Cybersecurity Issues in Insurance: Recent Trends and Developments



Authors from left to right:
Fred Karlinsky
Benjamin Zellner
Celeste Lawrence

In January 2015, health insurer Anthem, Inc. announced a major cyber breach that compromised the private health and personal information of approximately 80 million customers. Anthem has projected its cost stemming from this breach at upwards of $230 million, which will include the expense of future cybersecurity protection for affected and future customers. The attack was a critical reminder that more businesses, especially insurers, will be forced to confront cybersecurity issues into the foreseeable future. Fortunately, businesses, along with the federal and many state governments, heeded the lessons from Anthem's attack and undertook varying measures that yielded significant developments in cybersecurity just within the past year.

Cyber or data security encompasses the processes, procedures, technologies, and preventative measures used to protect information stored electronically on network systems from the threat of unauthorized disclosure. Threats originate from outsiders, such as hackers, organized criminal networks, and even foreign governments, as well as organizational insiders such as disgruntled employees and third party vendors. Insurance companies are particularly at risk from cyber attacks and other data breaches because of the large amount of private information on their policyholders that they store on their systems. Breaches can result in this information being compromised and potentially exploited by criminals, resulting in substantial exposure to the insurer.

It is therefore not surprising that insurance regulators have taken measures to evaluate the effectiveness of insurance companies' cyber defenses. Almost every state has enacted some sort of cybersecurity legislation, and over half of the state legislatures introduced or considered bills dealing with data breach notification requirements in 2015. Additionally, state regulators, individually and through the National Association of Insurance Commissioners (NAIC), have issued new guidance for insurers to consider in developing their cyber-defenses and related protocols.

The NAIC has also been active in addressing cybersecurity issues. In April, 2015 the Cybersecurity Task Force adopted the Principles for Effective Cybersecurity Insurance Regulatory Guidance (the Principles), which identify safeguards that regulators will expect insurers to have in place to protect consumers from cyber breaches. Moreover, the NAIC Roadmap for Cybersecurity Consumer Protections (the Roadmap), previously known as the Cybersecurity Consumer Bill of Rights, was adopted by the Executive

...a new model law could help to address the problem with the lack of uniformity of cybersecurity requirements.

Committee in December 2015. The Roadmap outlines what consumers should have a right to expect of insurance carriers and agents with regards to data collection and protection.

Some of those recommended "rights" were that consumers must know the information collected and stored by the insurer or its third party contractors; that consumers should expect companies to have privacy policies explaining their data collection practices; and that they should be notified by the company in the event of a breach and receive at least one-year of identity theft protection paid by the company if such a breach occurs. The adoption of the Roadmap was somewhat controversial because the actions it calls on insurers to undertake are often not required under state law. Some fear that the Roadmap will cause confusion for consumers, and could lead to overlapping or inconsistent obligations for insurers to comply with.

However, a new model law could help to address the problem with the lack of uniformity of cybersecurity requirements. On March 2, 2016, the Cybersecurity Task Force released a preliminary working and discussion draft of a new Insurance

Data Security Model Law, which, if adopted by the states, would create new requirements for insurers' cybersecurity programs and help to establish uniformity among state insurance cybersecurity laws. The model law defines "data breach" as "the unauthorized acquisition of personal information." "Personal information" is defined to include financial information, health information, and other private information of a consumer or entity. The model law requires insurers, producers, and third party service providers to take measures to protect from data breaches the personal information of consumers stored by the insurer, and provide notice to affected consumers and certain other entities in the event of a breach.

welcomia/shutterstock.com

Specifically, the model law requires insurance entities to implement an "Information Security Program" with the goal of protecting consumers' personal information from unauthorized breaches. The scale and scope of the Information Security Program must be appropriate relative to the size and complexity of the company and the sensitivity of the personal information to be protected. Companies are directed to use the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST), which includes several specific security measures ranging from software and hardware protections to the regular testing of cyber defenses. Companies' management would be required to assess their cyber preparedness, and provide reports to the board of directors.

The model law also requires insurance entities to adequately supervise third party service providers with access to the personal information of a company's consumers to ensure that the service provider maintains sufficient safeguards. Companies must require, by contract, that the service provider will maintain an Information Security Program, notify the company in the event of a breach, and allow the company to conduct audits, among other requirements.

The potentially expansive scope posed by cyber criminals has also drawn the attention of the federal government.

The model law also sets forth notification requirements for companies in the event of a breach. Many states already have notification requirements, but adoption of a model law may help to make the requirements more uniform from state to state. If there is a data breach, the company must notify law enforcement, the insurance commissioner, the consumer, and, in some circumstances, payment card networks or consumer reporting agencies. The timeframe to report the breach varies depending on who must be informed. Additionally, if the breach occurs at a third party service provider, the time to provide notice does not begin to run until the service provider notifies the company of the breach.

The model law specifically authorizes the commissioner to conduct examinations of an insurance entity's compliance with the law. Documents and other information furnished to the commissioner pursuant to an investigation would be confidential, although regulators from other states may share information with each other as part of their oversight of the company.

Lastly, the model law creates a private cause of action for persons whose consumer rights are violated as a result of an insurance entity's failure to comply with the law. There is a two year statute of limitations, and courts may award attorney's fees to the prevailing party. This provision could expose an insurance company to substantial liability because of the potential for class actions.

The NAIC Financial Examiner's Handbook was also updated in 2015 to include market exam protocols for financial examiners that ensure IT security becomes a consistent focus of state regulators. Furthermore, the NAIC will likely make revisions to its model laws (in addition to the new cybersecurity model law) to incorporate cybersecurity protections. Two model laws due for updates are the Insurance Information and Privacy Protection Model Act and the Model Privacy of Consumer Financial and Health Information Regulation. These laws establish standards for the collection, use and disclosure of information gathered in connection with insurance transactions with insurers, agents or support organizations

as well as establish rules to protect nonpublic personal financial and health information.

The states have also been actively assessing the insurance industry's cyber-threat preparedness, and state regulators have signaled that they will develop new cybersecurity requirements and conduct more cyber-focused examinations. The New York Department of Financial Services (NYDFS) in particular has been a leader in highlighting the challenges and risks posed to the insurance industry by cyber threats. In February 2015, NYDFS released its Report on Cyber Security in the Insurance Sector, which summarized the results of a survey NYDFS had earlier conducted. The report also described several measures NYDFS intends to take to strengthen insurers' cybersecurity measures, including: targeted assessments of "cybersecurity preparedness"; new regulations establishing cybersecurity standards; and increased scrutiny of agreements with third party vendors, which NYDFS has identified as a potential vulnerability in insurers' cybersecurity measures.

NYDFS has also analyzed insurers' Enterprise Risk Management (ERM) reports to evaluate how cybersecurity fits into a company's overall risk management framework. NYDFS expects that future ERM reports will include explicit reference to cybersecurity, and has indicated that it will revise its cybersecurity examination processes to ensure that its examiners are prepared to identify vulnerabilities and work to implement appropriate solutions. Other states have taken similar positions regarding cyber-focused examinations, and insurers and their vendors are well-advised to review their cybersecurity measures to ensure that they are prepared for threats and in compliance with all applicable requirements.

The potentially expansive scope posed by cyber criminals has also drawn the attention of the federal government. Several laws have been passed by Congress to help bolster the nation's cyber defenses, including laws meant to help protect U.S. industry. Of particular note is the Cybersecurity Act of 2015 (the "Act"), signed by President Obama on December 18, 2015. The Act seeks to combat cyber attacks by allowing the sharing of cyber threat indicators among private sector entities, as well as between the private sector and the government. The Act defines cyber threat indicators to include: information necessary to describe or identify malicious surveillance; known security vulnerabilities; methods to defeat security controls or exploit security vulnerabilities; malicious cyber command and control information; and actual or potential harm posed by particular threats. The Act also provides a liability safe harbor for information shared in good faith. Additionally, it authorizes companies to operate defensive measures on their own information systems and — with written consent — on the systems of other private entities and the federal government.

Maksim Kabakou/shutterstock.com

Efforts to combat cyber threats have also been underway internationally with the announcements of new regulations and agreements. On December 15, 2015, the European Union reached an agreement on new data protection rules aimed at modernizing and harmonizing the framework across the continent. The General Data Protection Regulation, as this agreement is called, is expected to be adopted before the summer. It will require organizations to report data breaches promptly to the authorities and the individuals affected. Furthermore, in September 2015, China reached an agreement with the United States in which it agreed not to conduct or support cyber attacks on American businesses or cybertheft of business secrets. Insurance entities with multinational operations are advised to keep abreast of these developments in order to remain in compliance with all applicable requirements.

The Cybersecurity Insurance Market

We have so far focused on potential cyber threats, but these threats have also created new opportunities for certain insurers. Specifically, the growth in cyber threats has created a new market for cyber liability insurance. According to the NAIC, managing cyber risks through insurance is expected to increase dramatically as businesses become aware that current policies do not adequately cover cyber risks.

Cybersecurity insurance is intended to mitigate losses from cyber threats, including data breaches, interruption to business operations, and network damage. Cyber liability policies are

damage. Cyber liability policies are designed to cover unique cyber risks, but these risks remain difficult for insurance underwriters to quantify because of the lack of data. Insurers rely on an applicant's risk management procedures and risk culture, creating more customized – and often more costly – policies. The type and size of a business, the number of customers, internet presence, and the type of data collected and stored are all factors that need to be considered in writing a cyber liability policy. It is hoped that cyber liability policies could become more streamlined and cost effective as the NAIC is currently developing new reporting requirements for insurers to better track cyber insurance policies issued in the marketplace.

Cybersecurity issues will not go away anytime soon. Indeed, cyber threats seem more likely to increase than to decrease for the foreseeable future. Regulators are still developing new requirements for insurers to comply with, and will likely devote substantial attention to companies' cyber defense going forward. And, while there are some signs that the market for cybersecurity insurance is maturing, significant uncertainties remain. Insurance companies and other insurance entities should monitor these developments to protect both themselves and their customers.

Fred E. Karlinsky is Co-Chair of Greenberg Traurig's Insurance Regulatory and Transactions Practice Group. With over twenty 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, he has extensive knowledge of national and international compliance matters and insurance-related legislative and regulatory initiatives. He can be reached at karlinskyf@gtlaw.com.

Benjamin Zellner focuses his practice on government law and policy matters. He is experienced handling a wide range of insurance regulatory and corporate transactions, including company and agent/agency compliance, throughout the country. Zellner can be reached at zellnerj@gtlaw.com.

Celeste Lawrence focuses her practice on government law and policy matters, including insurance regulatory, compliance matters and corporate transactions. Lawrence can be reached at lawrencece@gtlaw.com.

Greenberg Traurig, LLP is an international, multi-practice law firm with approximately 1800 attorneys serving clients from 37 offices in the United States, Latin America, Europe, Asia, and the Middle East. For additional information, please visit www.gtlaw.com.

This article first appeared in the Spring 2016 issue of The Demotech Difference, a publication of Demotech, Inc., www.demotech.com