and standardized the regulation of this complex and changing issue.

The draft model law is heavily based on the NYDFS's regulation, but is more narrowly focused to just insurance companies. The primary differences from NYDFS's regulation 23 NYCRR 500 and the proposed model law are few but important. The NAIC clearly recognizes that the Board of Directors of an insurance company is primarily responsible for its cybersecurity program. The model law is more explicit regarding security breaches involving reinsurers. The NAIC's version also require more extensive information be given to the insurance commissioner in the event of an attack, but provides for confidentiality protections to keep private information from being made public.

In the drafted model law, RRGs are subject to the law, but only in the state in which they are domiciled—not in those states in which they are registered. The Liability Risk Retention Act stipulates that RRGs are only to be regulated by their domicile state, regardless of how many other states they operate in.

Captives, as the draft law stands in version 6, are not explicitly excluded from the model law. Richard Smith, president of the Vermont Captive Insurance Association (VCIA)—the largest association of its kind—wrote in a statement regarding version 5 of the model law, "VCIA recognizes that the NAIC might, in the future, seek to incorporate an Insurance Data Security Model Law as part of its accreditation standards. We note that the accreditation standards do not apply to single-parent or association captive insurance companies, or any other insurance company that does business in a single jurisdiction."

One of the most contentious points in the NAIC's version is the language concerning "Oversight of Third-Party Service Provider Arrangements." There has been much debate about the language describing third-party providers and their role in an insurer's cybersecurity program.

Smith, in his comment letter on draft version 5, voiced concern over the third-party service provider section in regards the exemption for small businesses with ten or fewer employees—including independent contractors, "Small insurers often have fewer than ten employees but may retain a manager that is a large organization with thousands of employees, such as Marsh or Aon. We do not think it is the NAIC's intent, nor do we think it would make any sense to count all of the manager's employees for purposes of determining whether a small licensee qualifies for the exemption under Section 9." He asked for further clarification on that point.

The Insurance Data Security Law was approved by the Cybersecurity (EX) Working Group at the NAIC's Summer Meeting in August. Now it will go before the Innovation and Technology (EX) Task Force for approval before being brought to the NAIC Executive (EX) Committee. Once approved by the Executive Committee it will need to be voted on by all NAIC members. From there it will go to the states for individual adoption, so nationwide uniform regulation is still several years away.

As cybersecurity threats continue to loom large uniform regulation of cybersecurity programs has become imperative—both to regulators and to the industry. ■

Karrie Hyatt is a freelance writer who has been involved in the captive industry for more than ten years. More information about her work can be found at: www.karriehyatt.com.