Insurers Face Monumental Cybersecurity Challenges

Hackers enticed by troves of highly sensitive personal info

__Alice Kane__, senior counsel at __Clifford Chance__ in New York, advises property and casualty, life, and health insurance clients. She sat down with our editors to discuss cybersecurity in the insurance and financial services industry, including the NYDFS Cybersecurity Requirements for Financial Services Companies regulation, which went into effect on March 1 of this year, and the NAIC Insurance Data Security Model Law. She talks about how to develop the right approach to cybersecurity and what steps companies can take to ensure compliance with the new laws and regulations. Her remarks have been edited for length and style.

Prior to joining Clifford Chance, you served as the group general counsel of two Fortune 100 insurers, Zurich Insurance Group and New York Life Insurance Company. Were cyber issues top-of-mind when you started as an in-house lawyer?

Alice Kane: No, not to the degree they are today. Cybersecurity has evolved dramatically just in the past decade, and with the huge health insurance data breaches in the last few years, cyber-specific issues have come to the forefront in the insurance industry. Of course, because of the sensitive information given to insurers, especially personal financial and health information, data privacy and security have always been important issues for insurance companies.

Because of the products they sell, insurance companies have to collect very sensitive information about an individual's personal life. Life and health insurance companies often have an insured's entire medical history. Property and casualty insurance companies also collect personal information when they insure your property, car and home. Once the hackers became a real threat, cybersecurity became a real issue for the companies and regulators. Insurance companies, with their older legacy systems, are especially vulnerable.

What is going on right now with respect to cybersecurity in the insurance and financial services industries, and why is there a sudden uptake uptick in interest from regulators?

Kane: The banks had data breaches first, as you know, and it was mostly the hackers taking money out of accounts or demanding ransom not to. Then the insurance industry faced a number of well documented health insurance company data breaches in 2015. Medical and financial data belonging to as many as 11 million Premera Blue Cross customers were exposed. On the same day, Anthem, Inc. disclosed that criminal hackers had broken into its servers and potentially stolen over 78 million records. Premera, where I was insured, was hacked, so I have personally experienced the exposure of my medical information to unknown third parties. It is a real concern when your information has been taken by hackers and you have no idea how it will be used. I understand the fear and the feeling that there is so little individuals can do to protect themselves when it happens.

The state insurance regulators took note and started focusing on data protection and consumer notification in response to those data breaches. The New York Department of Financial Services (NYDFS) was the first state regulator to issue a Cybersecurity Regulation for all its licensed entities, including banks and insurance companies. The NYDFS, because they also regulate banks, had dealt with bank data breaches. So, they had professionals who were already, unfortunately, very aware and familiar with data breaches and the risks to the entity and the individual consumer.

Former Superintendent Ben Lawsky believed cyber attacks were the most important issue that the financial services system faced. As a matter of fact, that was one of the last and strongest warnings expressed as he was leaving office. Superintendent Lawsky and Executive Deputy Superintendent Maria Filipakis spent a number of years surveying and doing specific cyber examinations of both the banks and the insurance companies before NYDFS released the first-ever cybersecurity regulation. Globally and nationally, NYDFS was the first financial regulator ever to develop such an approach to the cyber threat.

The NYDFS did a lot of groundwork beforehand, trying to understand this complex issue from both the technical side and the industry side. Initially they sent a letter that outlined the major components of the proposed regulation, which required all licensed entities to establish enhanced cybersecurity programs, adopt written cybersecurity policies and procedures, and report cyber events to NYDFS. Then the first regulation came out for comment a year ago in September. After two comment periods, a final regulation was issued in December 2016. The implementation dates started this March, on a rolling basis.

At the same time, the National Association of Insurance Commissioners (NAIC), representing the 50 state insurance departments and the District of Columbia, in response to the Anthem and Premera breaches, conducted examinations, issued a statement of principles and began the process of developing a cybersecurity model law. After a few false starts and several rejected drafts, they introduced a proposed cybersecurity model law along the lines of the NYDFS approach, which is expected to be adopted by the Plenary Committee shortly.

Let's dig deeper into the NAIC's model cybersecurity law for insurance companies and the NYDFS cybersecurity requirement for its regulated financial services companies, which took effect on March 1 this year. I understand there are similarities but also important differences. Could you flesh those out and discuss some of the practical issues?

Kane: Let me start by emphasizing one critical point – the differences between the NAIC Model Law and the NYDFS Cybersecurity Regulation are not as important as the similarities. One similarity is the importance of board-level governance and responsibility. Both the regulation and the model law make it clear that cybersecurity is a board-level issue. Each regulated company must have a written cyber policy in place, and the board has to be aware of it, approve it and be routinely updated.

The NYDFS also instituted a certification process. In New York, either a board member or a high-level senior officer has to certify on an annual basis that the company is in compliance with the regulation. The NAIC model has a similar process. Clearly, regulators are taking this extremely seriously. When you require certifications from a board member or a high-level executive like the CEO or CIO, you get the attention and focus of the entire company.

Another requirement pertains to a cyber incident response and reporting obligations when an insurance company has a cyber event. There are slight differences as to timing and the substance of the reporting to regulators, but the two rules are otherwise in sync with each other.

Can you take us through a risk analysis for developing the right approach to cybersecurity? In particular, how do you advise the boards of insurance companies?

Kane: Some key issues for boards – and I have served in numerous capacities, including as secretary, chairman and independent director – involve having cyber expertise available and establishing an independent auditing process to ensure that cybersecurity programs and compliance are up to current standards and actually operating as expected.

On the governance side, we are hearing there is high demand for cyber experts to serve on boards. But even with that, an independent auditing process may still require outside expertise because board members are not there on a day-to-day basis.

The other thing you have to recognize is that everybody is going to get hacked.

Alice Kane *is a Senior Counsel at Clifford Chance in New York. She advises a wide range of clients in the insurance sector on regulatory and compliance matters, including in connection with the dynamic cybersecurity regulatory environment. Prior to joining Clifford Chance, Ms. Kane served as the Group General Counsel at Zurich Insurance Group and New York Life Insurance Company. She can be reached at Alice.Kane@CliffordChance.com.*

There is no perfect system. I was on a panel with Maria Filipakis, who developed the cybersecurity regulations in New York, and she made the point that many hacks are done by nation states. No company can successfully fight a nation state, but neither should regulators or companies lower their standards for strong cybersecurity policies. The best approach is find out what's out there, put measures in place to protect your data, keep current with technology, and stay aware of the most recent hacking events.

Companies have to be very transparent with regulators and the public if there is a breach. If companies have followed the regulations, have good policies and programs and report cyber events, I think there should be a safe-harbor protection from third-party lawsuits.

New York and the insurance industry are ahead of the rest of the country and the rest of the world. The Federal Reserve is looking at putting regulations in place. On the insurance side, the International Association of Insurance Supervisors (IAIS) is incorporating cybersecurity into its core principals of regulation.

Are there hidden issues that even sophisticated companies may not be aware of?

Kane: I'm not a technical expert, but I am absolutely sure there are. There are back doors. Third-party vendors are one of biggest vulnerabilities because a company is only as strong as its weakest link. If a vendor is working on your systems – for example, doing software updates – and they are not secure, or they have a bug that you don't know about, the company's systems are at risk.

For insurance companies that allow their agents to access systems to submit applications or file claims, the question is, what level of access is allowed. Vulnerability is not just limited to internal staff – it is a much broader problem.

What steps can companies take to prepare for cyber risks and ensure compliance with the new laws and regulations?

Kane: The insurance regulators are making requirements fairly prescriptive. If an insurance company follows the new regulations with the right level of expertise and with diligence, and if its senior executives and board are focused on cybersecurity, then the company is in the best position to withstand a data breach with minimal reputational fallout. The board and senior management involvement is critical, as is the annual compliance certification process I mentioned earlier.

The NYDFS also discusses the key the role of a chief information security officer (CISO). The CIO puts everything together in terms of technical people and outside help, but then you also have a CISO who reports to senior management and the board. The CISO is a cybersecurity expert – with the right level of expertise to confirm that the cyber program is being implemented as planned, and also that the board stays current with all of the technical changes, cyber developments and threats that are emerging every day.

What about non-U.S. jurisdictions? Can you shed some light on global developments and challenges in this area?

Kane: I attend the IAIS annual meetings and also the stakeholder meetings. After the financial meltdown, the IAIS was tasked by the G-20 and the Financial Stability Board with implementing a level of regulation for large global insurers. The IAIS is dealing with current insurance regulatory issues around the world and recently added cybersecurity to their Insurance Core Principles.

There's going to be more debate about how to regulate the industry. For one, there is the question of proportionality and what regulators can ask of a multinational company with information that is globally available, on the one hand, versus what they should require from a local company, on the other. These issues are on everyone's minds right now.

New York and the insurance industry are ahead of the rest of the country and the rest of the world.

Europe is implementing regulations left and right. Regulators are aware and want to get all industries up to a certain level of compliance to provide comfort to the public that these issues are being addressed and their personal data is secure. But despite these efforts, we must accept that no amount of regulation will ever provide 100 percent cybersecurity. The hackers are relentless and often are nation states.

Let's talk about emerging technologies such as blockchain, Bitcoin and InsurTech. Should your clients be thinking about these issues right now?

Kane: Blockchains are secure by design and use what's known as distributed ledger technology. A blockchain is a digitized, decentralized, public ledger. Originally developed as the accounting method for the virtual currency Bitcoin, blockchains are appearing in a variety of commercial applications today. In fact, a number of our insurance clients are looking at blockchain as a way to allow transactions on a more secure platform.

InsurTech is a potential disruptor of the traditional insurance industry. Many companies recognize this and are supporting startups that create value in the supply chain, reduce costs and provide invaluable customer or other insights using artificial intelligence.

Some insurance clients have set up quasi private-equity groups to fund InsurTech startups. So it's coming. Insurance is getting there later than some other industries, because it was FinTech first. But now we've gotten our own name, InsurTech, which is a big sign that we're in the game.

Beyond cyber, where do you see international and U.S. insurance regimes heading?

Kane: After the financial meltdown, it was clear that the regulated insurance entities were secure, but it was the holding company system and the unregulated entities that caused the failure of AIG. With that in mind, the IAIS started developing the Common Framework for the Supervision of Internationally Active Insurance Groups, ComFrame. The NAIC also modernized its approach to regulating insurance holding companies and adopted a Model Holding Company law with lead supervisors and supervisory colleges, where the regulators for these global companies meet with company executives and among themselves to provide comprehensive supervision.

On the insurance side, there is also a discussion about increased capital at holding company levels. In 2014 the IAIS developed the first-ever global insurance capital standard for global systemically important insurers. The IAIS has continued its work on a holding company capital standard and has recently issued a capital standard for internationally active insurance groups.

Recently, the NAIC announced that they will be working with the Federal Reserve to look at an insurance group capital calculation, maybe not capital at the holding company, but a capital calculation for a holding company.

Before we wrap up, is there anything we missed that our readers should know about in terms of what's going on with the insurance industry?

Kane: Well, one thing that really changed after the financial crisis is the communication among regulators globally. The NAIC was always the organization that allowed for communication among state regulators, but with an active IAIS and supervisory colleges for internationally active insurance groups, the communication among insurance regulators is truly global now. The insurance supervisors know each other and communicate on policy issues at the NAIC and IAIS. The supervisory colleges allow the significant regulators to meet and discuss specific company issues, and to meet and get to know company management to understand and evaluate the challenges and risks each global company faces as it does business around the world.