A CLEAR AND PRESENT DANGER

HOW INSURANCE COMPANIES CAN PROTECT THEMSELVES FROM ONLINE THREATS WITH CYBERSECURITY

Kent M. Bevan Dysart Taylor Cotter McMonigle & Montemore, PC

Cybersecurity is a serious issue that insurers face. The sooner that insurers address the potential for security breaches within their organizations, the more likely they are to prevent problems from occurring in the first place. In fact, the National Association of Insurance Commissioners (NAIC) says, "Recent high-profile data breaches have led regulators to work toward strengthening insurer defenses against attacks." In late 2014, the NAIC Executive Committee appointed the Cybersecurity Working Group to serve as the central focus for insurance regulatory activities related to cybersecurity.

THE ROLE OF INSURANCE COMPANIES AS CENTERS OF TRUST

Insurance companies are centers of trust in business and society, both as individual institutions and collectively as an industry. This stems from the fact that customers entrust their personally identifiable information (PII) to insurance companies in the course of doing business with them.

PII includes dates of birth, social security and bank account numbers, and other sensitive information. Unfortunately, this information is targeted by hackers who attempt to steal it by breaching institutions' electronic records. When this happens, those organizations can be subject to fines and litigation.

For example, as reported by the *Insurance Journal* in Oct. 2017, "Anthem Blue Cross Blue Shield and Premera Blue Cross suffered data breaches in 2015 that exposed the PII of approximately 78 million policyholders and cost those companies hundreds of millions in remediation expenses. In June 2017, Anthem agreed to pay $115 million to settle lawsuits arising from the breach. However, the total cost Anthem incurred was more than triple that amount and included $230 million for costs associated with incident response and $128 million on post-incident cybersecurity enhancements."

Some of the cybersecurity issues that insurers face in regard to protecting customer PII include:

- *They lack understanding of their existing cybersecurity measures or needs.* Cybersecurity is a complex topic to begin with. The field is also constantly changing as technologies develop. Thus, it's difficult for insurers to maintain current knowledge of cybersecurity issues, needs, and threats.

  To help with this, there are cybersecurity webinars available for mid-and-upper-level management to become more aware of the cybersecurity risks they face. There are also third-party cybersecurity experts who can perform a risk assessment for your company. While these options will cost some money, they may save a lot more by preventing a cybersecurity attack that could devastate your company and injure your company's reputation in the marketplace.

- *They believe they're safe when they're not.* There's a tendency for insurers to believe that all's well if they're not currently experiencing any problems managing or protecting PII. However, the reality may be that they're vulnerable and simply haven't been targeted yet. This is fertile ground for a crisis to develop overnight.

  For instance, perhaps your systems are password protected, but how strong are the passwords? Are some of the passwords several years old? Do you have any written cybersecurity policy about changing passwords every few months? What happens to those passwords when employees retire, transfer to another office or are terminated? This area can certainly be a point of vulnerability and needs to be addressed.

- *They have a culture that overlooks the importance of cybersecurity.* Insurers may also have cultures that present opportunities for breaches to occur either intentionally or inadvertently. For example, an article in the Harvard Business Review about a 2016 cybersecurity report by IBM indicates that 60 percent of all cyberattacks were the result of actions by company insiders. In these cases, 75 percent were malicious and 25 percent were human error. The article is entitled, "The Biggest Cybersecurity Threats Are Inside Your Company."

  Thus, some questions to ask about your culture include: Do employees

routinely or automatically open each and every email even when it seems suspicious? Do they click on attachments when there is some reason to suspect there may be a virus lurking in the attachment? What are their options in these situations? Is there only one IT person in the company who can respond to questions they may have?

MODEL CYBERSECURITY LAW AND BEST PRACTICES IN PROTECTING PII

The NAIC recently adopted an Insurance Data Model Security Law that provides a framework for how insurers can protect customer PII. The model's guidelines include:

- *Maintaining an information security program with ongoing risk assessment.* The most important aspect of cybersecurity for insurance companies is to have an established cybersecurity policy and plan. The plan must be a living document that's updated on an ongoing basis as technologies develop.

- *Overseeing third-party service providers that are part of the flow of customer data.* Insurers are still responsible for PII even when it flows to third parties through the claims process. This means insurers must be aware of their partners' cybersecurity policies and procedures as well.

- *Investigating data breaches and notifying regulators and clients.* Insurance companies have a responsibility to investigate and report on data breaches when they occur. Not only must they comply with government regulations in this regard, they must also report breaches to their customers according to the NAIC's Bill of Rights for insurance customers. Thus, a policy of preventing cybersecurity issues before they become problems is the best course of action for insurers.

Here are some best practices that insurance companies can implement to comply with the NAIC Data Model Security Law and protect their customers' PII:

- *Establish a dedicated cybersecurity role.* Insurance companies need a person or group of people within their organization that's primarily responsible for establishing and implementing cybersecurity policy. This role needs to be included among the top company executives or otherwise have decision-making authority that encompasses the entire organization.

  The person in this role must maintain current knowledge about cybersecurity technologies. Some examples of this role include a Chief Information Security Officer (CISO) or a Security Operations Center (SOC) that is a part of your insurance company's executive management team.

- *Conduct regular security assessments through outside consultation.* You should utilize the expertise of outside cybersecurity consultants on a regular basis. They can help you find cybersecurity professionals for your team, define policy parameters, and regularly test your system for vulnerability to breaches.

- *Create a culture that highly prioritizes cybersecurity.* The best way for insurers to counteract internal cybersecurity threats is through a culture that emphasizes the importance of protecting customer PII. As a result, the potential for a breach is reduced or removed whether it arises as a result of maliciousness or merely a lack of oversight. Some of the ways to establish a cybersecurity-focused culture include utilizing multifactor authentication and blockchain technology for whenever anyone needs to access your clients' PII in the normal course of business.

WHAT IS MULTI-FACTOR AUTHENTICATION?

Multi-factor authentication (MFA) is a method of ensuring that only the right person has access to the right information at the right time. For insurance companies, this means that individuals must prove who they are and that they have a good reason for accessing PII. To accomplish this, MFA systems require that users provide something they know, such as a PIN, in addition to something they possess, such as a keycard or token to access sensitive information. There are many different identification factors you can use. You can also hire an outside cybersecurity vendor to help you set up an MFA system depending on your needs.

WHAT IS BLOCKCHAIN AND HOW CAN IT HELP PROTECT THE INSURANCE INDUSTRY AGAINST CYBERSECURITY THREATS?

According to McKinsey & Company, a global management consulting firm, "A blockchain is a distributed register to store static records and/or dynamic transaction data without central coordination by using a consensus-based mechanism to check the validity of transactions. It is thus well-suited for applications requiring transparency on records with a permanent time and date stamp…" Some of the benefits insurers receive as a result of utilizing blockchain technology include:

- *Enhanced protection of PII* – Insurance customers' PII does not need to be stored on the blockchain. Instead, it remains on the user's personal device. Only its verification and related transactions are registered in the blockchain. This prevents PII from ever being exposed to breaches in the first place.

- *Reduce fraud* – According to the FBI, 5 to 10 percent of all insurance claims are fraudulent, costing non-health insurers more than $40 billion per year. Blockchain can reduce fraud through validation with a decentralized repository and historical record which can independently verify customers, policies and transactions for authenticity.

- *Increase efficiencies* – Blockchain can increase efficiencies by automating the underwriting and claims handling processes. For example, it can ensure that claims are only paid out if contract terms are met, such as a car insurance claim that is only paid out if the car is repaired in a garage preferred and predefined by the insurer.

Insurers will continue to face considerable challenges to protecting their clients' PII and other sensitive data for the foreseeable future. As security technologies develop, so will efforts to overcome them. That's why insurance companies need to take ownership of their cybersecurity needs and implement a plan to prevent breaches before they occur.

Kent M. Bevan is Of Counsel at Dysart Taylor in Kansas City, Missouri. His practice focuses on insurance law and litigation. Kent regularly writes alerts with analyses of recent court decisions involving insurance litigation which you can view at https://www.dysarttaylor.com/news-events/alerts. You can view his expanded bio at https://www.dysarttaylor.com/our-people/kent-m-bevan or contact him at kbevan@dysarttaylor.com.