REGULATING THE CYBERSECURITY OF INSURANCE COMPANIES IN THE UNITED STATES

M. Bob Kao*

Abstract

While cybersecurity has been an important issue for all business sectors due to the rapid development of and reliance on technology and the increasing sophistication of unlawful actors, it is particularly significant for insurance companies because of the nature of the industry. The internet makes it possible to collect and store massive amounts of data, and this in turn requires the utmost confidence of consumers in the companies collecting this data. The growing concern for cyber risks has compelled insurance regulators to devise and implement frameworks and rules for insurance companies to follow. In the United States, insurance regulation is controlled by the states. Invariably, the enthusiasm and speed of responses have been mixed. New York has implemented the Cybersecurity Requirements for Financial Services Companies, while South Carolina, Ohio, Michigan, and Mississippi have passed laws based on the Insurance Data Security Model Law published by the National Association of Insurance Commissioners (NAIC), a non-governmental entity created and composed of insurance commissioners of each state and territory. The specific provisions within these regulations differ, which creates inconsistencies throughout the United States. As more states adopt cyberspace policies regulating the insurance industry, the divergence could worsen. This paper examines the NAIC Model

* Research Associate, York Law School, University of York; PhD Candidate, Centre for Commercial Law Studies, Queen Mary University of London. I would like to thank Ken Montenegro for his technical advice, anonymous reviewers for the ACM Inaugural Symposium on Computer Science and Law for their constructive criticism of the manuscript, and the editors of *Transactions: The Tennessee Journal of Business Law* for their tireless efforts. All laws referenced in this paper are current as of September 1, 2019. All errors remain my own.

Law and regulations in various states, as well as advocates for a uniform standard across the United States based on the New York regulations due to its robust nature.

I. Introduction

Cybersecurity is a necessity for all individuals, organizations, businesses, and governmental agencies in today's connected world. Threats or attacks on one part of a network may be detrimental to a whole system due to the Internet of Things.[1] The fastest growing crime in the United States, cybercrimes are projected to cost US $6 trillion in damages worldwide in 2021, which has been characterized as "the greatest transfer of economic wealth in history."[2] Cyber crime is the fast growing crime in the United States and is projected to cost . . . . The most targeted industries for cybercrimes are healthcare, manufacturing, financial services, government, and transportation.[3] The international cyber security market devoted to protection from cyber attacks was valued at $136 billion in 2017, and the total global insurance premium for cyber policies is estimated to reach US $23 billion by 2025, up from roughly US$4 billion in 2019.[4]

The potential for catastrophic financial losses caused by breaches of cybersecurity has led many companies to purchase insurance designed to cover liabilities resulting from an attack.[5] These cybersecurity insurance

---

[1] Gerald Feltman, *The Next Great Battlefront*, *in* ISSUES IN MARITIME CYBER SECURITY 527, 530 (Joseph DiRenzo III, Nicole K. Drumhiller, & Fred S. Roberts eds., 2017).

[2] Steve Morgan, *Cybercrime Damages $6 Trillion By 2021*, CYBERSECURITY VENTURES (Dec. 7, 2018) https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[3] Steve Morgan, *2019 Cybersecurity Almanac: 100 Facts, Figures, Predictions and Statistics*, CYBERSECURITY VENTURES (Feb. 6, 2019), https://cybersecurityventures.com/cybersecurity-almanac-2019/.

[4] Morris Beck, *Global Cyber Security Market Analysis 2019 Dynamics, Trends, Revenue, Regional Segmented, Outlook & Forecast Till 2025*, INDUSTRY REPORTS (Apr. 5, 2019), https://industryreports24.com/69485/global-cyber-security-market-analysis-2019-dynamics-trends-revenue-regional-segmented-outlook-forecast-till-2025; Bruce Sussman, *5 Reasons Cyber Insurance Market Will Hit $23 Billion*, SECURE WORLD (April 16, 2019), www.secureworldexpo.com/industry-news/5-reasons-cyber-insurance-market-will-hit-23-billion.

[5] Be that as it may, it has been reported that 68% of businesses in the United States "have not purchased any form of cyber liability of data-breach coverage." *At a Glance: Cyber Security and Insurance*, CISCO, www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/cybersecurity-solutions/cyber-security-insurance-aag.pdf (last visited June 4, 2019). For more information on cyber risk insurance, *see, e.g.*, Christopher C. French, *Insuring Against Cyber Risk: The Evolution of an Industry (Introduction)*, 122 PENN ST. L. REV. 607 (2019); Mark Camillo, *Cyber Risk and the Changing Role of Insurance*, 2 J.

policies usually mandate that the policyholders maintain proper preventative measures and follow best practice guidelines in order for cyber risk coverage to be maintained.[6] While the insurers are mandating the insureds to take measures to be secure, it may be pertinent to ask whether the insurers themselves are maintaining cyber resilience.[7] In other words, what are insurance companies doing about their own cybersecurity?

The answer depends on where the insurance company is located, as insurance regulation varies by jurisdiction. The focus of this paper is on the United States. Due to the unique historical development of insurance regulation in the United States, the industry is mostly regulated by the individual states.[8] Consequently, the regulations by which the companies must abide are promulgated by state legislatures and enforced by state regulatory agencies, resulting in disparate standards across the country. Though the insurance industry trade organization, the National Association of Insurance Commissioners (hereinafter "NAIC"), serves as a national standard setting agency that seeks to harmonize insurance regulatory rules, it does not necessarily have the power to make harmonization mandatory.[9] Nonetheless, in the past couple of years, some

---

CYBER POL'Y 53 (2017); Margaret A. Reetz et al., *Cyber Risks: Evolving Threats, Emerging Coverages, and Ensuing Case Law*, 122 PENN ST. L. REV. 727 (2018). For a discussion on how cyber insurance can regulate the behaviour of the insureds, *see* Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Businesses*, 43 LAW & SOC. INQUIRY 417 (2018). For the content of cyber insurance policies, *see* Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY (2019).

[6] *Cybersecurity Insurance*, DEPARTMENT OF HOMELAND SECURITY, www.dhs.gov/cisa/cybersecurity-insurance (last visited Sept. 22, 2019); *see* Rachael M. Peters, *So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171, 1199–1201 (2014).

[7] While this paper uses the term "insurer," it should be noted that the regulations discussed herein are applicable to all entities regulated by the state insurance departments, unless explicitly excluded, including insurers, brokers, and agents.

[8] *See infra* Section III.

[9] The NAIC has long had an identity crisis. It originally identified itself as a private trade organization but eventually decided that it had characteristics of both "a group of public officials imbued with the public trust" and "an instrumentality of the states." Susan Randall, *Insurance Regulation in the United States: Regulatory Federalism and the National Association of Insurance Commissioners*, 26 FLA. ST. U. L. REV. 625, 638 (1999) (citing L.H. Otis, Just What Is the NAIC? Legal Status Up for Grabs, NAT'L UNDERWRITER (Prop. & Cas./Risk & Benefits Mgmt. ed.), May 22, 1995, at 3). Randall affirms that the NAIC is a "completely self-governing entity" that has "no power to compel the states or the

states, with New York leading the way, have begun to take the problem of cybersecurity seriously, and are mandating insurance companies doing business in their jurisdictions to follow cybersecurity guidelines.[10] The NAIC has also promulgated the Insurance Data Model Law (hereinafter "NAIC Model Law") for states to model after when drafting their own cybersecurity regulations.[11]

This paper examines the various cybersecurity regulations that have been passed as law in the United States, with a focus on New York's Cybersecurity Requirements for Financial Services Companies (hereinafter "NYDFS regulations") and the NAIC Model Law, Further, it argues that the hodgepodge of current regulations creates gaps in the regulatory ecosystem, which could potentially be exploited by opportunistic cybercriminals. To minimize this threat, more effort should be expended to harmonize states' regulations with the NYDFS regulations as the model because the latter is the strictest set of regulations that has been passed in the United States thus far.

Section II of this paper provides an introduction of different types of cyber attacks. Section III discusses the nature of insurance regulation in the United States where states, along with the NAIC, possess most of the regulatory power. Section IV examines the NYDFS regulations, the NAIC Model Law, and other insurance cybersecurity regulations in place modeled after the NAIC Model Law. It then highlights their deficiencies and advocates for harmonization to achieve stronger cyber resilience in the insurance industry. Finally, Section V concludes the paper.

II. Cyber Attacks

Anybody could be the victim of cyber attacks; however, insurance companies in particular may be targeted due to the vast amounts of

industry." *Id. But see* Daniel Schwarcz, *Is US Insurance Regulation Unconstitutional?,* 25 CONN. INS. L.J. 191 (2018). This will be further discussed in *infra* Section III.

[10] *See* Sara Merken, *States Imposing New Cybersecurity Requirements on Insurers,* BLOOMBERG LAW (April 4, 2019, 2:48 PM), https://news.bloomberglaw.com/privacy-and-data-security/states-imposing-new-cybersecurity-requirements-on-insurers.

[11] NAT'L ASS'N OF INS. COMM'RS MODEL LAWS, REGULATIONS AND GUIDELINES (NAT'L ASS'N OF INS. COMM'RS, VOLUME V) (2018) (hereinafter "NAIC MODEL LAW"). Kosseff argues that the federal government should be leading the charge on cybersecurity as state regulation is not adequate. *See generally* Jeff Kosseff, *Hamiltonian Cybersecurity,* 54 WAKE FOREST L. REV. 155. (2019).

valuable data they possess.[12] Cyber attacks are crimes that are "somehow related to the misuse of computers."[13] Cybercrime as a term is flexible, and may encompass different actions to different people.[14] Gordon and Ford divide cybercrimes into two broad categories, Type I and Type II. Type I has the following characteristics:

> 1. It is generally a singular, or discrete, event from the perspective of the victim.
> 2. It often is facilitated by the introduction of crimeware programs such as keystroke loggers, viruses, rootkits, or Trojan horses into the user's computer system.
> 3. The introductions can, but may not necessarily, be facilitated by vulnerabilities.[15]

Type II, on the other hand, has the following characteristics:

> 1. It is generally facilitated by programs that do not fit under the classification crimeware. For example, conversations may take place using IM (Instant Messaging) clients or files may be transferred using the FTP protocol.
> 2. There are generally repeated contacts or events from the perspective of the user.[16]

---

[12] Though individuals and government agencies are undoubtedly targets of cybercrimes in addition to businesses, the focus here is on the threats facing commercial entities. As such, issues related to cyberwarfare are outside the scope of this paper. For an introduction of cyberwarfare, *see* CYBER WARFARE: A MULTIDISCIPLINARY ANALYSIS (James A. Green ed., 2015); Pauline C. Reich et al., *Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity*, 1 EUR. J. L. & TECH. 1 (2010); Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, 14 MELBOURNE J. INT'L L. 1 (2013).

[13] David S. Wall, *The Internet as a Conduit for Criminal Activity*, *in* INFORMATION TECHNOLOGY AND THE CRIMINAL JUSTICE SYSTEM (April Pattavina ed., 2005).

[14] For a discussion on the qualitative differences between cybercrimes and traditional crimes, *see* Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PENN. L. REV. 1003 (2001).

[15] Sarah Gordon & Richard Ford, *On the Definition and Classification of Cybercrime*, 2 J. COMPUTER VIROLOGY 13, 14 (2006).

[16] *Id.* at 15. "FTP is short for File Transfer Protocol. A protocol is a set of rules that networked computers use to talk to one another. And FTP is the language that computers on a TCP/IP network (such as the internet) use to transfer files to and from each other." Pamela Statz, *FTP for Beginners*, WIRED (Feb. 15, 2010, 8:45 PM), https://www.wired.com/2010/02/ftp_for_beginners/.

Another way to classify cybercrimes is to divide them into two principles categories: cyber-dependent and cyber-enabled crimes.[17] The former are "crimes that can only be committed using a computer, computer networks, or other form of information communications technology" and are "primarily directed against computers or network resources."[18] Cyber-enabled crimes, by contrast, are "traditional crimes that are increased in their scale or reach by the use of computers, computer networkers, or other information communications technology" and do not require the use of information communications technology to effectuate.[19]That being said, it is believed that cybercrimes fall on a continuum with technology crimes on one end, and people crimes on the other.[20] Indeed, cybersecurity is not just information security and "is not necessarily only the protection of cyberspace itself, but also the protection of those that function in cyberspace, and any of their assets that can be reached via cyberspace."[21]

Cyber attacks can manifest themselves in many different forms.[22] Malware is malicious software that is installed in one's system through opening attachments or clicking links embedded with them.[23] Malware can block access to the system unless a ransom is paid, install malicious software, transmit data to the perpetrators, and render the system

---

[17] JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME 10-11 (2d ed. 2015). This classification, or a form of it is used in Australia, Canada, the United Kingdom, and the United States.

[18] MIKE MCGUIRE & SAMANTHA DOWLING, RESEARCH REPORT 75: CYBER CRIME: A REVIEW OF THE EVIDENCE CH. 1-4 (2013).

[19] *Id.* at CH. 2-4.

[20] Gordon & Ford, *supra* note 15, at 15.

[21] Rossouw von Solms & Johan van Niekerk, *From Information Security to Cyber Security*, 38 COMPUTER & SEC. 97, 101–03 (2013). *But see* Basie von Solms & Rossouw von Solms, *Cybersecurity and Information Security – What Goes Where?*, 26 INFO. & COMPUTER SEC. 2 (2018).

[22] The New York Department of Financial Services stated that from the notices they have received, "the majority of successful breaches involve common software technology used throughout business operations and have involved phishing attacks, social engineering threats, and issues relating to password composition and security and email security." Maria T. Vullo, Department of Financial Services, *Memorandum: DFS Cybersecurity Regulation – First Two Years and Next Steps* (Dec. 21, 2018), www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212018.pdf. For more details on different malware attack methods, *see* Aaron Emigh, *The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond*, 1 J. DIGITAL FORENSIC PRACTICE 245 (2006).

[23] *What Are the Most Common Cyber Attacks?*, CISCO, https://www.com/c/en/us/products/security/common-cyberattacks.html (last visited June 4, 2019).

inoperable.[24] Phishing is tricking the user into volunteering information by sending legitimate-looking communications that ask for the input of sensitive data.[25] Man in the middle attacks "occur when attackers insert themselves into a two-party transaction" and steal data.[26] Denial of service attacks send inordinate amounts of requests to the system to monopolize resources so legitimate requests could not be fulfilled.[27] A Structured Query Language (SQL) injection is when "an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not."[28] Zero-day exploits are attacks that occur in the window of time after vulnerabilities are announced, but before solutions are implemented.[29] This is certainly not an exhaustive list, and is merely illustrative of the types of cyber threats facing individuals and corporations. Regardless of the mode of attack, it is generally agreed that humans are the weakest link in cyber resilience.[30]

III. Insurance Regulation in the U.S.

States oversee insurance regulation in the United States, a power established by the 1868 U.S. Supreme Court case *Paul v. Virginia.*[31] In *Paul,* the insurance industry sought to federalize insurance regulations because the insurers were weary of abiding by the various regulations of multiple states.[32] However, the insurance industry failed the legal challenge and insurance regulation was kept under the purview of the states. Accepting this fate, states began taking the task seriously and "[b]y the 1940s, state regulation was fairly comprehensive."[33] In 1944, the Supreme Court reversed *Paul* in *United States v. South-Eastern Underwriters Association* and held that under the Commerce Clause, insurance companies are subject to federal regulation.[34] The NAIC, which was founded as the National

[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Steve Culp, *Cyber Risk: People Are Often the Weakest Link in the Security Chain*, FORBES (May 10, 2016), www.forbes.com/sites/steveculp/2016/05/10/cyber-risk-people-are-often-the-weakest-link-in-the-security-chain/.
[31] Paul v. Virginia, 75 U.S. 168 (1868).
[32] Randall, *supra* note 9, at 630.
[33] *Id.* at 632.
[34] U.S. v. Se. Underwriters Ass'n, 322 U.S. 533, 552–53 (1944).

Insurance Convention in 1871 by representatives from the different state insurance regulatory agencies, responded quickly to the opinion because it was "viewed as an assault on state regulatory and tax authority over the insurance industry."[35] The NAIC proposed a bill, the McCarran-Ferguson Act, which states:

> Congress hereby declares that the continued regulation and taxation by the several States of the business of insurance is in the public interest, and that silence on the part of the Congress shall not be construed to impose any barrier to the regulation or taxation of such business by the several States.[36]

The bill passed and mandated that, for laws related to insurance, there would only be federal pre-emption if the federal law is specifically related to the business of insurance and if the states do not regulate the business of insurance.[37] To ensure that the states kept their authority, the NAIC drafted model laws to demonstrate that the states were regulating insurance, and—to preclude federal intervention—most states passed laws based on the model laws.[38] Today, insurance regulation is by and large the responsibility of the states, but the federal government does play a role in certain areas in which it has explicitly chosen to do so.[39]

The purposes of insurance regulation are: "ensuring fair pricing of insurance, protecting insurance company solvency, preventing unfair practices by insurance companies, and ensuring availability of insurance coverage."[40] The state regulatory body is an executive branch department, or agency, headed by a commissioner or director of insurance. The

---

[35] Randall, *supra* note 9, at 633.

[36] McCarran-Ferguson Act, 15 U.S.C. § 1011 (1945). For a history of the McCarran-Ferguson Act and the re-emergence of the states as the insurance regulator, *see* Charles D. Weller, *McCarran-Ferguson Act's Antitrust Exemption for Insurance: Language, History and Policy*, 1978 DUKE L.J. 587 (1978).

[37] For arguments supporting more federal involvement in insurance regulation, *see* Christopher C. French, *Dual Regulation of Insurance*, 64 VILL. L. REV. 25, 57–70 (2019).

[38] *Id.* at 58.

[39] *Id.* at 45.

[40] Randall, *supra* note 9, at 629. *See* French, *supra* note 37, at 33–37; Spencer L. Kimball, *The Purpose of Insurance Regulation: A Preliminary Inquiry in the Theory of Insurance Law,* 45 MINN. L. REV. 471 (1961). For an overview of an important federal regulatory measure to ensure the solvency of nonbank financial institutions, the establishment of the Financial Stability Oversight Council (FSOC), *see* Christina Parajon Skinner, *Regulating Nonbanks: A Plan for SIFI Lite*, 105 GEO. L.J. 1379 (2017); *see also* Daniel Schwarcz & David Zaring, *Regulation by Threat: Dodd-Frank and the Nonbank Problem*, 84 U. CHI. L. REV. 1813 (2017).

Commissioner is usually appointed by the governor but is elected by the people in some jurisdictions.[41] This state agency "has broad, legislatively delegated powers to enforce state insurance laws, promulgate rules and regulations, and conduct hearings to resolve disputed matters."[42] Though the power lies in this state agency, Schwarcz argues that "[i]n practice…the most important and powerful entity in insurance regulation is, without question, not a state at all," but the NAIC.[43] He adds:

> [T]he NAIC's true power lies in its direct production of insurance regulatory materials that have the force of law, a category that includes over a dozen "handbooks" and "manuals." These materials dictate (among many other things) the information that insurers and other regulated entities must regularly report to regulators, the methodologies they must use to determine their capital levels, and the accounting standards that they must employ to calculate their assets and liabilities.[44]

These materials have the force of law because the states have laws mandating the insurance regulators and insurers adhere to these materials. Additionally, "when the NAIC updates or changes any of its various manuals… it also changes state insurance regulation" without going through state legislatures.[45] As the next section will show, the NAIC is playing a significant role in the realm of cybersecurity because the NAIC Model Law has been the basis for legislation by the states.

IV. Cybersecurity Regulations for US Insurers

This section introduces the history and selected provisions of the NYDFS regulations, the NAIC Model Law, and the regulations in other states that have passed measures based on the NAIC Model Law. It then

---

41 Randall, *supra* note 9, at 629.

42 *Id.*

43 Schwarcz, *supra* note 9, at 193.

44 Schwarcz, *supra* note 9, at 193, 199–200.

45 *Id.* at 200. Schwarcz argues that this "violates the basic separation of powers and non-delegation principles embedded in every state constitution." *Id.* at 202.

discusses these regulations' weaknesses, and advocates for harmonising the regulations to ensure uniformity throughout the country.

A. New York

Examining the NYDFS regulations is an obvious starting point because New York was the first state to pass cybersecurity regulations for its insurers. It is not a coincidence that New York was the first to act. The importance of New York as a financial centre necessitates it being an industry leader, and its regulations can be influential upon other states.[46] Some have argued the NYDFS regulations could serve as the blueprint for other states when drafting their own rules.[47]

New York created the New York Department of Financial Services (hereinafter "NYDFS") in 2011 after the merger of the New York State Banking Department and the New York State Insurance Department. The NYDFS proposed cybersecurity regulations governing the banks and insurance companies, the institutions it oversees, in September 2016.[48] It was the first such proposal in the United States, and was later the model for the NAIC Model Law. When the proposal was first introduced, it was met with immediate criticism. It was derided as not "risk-based, flexible, [or] workable" and the "required cybersecurity programs and policies did not account for the amount of risk that a company faces."[49] It was also seen as overly broad.[50] Some found the equal treatment of all companies, regardless of size for certain requirements, to be excessively burdensome for smaller companies.[51]

The NYDFS heeded the concerns and released new regulations in December 2016 to be implemented on March 1, 2017.[52] The regulation requires that entities covered by the NYDFS meet the mandated

---

[46] Harry Dixon, *Maintaining Individual Liability in AML and Cybersecurity at New York's Financial Institutions*, 5 PENN ST. J. L. & INT'L AFF. 72, 75 (2017).

[47] *See generally* Sabrina Galli, *NYDFS Cybersecurity Regulations: A Blueprint for Uniform State Statute?*, 22 N.C. BANKING INST. 235 (2018); Jeff Kosseff, *New York's Financial Cybersecurity Regulation: Tough, Fair, and a National Model*, 1 GEO. L. TECH. REV. 436 (2017).

[48] This paper refers to insurance companies, but it should be noted that the NYDFS regulations affect banks and other financial institutions equally.

[49] Kosseff, *supra* note 47, at 438.

[50] *See* Galli, *supra* note 47, at 244.

[51] Tracy Kitten, *Critics Blast New York's Proposed Cybersecurity Regulation*, BANK INFO SECURITY, (Oct. 14, 2016), www.bankinfosecurity.com/critics-blast-new-yorks-proposed-cybersecurity-regulation-a-9453.

[52] *See* N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.00–500.23 (2017). *Id.*

cybersecurity standards.[53] A Covered Entity is defined as, "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."[54] Section 500.02 mandates that the Covered Entity "shall maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of the Covered Entity's Information Systems" that is "based on the Covered Entity's Risk Assessment."[55] This cybersecurity program must contain measures for continuous monitoring "designed to assess the effectiveness" of the program, or engage in "periodic Penetration Testing and vulnerability assessments."[56] Entities are also required to "implement and maintain a written policy or policies . . . setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems."[57] There is a requirement of "conduct[ing] a periodic Risk Assessment of the Covered Entity's Information System sufficient to

---

[53] *Id.*

[54] *Id.* § 500.01(c).

[55] *Id.* § 500.02(a)–(b); *see generally id.* § 500.01(e) (defining "Information System" as "a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.").

[56] *Id.* § 500.05.

[57] *Id.* § 500.03; *see generally id.* § 500.01(g) (defining "Nonpublic Information" as "all electronic information that is not Publicly Available Information and is: (1) Business related information of a Covered Entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Covered Entity; (2) Any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements: (i) social security number, (ii) drivers' license number or non-driver identification card number, (iii) account number, credit or debit card number, (iv) any security code, access code or password that would permit access to an individual's financial account, or (v) biometric records; (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to (i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family, (ii) the provision of health care to any individual, or (iii) payment for the provision of health care to any individual."). This definition differs from the one initially proposed. Galli, *supra* note 47, at 244–45.

inform the design of the cybersecurity program."[58] The Covered Entities are also required to appoint a Chief Information Security Officer tasked with "overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy."[59] The Chief Information Security Officer is also responsible for "report[ing] in writing at least annually to the Covered Entity's board of directors or equivalent governing body."[60]

In addition, the Covered Entity must:

> [E]stablish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity, or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.[61]

A Cybersecurity Event is defined as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."[62] If a Cybersecurity Event were to occur, the Covered Entity "shall notify the superintendent as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred."[63]

Some Covered Entities are exempt from certain sections of the regulations: those with fewer than ten employees, those with less than five million dollars in "gross annual revenue in each of the last three fiscal years from New York business operations," and those with less than ten million dollars in "year-end total assets."[64]

These final regulations are noticeably more flexible and less stringent than the initial proposal by the NYFDS. In the original draft, the

---

[58] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.09(a) (2017).
[59] *Id.* § 500.04(a).
[60] *Id.* § 500.04(b).
[61] *Id.* § 500.16.
[62] *Id.* § 500.01(d).
[63] *Id.* § 500.17(a). Section 500.17(a) requires notification only if the Cybersecurity Event meets either of the following definitions: "(1) Cybersecurity Events impacting the Covered Entity of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity." *Id.*
[64] *Id.* § 500.19(a).

cybersecurity program had to contain a list of core functions, but did not offer any leeway. In comparison, the final version clarifies that the cybersecurity program "shall be based on the Covered Entity's Risk Assessment," which suggests there is flexibility depending on the company's risk assessment. The same language was also added to the section on Cybersecurity Policy in the final version to allow it to be based on the company's own risk assessment.

In terms of monitoring and testing the Risk Assessment, the original proposal included, at a minimum, annual penetration testing and quarterly vulnerability assessments.[65] In the final version, continuous monitoring was added as an option, but if the option of penetration testing and vulnerability assessments were chosen, the vulnerability assessment only needs to be conducted bi-annually, and both the testing and the assessment are done based on the Risk Assessment. While the Risk Assessment was required to be performed at least once a year in the initial proposal, it only needs to be "updated as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations" in the final version.[66]

Continuous monitoring means that ideally, security personnel would always remain vigilant and be quick to identify vulnerabilities or attacks, but it may also create a risk: the introduction of complacency. Complacency can result from, *inter alia*, confirmation bias or overfamiliarity. Confirmation bias is the "seeking or interpreting of evidence in ways that are partial to existing beliefs, expectations, or a hypothesis in hand."[67] If the same person or group of people are engaged in continuous monitoring, the lack of any issues in the beginning may sway them to subsequently look for similar evidence that signify the lack of problems and disregard evidence that are contrary to the narrative. Furthermore, possible cyber attacks could be missed, and as it has been shown in various contexts, routine actions may result in higher risks due to lack of vigilance.[68] For at least these two reasons, continuous

---

[65] *Id.* § 500.05 (proposed Sept. 13, 2016).

[66] *Id.* § 500.09(a).

[67] Raymond S. Nickerson, *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises*, 2 REV. GEN. PSYCHOL. 175, 175 (1998).

[68] *See generally* Maura Pilotti & Martin Chodorow, *Does Familiarity with Text Breed Complacency or Vigilance?*, 35 J. RES. IN READING 204 (2012) (concluding that increased familiarity with text when proofreading leads to an increased likelihood of overlooking errors); Jeremy D. Davey et al., *The Experiences and Perceptions of Heavy Vehicle Drivers and*

monitoring may lead to complacency, and vulnerabilities in the system not being detected due to inertia.

By contrast, the requirement of annual testing and quarterly assessments would mean that each task is discrete, and complacency could be countered by using different procedures or personnel.. Nonetheless, complacency could still remain a problem because it may be easier to ignore a report than to run a continuing process Furthermore, if the security team's activity is paced by regular penetration test exercises, the time between exercises might leave new vulnerabilities unmitigated for quite some time. Instead of choosing between the two, both continuous monitoring and annual testing plus quarterly assessments should be required for compliance to ensure that insurers have robust cybersecurity programs.

The requirement that the superintendent needs to be notified of Cybersecurity Events was changed significantly from the original version, which states:

> Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event. Such Cybersecurity Events include, but are not limited to:
>
> > (1) any Cybersecurity Event of which notice is provided to any government or self-regulatory agency; (2) any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information.[69]

The final version requires notification must be "as promptly as possible but in no event later than 72 hours from a determination that a

Train Drivers of Dangers at Railway Level Crossings, 40 ACCIDENT ANALYSIS & PREVENTION 1217 (2008) (discussing driver complacency due to high levels of familiarity); H.L. Hansen et al., *Occupational Accidents Aboard Merchant Ships*, 59 OCCUPATIONAL & ENVTL. MED. 85 (2002) (observing that most accidents aboard ships occur when performing routine duties); Ruth M.W. Yeung & Joe Morris, *Food Safety Risk: Consumer Perception and Purchase Behaviour*, 103 BRIT. FOOD J. 170 (2001) (discussing the relationship between the information provided about certain foods and the consumer's willingness to purchase that food).

[69] N.Y. COMP. CODES R. & REGS. tit. 23, § 500.17(a) (proposed Sept. 28, 2016).

Cybersecurity Event has occurred."[70] Furthermore, subsection (a)(2) was changed to "Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations(s) of the Covered Entity."[71]

The difference between "in no event later than 72 hours after becoming aware of such a Cybersecurity Event"[72] and "in no event later than 72 hours from a determination that a Cybersecurity Event has occurred"[73] is significant. While the timeframe is identical, "becoming aware" is a much lower threshold. Being aware of the attack requires minimal effort, whereas making a determination may necessitate a significant amount of time and effort from personnel to study and investigate the problem before reaching the conclusion that the incident was indeed a Cybersecurity Event. Commenting on section 500.17(a), Brian Mund states:

> A 'determination' connotes a high standard of certainty, and goes far beyond mere suspicion of a potential cybersecurity incident. The definition of 'determination' is instructive in this regard: the New Oxford American Dictionary defines 'determination' as "the process of establishing something exactly, typically by calculation or research." However, one only reaches a point of exactitude after investigative research. Therefore, a determination transpires at some unspecified time *after* the initial detection of a potential cybersecurity breach. The current Regulation impliedly enables a regulated entity's response to disentangle these two events into discrete stages—initial detection and determination—creating a buffer extending the time before the Regulation's 72 hours begin tolling.[74]

He contrasts "determination" with "initial detection," which is roughly equivalent to the awareness language in the initial proposal.[75] The current regulation does create a temporal gap and allow for a large amount of

---

[70] *Id.* § 500.17(a).
[71] *Id.* § 500.17(a)(2).
[72] *Id.* § 500.17(a).
[73] *Id.* (proposed Sept. 13, 2016).
[74] Brian Mund, *The Problem with the New York Cybersecurity Guidelines*, YALE J.L. TECH. BLOG (Nov. 7, 2017), https://yjolt.org/blog/problem-new-york-cybersecurity-guidelines (citations omitted).
[75] *Id.*

discretion, as determination is left undefined without any specific guidance.

The deletion of "reasonable likelihood of materially affecting the normal operation of the Covered Entity" also heightens the threshold for reporting. Additionally, while the threshold in the original subsection (a)(2) included the language "actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information," it was amended to be "reasonable likelihood of materially harming any material part of the normal operations(s)." The original requirement allowed for *potential* tampering and access, whereas the current regulation inserted the language of *materiality*, requiring the standard of material harm of a material part. The definition of material, again, is flexible, and could be defined by the Covered Entity differently to avoid triggering the notice requirement should it have the desire to obfuscate. Proponents of the materiality language argue that it eliminates the need to report low level "cyber-sniffing" which "would be incredibly burdensome, and likely would divert precious resources from addressing other more serious cyber-related risks."[76] The counterargument is that if such routine cyber-sniffing were routine, generating a short report should not be time-consuming and could become an automated process, with the upside being that the NYDFS would have a complete record of attempted attacks.

Finally, the category of exempt entities was also broadened in the final version. While the final regulations were worded in the alternative, the entity must satisfy all the requirements in order to be exempt from certain sections of the regulation in the initial proposal. Previously, the exempted entities were those with "fewer than 1000 customers in each of the last three calendar years," have "less than $5,000,000 in gross annual revenue in each of the last three fiscal years," and have "less than $10,000,000 in year-end total assets…including assets of all Affiliates." In addition to nixing the cumulative condition, the first criterion was changed from being based on the number of customers to the number of employees; the second requirement was amended to include gross annual revenue from New York business operations only; and the third requirement eliminated counting the total assets of affiliates. The new regulations appear to be much easier to satisfy, meaning more insurers would be exempt from parts

[76] *New York Department of Financial Services Cybersecurity Rules Revised and Delayed*, HOGAN LOVELLS (Dec. 30, 2016), https://www.hoganlovells.com/~/media/hogan-lovells/pdf/publication/2016/cybersecurity_alert_ny_department_of_financial_services_cybersecurity_rules_revised_and_delayed.pdf?la=en.

of the NYDFS regulations. Nonetheless, proponents, insurers who presumably would seek less regulation, have praised the regulation for "its sensible, risk-based approach instead of an across-the-board, bright-line rule that applies regardless of the actual risk of harm" and "provides an incentive for companies to more effectively allocate their cybersecurity resources."[77] This new risk-based approach is also tied to the Risk Assessment, making each plan tailored for each company's situation.[78]

Unsurprisingly, and to its credit for completeness, the regulatory measures in the NYDFS regulations fit all four groups of responses against cyber risks if viewing cybersecurity from a regulation perspective, as proposed by Sales:

> (1) monitoring and surveillance to detect malicious code, (2) hardening vulnerable targets and enabling them to defeat intrusions, (3) building resilient systems that can function during attacks and recover quickly, and (4) responding in the aftermath of attacks.[79]

All in all, while the final regulations appear to be much more flexible, it does offer a tremendous amount of wiggle room for the Covered Entities. The flexibility may mean that the insurer can be nimbler in designing plans specific to its situation or respond to any changing conditions, and only notify the NYDFS when the attack is real and/or caused harm as opposed to possible false alarms. This is a generous reading of the situation and assumes that insurers would act in good faith to combat the problem of cybercrimes.[80] From a more cynical perspective, the current regulations compared to the initial proposal allow insurers to define the undefined terms in ways that would serve their own best interest, which may not be cyber resilience. Everything from the risk assessment, determination, and continuous monitoring could be gamed so that while the insurers' obligations are low, the threshold to notify the NYDFS are high. At this point, it is unclear whether the current

---

[77] Kosseff, *supra* note 47, at 441–42.

[78] *New York Department of Financial Services Cybersecurity Rules Revised and Delayed*, *supra* note 76.

[79] Nathan A. Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1508 (2013).

[80] *FAQs: 23 NYCRR Part 500 – Cybersecurity*, N.Y. ST. DEPT. OF FIN. SERVS., www.dfs.ny.gov/industry_guidance/cyber_faqs (last visited June 4, 2019) (The New York DFS "trusts that Covered Entities will exercise appropriate judgment as to which unsuccessful attacks must be reported and does not intend to penalize Covered Entities for the exercise of honest, good faith judgment").

regulations are sufficient, but the potential for abuse unquestionably exists and compliance requires the insurers to act as good corporate citizens who would abide by the spirit of the regulations. Jeff Kosseff suggests that the NYDFS should "issue non-binding guidance that provides examples of compliance with this risk-based framework," and companies should document their decision-making reasoning to avoid the NYDFS from accusing them of insufficient safeguarding.[81] This suggestion is useful, but for another reason also, which is that documenting the reasoning at every step could show that the Covered Entities are making decisions in the best interest of their cybersecurity and the cybersecurity of their customers rather than for other nefarious interests such as, for example, protecting their own reputations.

B. NAIC Model Law

The NAIC Model Law was adopted in October 2017 and is formally entitled the Insurance Data Security Model Law. It has been endorsed by the US Department of the Treasury.[82] The NAIC Model Law serves as guidelines to the states to adopt in their own jurisdictions.83 Unlike the NYDFS regulations, the NAIC Model Law only applies to insurers, and excludes other types of financial institutions. The remainder of this section addresses some of the differences between the NAIC Model Law and the NYDFS regulations.

The definitions of Cybersecurity Event differ between the NAIC Model Law and the NYDFS regulations. The former states that a Cyber Security event means: "[A]n event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System."84 It then includes two scenarios that would

---

81 Kosseff, *supra* note 47, at 442. The New York DFS has issued a memorandum and maintains a FAQ page on its website that contain further guidance on the regulations. None of the other states mentioned in this paper have issued any formal guidance thus far. Vullo, *supra* note 22; N.Y. ST. DEPT. OF FIN. SERVS., *supra* note 80.

82 Don Jergler, *The State of NAIC's Data Security Model Law*, *Insurance Journal*, INSURANCE JOURNAL (Sept. 21 2018), www.insurancejournal.com/news/national/2018/09/21/500119.htm.

83 Kim Mobley & Carly Kanwisher, *Impact of NAIC's Insurance Data Security Model Law*, JOHNSON LAMBERT BLOG (July 2018), www.johnsonlambert.com/post/impact-of-naics-insurance-data-security-model-law/.

84 NAIC INSURANCE DATA SECURITY MODEL LAW § 3(D) (NAT'L ASS'N OF INS. COMM'RS 2017).

not be defined as a Cybersecurity Event, exemptions not in the NYDFS regulations. The definition does not include "the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization" or "an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed."85 This is a much more exclusive standard than that of the NYDFS regulations, as it appears to exclude unsuccessful attacks, because there is no language on potential attacks and it has two further exemptions as noted above.

These exemptions appear to create loopholes. Encryption is the bedrock of cyber security.[86] It is "the conversion of data from a readable format into an encoded format that can only be read or processed after it's been decrypted."[87] The encrypted data is unintelligible and can only be read if a key or cipher is used to unscramble the information.[88] If the encrypted data is stolen, it is incomprehensible and useless without the key or means to decrypt it.[89] Burdon and his colleagues note that "[t]he apparent benefit of cryptography is that it substitutes the problem of protecting the secrecy of a potentially large amount of plaintext, for the problem of protecting the secrecy of a much smaller key."[90]

---

85 *Id.*

86 Encryption has been the subject of debate between law enforcement and the technology industry because the former has been advocating for the latter to assist in their investigations by "provid[ing] backdoors or assistance when users encrypt their communications." Shannon Gross, *A Mystery Wrapped in an Encryption: Surveillance and Privacy in the Encrypted Era*, 15 NW. J. TECH. & INTELL. PROP. 73, 74 (2017). Although the general concern has been about user privacy, the existence of backdoors could create another point of vulnerability that hackers could target and exploit. Stephanie K. Pell, *You Can't Always Get What You Want: How Will Law Enforcement Get What It Needs in a Post-CALEA, Cybersecurity-Centric Encryption Era?*, 17 N.C. J.L. & TECH. 599, 609–10 (2016).

87 *What is Data Encryption?*, KASPERSKY, www.kaspersky.com/resource-center/definitions/encryption (last visited June 4, 2019). One federal bill defined encryption as "the protection of data in electronic form in storage or in transit using an encryption technology that has been adopted by an established standards setting body which renders such data indecipherable in the absence of associated cryptographic keys." Data Security and Breach Notification Act of 2015, S. 177, 114th Cong. § 6(6) (2015). 139 § 13(4). Encryption is not defined by the NYDFS regulations.

88 *What is Data Encryption?*, *supra* note 87

89 WENBO MAO, MODERN CRYPTOGRAPHY: THEORY AND PRACTICE 24 (2004).

90 Mark Burdon, Jason Reid & Rouhshi Low, *Encryption Safe Harbours and Data Breach Notification Laws*, 26 COMPUTER L. & SEC. REV. 520, 522 (2010).

The first exemption states that if only the scrambled data is stolen and not the key to decipher it, the event would not trigger the notification requirement of the law.[91] This is known as the encryption safe harbor and is common among existing data security laws.[92] There are two main rationales for including encryption safe harbor provisions:

> First, to reduce the risks of notification fatigue and the regulatory compliance burden on organisations and regulators, by requiring notification only in circumstances where there is an appreciable risk of identity fraud. Second, to encourage both private and public sector organisations to adopt encryption technologies for the collection and storage of personal information thus strengthening their information security management practices.[93]

The safe harbour provision acts as "an adjunct to the primary aim of the laws, the mitigation of identity theft crimes, and has been developed as a counterbalance to corporate fears of the compliance implications of over-notification that potentially conflict with the consumer protection aims of data breach notification laws."[94]

Both rationales may be facially valid, but they do create more risk than if the exemption did not exist. In fact, the reliance on encryption and push for its use may be misplaced due to its "two fundamental limitations as a security technology. First, encryption can protect data at rest and in motion but cannot protect data while the data is actually being processed. Second, encryption is only as secure as the weakest link in the system within which it is deployed."[95]

Under the NAIC Model Law, if an attack did not include the acquisition of "the encryption, process, or key," but a subsequent attack

---

[91] *See* Samuel Lee, *Breach Notification Laws: Notification Requirements and Data Safeguarding Now Apply to Everyone, Including Entrepreneurs*, 1 ENTREPRENEURIAL BUS. L. 125, 133 (2006) (stating California does not require notification where personal information is encrypted).

[92] *Id.* at 143 (stating California "essentially serve[s] as a de-facto standard").

[93] Burdon et al., *supra* note 90, at 520. Burdon notes that "the use of encryption exemptions is directly linked to corporate compliance cost reduction and the development of market incentives to enhance corporate information security measures." Mark Burdon, *Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws*, 27 SANTA CLARA COMPUTER & HIGH TECH. L.J. 63, 89 (2010).

[94] Burdon, *supra* note 93, at 92.

[95] Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible*, 24 BERKELEY TECH. L.J. 1133, 1146 (2009).

led to its acquisition, would this be considered a Cybersecurity Event? The two attacks combined would be considered a Cybersecurity Event under the definition, but each one on its own would not be. Depending on whether the definition has been met, the response would be different, yet, the damages incurred would probably be similar. Is there a temporal limit to the definition of a Cybersecurity Event? Can multiple assaults be considered different stages of one Cybersecurity Event? How should the continuous exploitation of the same vulnerability be classified? The same mode of attack could either trigger the investigation reporting requirements or not—purely depending on how each insurer interprets the regulations and its obligations. In addition, the encryption on the stolen data may have been decrypted by alternate means without the need for the key.[96] This would undoubtedly be the unauthorized use of Nonpublic Information that could lead to massive amounts of damages, yet the existence of the safe harbor provision means that the state insurance commissioner would not have to be informed in this type of breach.[97]

The second exemption means that an acquisition of Nonpublic Information is not considered a Cybersecurity Event if the information were not used for nefarious purposes or released publicly, and has been returned or destroyed. As the object of theft is information, it could not be truly destroyed. One copy may be, but the information could have been replicated and stored elsewhere. Similarly, the data may have been returned but the NAIC Model Law is silent on the perpetrator keeping a copy, which could be used or released later. Though the attack may not be a Cybersecurity Event at first, it becomes one when it is released or used at a subsequent time. This raises the same temporal limit issue and the question of why the investigation and reporting requirements are not triggered the first time around, when there was obviously a vulnerability that was exploited leading to the theft of the Nonpublic Information. Limiting reporting to only when customer data is jeopardized for certain also misses the point of cybersecurity, which "refers to the integrity of a technological system" and "is more broadly focused on attacks on

[96] Kerr and Schneier note three types of encryption workarounds that can be used to decrypt data in the context of law enforcement, but they warn that these same methods can be used for more nefarious purposes too. Orin S. Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 995–96, 1005–11 (2018).

[97] *See* Burdon et al., *supra* note 90, at 526–31.

networks and systems, in addition to information."[98] Just because the data was not compromised in the attack does not mean the attacker did not find a vulnerability in the system that could be exploited again to mount other types of attacks that could not only lead to the release of the data but also threaten the technological infrastructure. Mandating the report of the first attack, however innocuous it may seem, is a good information sharing practice that could spur more coordinated responses at the outset.

Excluding the above, the NAIC Model Law is substantially similar to the NYDFS regulations, though it is more detailed in certain sections. The NAIC Model Law mandates the implementation of an Information Security Program to "mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities,"[99] implement appropriate security measures based on risk assessment,[100] designate a person to be in charge of the Information Security Program,[101] and establish an incident response plan.[102] The NAIC Model Law provides more guidance regarding investigation and notification that do not exist in the NYDFS regulations, including what determinations need to be made during the investigation and what information to provide the commissioner.[103] Notification is required "in no event later than 72 hours from a determination that a Cybersecurity Event has occurred" and one of two criteria has been met.[104] The notification must occur if the state is the state of domicile for the company, or if there is reasonable belief that "the Nonpublic Information involved is of 250 or more Consumers residing in this State" and either notice is required to be provided to another government body, self-regulatory, or supervisory body; or the event "has a reasonable likelihood of materially harming" a consumer resident to the state or "[a]ny material part of the normal operation(s)."[105] The requirement to report within 72 hours after a determination has been made and the materiality language are the same as the requirements in the NYDFS regulations. The significant difference is that for Nonpublic Information, 250 consumers in the state must be involved before the notification

98 Kosseff, *supra* note 47, at 443.
99 NAIC MODEL LAW § 4(D)(1).
100 *Id.* § 4(D)(2).
101 *Id.* § 4(C)(1).
102 *Id.* § 4(H).
103 *Id.* § 5, 6(B).
104 *Id.* § 6(A).
105 *Id.* § 6(A)(2).

requirement [106]is triggered. Additionally, the NAIC Model Law requires that notification be made to customers per the relevant state law, while the NYDFS regulation is silent on such notifications.

C. Other States

The states of South Carolina, Michigan, Ohio, Mississippi, Connecticut, Delaware, and New Hampshire have followed New York by passing their own cybersecurity regulations overseeing the insurance industry. The South Carolina Insurance Data Security Act was signed into law on May 9, 2018, by the governor and is "the first in the nation to pass this important and timely legislation which is modelled after the NAIC Insurance Data Security Model Law."[107] The South Carolina Department of Insurance aims to work "closely with the NAIC in an effort to ensure consistency among the states as this legislation is enacted."[108] Ohio's version went into effect in March 2019.[109] The Michigan law was signed by the Governor on December 28, 2018. Mississippi's was signed into law in April 2019.[110] Connecticut passed its Insurance Data Security law as part of its omnibus budget bill on June 26, 2019, while Delaware and New Hampshire enacted their laws within days of each on July 31, 2019, and August 2, 2019, respectively.[111]

All seven states follow the NAIC's definition of a Cybersecurity Event, but Michigan adds further exemptions in its law. The definition does not include "[t]he unauthorized access to data by a person" if "[t]he person

---

106 *Id.* § 6(C).

107 Raymond G. Famer, South Carolina Department of Insurance, Bulletin Number 2018-2: South Carolina Insurance Data Security Act: 2018 SC Act No. 171, June 14, 2018.

108 *Id.*

109 Jennifer Orr Mitchell & Jared M. Bruce, *Ohio Enacts New Cybersecurity Requirements for Insurers*, NAT'L L. REV. (Feb. 22, 2019), www.natlawreview.com/article/ohio-enacts-new-cybersecurity-requirements-insurers.

110 Sara Merken, *States Imposing New Cybersecurity Requirements on Insurers*, BLOOMBERG L. (Apr. 5, 2019), https://news.bloomberglaw.com/privacy-and-data-security/states-imposing-new-cybersecurity-requirements-on-insurers.

111 Mitchell R. Harris, *Connecticut Adopts Insurance Data Security Law: What You Need To Know*, MONDAQ (July 23, 2019), http://www.mondaq.com/unitedstates/x/828652/Security/Connecticut+Adopts+Insurance+Data+Security+Law+What+You+Need+To+Know; *see also* Malia K. Rogers, Gregory Szewczyk & Philip N. Yannella, *Delaware and New Hampshire Join Growing List of States With New Insurance Data Security Laws*, NAT'L L. REV. (Aug. 9, 2019), https://www.natlawreview.com/article/delaware-and-new-hampshire-join-growing-list-states-new-insurance-data-security-laws.

acted in good faith in accessing the data" and "the access was related to the activities of the person."[112] The first element appears to allow for accidental or innocent access of the data, and the second element appears to mean that if it was done in the course of the person's lawful activities, the incident would not be a Cybersecurity Event. It is unclear what the motivation is for exempting these two scenarios where the access is still unauthorized. If the person were able to gain access without authorization, it would be useful for this breach to be documented and a response be initiated by the company to ensure that similar vulnerabilities in the system could not be exploited by hackers in the future. Notifying the state insurance commissioner of the breach would also aid in this process.

For notification to the insurance commissioner, South Carolina, like the NYDFS regulations and NAIC Model Law, mandates that it be done no later than 72 hours after a determination has been made.[113] Ohio, Mississippi, New Hampshire, and Delaware allow for three business days after a determination,[114] and Michigan requires the notification be made within ten business days after a determination.[115] Contrary to the clock starting when a determination of a Cybersecurity Event has occurred, Connecticut requires that notification be effected within "three business days after the date of the cybersecurity event."[116] Surprisingly, Mississippi, Ohio, and Michigan specifically only require the insurer to notify the insurance commissioner for Cybersecurity Events that involve Nonpublic Information. Cybersecurity Events where the infrastructure is attacked would not require notification. This distinction does not exist in the NYDFS regulations, the NAIC Model Law, or South Carolina law, where notification is required for all attacks defined as a Cybersecurity Event, provided the other criteria for notification are met. Not requiring the notification of the commissioner of Cybersecurity Events targeting the Information System itself, or the infrastructure, also means that potentially

---

112 MICH. COMP. LAWS SERV. § 500.553(c)(ii) (LexisNexis 2018).

113 S.C. CODE ANN. § 38-99-40(A) (2018).

114 Act of July 31, 2019, § 1, (codified as amended at DEL. CODE ANN. tit. 18, § 8606(a) (2019); Act of April 3, 2019, § 6(1), 2019 Miss. Laws 14 (establishing the insurance data security law); Act of Aug. 5, 2019, ch. 420-P:6(I), 2019 N.H. Laws 8 (to be codified at N.H. REV. STAT. ANN. § 420-P(6)(I); Act of Mar. 20, 2019, § 1, § 3965.04(A), 2019 Ohio Laws 22.

115 Act of Dec. 28, 2018, § 559(1), 2019 Mich. Pub. Acts.

116 Public Act No. 19-117, § 230(e)(1), 2019 Conn. Acts 5 [Reg.] Sess.

significant damages would not have to be reported, as attacks on the infrastructure could lead to critical failures in the entire insurance industry that cripple its operations, which are matters that go beyond the unauthorized sharing of data. The emphasis on data and privacy in the Mississippi, Ohio, and Michigan laws miss the point of a holistic view of cybersecurity.[117]

The amendment in Michigan to allow for ten days for notification is overly generous, considering that a flexible time period is already built into the law to allow for the attacked company to make a determination that the incident was indeed a Cybersecurity Event before notification per the earlier discussion. If the purpose of notification to the insurance commissioner is to ensure that vital information that could be useful to other insurers or other stakeholders is shared, a ten-day timeframe would defeat the purpose. Prompt notification to the commissioner would allow the office to determine whether it is just one of multiple attacks on different insurers, and whether a warning to other insurers would be necessary.[118] This warning could include the vulnerabilities being exploited and could help other insurers make adjustments to their systems if the warning were timely. By contrast, Connecticut has been the lone state to tighten the notification time period by setting it within three days of the occurrence of the attack. Starting the clock at occurrence eliminates the possibility of the company dragging its feet in its investigation by not officially making a determination. The time period also facilitates swift responses to be implemented not only by the company directly affected, but also by the insurance commissioner who would be notified shortly after the occurrence. Connecticut's provision does raise the issue of what would happen if the attack is discovered more than three days after it first started: a possible point of contention that would require clarification by the state insurance commissioner.

While these states all claim to have passed their insurance cybersecurity laws following the NAIC Model Law, it appears that some critical deviations in the regulations of Mississippi, Michigan, and Ohio would expose vulnerabilities and will not entirely accomplish the mission of these laws. There is no legitimate reason for only mandating notification for one

---

[117] Kosseff, *supra* note 47, at 443.

[118] The New York Department of Financial Services stated that in response to notices of Cybersecurity Events, it "may identify from the information provided a circumstance or trend that subject to confidentiality warrants providing certain information to other regulated entities regarding a potential threat." Vullo, *supra* note 22, at 2.

kind of Cybersecurity Event, and there is no logical reason the insurer would need ten days after determining an attack occurred before notifying the insurance commissioner. In fact, the clock can start at the occurrence rather than the determination of the attack. These differences make the states' claims they were following the NAIC Model Law spurious because they fundamentally change the requirements and criteria for notification, one of the key aspects of these regulations.

D. Need for Harmonization

The above discussion has shown that some states have begun to take cybersecurity issues in the insurance industry seriously. Other states will surely follow suit and enact their own laws, but the question remains as to whether they will devise unique provisions or learn from the field of existing provisions.

While the NAIC has released its Model Law hoping all states would have identical or substantially similar legislation concerning regulating cybersecurity in the insurance industry, states have not been reluctant to amend the NAIC Model Law to weaken its provisions. This is in addition to the inclusion of the safe harbor provision in the NAIC Model Law on the definition of a Cybersecurity Event that already made it less stringent than the NYDFS regulations. The disparity among the laws means that insurers that operate in multiple states may have to abide by each state's different regulations and expend more time and effort to be compliant. However, this is not the most significant issue. More important, the haphazard patchwork of regulations introduces gaps in the cybersecurity of the insurance industry in the United States, which is undoubtedly all interconnected.

The NAIC and the federal government, due to their purported influence, should advocate for more cooperative efforts between states, not only in harmonizing the laws on paper, but also foster practical collaborations so there is communication among the state insurance regulatory agencies. The insurance departments should provide guidance to further clarify the regulations that might be subject to interpretation, such as whether multiple assaults can be considered one Cybersecurity Event, as discussed earlier. Without clarification, insurers may interpret the provision differently, resulting in their being held to inconsistent standards and possibly jeopardizing the industry's cyber resilience. The sharing of information may help insurers learn from each other about vulnerabilities

or modes of attack so they can plan ahead and take measures to enhance the strength of their systems.[119] After all, what is the point of notification of past breaches if they cannot serve as lessons for the future? Further, in the long run, as the Treasury Department has intimated, it is necessary for the federal government to step in and adopt a single law on cybersecurity for the insurance industry due to the unlikelihood of uniform laws being adopted across the United States, despite the existence of the NAIC Model Law.[120] One way to do this is to empower the Federal Insurance Office to coordinate a national cybersecurity strategy so there is uniformity across the country.[121] The need for harmonization is clear because even with only 10% of the states adopting some kind of measure for insurance industry cybersecurity thus far, significant variance already exists.

Whatever route is taken, the safe harbor provision which exempts notifications if Nonpublic Information is encrypted and the key is not taken at the same time, should be eliminated. Whether notice is required should be risk-based, meaning it should be evaluated on a case-by-case basis and be mandated when the risk of further damage is high, instead of being subject to a blanket safe harbor provision that is included in all the regulations herein save the NYDFS regulations. While the NYDFS regulations is already a watered-down version of its original proposal, it is

---

119 Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 986, 1028-30 (2018); Kathryn E. Picanso, *Protecting Information Security Under a Uniform Data Breach Notification Law*, 75 FORDHAM L. REV. 355, 360 (2006).

120 Gloria Gonzalez, *Treasury Recommends Revamping Federal Insurance Office, Adopting Uniform Cyber Rules*, BUSINESS INSURANCE (Oct. 27, 2017), https://www.businessinsurance.com/article/20171027/NEWS06/912316842/Treasury-recommends-revamping-Federal-Insurance-Office,-adopting-uniform-cyber-r.

121 French, *supra* note 37, at 67–70 (arguing that the Federal Insurance Office, which was established under the Department of the Treasury by the Dodd-Frank Wall Street Reform and Consumer Protection Act, can work together with the state insurance regulators to provide a dual track insurance regulation scheme); *see* Randall, *supra* note 9, at 664–86 for arguments for the continuing dominance of state insurance regulation. *See* Jacqueline May Tom, *A Simple Compromise: The Need for a Federal Data Breach Notification Law*, 84 ST. JOHN'S L. REV. 1569, 1592-602 (2010) (arguing for a federal law with strict notification requirements that preempts state laws); *see also* Dana J. Lesemann, *Once More unto the Breach: An Analysis of Legal, Technological, and Policy Issues Involving Data Breach Notification Statutes*, 4 AKRON INTELL. PROP. J. 203, 236–37 (2010). *But see* Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 308–09 (2009) (warning against federal regulation and arguing that "allowing the market to correct the data breach problem state-by-state is the best way to ensure that the level of rigor is properly calibrated.").

still significantly stronger than the NAIC Model Law and the laws in the other states. Should there be any effort to harmonize the laws in the United States, the NYDFS regulations should serve as the foundation rather than the NAIC Model Law, which is not as robust as it could be to protect the country's insurance industry.

V. Conclusion

Cybersecurity is obviously a major concern for the insurance industry. State insurance departments have recently begun to take the issue seriously by regulating insurer's behaviour prior to and after Cybersecurity Events. New York paved the way with its law, and the NAIC subsequently released the NAIC Model Law. Nonetheless, the purported adoption of the NAIC Model Law in a handful of states have already created different standards that insurers operating in multiple states would have to comply. In order to achieve security across the board and uniform cyber resilience in the American insurance industry, harmonization of the regulatory measures must be strived for, based on the NYDFS regulations, as cybersecurity is only as strong as its weakest link.