NAMIC® ADVOCACY

UNDERSTANDING THE EVOLVING CYBERSECURITY STANDARDS LANDSCAPE FOR INSURERS

Paul Tetrault
State & Policy Affairs Counsel
National Association Of Mutual Insurance Companies

NAMIC®
ISSUE ANALYSIS

LEAD AUTHOR

Paul Tetrault
State & Policy Affairs Counsel
ptetrault@namic.org
978.969.1046

CO-AUTHORS

Andrew Pauley
Government Affairs Counsel
apauley@namic.org
202.580.6746 x1303

Jon Bergner
Assistant Vice President, Federal Affairs
jbergner@namic.org
202.580.6751

NAMIC'S ADVOCACY LEADERSHIP

Jimi Grande
Senior Vice President, Government Affairs
jgrande@namic.org
202.580.6745

Erin Collins
Assistant Vice President, State Affairs
ecollins@namic.org
317.876.6473

Jon Bergner
Assistant Vice President, Federal Affairs
jbergner@namic.org
202.580.6751

Michelle Rogers
Assistant Vice President,
International & Regulatory Affairs
mrogers@namic.org
317.876.4270

NAMIC is the largest property/casualty insurance trade association in the country, with more than 1,400 member companies. NAMIC supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC members represent 40 percent of the total property/casualty insurance market, serve more than 170 million policyholders, and write more than $253 billion in annual premiums.

TABLE OF CONTENTS

Introduction 2

The Gramm-Leach-Bliley Act 2

State Security Breach Laws 3

Recent State Activity 4

- The NAIC Cybersecurity Task Force 4
- The NAIC Model Law 4
- Influence of the New York Regulation 5

Federal Data Security and Breach Standards 7

- NIST Cybersecurity Framework 7
- Congressional Efforts 9
- Cyber Threat Information-Sharing 10

The European Union's Data Protection Directive and GDPR 10

Policy Questions 12

Conclusion 13

INTRODUCTION

The amazing benefits of a technologically advanced and interconnected society have not been attained without the price of sobering exposure to substantial and even potentially catastrophic harm. The headlines regularly convey the latest security breaches, typically involving increasing volumes of a variety of information being accessed or stolen, affecting a larger number of individuals as potential victims.

Unsurprisingly, the insurance industry, given its role in supporting risk management by businesses and individuals, has not been immune in this area. It naturally follows that policymakers charged with protecting insurance consumers have expressed concern and explored ways to ensure that companies are acting in an appropriate and responsible manner regarding cybersecurity-related issues. In the United States, Congress, state legislatures, the National Association of Insurance Commissioners, and state insurance regulators have proposed and/or adopted a variety of public policy measures affecting insurers in response to the cybersecurity threat, and policymakers abroad have acted in similar fashion to protect their own consumers. The resulting laws and regulations were developed over a period of many years, with varying points of emphasis affecting insurers and other entities in different ways. The outcome has sometimes been criticized as a "patchwork" of laws and regulations that makes compliance a challenge.[1]

Given this history and the spate of recent activity, including the notable development by the NAIC of a cybersecurity model law intended to apply specifically to insurers and other licensees of state insurance departments, it is worth assessing how cybersecurity regulation efforts should and do function within the broader scheme of insurance regulation.

To understand this context, it is helpful to first consider the purpose of insurance regulation. Such regulation is to ensure consumer protection in two ways: by making sure insurers stay solvent so they can pay the claims they are contractually obligated to pay and by making sure insurers treat policyholders and claimants in a fair and equitable manner.[2] Regulatory concerns regarding cybersecurity of insurers arguably implicate both aspects of insurance regulation. Cybersecurity issues pose a real financial threat to insurers such as to conceivably threaten their financial strength and ultimately their solvency. The fact that insurers collect, use, and store sensitive personal information about consumers, their policyholders, and their obligation to act reasonably in how they protect that information and respond to a situation when the information is stolen or otherwise compromised is a concern for insurance regulators.

THE GRAMM-LEACH-BLILEY ACT

The first significant public policy measure addressing U.S. insurers' duty to protect sensitive information they collect from consumers was the Gramm-Leach-Bliley Act[3], more formally known as the Financial Services Modernization Act of 1999. The legislation was the product of several years of public policy discussion around broad concerns regarding the structure and flexibility of financial institutions, including banks, securities firms, and insurers.

Regarding information security, the law requires financial institutions to protect the consumer information they collect. Companies must design and implement safeguard programs, regularly monitoring and testing it. The law also requires companies to provide customers with notice of the company privacy policy and describe the conditions under which the company may disclose nonpublic personal financial information to nonaffiliated third parties and allow the customers to opt out of such information sharing.

[1] See, e.g., "An Emerging Patchwork Of Cybersecurity Rules." Michael Bahar, Susan Krawczyk, Ben Marzouk, Tony Ficarrotta, and Issa Hanna, Law360, August 29, 2017.
[2] "State Insurance Regulation." National Association of Insurance Commissioners, http://www.naic.org/documents/topics_white_paper_hist_ins_reg.pdf. The paper notes that "All regulatory functions will fall under either solvency regulation or market regulation to meet these two objectives."
[3] See https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act.

The enforcement of the GLBA's privacy requirements for insurers is left to the states as the statute allows states to adopt requirements regarding the privacy and disclosure of nonpublic personal financial information applicable to the insurance industry. To promote consistency among state standards, the NAIC developed and adopted a model privacy regulation and model bulletin.[4]

STATE SECURITY BREACH LAWS

Neither GLBA nor the NAIC privacy model established requirements for insurers to notify consumers in the event of a security breach. States, however, began enacting security breach statutes of general application to all businesses starting in 2002. California was the first state to enact such a law[5], defining personal information and security breach and requiring affected businesses to notify affected consumers. Many states followed suit during the next few years.

The vast majority of states have had breach laws on the books for many years and several have updated them over time to expand their reach or enhance consumer protections. While a few states neglected to enact such laws for many years, by 2018 all 50 states had done so.[6]

While details vary, common provisions of state breach notification laws include[7]:

- Notification to affected state residents without unreasonable delay or within set time frames;
- Notification to certain agencies including state attorneys general and/or consumer reporting agencies under certain circumstances;
- Notification exceptions for good-faith access by an employee, encryption of the data, and determinations of low risk of harm;
- Specific requirements for the content of the notification; and
- Civil penalties enforced by the state's attorneys general.

State data security and breach laws are generally enforced by the states' attorneys general. It has been observed that the involvement of attorneys general in the development of policy regarding data security and breach issues is "increasing as they grapple with changing technologies and threats, bringing to bear rapidly evolving state laws and their relatively broad consumer protection authority to engage private-sector custodians of personal data such as retailers, financial institutions, technology companies and health systems."[8]

Given their heightened role in enforcement of such laws, it is not surprising that many attorneys general have vociferously opposed federal legislation that would preempt such laws.[9]

[4] See http://www.naic.org/documents/legal_bulletin_gramm_leach_bliley_act_annual_privacy_notices.pdf.
[5] See http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.
[6] South Dakota and Alabama were the final states to act in this area.
See http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx for a full list of enactments.
[7] See https://www.lexology.com/library/detail.aspx?g=a9fadf95-6a31-4ad7-abbc-e9b13074ae52.
[8] "State Attorneys General Play Growing Data Privacy Role." J. Jasen Eige and Katherine Schroth, Law360, January 10, 2017, https://www.law360.com/corporate/articles/879583/state-attorneys-general-play-growing-data-privacy-role?nl_pk=7c0df956-f296-4967-8da5-e6bb8335f151&utm_source=newsletter&utm_medium=email&utm_campaign=corporate.
[9] See press release of Illinois Attorney General Lisa Madigan describing letter signed by 32 attorneys general opposing federal preemption legislation, http://www.illinoisattorneygeneral.gov/pressroom/2018_03/20180319b.html.

RECENT STATE ACTIVITY

THE NAIC CYBERSECURITY TASK FORCE

The NAIC took its first significant step toward developing cybersecurity policy measures when it established its Cybersecurity Task Force, which was formed in November 2014 as a task force reporting to the NAIC's Executive Committee. At the time it was established, the task force had a rather unambitious agenda. Its duties were to monitor issues, collect information, and make undefined recommendations to the Executive Committee. The task force's focus was intensely sharpened, however, in January 2015 when health insurer Anthem revealed it had experienced a breach that affected some 80 million consumers, putting insurance regulators on notice that insurance companies were prime targets of hackers.[10]

The task force soon entered a period of swift activity that is not the norm for NAIC proceedings.[11] It issued hastily developed products, offering interested parties very short time frames to weigh in with comments suggesting modifications. It started by developing a set of principles[12] intended to guide insurance regulators in addressing cybersecurity concerns. The task force then moved on to the development of a so-called "bill of rights" that consumers could or should expect in the wake of a breach affecting information held by an insurance company. Whether the document should describe rights under existing law as opposed to aspirations that might be addressed in a model became the point of significant contention, and it was modified and retitled as a "roadmap" for consumer expectations meant to be fulfilled by laws that would be enacted.[13]

Recognizing the potential solvency implications of insurers' exposures to loss from cybersecurity risk, the task force also developed updates to the NAIC's Financial Examination Handbook for revised cybersecurity protocols.[14]

THE NAIC MODEL LAW

The NAIC task force next turned to what would be its capstone project, the development of an "Insurance Data Security Model Act." The purpose of the act was to establish standards for insurers and other licensees of insurance departments for the creation and oversight of a program to nonpublic personal information as defined by the model and to set out requirements for licensees to follow in the wake of a defined cybersecurity event.

The first draft of the model – addressing data security requirements as well as describing a new breach-response protocol including consumer notification requirements – was exposed for comment in March 2016. Interested parties were given 21 days to submit comments, a process that resulted in 128 pages of commentary citing a wide range of issues with the draft.

Modifications addressing a number of issues raised by NAMIC and other interested parties were made in the next draft, but there were still many matters that needed to be worked through, necessitating a two-day session of in-person meetings and subsequently the formation of a drafting group of regulators and interested parties that convened in November 2016. NAMIC participated in both forums, advocating for changes to make the model more risk-based and flexible to recognize the diversity of licensees to which it would apply, as well as feasible and workable from a compliance perspective.

---

[10] "Massive breach at health care company Anthem Inc." Elizabeth Weise, USA Today, February 4, 2015. https://www.usatoday.com/story/tech/2015/02/04/health-care-anthem-hacked/22900925/.

[11] In addition to the Anthem breach, the NAIC may have been motivated to move quickly in this area as a result of comments by leadership at the Federal Insurance Office regarding the need to develop cybersecurity public policy strategy. See "Feds Seek Unified Approach with Insurers to Cyber Threat." Mark Hollmer, Insurance Journal, April 9, 2015. https://www.insurancejournal.com/news/national/2015/04/09/363770.htm.

[12] See http://naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[13] See http://www.naic.org/documents/committees_ex_cybersecurity_tf_related_roadmap_cybersecurity_consumer_protections.pdf.

[14] See http://www.naic.org/cipr_topics/topic_cyber_risk.htm.

INFLUENCE OF THE NEW YORK REGULATION

While the NAIC deliberations over its proposed model law were ongoing, the New York Department of Financial Services had been focusing on cybersecurity issues and developing a proposed regulation to establish standards for all financial services entities under its jurisdiction, including banks and insurance companies.

Initially, the New York initiative was viewed as problematic by some other state regulators concerned about the complications of various states adopting differing measures rather than following a model law approach. However, once the regulation[15] was adopted in final form in March 2017, regulators involved in the NAIC project started to think about whether the New York regulation – touted prominently by the DFS as the first of its kind in the nation[16] – might serve as a model for the model law.

Another significant development that took place around the same time was the advancement of the idea of bifurcating the model's data security requirements from the insurance-only security breach content to focus on the former in recognition of many areas of disagreement surrounding the latter. That idea was discussed favorably at the NAIC's 2017 Spring National Meeting, as was the notion of incorporating aspects of the New York regulation following a presentation by DFS Superintendent Maria Vullo. The revised draft of the model that was issued following that meeting reflecting both concepts was not far from the ultimate final version.

Substantive changes were being made right up to the last minute before the model's adoption. One late addition was a drafting note stating that the drafters of the model intend that compliance with New York's regulation constitutes compliance with the NAIC model. It is unclear how that provision will affect the implementation and application of the model law in practice.

[15] See https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.
[16] See DFS press release https://www.dfs.ny.gov/about/press/pr1612281.htm.

Among the key elements of the model are:

- It would require licensees to develop, implement, and maintain a comprehensive written Information Security Program and to designate someone to be responsible for the system.
- It would require a risk assessment of policies and procedures and safeguards in areas including employee training, system design; implementation of safeguards to address identified threats; and an annual assessment as well as mitigation of identified risks.
- It calls for involvement of the licensee's board through an annual report regarding the status of the safeguard program.
- It requires licensees to "exercise due diligence" in selecting third-party service providers.
- It requires submission of an annual certification of compliance to the licensee's domestic commissioner and documentation of remedial efforts to respond to identified issues.
- It requires licensees to promptly investigate any cybersecurity events to determine nature and scope, to identify nonpublic information that may have been involved, and to take steps to restore security. Records regarding such events must be kept for five years.
- It requires licensees to notify the commissioner "as promptly as possible but in no event later than 72 hours" after it has been determined that a cybersecurity event has occurred. Such notice must include as much information as possible (when, how, who, etc.), and the licensee has an ongoing obligation to update information to commissioner.
- It provides confidentiality protection to information in the control or possession of the department.

While the development of the model law has been completed, there are a few key questions that have never been answered. One is whether there is a need or appetite for a state law that applies only to insurance entities, as opposed to all business entities. During the drafting process, when the draft still contained extensive new security breach protocols for insurance licensees, several insurance commissioners expressed skepticism about the prospect of introducing such a bill in their respective states.

Another important question is whether the NAIC will make the model law an accreditation requirement, meaning it would have to be enacted in sufficiently similar manner in each state. While insurers and regulators alike have cited enhanced consistency and uniformity as a goal of the model law initiative, it is not certain that the accreditation program is an appropriate means of achieving that goal. Although a cybersecurity event can affect an insurer's financial situation, the model law is not a financial model law in the normal sense of other NAIC accreditation requirements. In addition, cybersecurity risk is already recognized and accounted for in the evaluation of an insurer's financial strength through enterprise risk and related assessments.

As the NAIC model law is introduced in state legislatures, it has been and will continue to be subject to proposed amendments by interested parties. One element that many stakeholders advocated for, but was left out of the model, was language to specify that the law would represent the exclusive cybersecurity standards for licensees to which it applies to eliminate the potential for conflicting or inconsistent standards. Additionally, while the model contains confidentiality language to protect information submitted by a licensee to an insurance department following a breach, there will be efforts to strengthen its provisions to be more consistent with other NAIC model laws in this area.

FEDERAL DATA SECURITY AND BREACH STANDARDS

NIST CYBERSECURITY FRAMEWORK

An important backdrop to any discussion of cybersecurity public policy is the National Institute of Standards and Technology's Cybersecurity Framework.[17] NIST, a nonregulatory agency of the U.S. Department of Commerce, was charged by President Obama in February 2013 by Executive Order 13636 with the creation of the Cybersecurity Framework that "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible."[18] The Cybersecurity Enhancement Act of 2014 further addressed and reiterated NIST's role in designing the Framework.[19]

After a relatively transparent process seeking public- and private-sector stakeholder input via workshops and comment periods, among other avenues, NIST released the Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 on February 12, 2014. The document advanced a risk-based approach to managing cybersecurity risk.[20] Among the more pertinent aspects of Version 1.0 of the Framework is the "Overview," which consists of three parts: the Framework Core, Implementation Tiers, and Profile.

The Framework Core encompasses homogenous critical infrastructure issues and consists of five components, including the functional needs to "Identify, Protect, Detect, Respond, and Recover."[21] The Implementation Tiers, which entail analysis of the four categories of partial, risk-informed, repeatable, and adaptive, "reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints."[22] Finally, the Framework Profile "can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario" that factors in the organization's business requirements, risk tolerance, and resources.[23]

Additionally, the Framework Roadmap is a companion to the Framework that seeks to ascertain and develop areas of high priority for alignment, development, and collaboration. There are at least 14 topics being explored in this regard.[24]

Pursuant to its executive mandates, NIST has stated from a policy standpoint the Framework is a "living and breathing" document that will continually be updated due in part to stakeholder feedback, emerging technology, and new cyber threat determinations. Along those lines, on or about April 16, 2018, Version 1.1 of the Framework was released.[25] It sought to

[17] The mission of NIST is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." NIST's "vision" includes "being the world's leader in creating critical measurement solutions and promoting equitable standards. NIST's efforts stimulate innovation, foster industrial competitiveness, and improve the quality of life." See https://www.nist.gov/about-nist/our-organization/mission-vision-values.

[18] See https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

[19] See https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[20] See https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[21] Id.

[22] Id.

[23] Id.

[24] See https://www.nist.gov/cyberframework/online-learning/introduction-framework-roadmap. Topics include confidence mechanisms, cyber-attack lifecycle, cybersecurity workforce, cyber supply chain management, federal agency cybersecurity alignment, governance and enterprise risk management, identity management, international aspects, impacts and alignment, measuring cybersecurity, privacy engineering, referencing techniques, small business awareness and resources, Internet of Things, and secure software development.

[25] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

provide a more comprehensive treatment of identity management and additional description of how to manage supply chain cybersecurity.[26] An additional development for the Framework occurred on or about May 11, 2017, when President Trump issued Executive Order 13800 mandating use of the Framework for all federal agencies.[27]

Other than President Trump's Executive Order concerning federal agencies, the Framework has always been a voluntary tool for private-sector entities to adopt on their own timetable and within their existing enterprise-wide risk management. Practical and emerging use by the private sector, including the insurance industry, has shown to be a forthcoming if not an already informally implemented foundational consideration.

For state-based insurance regulators, the NAIC mentioned the Framework standards in its 2015 document dealing with principles for cybersecurity guidance.[28] Internationally the Framework is becoming, or has already become (depending upon perspective) a potential benchmark for cybersecurity risk management discussions.[29] Further, in addition to Executive Order 13800 on the federal landscape, the Financial Stability Oversight Council, created under the Dodd-Frank Act, noted in its 2017 annual report that the NIST Framework is not supposed to be a regulatory standard per se. It noted instead that financial regulators should remain actively engaged with NIST and keep abreast of Framework developments and leverage as well as utilize that knowledge when addressing their regulated entities to "provide baseline protections across the sector."[30]

As far as uptake of the Framework by companies, there is minimal data but a great deal of discussion about usage as different industries apply it in their own unique way. Descriptive determinations are difficult because entities may fully implement or partially implement based on their current needs and perceived risks. Nevertheless, NIST states it believes that research has shown that at least 30 percent of U.S. organizations in 2015 used the Framework and that number should rise to 50 percent in 2020.[31]

This trend has allowed insurance companies to engage the Framework in underwriting decisions. Effective utilization of the Framework may allow an insurance company to understand the cyber "culture" of the company for better pricing of rates as cyber insurance continues to develop.[32]

As liability for cyber exposure increases, there is an increased incentivization for those businesses or individuals to cover that risk and purchase cyber insurance. Since cyber insurance continues to evolve with data on frequency and severity that allows pricing models to understand loss history, the Framework will inevitably factor into such models.[33]

Consequently, as it continues to grow as a working document through its implementation, the Framework will most likely play an ever-increasing role in the insurance industry either directly or indirectly.

---

[26] https://www.nist.gov/sites/default/files/documents/2018/04/16/letter_to_stakeholders_-_cybersecurity_framework_v1.1.pdf.

[27] See https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/.

[28] See http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

[29] See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf.

[30] See https://www.treasury.gov/initiatives/fsoc/studies-reports/Documents/FSOC_2017_Annual_Report.pdf. The Annual Report also re-emphasized international usage of the Framework by stating "the Council supports approaches to creating a common lexicon within both the domestic and international financial sectors. Work was initiated in this regard with the release of the G7's Fundamental Elements of Cybersecurity for the Financial Sector, which drew upon the NIST Framework and the approaches of other G7 countries to create a succinct set of non-binding effective cybersecurity risk management practices for public and private entities."

[31] See https://www.nist.gov/industry-impacts/cybersecurity. In addition, the research indicates 16 critical infrastructure sectors and more than 20 states utilize the Framework.

[32] See https://www.nist.gov/news-events/events/2016/04/cybersecurity-framework-workshop-2016. Day 3, Part 3 wherein a discussion occurred on the topic of insurance as it relates to the Framework.

[33] Beyond the scope of this document but deserves mention, discussions have occurred on implementation of the U.S. Department of Homeland Security's Cyber Incident Data and Analysis Repository pilot project and the working group Cyber Incident Data and Analysis Working Group to facilitate "the concept of a trusted cyber incident data repository among insurers, chief information security officers (CISOs), and other cybersecurity professionals within the framework of the Cyber Incident Data and Analysis Working Group (CIDAWG)." CIDAWG has released three white papers on the issue. See https://www.dhs.gov/publication/cyber-incident-data-and-analysis-working-group-white-papers.

CONGRESSIONAL EFFORTS

While Congress was the first among the policymaking bodies to take action in this area with the passage of the Gramm-Leach-Bliley Act, the last two decades have passed with the most significant developments and actions coming from other policymaking entities. Over the last four sessions of Congress, as more and more data breaches made headlines, there has been an evolving attempt to establish national standards for U.S. businesses for data protection and security breach responses. This effort is in line with a public opinion poll that found an overwhelming percentage of Americans would favor a national standard for security breaches.[34]

Beginning in the 112th Congress the discussion in Washington revolved around whether or how to mandate that all businesses comply with data security regulations, as well as exploring what kind of incentives could nudge businesses to protect their networks on their own. The House and Senate took two conflicting approaches, with the Senate granting the Department of Homeland Security the authority to determine what constituted critical infrastructure and then to set security standards that businesses would have to comply with or face penalties; later versions of the bill made the standards voluntary. The House bill eschewed setting specific standards at all. The bills were so far apart in approach that little effort was made to reconcile them before Congress adjourned.

The 113th Congress again attempted to address the federal role in preparing our nation for cyber threats. The Senate moved a bill formally codifying a project by the National Institute of Standards and Technology to draw up voluntary cyber guidelines for businesses. It called for a national research program to study the country's electronic vulnerabilities and for the development of secure ways of dealing with them. Finally, it proposed a nationwide public-awareness campaign to teach Americans about cybersecurity. Critics argued that the bill was too watered-down and did not do nearly enough to prepare our country for an attack. That bill, too, went nowhere.

Further progress was made in the 114th Congress. Both the Senate and House introduced a variety of legislation that attempted to create national data security and breach notification standards, but the debate ultimately focused on two bills. In April 2015, Sens. Tom Carper, D-Del., and Roy Blunt, R-Mo., introduced the Data Security Act, and in May 2015, Reps. Randy Neugebauer, R-Texas, and John Carney, D-Del., introduced companion legislation in the House. Originally, the bill was designed to carve out all financial services organizations from the new data security and breach investigation and notification requirements because they are already covered under the GLBA. However, it was ultimately modified to apply the standards to insurers, excluding health insurers, to be enforced by the functional state regulators. Importantly, strong preemption language would have prevented the states from rebuilding a patchwork of varied and potentially onerous standards on top of the national standard. While the House Financial Services Committee passed the bill, it did not reach the full House floor for a vote and did not move in the Senate.

[34] A poll commissioned by the U.S. Chamber of Commerce found that 86 percent of respondents indicated support for a national notification standard, with 57 percent strongly in support. See http://www.instituteforlegalreform.com/resource/ilr-summit-series-2016-are-americans-concerned-about-data-privacy-

There remained a strong appetite at the outset of the new Congress in 2017 to complete work on federal cybersecurity standards. Rep. Blaine Luetkemeyer, R-Mo., chairman of the House Financial Services Subcommittee on Financial Institutions, has been working on a bill similar to the Neugebauer-Carney legislation from the previous Congress. Despite some concern about crafting a workable mechanism by which the federal standards could be enforced by the state insurance regulators, under the draft Luetkemeyer legislation the insurance industry, excluding health insurers, would be subject to the new standard and existing state standards would be preempted. As of this writing, the draft bill has not yet been officially introduced.

Throughout 2018 the House Financial Services Committee expressed a commitment to move Luetkemeyer's bill forward through the committee process once introduced, but even if that happens, that is only one piece of the puzzle. For this issue, the House Energy and Commerce Committee has shared jurisdiction, which means, at the very least, its members would need to sign off on the legislation before it could go to the floor for a vote. As of mid-2018, the Energy and Commerce Committee dialogue has been very high-level and principles-based and no competing legislation has been introduced. Because this issue remains very complicated, it is unlikely that the House will be able to pass a bill in the near term. Additionally, the Senate has no similar legislation introduced – the chances of a federal data security and breach notification standard becoming law in 2018 is close to zero.

CYBER THREAT INFORMATION SHARING

While not acting on comprehensive legislation to establish a national security breach standard, Congress did pass the Cybersecurity Information Sharing Act in 2015, incentivizing the sharing of cyber-threat information between the private sector and government agencies. The increasing complexity of cyber incidents led many to conclude that businesses needed to improve their awareness of cyber threats and to enhance their protection and response capabilities in collaboration with government agencies. It was thought that if cyber threat indicators were shared among both public and private organizations, all would benefit from lessons learned from an attack on a single organization. This would lead to attack prevention and better law enforcement against cyber criminals.

The main provision in CISA provides protections from liability, non-waiver of privilege, and Freedom of Information Act disclosures to encourage companies to voluntarily share information – specifically, information about "cyber threat indicators" and "defensive measures" – with the federal government, state and local governments, and other companies and private entities. To qualify for these protections the information shared must meet strict requirements, such as the removal of personal information. It remains unclear as to how much this legislation has incentivized information-sharing by private companies or how much impact the new framework is actually having on improving the nation's cybersecurity. Further legislative activity may be needed in this area to accomplish the goal of a robust sharing of cyber threat information in the United States.

THE EUROPEAN UNION'S DATA PROTECTION DIRECTIVE AND GDPR

In addition to being subject to the laws and regulations enacted by Congress and the states, U.S. insurers may be required to comply with the General Data Privacy Regulation if they market products and services overseas. The GDPR is a broad information protection standard that applies to the personal information of European Union citizens. It became effective May 25, 2018.[35]

The GDPR is the product of several years of development and replaces the Data Protection Directive, which had been in effect since 1995. Among its notable features, it will require that companies report data breaches to regulatory bodies within

[35] See https://ec.europa.eu/info/law/law-topic/data-protection_en

72 hours; it will enhance privacy rights of individuals, such as by requiring affirmative consent for use of their personal information; and it will establish significant fines and private-action remedies for violations of the regulation.

In addition, the GDPR also:

- Establishes the concept of the "right to be forgotten," which requires companies to destroy data upon request "without undue delay"[36];
- Establishes the concept of data portability, meaning companies must provide a portable copy of all personal information to enable the individual to transmit or supply to others to transmit or supply to others;
- Requires data protection impact assessments[37]; and
- Requires the appointment of data protection officers or DPOs.[38] The GDPR defines responsible parties as "controllers" and "processors" and increases their respective responsibilities (especially with respect to the latter).[39]

A particular concern of U.S. insurers is the breadth of the regulation and apparent intent to hold insurers responsible extra-territorially. Insurers could see not only fines and penalties but individual lawsuits and massive class-action type of recoveries for violations of these rather broad regulations.[40] The consent provision must be analyzed as well as it may hinder operations to an extent that could make EU operations more difficult or create a significant barrier to entry into its common market. While

[36] GDPR (2016), Article 17.

[37] "3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c) a systematic monitoring of a publicly accessible area on a large scale." GDPR (2016), Article 35.

[38] GDPR (2016), Article 37.

[39] "(7) 'Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." GDPR (2016), Article 4, Sections 7 & 8.

[40] See GDPR (2016), Articles 79-82 – Contains allowances for individual and collective redress including "any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered." Also, "the data subject shall have the right to mandate a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law."

there are exceptions, the broad and vague language used will create regulatory and litigation concerns regarding ascertaining the meaning of each clause and its applicability. Further, the fact that the document is intent on providing a "fundamental right" may be in conflict with the nuances and technical needs of the insurance industry in processing needed information for basic services, including underwriting, fraud reporting, claim processing, litigation retention, reinsurance transactions, and other necessary business requirements to share information. Whether the "data subject" can hinder this needed usage is debatable and undetermined.

Additionally, the right to erase a person's data, assuming it is even possible in today's information age with redundant IT systems and regulations on disaster recovery for instance, is potentially problematic and may contradict U.S. state-based regulatory requirements for financial and market conduct record retention as well as U.S. Treasury and other federal agency requirements. Further, the cost of compliance will factor into the equation as data portability, privacy impact assessments, and the need for DPOs increase compliance expenditures. These concerns will have to be worked through in the coming years. U.S. insurers, however, must engage in a sufficient compliance effort or face the potential large-scale impact of this broad stroke of regulation.[41] The tenor and exact execution of this authority have yet to be realized.

Given that GDPR is considered a more robust and pro-consumer statute, it will undoubtedly have an influence on future public policy discussions regarding cybersecurity in other jurisdictions.

POLICY QUESTIONS

The multiplicity of statutory and regulatory measures at various levels of government intended to address cybersecurity concerns shows that policy development in this area has been and will continue to be dynamic rather than static. In light of this, it is worth considering what are the necessary and appropriate over-arching goals of cybersecurity regulation of insurers.

State insurance regulators have been described as the "cops on the beat" regarding cybersecurity oversight of insurers.[42] However, it is worth questioning whether this is a fit analogy as it portrays regulators as prepared to catch insurers doing something wrong regarding cybersecurity and impose punitive measures. The characterization fails to recognize that an insurer, like any entity that experiences a malicious cyber-attack, should be recognized as a victim along with affected consumers. Regulators should view their role as a collaborative, united with insurers in the effort to minimize cybersecurity security risks that can affect the entity and ultimately the consumers it serves.

Significantly, it also has to be recognized that no public policy measure is going to eliminate all security breaches. While some can be prevented, and the impact of those that do occur can be minimized, there is an element of inevitability regarding breaches that must be reckoned with. As stated by then-FBI Director Robert Mueller in 2012 and repeated often by many since, "there are only two types of companies: those that have been hacked and those that will be."[43] Insurers are not exempt from that conclusion.

[41] In addition to monetary fines and court action for damages, the "Supervisory Authority" of the member state(s) can impose "corrective powers" including temporary or definitive limitations including a ban on processing of information, withdrawal of the voluntary certification accreditation, and suspend data flow to a recipient. The member state can pursue criminal investigation including deprivation of profits. See e.g., GDPR (2016), preamble paragraphs 129 and 149; and Articles 42, 43 and 58.

[42] See testimony of Adam W. Hamm, commissioner North Dakota Department of Insurance on behalf of the National Association of Insurance Commissioners before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies Committee on Homeland Security, United States House of Representatives, "The Role of Cyber Insurance in Risk Management," March 22, 2016.
See http://www.naic.org/documents/government_relations_160322_testimony_hamm_cyber_insurancer_risk_managment.pdf.

[43] Prepared Remarks of Robert S. Mueller, III, director, Federal Bureau of Investigation, RSA Cyber Security Conference, San Francisco, Calif., March 1, 2012, https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

Beyond that, it must be recognized that there are incentives other than regulatory requirements and associated penalties that may be sufficient to prompt commercial entities, including insurers, to adopt best practices and appropriate measures to protect themselves and the consumers they interact with from cybersecurity threats. If motivators like reputational risk and the goal of maintaining consumers can do the job, then it is reasonable to question the need for more expansive and aggressive regulatory measures that have associated costs and other potentially adverse unintended consequences.

An interesting juxtaposition of views on this point was presented by comments from two prominent federal sources in late 2017. First, the Treasury issued a report on creating economic opportunities in the areas of asset management and insurance, including among its recommendation, "prompt adoption of the NAIC Insurance Data Security Model Law by the states."[44] Then, just weeks later, Arthur Lindo, senior associate director of the Federal Reserve's Division of Supervision and Regulation, made headlines when he commented at a New York banking conference that, "I don't think the solution to the cybersecurity problem rests in regulation," adding, "We're going to try a more flexible approach."[45]

Apart from the question of whether more, or more stringent, regulations are necessary, it is highly questionable whether it makes sense for the states to have different breach requirements, with distinctions in application and enforcement even if most take common approaches. A related question is whether federal preemption regarding creation of national standards should or should not be viewed as a potentially problematic encroachment on the state insurance regulatory system.

CONCLUSION

Cybersecurity issues are not going away. To the contrary, they are expected to evolve and potentially increase over time. As the regulatory landscape continues to develop in response to such evolution and growth, insurers will need to be active participants in public policy debates. And because cybersecurity issues are something that all citizens have some awareness of, it is natural to expect the policymakers who represent their interests at all levels – local, state, federal, and even international – to be active in this area. Ultimately, cybersecurity will need to remain a top priority for insurers.

[44] U.S. Treasury Report, "A Financial System That Creates Economic Opportunities – Asset Management and Insurance," https://www.treasury.gov/press-center/press-releases/Documents/A-Financial-System-That-Creates-Economic-Opportunities-Asset_Management-Insurance.pdf.
[45] "Regulation Can't Solve Cybersecurity Problems, Fed Official Says." Yalman Onaran, Bloomberg.com, November 6, 2017, https://www.bloomberg.com/news/articles/2017-11-06/regulation-can-t-solve-cybersecurity-problems-fed-official-says.

NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

3601 Vincennes Road | Indianapolis, IN 46268 | 317.875.5250
20 F Street, NW, Suite 510 | Washington, D.C. 20001 | 202.628.1558

NAMIC

NATIONAL ASSOCIATION OF
MUTUAL INSURANCE COMPANIES