Bloomberg BNA

Privacy and Security Law Report®

Cybersecurity Insurance

Insurance companies sit on large stores of personal data, putting them particularly at risk of a data breach. That risk has resulted in greater involvement by insurance industry major players, such as the National Association of Insurance Commissioners, as well as enhanced state regulation. In light of this changing landscape, insurance companies need to plan ahead in order to protect themselves from the repercussions of data breaches, the authors write.

Insurance

Ninety-Nine Problems but a Breach Ain't One: Cybersecurity Lessons for Insurers

By Dawn B. Williams and Christine A. Stoddard

In the movie *Wall Street*, the character Gordon Gekko famously states that information is the most valuable commodity he knows. These days, the same could be said of data, which can now be bought, sold, and, increasingly, stolen. In light of the numerous data breaches affecting companies in the U.S. and around the world, cybersecurity has become a hot topic. In fact, October has now been named National Cyber Security Awareness Month.

It seems that no one is safe—everyone from private companies like Target Corp. to government agencies like the Internal Revenue Service have found themselves facing costly data breaches. And insurance companies are sitting on large stores of personal data, putting them particularly at risk. This is significant, as both the cost and frequency of data breaches continue to grow each year. The increased risks have resulted in greater involvement by major players in the insurance industry, such as the National Association of Insurance Commissioners (NAIC), as well as enhanced regulation by state officials. For all of these reasons, it is vitally important that insurance companies take steps to protect themselves in order to help prevent breaches, manage the after-effects of those that occur and deal with inevitable compliance and enforcement initiatives.

The Cost of Data Breaches Continues to Rise

While others players in the financial services sector, such as banks, have seemingly led the pack in terms of both cybersecurity advancements and cybersecurity breaches, the insurance industry is quickly catching up on both fronts. Anthem Inc., which suffered one of the world's biggest data breaches, is a cautionary tale. In early 2015, the health insurer learned that hackers had infiltrated its system and gained access to nearly 80 million records, including Social Security numbers, ad-

 ISSN 1538-3423

dresses, e-mails and other personal information. The cause was mundane: Anthem failed to encrypt its data, and hackers were able to access the system after obtaining an employee's login information. Another health insurance company, Premera Blue Cross, suffered a data breach that affected 11 million people. According to CNN, it took the company eight months to even realize the breach had occurred. This is not unusual; the Ponemon Institute reports that the average time to respond to malicious attacks is 229 days, with an additional 82 days required to contain the damage. And every day that a breach goes unnoticed can increase the company's ultimate costs.

This is especially concerning because cyberattacks are not only becoming more common, but more sophisticated. A number of factors play a role in the increased risks insurance companies face; as noted by the New York State Department of Financial Services, personal financial, health and other information is becoming more valuable on the black market, making cyberattacks more attractive. Additionally, as technology costs decrease, cyberattacks also become easier to accomplish. And while the value of this new commodity may not be known from the hackers' perspective—indeed, these groups and individuals, which range from company employees to foreign governments, may have various motives—the cost to companies is more easily measured.

The increased data breach risks have resulted in greater involvement by major players in the insurance industry, such as the National Association of Insurance Commissioners.

According to a 2016 report by the Ponemon Institute, the average organizational cost of a cybersecurity breach in the U.S. is now over $7 million. The average cost per record is $158, but this can be significantly higher for insurance companies. It is also higher in the case of malicious attacks, which account for half of data breaches in the U.S. and increase the average to approximately $236 per record. The resulting expenses can add up quickly; according to estimates, the Anthem data breach will cost well over $100 million (the amount covered by its cybersecurity insurance policy), with some estimates as high as $16 billion.

There are reasons these costs are so significant. After a data breach occurs, companies must conduct investigations, identify the records that have been stolen and notify customers and regulators. Often large amounts of money are spent on legal fees related to both compliance and litigation. A 2016 Data Breach Investigations Report by Verizon Inc. found that legal guidance accounted for more than half of the total average cost of a data breach, followed closely by forensic investigations. Companies typically incur expenses not only to enhance their own protection moving forward but also to provide identity protection services to victims. There are also costs associated with ongoing customer communications and public relations.

Yet data breaches can have even more extensive and long-lasting ramifications; the Ponemon Institute notes that, in addition to the direct costs of the breach, the most significant cost is often lost business or churn. The average cost of lost business for U.S. companies after a breach is nearly $4 million, and companies in the financial services industry are the most likely to lose customers after a cyberattack. In a recent RAND survey, 11 percent of respondents stated that they had stopped dealing with a company after learning their information had been compromised.

Insurance companies suffering a data breach also face exposure to litigation, particularly class action lawsuits. As noted in the Carlton Fields 2016 Class Action Survey, data privacy class actions showed a modest increase in 2015, though they still account for fewer than 5 percent of all class action matters faced by large companies. Thus far, these consumer class actions have had only limited success in courts. The main stumbling block for plaintiffs looking to bring lawsuits is standing, as they must show they have suffered concrete, particularized, and imminent harm—which can be difficult when the stolen data has not been used. However, some courts have recently found the risk of future identify theft suffices to establish the injury required for standing. In light of these successes, and the increase in data breaches overall, data privacy litigation may gain more transaction in the coming years. For this reason, nearly a quarter of corporate counsel predict that the next big wave of litigation will be data breach class actions.

The Industry Responds and Regulation Increases

The NAIC has played an active role in this arena, naming cybersecurity as one of its key priorities and backing its statement up by taking numerous steps in support of that goal. It created the Cybersecurity (EX) Task Force to focus on cybersecurity regulatory activities, and it has recently focused on providing direction to both regulators and insurers. State insurance regulators share responsibility with insurance companies to promote uniform security standards in the industry and protect consumer information, and, to that end, the NAIC has set forth Principles for Effective Cybersecurity to provide guidance to both regulators and insurers in accomplishing those goals.

Nearly a quarter of corporate counsel predict that the next big wave of litigation will be data breach class actions.

The NAIC has also promulgated a Cybersecurity Bill of Rights, now known as the NAIC Roadmap for Cybersecurity Consumer Protections, which describes what insureds can expect with regard to an insurer's use of their personal information. Although requirements differ under state laws and regulations, the roadmap expresses the NAIC's expectation that, among other things, insurance companies will make certain information regarding their privacy policies available to consumers, take reasonable steps to safeguard consumer

  PVLR ISSN 1538-3423

data, provide specific notices in the event of data breaches and provide identity theft protection to consumers when such attacks occur.

In light of this push by the NAIC, insurance companies are likely to see increased regulatory action in this area. About one-third of states currently have some version of the NAIC Insurance Information Privacy Protection Model Act, which was meant to set standards for the use and disclosure of insurance data and enable consumers to access information regarding data collection. Additionally, all but three states (Alabama, New Mexico and South Dakota) now have laws in place regarding notifications that companies must send to consumers after a breach, and states take these requirements seriously. Even though Anthem was quick to publicly announce that it had suffered a data breach, the company took much longer to formally notify all affected individuals, which resulted in criticism by both the Senate health committee and a group of state attorneys general. Many state attorneys general are also empowered to investigate and enforce these laws with injunctive relief and civil penalties, which Beth Israel Deaconess Medical Center in Massachusetts learned the hard way after being fined $100,000 for the unauthorized release of patient data on a doctor's computer. Over thirty state attorneys general are also involved in a joint enforcement action against Target based on Minnesota's breach notification statute.

The NAIC has also encouraged state regulators to provide oversight in this area through market conduct examinations. Where violations are uncovered, these examinations can result in fines or other remedial measures. The NAIC has amended examiner handbooks to provide guidance in this area, and companies are already seeing this increased focus on examinations in action. Two days after Anthem disclosed its data breach, state insurance regulators announced they would be conducting a market conduct exam, the results of which are still pending. Insurance companies should prepare for such examinations the same way they prepare for a data breach—by assessing their risks, ensuring proper procedures are in place in the event a breach occurs, and taking steps to reduce the attendant costs. Insurers would also be wise to document such measures in advance of any regulatory scrutiny.

The NAIC has gone further in propounding a model law regarding the handling of data by insurance companies. Initially released in March 2016, the Insurance Data Security Model Law is meant to provide standards related to data security, investigation and breach notification. The law provides detailed requirements for security measures, requires insurers to perform threat assessments and obligates companies to monitor their third-party service providers. Further, it sets forth requirements for notification in the event of a data breach and enables state regulators to impose monetary penalties for violations.

The National Association of Insurance Commissioners has encouraged state regulators to provide oversight over data breaches through market conduct examinations

The 12-page draft inspired 131 pages of comments from interested parties and led the NAIC to publish a revised version in August, soliciting additional comments. The revised version includes a number of significant changes. Importantly, it provides some additional protection to insurers facing a breach by creating a liability carve-out where companies adequately encrypt their data and defining harm to consumers to require a ''reasonable likelihood'' of injury, which may have implications for insurers facing class action lawsuits. It also provides greater flexibility to regulators in conducting examinations and enforcing the law's provisions, and it further accounts for differences in the size of insurers and the sensitivity of the information they possess. However, it expands post-breach notification requirements, which has caused concern amongst insurers, who are already subject to various different state standards regarding notification. The public comment period for the new draft closed in September 2016, leaving insurance companies anxiously awaiting future revisions.

How Insurers Can Protect Themselves In light of this changing landscape, insurance companies need to plan ahead in order to protect themselves from the repercussions of a data breach. Insurers are targets due to the vast amounts of personal, financial, and medical data that they hold; yet, too often, they can be caught unprepared. A report by the New York State Department of Financial Services found that 42 percent of insurers had experienced at least one data breach in recent years, but only 51 percent had budgets in place to deal with such incidents. As cyberattacks become more prevalent, it is important for companies to implement strategies both to prevent data breaches and to deal with the resulting expenses well in advance.

With so much at stake as the frequency and extent of data breaches continue to increase, companies must plan ahead in order to protect themselves.

Insurance information is particularly vulnerable because it often must be shared—for example, health insurers disclose information with doctors and hospitals, which create points of weakness that put data at risk. Insurers also engage the services of numerous third party service providers. Therefore, it is critical that insurers segregate sensitive information and limit access to personal data unless strictly necessary. The NAIC has emphasized that companies must ensure their third

party service providers have appropriate controls in place to safeguard insureds' information.

The implementation of data protection tools also goes a long way towards curtailing the effects of a breach. For example, the simple use of encryption can significantly decrease expenses—or even prevent a breach altogether. Hackers are becoming more sophisticated, although sometimes the cause of a data breach is not; the New York Times reported, for example, that hackers accessed the personal and financial information of 76 million households held by JPMorgan because the bank's security team had not upgraded one of its servers to use the standard two-factor authentication, which requires a second one-time password for access. This occurred despite the fact that the company spends a reported $250 million on cybersecurity each year.

Targeted expenditures are thus helpful, but not enough—vigilance is key. A large part of this involves training employees, who can be a company's weakest link. The NAIC has emphasized the importance of training employees about cybersecurity issues and practices, and security experts reiterate that security works best when it is well-integrated within a company. Employees should be trained and warned about tactics such as social engineering, one of the most common causes of data breaches, in which hackers trick individuals in order to access company data. This can be accomplished through various forms of contact with employees—over the phone, in person, or online. Phishing scams are one of the most common techniques, pursuant to which hackers attempt to cause employees to click on a link or download an attachment that will install malware. Verizon reports that 13 percent of people will click on a phishing attachment, often very quickly. Keeping employees informed and alert can have a significant impact on a company's ability to avoid or contain a data breach.

In addition to measures meant to prevent a breach, there are numerous ways to cut down costs in the event one occurs. The amount of time it takes to detect a data breach can have a significant effect on its cost. The NAIC believes that having an incident response plan is essential to an insurer's cybersecurity program. In fact, the Ponemon Institute reports that having a dedicated response team is the most effective way to reduce expenses.

Insurers can and should gain insights from other organizations and industries as well. In promulgating its Principles for Effective Cybersecurity, the NAIC incorporated standards relied upon by the Securities Industry and Financial Markets Association as well as the cybersecurity framework set forth by the National Institute of Standards and Technology, noting that guidance for insurers should be consistent with such nationally recognized standards. The NAIC has also stated that insurers should use information-sharing in order to remain informed about threats. More and more, data security is a collaborative endeavor; the NAIC, insurance commissioners, and state regulators are all part of the Treasury Department's Financial Banking and Information Infrastructure Committee as well as the White House's Regulatory Cybersecurity Forum for Independent and Executive Branch Regulators, and they have worked with the federal government and other regulators to identify and manage security threats. Information sharing efforts can go a long way towards reducing the costs of a breach in the long-run.

Ultimately, preparation is essential. With so much at stake as the frequency and extent of data breaches continue to increase, companies must plan ahead in order to protect themselves. Insurers are experts at managing risk—and it is crucial that they manage their own in order to avoid the devastating consequences of a data breach.

   ISSN 1538-3423

PVLR ISSN 1538-3423