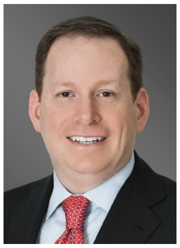
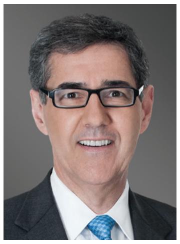
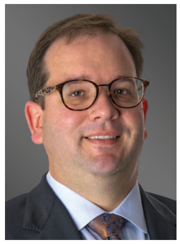
Cybersecurity and Data Privacy in the Insurance Industry: Maintaining a Culture of Compliance with Evolving Standards


By Fred E. Karlinsky, Richard J. Fidei, Timothy F. Stanfield, Christian Brito

In recent years, there have been several major data breaches involving large companies that have exposed and compromised the sensitive personal information of millions of consumers across the United States. Despite record-shattering data breaches, the United States has yet to develop a uniform and comprehensive regulatory scheme for data. Instead, there are piecemeal responses at the federal level, which, at times, compete with individual state laws.

Despite record-shattering data breaches, the United States has yet to develop a uniform and comprehensive regulatory scheme for data.

The EU General Data Protection Regulation (GDPR) only complicates matters further, because those standards and the regulators that enforce them are not bound by United States regulatory and litigation norms.

The U.S. government has generally approached privacy and security by regulating data security for specific sectors like healthcare and finance. A good example is the Health Insurance Portability and Accountability Act (HIPAA), which is the United States' primary health privacy and security law, and applies only to "covered entities" holding "protected health information." Separate privacy laws govern specific areas of the U.S. health-care system. For example, student immunizations and other school health records are generally covered by the Family Educational Rights and Privacy Act (FERPA), which was enacted in 1974.

FERPA, in turn, intersects with and sometimes conflicts with the Children's Online Privacy Protection Act of 1998, which protects data of children under the age of 13.

California enacted the first data-breach notification law in 2003, and was followed by 48 states that have since passed laws requiring individuals to be notified if their information is compromised. These laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and even what constitutes a breach. Notification requirements also vary greatly among states. For example, New Jersey requires that the state police Cyber Crimes Unit be notified, while Maryland requires that the state's attorney general be notified before any affected individual is notified.

The California Consumer Protection Act (CCPA), which takes effect on January 1, 2020, is arguably the most comprehensive privacy law in the United States. Inspired by the GDPR, the CCPA requires companies to comply with numerous requirements related to collecting and processing the personal information of California consumers, including a 12-month look-back period for consumer requests. Companies that fail to comply with these new privacy regulations may face regulatory enforcement actions, steep fines, consumer litigation and loss of customer goodwill.

The insurance industry and financial services sector are subject to some of the most recent and comprehensive data privacy and protection laws and regulations in the United States. Insurance regulators across the country have taken note of high-profile breaches involving U.S. insurers and have made cybersecurity and consumer data protection a top priority. As a result, some states have developed comprehensive cybersecurity laws and regulations that specifically apply to the insurance or financial services industries.

The New York Department of Financial Services' landmark Cybersecurity Regulations for insurance companies and financial institutions were passed in 2017 and have since taken effect. The rule requires insurance companies, banks, and other financial services companies regulated by the New York DFS to adhere to strict standards to protect consumers from cyber threats.

This article first appeared in the Winter 2020 issue of *The Demotech Difference*, a publication of Demotech, Inc., www.demotech.com.
To obtain your own copy contact BAlbert@demotech.com.

The rule implements a host of requirements including the creation and filing of an annual risk assessment, which will be used to evaluate an entity's cybersecurity policies. The assessment must include how identified risks will be evaluated; how the entity's systems and controls will be evaluated for adequacy; and how risks will be either accepted or mitigated. Another key requirement of New York's regulation is the establishment of a cybersecurity policy.

This policy should be developed based on the risk assessment, and must be approved by the company's board of directors, or board committee, as appropriate. The policy is the company's statement of how it will protect data. There are required elements of the policy, including software protections, physical safeguards, training requirements and breach response plans. The decision-making process behind the development of the policy, and any subsequent amendments, should be well documented because, like the risk assessment, the cybersecurity policy can be reviewed by regulators and their examiners.

Companies must have written policies for ensuring third-party contractors do not compromise data. The policies must include guidance for identifying risks posed by third-party service providers, minimum standards that must be adopted by contractors, guidance for selecting contractors, and guidance for the periodic evaluation of service providers.

Although planning for cybersecurity breaches is implicit in the requirements, there is a specific requirement for incident response plans. These written plans must be prepared in advance based on the risk assessment, and should describe the procedures personnel will follow and the roles and responsibility of remediating or mitigating the harm caused. There is also a notice requirement to the superintendent of the New York DFS for certain types of breaches, which, although important, is not a blanket requirement to report every breach. If the entity must report the breach to another government agency or supervisory body, such as the Financial Industry Regulatory Authority or another insurance department, then notice must also be provided to the superintendent of the New York DFS. Other breaches must only be reported if there is a "reasonable likelihood of material harm" to the entity.

In early 2016, the National Association of Insurance Commissioners (NAIC) began drafting the Insurance Data Security Model Law. This model was adopted by the NAIC in October 2017 following extensive deliberations and input from state insurance regulators, consumer representatives and the insurance industry. State adoption of the model is critical for state insurance regulators to have the tools they need to better protect sensitive consumer information.

The New York cyber regulation had a significant impact on the development of the NAIC model. The model requires

Rawpixel.com/shutterstock.com

insurers and other entities licensed by a state department of insurance to develop, implement and maintain an Information Security Program (ISP). Licensees investigate cybersecurity events in accordance with its requirements and notify the state's insurance commissioner of any cybersecurity events.

The ISP must contain administrative, technical and physical safeguards for the protection of non-public information and the licensee's information security system. The ISP should also be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the non-public information used by the licensee or in the licensee's possession, custody or control. The ISP must be developed and maintained based on an ongoing internal risk assessment.

Alabama, Delaware, Ohio, Michigan, Mississippi, and New Hampshire now join South Carolina as early adopters of the NAIC law, and versions of it have been introduced in Connecticut, Nevada and Rhode Island. Connecticut recently enacted a new law that more closely follows the New York Cybersecurity Regulation than the NAIC model.

It is important to note that, since each state will likely adopt its own version of the NAIC model, the New York Cybersecurity Regulation, or some variant of the two, we can expect to see varia-tion between state requirements over the next several years. Companies will need to decide how best to approach compliance with potentially inconsistent requirements.

In that regard, companies must ensure that they have robust compliance protocols in place to stay abreast of new and developing laws, in order to ensure that they achieve a culture of compliance within required timeframes. In addition, given the ever-evolving U.S. regulatory landscape, companies should begin implementing certain internal cybersecurity measures prior to adoption by regulators.

To that end, companies can look to legal and regulatory schemes like the New York DFS Cyber-security Regulation, the California Consumer Privacy Act, and the NAIC model as examples of requirements they will likely be required to comply with in the future.

Companies should conduct an annual risk assessment. The risk assessment should be used to in-form the entity's cybersecurity written policies and procedures. Written guidelines must include how identified risks will be evaluated, the adequacy of the entity's systems and controls, and how risks will be either accepted or mitigated. The assessment should be a meaningful review of the company's cyber resiliency. If done right, it should help an entity understand its vulnerabilities and plan accordingly. Some key areas that the cybersecurity program must cover include soft-ware protections, physical safeguards, training and breach response plans.

Insurance company boards must be involved in their companies' cybersecurity and data privacy activities and must go beyond merely "check-the-box" compliance. Cybersecurity risk is quickly morphing into enterprise risk, which creates the need for a whole-company approach. This means that cybersecurity is not just a problem for the company's IT department — today, it is everyone's problem, especially the board's.

Fred E. Karlinsky is Co-Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. Fred has more than 25 years of experience representing the interests of insurers, reinsurers and a wide variety of other insurance-related entities on their regulatory, transactional, corporate and governmental affairs matters. Fred is a recognized authority on national insurance regulatory and compliance issues and has taken a leadership position in many insurance trade organizations, has led many industry-driven legislative and regulatory initiatives, and is a sought after thought leader who has spoken and presented to insurance executives and governmental officials, both nationally and internationally.

Richard J. Fidei focuses his practice on national insurance regulatory and compliance matters. He represents a wide variety of insurance entities including insurance companies, health plans, reinsurers, managing general agencies, brokers, third-party administrators, claims companies 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

Funtap/shutterstock.com

other operational and regulatory issues applicable to insurance entities.

Timothy F. Stanfield is Of Counsel with the Florida Government Law & Policy Practice. He represents a broad array of private and public-sector clients before the Florida Legislature, Cabinet and State agencies. Tim's practice is largely focused on regulated industries to include insurance, land use, and alcoholic beverages, including addressing 'tied house evil' issues. He also represents local governments, trade associations, and clients participating in Florida's procurement process. Tim has more than a dozen years of lobbying experience, and is known within Florida's Capitol for his deep subject matter knowledge and strategic thinking.

Christian Brito 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.

About Greenberg Traurig, LLP: Greenberg Traurig, LLP (GT) has approximately 2100 attorneys in 41 locations in the United States, Latin America, Europe, Asia, and the Middle East. Web: www.gtlaw.com Twitter: @GT_Law.