protiviti®

*Face the Future with Confidence*

# Cybersecurity Regulatory Issues in the Insurance Industry

Internal Audit, Risk, Business & Technology Consulting

# Introduction

The past two years have seen a dramatic increase in the amount of successful cyber-attacks in the insurance industry. Taken together, over 100 million Americans have had their personally identifiable information compromised in insurance sector data breaches. Cybercriminals know that insurance companies use and store large amounts of personal information on their policyholders, and as such, the bull's-eye on the insurance sector will continue to grow.

Three Protiviti managing directors: Adam Hamm, former North Dakota insurance commissioner, president of the National Association of Insurance Commissioners (NAIC) and chairman of its Cybersecurity Task Force; John Rao, leader of Protiviti's insurance industry practice with more than 25 years of industry experience; and Scott Laliberte, Protiviti's global leader of security and privacy solutions, share their expert opinion on the latest regulatory and cyber-related challenges facing insurers today.

Insurers are under pressure to embrace innovation and to modernize their systems and infrastructure to better compete with financial technology, or fintech, companies, which are encroaching on their traditional market space. With the advent of smartphones and digital devices, consumers are demanding financial services that are available anytime, anywhere, 24/7/365. The insurance industry is not exempt from this changing market dynamic that emphasizes real-time services with a more seamless customer experience. Some firms are seeking to modernize their legacy infrastructure, with many more relying on outsourcing to provide the services their customers are demanding, while also improving their cybersecurity defenses.

In addition to dealing with the onslaught of regulatory change, insurance companies need to be mindful of the cybersecurity risks posed by modernization projects and increased outsourcing.

# Regulatory Pressure

State insurance regulators have been working extremely hard to address the issue of cybersecurity. The National Association of Insurance Commissioners (NAIC) established a national Cybersecurity Task Force at the end of 2014.[1] The ultimate goal of the Cybersecurity Task Force is to put in place a comprehensive regulatory framework for cybersecurity. To meet this goal, the task force worked on and completed a number of important projects in 2015 and 2016.

The first project in 2015 put in place a set of guiding principles that would serve to communicate insurance regulators' overall strategy for cybersecurity.[2] A set of twelve guiding principles adopted in the spring of 2015 included, among others, obligations to protect sensitive customer information and a recognition that there is no one-size-fits-all solution, recommending that protection efforts should be scaled to the size and capacity of the regulated entity. The principles stressed the importance of incident response planning and robust oversight of the cybersecurity capabilities of vendors contracted by insurers. They also suggested incorporating cybersecurity into insurers' enterprise risk management processes, and encouraged board of directors and senior management to thoroughly understand the threat cybersecurity presents to the insurer.

The second project in 2015 sought to enhance the data security review and analysis, which is conducted by financial examiners when insurance companies undergo either a statutory or a targeted financial examination. A statutory financial exam must occur at least once every five years; a targeted financial exam occurs when facts and circumstances lead an insurance regulator to believe it is necessary. The *Financial Condition Examiners Handbook* was updated in 2015 to provide financial examiners with the necessary tools to take a much deeper dive into the cybersecurity posture of an insurer. These updates and revisions allowed for reviews of the insurers' cybersecurity training and education programs, incident response plans, postmediation analysis, third-party vendors, understanding of cybersecurity roles, and responsibilities and how cybersecurity efforts are communicated to the board of directors. These handbook enhancements are used on all financial examinations in 2016 and beyond.

The third project in 2015 put in place a formal mechanism to collect and analyze data concerning the cyber liability insurance market. Hundreds of insurance companies now sell cyber liability insurance products to American businesses. As such, insurance regulators need to gather information regarding this rapidly developing market to understand both the dynamics of this market and whether any solvency issues are developing. Cybersecurity risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate for this lack of data by setting pricing that relies on qualitative assessments of an applicant's risk management procedures and culture, which results in cyber policies being more customized and costly.

To accomplish this third project, insurance regulators adopted a Cybersecurity Insurance Coverage Supplement to the Annual Financial Statement.[3] The Annual Financial Statement must be prepared and filed with the NAIC by all property and casualty insurance companies

[1] "Insurance Regulators Establish Cybersecurity Task Force," *National Association of Insurance Commissioners (NAIC)*, published on November 19, 2014: www.naic.org/Releases/2014_docs/insurance_regulators_establish_cybersecurity_task_force.htm.

[2] "Principles for Effective Cybersecurity: Insurance Regulatory Guidance," *NAIC*, published on April 16, 2015: www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[3] www.naic.org/documents/committees_c_150312_blanks_proposal.pdf.

by the end of the first quarter of each year. With the addition of the Insurance Coverage Cybersecurity Supplement, any property and casualty insurance company selling cyberliability insurance products must also complete this supplement. The information that needs to be disclosed includes premium volume, claims reported, losses paid, defense and cost containment expenses paid, and the number of policies in force.

The fourth and final project in 2015 was the development of a road map for cybersecurity consumer protections.[4] Insurance regulators wanted to identify the rights that insurance consumers should have both before and after a data breach. The road map, which includes six separate consumer rights, was adopted in December 2015. It includes the right to know the types of personal information that is being collected and stored, the right to receive the privacy policy of an insurer, the right to have personal information protected, the right to receive a notice within 60 days after a data breach is discovered that explains the type of information involved in the breach and the actions being taken in response, and the right to receive at least one year of identity theft protection paid for by the insurance entity involved in the data breach.

In 2016, the NAIC's Cybersecurity Task Force turned its attention to drafting a formal cybersecurity model law.[5] The purpose and intent of the model law is to establish the exclusive standards for data security, investigation and notification of a data breach applicable to all insurance licensees. The model law will lay out definitions and expectations for insurance information security, breach response and the role of the regulator. Recognizing that one size does not fit all, the model law will allow for licensees to tailor their information security program depending on the size, complexity, nature and scope of activities and the sensitivity of consumer information to be protected. Most importantly, the model law is intended to create certainty and predictability for insurance consumers and licensees as they plan, protect information and respond in the difficult time immediately following a breach.

Over the course of 2016, the Cybersecurity Task Force worked on and exposed two separate and complete drafts of its Insurance Data Security Model Law and acquired extensive public feedback.[6] As 2017 begins, the Cybersecurity Task Force is now close to completion of the model law. Once complete, the model law can begin to be introduced into state legislatures for adoption and implementation.

In addition to the work of the NAIC's Cybersecurity Task Force, at least one state is also drafting its own cybersecurity regulations. New York's Department of Financial Services (NYDFS) has been working on its own cybersecurity regulations and recently announced that the final version of its regulations will be ready for adoption in March 2017.[7] Once they are officially adopted, any financial services company licensed by the NYDFS will have to incorporate the new regulations into their business operations. These new regulations mandate the implementation of a comprehensive cybersecurity policy that covers topics such as records management and third-party security, and which also places overall responsibility for cybersecurity on the board of directors and senior management.

[4] "NAIC Roadmap for Cybersecurity Consumer Protections," *NAIC*, published in 2015: www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf.

[5] www.naic.org/documents/committees_ex_cybersecurity_tf_160524_draft_ins_data_sec_model_law.pdf.

[6] www.naic.org/cmte_ex_cybersecurity_tf.htm

[7] New York Codes, Rules and Regulations (NYCRR) Title 23 Financial Services, Regulations of the Superintendent of Financial Services, Part 500, "Cybersecurity Requirements For Financial Services Companies," *New York State Department of Financial Services (NYDFS)*, December 28, 2016: http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

## Call to Action

This rapid development of cybersecurity "rules of the road" by America's insurance regulators requires boards of directors and senior management of insurance companies to think critically about a number of risk and compliance related issues, including:

01 How will their organization perform on a statutory or targeted financial exam concerning a review of their organization's cyber posture and data security?

02 If they are licensed in New York, how will they perform on a NYDFS review or examination of their cybersecurity processes and protocols?

03 Once the NAIC model is in place and starts to be adopted in more U.S. states, how will they perform on a state's review or examination of their cybersecurity processes and protocols?

04 If they sell any cyber liability insurance products, will the information they are now required to disclose to insurance regulators raise any questions that they will need to be prepared to answer or address?

It is far better for an insurance company to know the answer to these four questions, as well as take any necessary proactive steps, before a damaging data breach happens or before an insurance regulator commences a review and/or examination.

# Modernization, Innovation and Cybersecurity

Insurers, grappling with a low interest rate environment, are seeking to cut costs and drive product innovation to tap into new sources of revenue.[8] Modernizing legacy systems enables firms to leverage new technology and improve their product offering and customer experience, but it also generates new risks and control challenges.

Insurance companies that are working toward implementing cloud services and agile development, among others, are introducing new risks into the organization, which may not necessarily fit the control models and audit procedures of existing regulations. For example, insurers may need to consider how to build control points into their agile adoption process without slowing down the move to production. Traditional controls such as secure code review, security testing and change control must adapt to fit into the fast-moving agile environment. Cloud services also potentially complicate and change the traditional security and audit models. Given the third-party, multi-tenant nature of cloud services, audit procedures can be more complicated.

Organizations that are moving to the cloud need to consider security and privacy controls as well as vendor risk management when they are developing their initial cloud adoption strategy.[9] Although security and privacy concerns can be a principal barrier hindering cloud adoption for many firms, security capabilities in the cloud have matured significantly in recent years, substantially eliminating this as an obstacle to adoption. And, given the important role that cloud services will provide in a firm's infrastructure, close attention must be paid to selecting the right partner(s), developing appropriate contractual terms, aligning service levels to delivery capabilities and effectively managing the supplier relationships over time. Regulatory compliance can pose a challenge for insurers when choosing cloud vendors in terms of multi-tenancy, cross-border data sharing, and outsourcing of regulatory and compliance requirements. Periodic due diligence is also required to assess whether data security, vendor services and IT controls are up to date.

Aside from cloud service providers, there is an increased trend for insurers to outsource more services. As such, insurance companies need to pay closer attention to the cyber risk posed by vendors and ensure they have a robust vendor risk management program in place. The population of third-party providers can range from those specifically handling sensitive data to those that provide security services and key controls to the environment but which do not handle data to those that pose no risks to the security environment.

Organizations must perform risk assessments of their third-party providers to understand the security risks posed by each relationship, to develop a plan to address those risks through contracts and appropriate due diligence.

[8] See Protiviti White Paper, "Modernizing Legacy Systems in Insurance: The Case for Transforming Core IT Systems in the Insurance Industry," December 2016: www.protiviti.com/sites/default/files/united_states/insights/modernizing-legacy-systems-in-insurance-protiviti.pdf.

[9] See Protiviti White Paper, "Cloud Adoption: Putting the Cloud at the Heart of Business Strategy," August 2016: www.protiviti.com/US-en/insights/cloud-adoption-putting-cloud-heart-business-and-it-strategy.

## Call to Action

The rapid growth of third-party providers and the increased risk they pose requires firms to adopt a more pragmatic approach to adequately control the risk without exhausting their limited resources dedicated to managing third-party risk. To better manage this risk, insurance companies need to consider the following four key action points:

01 Ensure security is appropriately included in modernization plans. Make sure security representation is included in the planning and project execution phases.

02 Recognize security models will need to change with new areas such as agile and cloud adoption. Begin work early to understand and incorporate appropriate controls into the plans. Acknowledge that these are new areas which may require expertise not currently on staff. Additional training and education may be required to ensure the organization can address these new areas.

03 Consider how regulators will examine these modernized environments using the new frameworks. Begin gap assessments of the modernized environments early in the process to ensure appropriate controls, evidence and governance will support imminent examinations.

04 Begin to inventory and assess third-party providers to understand the risks they pose and develop a risk management plan.

# Final Thoughts

The convergence of three phenomena, increased regulation and the need for modernization and innovation, combined with an exponential increase in cyber risk, creates a major challenge for insurance companies that demands attention. Firms need to evaluate new technologies against the upcoming regulatory requirements and heightened cyber risk, which may identify many gaps in the existing risk and control framework that will need to be addressed. On the flip side, this process may also identify many opportunities for insurers to implement innovative controls to manage risks more effectively, such as user behavior analytics (UBA), which provides continuous detection of bad actors based on advanced analytics.

Cybersecurity and technology represent immense challenges and opportunities for all insurers and financial services companies. From a defensive perspective, an organization needs to be in a position to protect its information and data to the greatest extent possible. It also needs to be able to recover as quickly as possible in the event it is breached while balancing the need to conduct business quickly and with reasonable resources. From an offensive perspective, an organization needs to be able to take advantage of technology to meet the expectations of its customers and gain a competitive advantage in the market.

## ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

## HOW PROTIVITI CAN HELP

Protiviti is uniquely situated to help organizations protect their data and utilize technology to help grow their business to gain a competitive advantage in the market. Protiviti's deep technical understanding, combined with strong business and industry expertise, positions it well to help its clients in the insurance industry.

Protiviti has the expertise and tools to help organizations assess, understand and address cybersecurity vulnerabilities in the insurance industry. Our innovative approaches to managing risks in both traditional and modernized environments enable us to advise clients on pragmatic solutions to address risks while balancing the needs the business. We also have teams ready to rapidly deploy to help companies in the midst of a cyber crisis. Our incident response teams are trained to address the immediate issue of the crisis and also identify and address the root cause of the problem.

## CONTACTS

**John Rao**
Managing Director
+1.212.708.6372
john.rao@protiviti.com

**Adam Hamm**
Managing Director
+1.312.476.6334
adam.hamm@protiviti.com

**Scott Laliberte**
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

## THE AMERICAS

### UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

### ARGENTINA*
Buenos Aires

### BRAZIL*
Rio de Janeiro
Sao Paulo

### CANADA
Kitchener-Waterloo
Toronto

### CHILE*
Santiago

### MEXICO*
Mexico City

### PERU*
Lima

### VENEZUELA*
Caracas

## EUROPE MIDDLE EAST AFRICA

### FRANCE
Paris

### GERMANY
Frankfurt
Munich

### ITALY
Milan
Rome
Turin

### NETHERLANDS
Amsterdam

### UNITED KINGDOM
London

### BAHRAIN*
Manama

### KUWAIT*
Kuwait City

### OMAN*
Muscat

### QATAR*
Doha

### SAUDI ARABIA*
Riyadh

### SOUTH AFRICA*
Johannesburg

### UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

## ASIA-PACIFIC

### CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

### JAPAN
Osaka
Tokyo

### SINGAPORE
Singapore

### INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

### AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM



protiviti®