STAYING COMPLIANT AMID ESCALATING CYBER THREATS

Data privacy breaches occur daily and are estimated to cost $5.5 million per breach while the worldwide cost of cybercrime is estimated to be $388 billion annually. In addition to the risk of significant financial loss, cyber attacks can ruin a company's reputation virtually overnight.

Although companies in the health care, hospitality and retail industries are considered the prime targets of cyber attacks, companies in the insurance industry share the same risks of financial and reputational loss. In fact, a recent report found that despite increased focus on data security, approximately 40 percent of the 46 major insurance organizations have experienced data breaches in the past 12 months.

The insurance industry has responded to the need for financial protection because of cyber risks by offering cyber liability insurance coverage. However, the insurance industry must recognize that it, too, is vulnerable to cyber attacks and subject to a myriad of data privacy laws and regulations. This article discusses compliance obligations that insurance companies face in the wake of these complex local, national and international regulatory schemes.

The Gramm-Leach-Bliley Act

A federal law enacted in 1999 to reform the financial services industry and to address concerns relating to consumer financial privacy, the Gramm-Leach-Bliley Act established a Privacy Rule and a Safeguards Rule applicable to nonpublic consumer personal information held by any "financial institution," which is broadly defined to include insurers, as well as insurance agents and brokers. Under the Privacy Rule, these financial institutions must send their customers privacy notices describing their protections with respect to the customers' nonpublic consumer personal information, as well as "opt-out" notices before the customers' nonpublic personal information is shared with nonaffiliated third parties.

The Safeguards Rule requires financial institutions to develop a written information security plan to protect the security and confidentiality of customer information. Violations of the Act, which preempts weaker state laws, may be enforced by the Federal Trade Commission, state insurance authorities and other federal agencies.

In 2000, the National Association of Insurance Commissioners (NAIC) adopted the Model Privacy of Consumer Financial and Health Information Regulation to implement the insurance industry privacy obligations under the Gramm-Leach-Bliley Act. The Model Regulation, which is similar to the Act, has been adopted in the vast majority of states.

HIPAA Privacy and Security Rules

The federal Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, established national health information privacy standards applicable to health care providers, health plans (including health insurance companies, HMOs and company health plans) and health care clearinghouses holding individuals' "protected health information." The HIPAA Privacy Rule, promulgated in 2000, generally prohibits the unauthorized disclosure of protected health information. Covered entities must also require by contract any "business associates" to whom they disclose protected health information—for example, insurance brokers and agents, third-party administrators of health plans, accounting firms providing services to health care providers—to appropriately safeguard the information.

The HIPAA Security Rule, promulgated in 2003, requires covered entities to maintain "reasonable and appropriate" safeguards for protecting electronic health information, which must be documented in written policies and procedures. The HIPAA Privacy and Security rules, violations of which may result in civil and criminal penalties, generally preempt less stringent state laws.

The HITECH Act and Breach Notification Requirements

The Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted in 2009 to combat the privacy and security concerns associated with the electronic transmission of health information. The act strengthens penalties for HIPAA violations, extends HIPAA violation liability to business associates (such as insurance brokers and agents), es-

tablishes an audit program mandate, and authorizes state attorneys general to bring civil enforcement actions for HIPAA violations. To implement the audit program mandate, the U.S. Department of Health and Human Services began a privacy and security audit pilot program in November 2011, and 115 audits will be conducted through December 2012.

The HITECH Act's breach notification regulations require HIPAA-covered entities to report data breaches affecting 500 or more individuals to the affected individuals, the U.S. Department of Health and Human Services, as well as to "prominent media outlets serving a state or jurisdiction." Breaches affecting fewer than 500 individuals must be reported to the department annually. In addition, business associates must notify covered entities of any breaches.

State Data Privacy Laws

Over the past several years, 46 states have enacted laws governing data privacy and security. To comply with these laws and minimize the risk of a data breach, businesses, including those in the insurance industry, must adopt security measures to protect the personal information of both their customers and their employees.

Under the data privacy laws of California and Rhode Island, for example, businesses holding unencrypted personal information of state residents must implement "reasonable security procedures and practices" and must require by contract third parties to whom they disclose such information to implement those safeguards. Further, the laws of both states require notification to affected residents of any data security breaches "in the most expedient time possible."

The Massachusetts data privacy regulations, which became effective in March 2010, are among the most burdensome in the country. The regulations apply to every "person" or other entity, including companies both inside and outside of Massachusetts, holding personal information of Massachusetts residents.

They require such entities to establish physical, administrative and technical information security measures to safeguard personal information and to develop a "written comprehensive information security program" outlining those measures. Covered entities must also require their third-party service providers (for example, payroll providers, outsourcers, contractors) to implement security measures by contract and must ensure encryption of records containing personal information stored on portable devices or transmitted over wireless networks.

In the event of a data security breach, covered entities are required to give notice to any affected Massachusetts residents, as well as to the Massachusetts Attorney General's Office and the Massachusetts Office of Consumer Affairs and Business Regulations. The Massachusetts attorney general is authorized to enforce the Massachusetts data privacy laws by bringing civil actions, which may result in substantial liability.

Under Connecticut's data privacy laws, any business holding personal information must safeguard it to prevent misuse by third parties, and any business that collects Social Security numbers in the course of its business must create a "privacy protection policy" establishing safeguards for those Social Security numbers. The laws also require those doing business in Connecticut to disclose any security breach involving unencrypted personal information to state residents and the state attorney general "without unreasonable delay."

In August 2010, the State of Connecticut Insurance Department issued Bulletin IC-25 regarding information security incidents, which applies to all entities regulated by the department, including insurance producers, property and casualty insurers, life and health insurers, public adjusters, casualty claim adjusters, and pharmacy benefit plans. The bulletin requires regulated entities to notify the Connecticut insurance commissioner of any information security breach of a Connecticut insured, member, subscriber, policyholder or provider, including those involving their business associates, within five days. The departments of insurance of several other states, including Rhode Island, Ohio and Wisconsin, have issued similar bulletins and regulations requiring insurers to notify the departments in the event of a data breach.

The Payment Card Industry Data Security Standard (PCI-DSS), an international information security standard established by the Payment Card Industry Security Standards Council, imposes a set of security requirements on organizations that handle cardholder information for major credit and debit cards, including protecting cardholder data as well as maintaining a secure network, a vulnerability management program and an information security policy. Several states, including Nevada, have incorporated the PCI-DSS requirements into their data security laws.

International Data Privacy Laws

Insurers conducting business overseas must understand the compliance challenges posed by international data privacy laws. Significantly, the European Union Data Protection Directive (Directive 95/46/EC) represents one of the strictest data privacy frameworks in the world.

The directive governs the processing

Cyber Threats | p. 36

AN EPIDEMIC: PERSONAL HEALTH INFORMATION BREACHES

Since the HITECH Act became effective in 2009, more than 477 data breaches involving nearly 21 million individuals' unsecured personal health information have been reported.

Examples of recent health information breaches include the following:

- **In March 2012, Blue Cross Blue Shield** of Tennessee, the largest health insurer in the state, settled the first enforcement action resulting from a HITECH Act breach report for $1.5 million. The action was based on an incident involving the theft of 57 unencrypted computer hard drives.
- **In March 2011, Health Net**, a California-based health insurance company, reported a data breach affecting 1.9 million individuals, which occurred when it lost server drives containing personal health information.
- **In July 2012, Accretive Health Inc.**, a Chicago-based health care consulting company and debt collection agency, reached a settlement with the Minnesota attorney general in the first direct enforcement action against a HIPAA business associate under the HITECH Act. Accretive agreed to pay $2.5 million and to cease business operations in Minnesota for at least two years due to its failure to properly safeguard health information and its unlawful collection tactics.
- **In September 2011, Tricare Management Activity**, a U.S. military health care/insurance program, reported a data breach affecting 4.6 million individuals due to the theft of electronic health record backup tapes from a vendor that handled Tricare's data. The breach resulted in the filing of several class actions seeking $4.9 billion in damages against both Tricare and its vendor.
- **In July 2012, a major Boston hospital** reported a data breach resulting from the theft of a physician's laptop, which affected as many as 3,900 patients.

Cyber Threats | continued from p. 17

of personal data and the free movement of such data and applies to all companies processing data of European residents. It permits processing of personal data only under specified circumstances, such as when the data subject has given consent or it is necessary to fulfill a contract or meet another legal obligation.

Under the directive, personal data must be processed in accordance with certain data protection principles, including the requirements that it be processed fairly and lawfully; collected only for specified, explicit and legitimate purposes; and be adequate, relevant and not excessive in relation to the purposes for which it is processed. Further, covered entities are required to implement appropriate technical and organizational measures to safeguard the data.

The directive prohibits the transfer of personal data to a non-EU country unless that country's level of protection is deemed adequate. U.S. data privacy laws have been deemed inadequate. As a result, the U.S. Department of Commerce and the European Commission negotiated the U.S.-EU Safe Harbor Framework in 2000, under which U.S. companies are permitted to receive personal data transfers from the EU if they certify that they will comply with requirements similar to those imposed by the EU Data Protection Directive. U.S. companies failing to comply with the Safe Harbor Framework have recently been subject to Federal Trade Commission enforcement actions.

In light of the growing risk of cyber threats to all businesses, including insurance companies, attorney-directed data risk assessments have become critical in detecting vulnerabilities and ensuring compliance with applicable laws. It is recommended that outside counsel be retained to preserve the attorney-client privilege applicable to any reports or other communications relating to the assessment. Such documents may also be protected by the work-product doctrine if they are prepared in anticipation of litigation, or by the "self-critical analysis privilege," which some courts have recognized in limited circumstances.

President Obama recently declared that "the cyber threat to our nation is one of the most serious economic and national security challenges we face." While companies in the insurance industry may recognize that other businesses face these cyber liability risks, they should not disregard their own vulnerabilities and compliance obligations. Complying with the complex web of data privacy laws is challenging but necessary to mitigate the liability and reputational damage that often results from data breaches today. ■

David M. Governo is the founding partner of Governo Law Firm LLC, an 18-attorney law firm in Boston, Mass. He may be reached at dgoverno@governo.com.

Corey M. Dennis is an attorney at Governo Law Firm LLC, where he practices complex litigation and dispute resolution. Dennis may be reached at cdennis@governo.com