Roger Williams University Law Review

Volume 24 | Issue 1 Article 6

Winter 2019

The Insurance Data Security Model Law: Strengthening Cybersecurity Insurer-Policyholder Relationships and Protecting Consumers

Koyejo-Isaac Idowu
J.D. 2019, Roger Williams University School of Law

Comments

The Insurance Data Security Model Law: Strengthening Cybersecurity Insurer-Policyholder Relationships and Protecting Consumers

Koyejo-Isaac Idowu*

> *"Regulators have a critical role to play in protecting consumers as the cyber landscape continues to evolve and this model law sets cybersecurity customs for insurers to help safeguard consumers."*[1]

INTRODUCTION

In the current age of vast technological development, cybersecurity is one of the fastest growing industries in the United States.[2] Gone are the days where a standard, off-the-rack firewall could protect one's technology from danger. Today, individuals and

* Candidate for J.D., Roger Williams University School of Law, 2019; B.A., B.S., University of Rhode Island, 2015.

1. Press Release, Nat'l Ass'n of Ins. Comm'rs, NAIC Passes Insurance Data Security Model Law (Oct. 24, 2017), https://www.naic.org/Releases/2017_docs/naic_passes_data_security_model_law.htm [https://perma.cc/8PXF-FR9A].

2. *See* Eric Nordman & Dan Daveline, *Report on the Cybersecurity Insurance Coverage Supplement*, NAT'L ASS'N OF INS. COMM'RS & THE CTR. FOR INS. POL'Y & RES. (Aug. 27, 2016), https://www.naic.org/documents/committees_ex_cybersecurity_tf_report_cyber_supplement.pdf [https://perma.cc/55B5-C77X].

companies face the challenges that arise from increasingly sophisticated hackers who use cutting edge technology to engage in debilitating destruction from the comforts of their own homes.[3] Of course, this phenomenon is not entirely new; computer hackers have taken various forms over the last two decades.[4] However, companies' complete reliance on technology to run their businesses and to store sensitive consumer information has empowered hackers and further incentivized them to go beyond merely manipulating and stealing such information. Instead, hackers use that misappropriated information to extort companies.[5] When such an attack occurs, companies are at the mercy of the unknown wrongdoer, and the *best* case scenario for a large publicly-traded company often means stopping the flow of sensitive company or consumer information in a "timely" manner and experiencing worldwide embarrassment before settling cases for millions of dollars with those consumers who rightfully sue the company for its ineffective security measures.[6]

To minimize cybersecurity risks and reduce the likelihood of high-profile cyber breaches, companies have embraced cybersecurity risk management, which involves adopting measures not only to protect information by preventing breaches, but also to react to breaches once they occur.[7] Companies began purchasing

---

3. Abigail Summerville, *Protect Against the Fastest-Growing Crime: Cyber Attacks*, CNBC (July 26, 2017, 3:53 PM), https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html [https://perma.cc/2JK3-JNZZ] ("Cyber attacks are increasing in size, sophistication and cost.").

4. *See* Bill Gertz, *NSA: Cyber Attacks Are Becoming More Sophisticated, Aggressive, and Disruptive*, THE WASH. FREE BEACON (Nov. 16, 2017, 5:00 AM), http://freebeacon.com/national-security/nsa-cyber-attacks-becoming-sophisticated-aggressive-disruptive/ [https://perma.cc/FV9D-YFTU].

5. *See* Anthony Cuthbertson, *Ransomware Attacks Rise 250 Percent in 2017, Hitting U.S. Hardest*, NEWSWEEK (May 23, 2017, 1:37 PM), http://www.newsweek.com/ransomware-attacks-rise-250-2017-us-wannacry-614034 [https://perma.cc/2LBK-Z6RG].

6. Megan Santosus, *What is the Worst Case Scenario for Cyber Attacks?*, MY TECH DECISIONS (Jan. 31, 2017), https://mytechdecisions.com/network-security/worst-case-scenario-cyber-attacks/ [https://perma.cc/Q4XJ-UL27] ("While such incidents certainly lead to much hand wringing, cyber attacks perpetrated on individuals, companies and countries can have significant fallout that outlasts the current news cycle. At best, cyber attacks can be a nuisance, and at worst, they can have devastating and long-lasting negative implications.").

7. *See* Anne Obersteadt, *Cybersecurity*, NAT'L ASS'N OF INS. COMM'RS &

cybersecurity insurance to prepare themselves for the increasing likelihood of devastating cyber-related issues.[8] As part of a relatively new industry, cybersecurity insurers demanded an assessment of the companies' cyber risk, which is very difficult to quantify.[9] Previously, companies had not collected data or given much thought to cybersecurity issues that may afflict their business and could not provide detailed actuarial data to insurers.[10] As a result, cybersecurity insurance policies were expensive and the scope of the coverage varied significantly.[11] Most companies either refrained from purchasing insurance and hoped that they would not be the next major cyber breach victim, or purchased insurance and hoped that the coverage would be there when they needed it.[12]

While the advent of cybersecurity insurance provided companies with relief, it raised concerns for consumers, as they feared that companies would be less inclined to invest in measures to protect their information.[13] Consumers pressured their state legislatures to enact laws that required companies to develop and implement comprehensive cybersecurity programs.[14] States

---

THE CTR. FOR INS. POL'Y & RES. (July 2014), https://www.naic.org/cipr_newsletter_archive/vol12_cyber_liability.pdf [https://perma.cc/AC3K-A36C].

8. *Id.*

9. *Id.* ("However, cyber risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate by relying on qualitative assessments of an applicant's risk management procedures and risk culture.").

10. Jayleen R. Heft, *7 Challenges Insurers Face in the Cyber Insurance Market,* PROP. CASUALTY 360 (Mar. 8, 2017), http://www.propertycasualty360.com/2017/03/08/7-challenges-insurers-face-in-the-cyber-insurance?slreturn=1514746107&page=7 [https://perma.cc/SH6N-LEFZ] (discussing the "lack of sufficient cyber data to enable accurate underwriting").

11. *See id.*

12. Kathleen Richards, *Is Cyberinsurance Worth the Risk? Immature Products and a Lack of Standardization Raise Critical Questions About First-Party Risk and Third-Party Liability*, TECH TARGET (Aug. 2014), http://searchsecurity.techtarget.com/feature/Is-cyberinsurance-worth-the-risk [https://perma.cc/9V7X-Z6RE] ("As established insurance providers and startups rush to sell cyberinsurance to companies of all sizes, many enterprises still can't find insurance policies due to the lack of product standardization and complexities of establishing adequate coverage.").

13. *See* Joseph Carson, *Majority of Companies Are Failing at Cyber Security Metrics, and Investing Blindly*, THYCOTIC (Nov. 22, 2017), https://thycotic.com/company/blog/2017/11/22/companies-fail-at-cyber-security-metrics-invest-blindly/ [https://perma.cc/T58J-N36X].

14. Karen Turner, *The Equifax Hacks Are a Case Study in Why We Need*

generally responded with legislation that forced companies to consider cybersecurity protection measures, but most laws lacked the force necessary to facilitate a meaningful change in companies' cyber practices.[15] The states' failures to impose adequate mandates are understandable. After all, effective cybersecurity regulation requires a level of proficiency in a complicated and ever-changing field of study. For that reason, regulators should (1) consult experts in the cybersecurity field, and (2) gain knowledge about the industry.

This Comment recommends that states adopt the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (the "Model Law") and expand its application to all businesses.[16] NAIC has actively engaged experts to increase

---

Better Data Breach Laws, VOX (Sept. 14, 2017, 10:17 AM), https://www.vox.com/policy-and-politics/2017/9/13/16292014/equifax-credit-breach-hack-report-security [https://perma.cc/7TVJ-BA5Q] ("Companies aren't incentivized to put their customers first. Whether it's minimizing how much of our information they collect, fortifying security, or simply telling us they've been breached, we can't depend on these companies in good faith. It's up to government regulators to keep them in check.").

15. *Cybersecurity Legislation 2017*, NAT'L CONF. OF ST. LEGIS. (Dec. 29, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx [https://perma.cc/9N9X-EXFW].

> At least 42 states introduced more than 240 bills or resolutions related to cybersecurity. Some of the key areas of legislative activity include [(1)] improving government security practices; [(2)] commissions, task forces and studies; [(3)] funding for cybersecurity programs and initiatives; [(4)] targeting computer crimes; [(5)] restricting public disclosure of sensitive security information; and [(6)] promoting workforce, training, economic development.

Id.

16. Kambon R. Williams, *NAIC's Model Law Opens Door for State Data Security Standards*, LEXOLOGY (Dec. 19, 2017), https://www.lexology.com/library/detail.aspx?g=06c6619e-cff5-4ccd-8d33-4ca44f5bb480 [https://perma.cc/N72N-T79N]. The Model Law requires insurers and licensees to comply with six main requirements:

> [(1)] Creation of a comprehensive Information Security Program based on a risk assessment that identifies risks to the business, including its use of Third-Party Service Providers, and determination of which security measures are appropriate to implement; [(2)] designation of an individual to oversee the Information Security Program; [(3)] oversight by the Board of Directors; [(4)] oversight of Third-Party Service Provider agreements; [(5)] establishment of an incident response plan; [(6)] investigation and notification of Cybersecurity Events within 72 hours from a determination that a reportable

its cybersecurity expertise as it created this Model Law.[17] The Model Law provides the detail necessary to ensure that companies remain up to speed with newly encountered cybersecurity threats by requiring companies to implement comprehensive cybersecurity programs that set procedures for breach prevention and response.[18] States should adopt the Model Law and apply it to all businesses for four main reasons. First, the Model Law will help to provide uniformity, which allows companies to understand their duties when it comes to cybersecurity. Second, the Model Law will ensure that businesses act prudently in maintaining effective cybersecurity measures, which will protect consumers. Third, the Model Law will repair the discord between cybersecurity insurers and policyholders. Finally, *complete* compliance with the Model Law can serve as a standard of care in data breach lawsuits brought by consumers for all businesses based on the law's data security standards.[19]

Part I of this Comment will introduce the New York State Department of Financial Services Cybersecurity Regulation (the "DFS Regulation"), the state law that most significantly influenced the Model Law.[20] Part II will discuss the growth in cybersecurity insurance and the challenges that exist in obtaining effective cybersecurity coverage. Part II will also describe the Model Law's core requirements and explain how they not only force companies to take a proactive and continuous approach to guard against data breaches, but also resolve many of the challenges that insurers and policyholders face when determining the scope of a company's cybersecurity insurance. Part III will examine Ohio's most recent

---

> Cybersecurity Event has occurred; and providing an annual certification of compliance to the Insurance Commissioner by February 15 of each year.

Id.

17. *See* Ted Nickel, *The Year Before Us: Perspectives from NAIC President Ted Nickel*, NAT'L ASS'N OF INS. COMM'RS & THE CTR. FOR INS. POL'Y & RES. (Mar. 2017), http://www.naic.org/cipr_newsletter_archive/vol21_nickel.pdf [https://perma.cc/R4FR-6GVW] ("The Cybersecurity Task Force formed a drafting group consisting of several state insurance regulators, trade and industry groups, and consumer representatives to work on . . . the proposed Insurance Data Security Model Law. The drafting group has been meeting regularly since November 2016.").

18. *Id.*

19. *Id.*

20. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.0–.23 (2017).

cybersecurity bill, compare it to the Model Law, and explain how the Model Law serves as the next logical step to meet the goals that states have been actively trying to achieve. It will argue that the Model Law has incorporated innovative and advanced cybersecurity risk-management approaches, making it the most complete data security law alongside New York's DFS Regulation. It will highlight the NAIC's use of principles that are "gaining wider acceptability as best practices to prevent, respond to, and mitigate cyber threats."[21] Part III will also recommend that the Model Law standards serve as the standard of care for businesses in data breach cases brought by consumers. Part IV will address the U.S. Department of the Treasury's (the "U.S. Treasury") qualified support of the Model Law. It will argue that the Model Law is the most effective way to reach *functional* uniformity and that the five-year timetable recommended by the U.S. Treasury for states to attain uniformity is unreasonable in light of the novel nature of the cybersecurity industry. Ultimately, this Comment will argue that the Model Law and further work by the NAIC and state regulators to develop a uniform breach notification model law provide the surest path to attaining everyone's goal: providing protection to consumers and uniform cybersecurity laws to establish stability for insurers and policyholders.[22]

---

21. Shaun Healy Clifford et al., *'Tis the Season . . . for Insurance Model Laws: NAIC Tackles Data Security,* FAEGRE BAKER DANIELS LLP (Oct. 30, 2017), https://www.faegrebd.com/tis-the-season-for-insurance-model-laws [https://perma.cc/9DDY-LDHM] ("It bears noting that many of the principles outlined in the Data Security Model are gaining wider acceptability as 'best practices' to prevent, respond to and mitigate cyber threats domestically and internationally.").

22. This Comment focuses on the importance and effectiveness of state data security and data breach laws and, therefore, a detailed overview of federal data security and data breach laws is beyond the scope of this Comment. Still, it is worth highlighting the well-known federal laws relating to privacy and cybersecurity.

Aside from state laws, the United States legal framework on privacy and cybersecurity "consists of federal laws as well as best-practice guidelines developed by government agencies and industry groups." Clayton Utz, *California Dreaming: Your Data Would Be Safe and Secure, if It Was in LA*, LEXOLOGY (Feb. 15, 2018), https://www.lexology.com/library/detail.aspx?g=21d38fca-a75a-4b28-aff3-57397c243081 [https://perma.cc/2K8C-UEXF].

Particularly, the Federal Trade Commission Act, which prohibits unfair or deceptive practices for consumer protection, "has been used as a basis for the Federal Trade Commission (FTC) to take enforcement action against

I. THE LAW THAT INSPIRED THE MODEL LAW: NEW YORK'S DFS REGULATION

A. The Development of the DFS Regulation

Similar to other states, New York responded to residents' requests for more cybersecurity protection.[23] However, it responded in a fundamentally different manner than any other state when it passed the DFS Regulation.[24] The DFS Regulation instantly garnered national recognition for its "trailblazing risk assessment-based approach" to cybersecurity, and New York became "the first state in the country to enact a law requiring banks, insurance companies, and other financial services institutions to maintain a cybersecurity program."[25] The DFS Regulation sought to provide "minimum cybersecurity

---

companies for failing to comply with posted privacy and security policies and unauthorized disclosure of personal information." *Id.*

In fact, the FTC is currently conducting investigations of the Equifax and Facebook data breaches. *See* Marguerite Reardon, *Google and Facebook Could Face FTC Antitrust Scrutiny*, CNET (Feb. 14, 2018, 2:31 PM), https://www.cnet.com/news/google-and-facebook-could-be-in-ftc-crosshairs-over-anti-trust-concerns/ [https://perma.cc/Q6H4-MTK7].

Additionally, there are several industry specific laws that address privacy and cybersecurity concerns by requiring financial institutions, healthcare organizations, and federal agencies "to protect their systems and information." *See A Glance at the United States Cyber Security Laws*, APPKNOX https://blog.appknox.com/a-glance-at-the-united-states-cyber-security-laws/ [https://perma.cc/EB7J-AAVF]. These laws include: (1) the Financial Services Modernization Act (the Graham-Leach-Bailey Act); (2) the Health Insurance Portability and Accountability Act (HIPAA); and (3) the Federal Information Security Management Act. *Id.*

23. W. Todd Hicks, *New York Takes the Lead on Cybersecurity Regulation,* N.Y. L. J. (July 28, 2017, 2:01 PM), https://www.law.com/newyorklawjournal/almID/1202794215685/ [https://perma.cc/K77Q-A7BU] (discussing New York's "groundbreaking cybersecurity rules" and suggesting that "the New York regulatory framework offers a viable model for other jurisdictions to adopt, particularly as global cyberattacks make cyber defense an urgent matter").

24. COMP. §§ 500.0–.23.

25. Elana Ashanti Jefferson, *5 Things to Know About the NAIC's New Cybersecurity Model Law*, PROP. CASUALTY 360 (Nov. 20, 2017), http://www.propertycasualty360.com/2017/11/20/5-things-to-know-about-the-naics-new-cybersecurity?page_all=1&slreturn=1514311477 [https://perma.cc/7QG3-JDZF]; *Cybersecurity Alert*, AKIN GUMP STRAUSS HAUER & FELD LLP (Oct. 31, 2017), https://www.akingump.com/images/content/6/1/v2/61773/cybersecurity-alert-naic-issues-insurance-data-security-model.pdf [https://perma.cc/3QW9-4PVQ].

requirements that should protect consumers while preventing future cyber breaches."[26]

After the DFS Regulation went into effect on March 1, 2017, the cybersecurity community and other states took notice.[27] Specifically the NAIC, which plays a crucial role in cybersecurity insurance, praised the regulation and ultimately used its "risk assessment-based approach" in forming its own innovative Model Law for states to adopt.[28] Similar to the DFS Regulation, the Model Law "creates rules for insurers, agents[,] and other licensed entities covering data security, investigation[,] and notification of [a] breach [of data security]."[29] The main difference is that the Model Law applies exclusively to insurance providers, whereas the DFS Regulation applies to insurance providers, banks, and other financial institutions.[30] Moreover, despite minor substantive differences, the Model Law specifically states that a "licensee" that is in compliance with the DFS Regulation is also in compliance with the Model Law.[31] Although both cybersecurity regulations are limited to a subset of companies within particular industries, cybersecurity experts believe that these regulations "could become a model for other industries or even policies at the national level."[32]

---

26. Jefferson, *supra* note 25. The minimum cybersecurity requirements include: (1) controls; (2) risk-based minimum standards; (3) required minimum standards; and (4) accountability. *Id.*

27. Carol J. Gerner & Laurie A. Kamaiko, *United States: Other States Start to Follow New York Lead on Cybersecurity of Regulated Entities*, MONDAQ (May 5, 2017), http://www.mondaq.com/unitedstates/x/591518/Security/Other+States+Start+to+Follow+New+York+Lead+on+Cybersecurity+of+Regulated+Entities [https://perma.cc/32NY-86ND].

28. *See* INS. DATA SEC. MODEL LAW § 4(A) (MODEL REG. SERV. 2017) http://www.naic.org/store/free/MDL-668.pdf [https://perma.cc/9V3Y-RQCA].

29. Nat'l Ass'n of Ins. Comm'rs, *NAIC Passes Insurance Data Security Model Law,* NAT'L ASS'N OF INS. COMM'RS & THE CTR. FOR INS. POL'Y & RES. (Oct. 24, 2017), http://www.naic.org/Releases/2017_docs/naic_passes_data_security_model_law.htm [https://perma.cc/QXJ6-WEPD].

30. Williams, *supra* note 16.

31. *See* INS. DATA SEC. MODEL LAW § 3(I). A licensee is:

> [A]ny Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

Id.

32. Brennan Weiss, *New York Is Quietly Working to Prevent a Major Cyber*

B. *The Adoption of the Model Law*

The NAIC adopted the Model Law on October 24, 2017, for the purpose of developing a nationwide standard for insurance companies with regard to cybersecurity.[33] The NAIC aimed to "establish standards for data security, the investigation of cybersecurity events and notification of the commissioner of cybersecurity events."[34] The NAIC board of directors is confident that the states will adopt the Model Law and regulators indicate that "several states plan to include a version of the [Model Law] in their upcoming legislative packages."[35] The Model Law has the opportunity to resolve critical issues in a cybersecurity insurance industry where demand is growing, but agreeable coverage is hard to come by.[36]

II. GROWTH AND CHALLENGES IN CYBERSECURITY INSURANCE COVERAGE

A. *The Increasing Prevalence of Cybersecurity Insurance*

Over the last several years, the cybersecurity insurance market has grown at an exponential rate as more and more high profile cybersecurity breaches made headlines, spurring demand that cybersecurity insurance continues to develop at a similarly swift

---

Attack that Could Bring Down the Financial System, BUS. INSIDER (Feb. 25, 2018), http://www.businessinsider.com/new-york-cybersecurity-regulations-protect-wall-street-2018-2 [https://perma.cc/E3TP-CMGQ].

33. *Cybersecurity Alert*, *supra* note 25.

34. Christopher M. Brubaker, *NAIC Adopts Model Law on Cybersecurity: Will States Adopt It?*, THE LEGAL INTELLIGENCER (Dec. 26, 2017), https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2017/12/26/naic-adopts-model-law-on-cybersecurity-will-states-adopt-it/ [https://perma.cc/6JL8-SERP].

35. Healy Clifford et al., *supra* note 21.

36. Jeff Sistrunk, *4 Cyberinsurance Battlegrounds to Watch*, LAW360 (July 2, 2015), https://www.law360.com/articles/674618/4-cyberinsurance-battlegrounds-to-watch [https://perma.cc/AC4L-E67V].

> [C]yber policies should have flexibility, providing the insurance company with the assurance that the policyholder is doing what it can to keep up with threats and providing companies the peace of mind that a policy will protect them . . . the question is what the middle ground is; there should be a *standardized method to determine security requirements*.

Id. (emphasis added).

rate.[37] In fact, members of the cybersecurity community "expect worldwide spending on [c]ybersecurity products and services to eclipse $1 trillion for the five-year period from 2017 to 2021."[38] Most attribute the boom in this industry to highly publicized cyberattacks, which have brought the need for such insurance into sharper focus.[39] As a result, the number of carriers offering cybersecurity insurance has increased.[40] In 2016, "the total cybersecurity insurance market in the United States was $2.49 billion. This figure includes the standalone and package cybersecurity insurance premiums . . . ."[41] Because "fewer than 10% of companies are thought to purchase cyber insurance today," these figures will only grow with time.[42] In light of companies' increasing dependence on cybersecurity insurance, it is crucial for the industry to provide clear and effective policies. In many respects, big business and the economy depend on it.[43] However, there are several challenges that plague cybersecurity insurance as

---

37. Nordman & Daveline, *supra* note 2.

> The cyber insurance marketplace has grown to over $2 billion in gross written premiums with industry prognosticators forecasting it to double by 2020. The number of carriers offering cyber insurance has increased following a spate of cyberattacks that have brought the potential and need for such insurance into sharper focus.

Id.

38. *Id.*

39. Heft, *supra* note 10 ("[T]he threat of cyber attacks is the biggest fear of businesses.").

40. Nordman & Daveline, *supra* note 2.

41. Eric Nordman, *Report on the Cybersecurity Insurance Coverage Supplement*, NAT'L ASS'N OF INS. COMM'RS & THE CTR. FOR INS. POL'Y & RES. (Aug. 6, 2017), https://www.naic.org/meetings1708/cmte_ex_cswg_2017_summer_nm_materials.pdf?1537315264253 [https://perma.cc/BK7B-TV7K].

42. Nordman & Daveline, *supra* note 2 ("The cyber market is growing by double-digit figures year-on-year, and could reach $20 billion or more in the next 10 years.").

43. Joe Rosengarten, *Rising Cyber Risks Grabbing Global Attention*, INS. BUS. (Jan. 24, 2018), https://www.insurancebusinessmag.com/us/news/cyber/rising-cyber-risks-grabbing-global-attention-90261.aspx [https://perma.cc/BFB2-RMBD].

> The financial impact of cyber attacks are also on the rise. The Global Risks Report (GPRS) cited a 2017 study of 254 companies across seven countries which put the annual cost of responding to cyberattacks at $16.2 million per company, a 27.4% year-on-year increase. "The cost of cybercrime to businesses over the next five years is expected to be US $8 trillion," the report said.

Id.

the industry seeks to strike a balance between protecting policyholders—which also protects the third parties whose information policyholders possess—while also protecting insurers that try to identify countless risks and costs associated with undertaking particular applicants.[44]

B. The Model Law Is Able to Minimize Cybersecurity Insurance Challenges and Facilitate the Market's Growth Potential

Despite the growth projections of the cybersecurity insurance market, cyber experts still contend that "cyber insurance remains a relatively small niche market" due to hesitance on the part of insurers and applicants.[45] In light of companies' high demand for cyber protection and the immense opportunity for insurers to make money, the parties' hesitance appears illogical at first blush.[46] However, a closer examination of insurers' and applicants' concerns confirms that both sides are facing legitimate obstacles, which are ultimately "preventing faster, more profitable expansion" of the cybersecurity insurance market.[47]

C. Challenges for Insurers

Insurers are tasked with the difficult job of providing cyber coverage to applicants without having the requisite data to help underwrite and price an applicant's cyber risk.[48] Customarily,

---

44. Heft, *supra* note 10.

45. Sam J. Friedman, *Data Obstacles Hamper Cyber Insurance Growth*, PROP. CASUALTY 360 (Mar. 24, 2017), https://www.propertycasualty360.com/2017/03/24/data-obstacles-hamper-cyber-insurance-growth/?ref=navbar-next [https://perma.cc/CF5N-CJG8].

46. L.S. Howard, *Confusing, Costly Cyber Policies Create Obstacles to Market Growth: Deloitte*, INS. J. (Mar. 3, 2017), https://www.insurancejournal.com/news/international/2017/03/03/443518.htm [https://perma.cc/K6HU-VLF5] ("Despite the rising profile of cyber risks, buyers have failed to widely embrace cyber coverage. At the same time, insurers generally have remained cautious about writing the coverage on a large scale basis.").

47. Sam Friedman, *Clearing Cyber Risk Speed Bumps: Why Insurers May Need a New Approach*, DELOITTE INSIGHTS (Mar. 22, 2017), https://www2.deloitte.com/us/en/pages/financial-services/articles/clearing-cyber-risk-speed-bumps.html [https://perma.cc/8J9T-RGPA].

48. Howard, *supra* note 46.

> The lack of historical data makes it difficult [for insurers] to build predictive models because (1) insurers haven't been selling cyber

insurers have used two sources of information in the underwriting process: (1) their own information that they amassed about the risks common in a particular industry; and (2) information that they requested from applicants.[49] These sources are then used to develop predictive models to calculate an applicant's risk and an appropriate policy price.[50] However, the novel nature of the cyber insurance industry has left insurers struggling to obtain any meaningful data to use for underwriting. To make matters worse, not only do insurers lack their own comprehensive data related to cyber security events, but they also receive very little information from the applicants.[51] As a result, insurers typically cannot rely on a company's documented breach data to make risk assessments and instead must make them entirely on their own.[52] Ultimately, the lack of information perpetuates "*a 'vicious circle'* of data-related issues hindering the growth of stand-alone cyber coverage in the high-end commercial market."[53] This vicious circle contains four major stages: (1) insurers' lack of information; (2) insurers' decision to underwrite narrowly; (3) companies' reluctance to seek coverage; and (4) insurers' inability to secure policies, which prevents insurers from acquiring the information necessary to assess companies' risks. This then circles back to the first stage of insurers' lack of information.[54] In the end, insurers and companies are left in the same detrimental position that they started.

Additionally, the continued sophistication of technology means that threats constantly take new forms, causing "insurers [to] adapt

---

> insurance long or widely enough to generate their own data, (2) there is no centralized source of information about cyber events, and (3) many cyber attacks go unreported and undetected.

Id.

49. *Id.*
50. *Id.*
51. *Id.*
52. Heft, *supra* note 10.
53. Friedman, *supra* note 47. The vicious circle includes the following:

> The lack of sufficient, relevant data undermines insurer confidence in underwriting and pricing. That prompts many to offer relatively low limits for fairly restricted coverage. That discourages buyers from taking out a policy, which limits insurer experience with the exposure. That limits data availability and starts the circle all over again.

Id.

54. *Id.*

to one type of attack only to face a new threat technique."[55] Undoubtedly, this makes "risk management an ongoing predicament" as insurers struggle to quantify the risk that an applicant poses. In a field that is premised on risk calculations and devising tools to project future behavior, insurers do not feel comfortable navigating areas where predictability is significantly hindered. Similarly, insurers often fear the possibility of being "overwhelmed by a sudden aggregation of losses," which is another unique threat that cyber insurance may pose.[56]

D. Challenges for Applicants

As one could imagine, the obstacles that the insurers face directly impact the quality of coverage they provide, which is the central predicament for applicants. Insurers tend to underwrite conservative and narrow policies in order to minimize the risk of providing insurance to companies with largely unknown risks in a potentially lucrative, yet perpetually evolving industry.[57] For example, insurers are able to avoid providing coverage by including certain policy exclusion language.[58] Further, even when an event

---

55. Heft, *supra* note 10.

56. Friedman, *surpa* note 47. "[Insurers] fear a systemic event that cascades across the country or around the world following an attack against a website host, cloud provider, or email server, triggering claims by a large percentage of their policyholders simultaneously." *Id.*

57. *Id.*

58. *See* Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. 16-35614, 2018 U.S. App. LEXIS 5682, at *1 (9th Cir. Mar. 6, 2018). This case focuses on cyber criminals' use of schemes to deceive businesses into authorizing transfers of money to fraudulent bank accounts. *See* Jeff Sistrunk, *9th Circ. Panel Wrestles with Email Scam Coverage Battle*, LAW360 (Mar. 12, 2018, 7:38 PM), https://www.law360.com/articles/1020969/9th-circ-panel-wrestles-with-email-scam-coverage-battle [https://perma.cc/CYP3-SL5T]. In 2013, an Aqua Star employee was tricked "into wiring more than $700,000 to overseas bank accounts controlled by a fraudster who posed as one of the company's seafood vendors." *Id.* The hacker used an email that led the employee to believe the receiving party was Zhanjiang LongWei Aquatic Products Industry Co. Ltd. *Id.* Travelers denied coverage and relied on "Exclusion G" in the policy, which precluded "coverage for losses 'resulting directly or indirectly from the input of electronic data' *by a person with authority to enter the insured's computer system*." *Id.* (emphasis added). In July 2016, a U.S. District Court judge ruled in favor of Travelers for this very reason. *Id.* Currently, the case is before the Ninth Circuit, and Aqua Star is arguing that the computer fraud provision includes "coverage for a direct loss of money that is '*directly caused by' computer fraud*—defined as the 'use of any

may be covered, the terminology in cybersecurity policies differs significantly depending on the insurer, so a policyholder typically does not have the benefit of relying on interpretations of other contracts or similar precedent.[59] Insurers' sweeping risk-averse approach and lack of uniform language spells trouble for companies who often do not realize that a "cyber" breach is not covered under its cyber policy or its traditional insurance policy until it is too late.

E. Reducing Insurers' and Applicants' Cybersecurity Challenges

Having identified the most fundamental obstacles for insurers and applicants, the next logical step is to consider how to eliminate the "vicious circle" that is preventing the cybersecurity industry from reaching its true growth potential.[60] To that end, cyber experts suggest that requiring companies to implement comprehensive data security programs is the proper approach to eliminating the obstacles currently weighing down the cyber insurance market.[61] From this perspective, instead of relying entirely on the largely unpredictable and seemingly narrow protection of cybersecurity insurance, companies are in a better position to assess their own risks, implement appropriate safety measures (likely based on the instruction of cyber security experts), and ensure that a proper protocol is in place in the event a breach occurs.[62] Among one of the first of its kind, the Model Law provides

---

computer to fraudulently cause a transfer of money.'" *Id.* (emphasis added).

59. Howard, *supra* note 46 ("Cyber policies lack standardization. Cyber insurance coverage is often written using customized policies, which results in different coverage terms, conditions and exclusions from carrier to carrier . . . .").

60. Friedman, *supra* note 47.

61. Howard, *supra* note 46 ("[Insurers should] [d]evelop[] a 'risk-informed model' rather than a definitive predictive model for cyber risks. With a risk-informed model, underwriting and pricing assessments would focus on 'specific risk-management steps applicants could take to be secure (prevention), vigilant (detection) and resilient (loss control and recovery) in their cyber-related operations.'").

62. Eli Durado, et al., *Economic Perspectives: Cybersecurity Policy Reforms for the 21st Century*, MERCATUS CTR.: GEO. MASON UNIV. (Nov. 9, 2015), https://www.mercatus.org/publication/economic-perspectives-cybersecurity-policy-reforms-21st-century [https://perma.cc/L77U-NDHF] ("Companies and firms, on their own, are best able to solve cybersecurity issues because they have the quickest access to information about relevant threats. The best evidence shows that private firms do, in fact, spend a lot of money securing their own assets.").

instructions and lays out minimum standards, which provide companies with the necessary framework to effectively engage in measures of breach prevention.[63]

F. Examining the Model Law

The Model Law not only provides a structure for proper breach-prevention measures, but also alleviates many of the challenges that the cybersecurity industry has faced regarding developing fair policies that insurers and policyholders could feel confident about. Principally, the Model Law requires insurers and licensees to comply with requirements in six major areas.[64] First, licensees must create an Information Security Program.[65] This requires licensees to conduct a risk assessment to identify the hazards of its business, including the use of third-party service providers, and to determine appropriate security measures to implement. Second, licensees must name an individual to run the daily operations of the Information Security Program.[66] Third, licensees' boards of directors must oversee the implementation of the Information Security Program.[67] Fourth, licensees are required to oversee the manner in which third-party service providers protect the information that the companies share with them.[68] Fifth, licensees must establish an incident response plan to follow in the event of a data breach.[69] Finally, licensees must follow particular procedures with regard to investigating cybersecurity events and reporting them to the appropriate state insurance commissioner(s).[70] Fundamentally, the requirements are focused on the company's ability to assess risk, implement security measures through the development of a program, and create a response plan to follow in post-breach situations.[71]

One of the most important requirements of the Model Law is that insurers must engage in a risk-based assessment of their

63. Williams, *supra* note 16.
64. *Id.; see also supra* text accompanying note 16.
65. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *Id.*
70. *Id.*
71. *Id.*

business and any third-party service providers for the purpose of determining the proper security measures to implement.[72] This assessment and security installation forces businesses to examine their cybersecurity vulnerabilities, and likely contact the appropriate cyber experts to reduce the risk of not complying with this provision of the Model Law. In addition to its general benefit of serving as an excellent safety practice for any well-run business, the assessment will also benefit cybersecurity insurers when the regulated company seeks cybersecurity insurance. The insurers' concern about being unable to assess a company's risk will be alleviated because insurers will be able to use the company's own risk-based assessment and its subsequent security measure decisions to determine the company's risk.[73] In this regard, the Model Law may stop the "vicious circle" that has stunted the growth of the cybersecurity insurance industry.

In addition to forcing companies to assess their own risks and implement appropriate measures, the Model Law also requires regulated entities to perform a risk-based assessment and implement appropriate measures for the third-party service providers with which they do business.[74] This mandate is particularly useful in easing cybersecurity insurers' fears of what is known as the "catastrophic accumulation of cyber exposures."[75] Here, because companies have a legal obligation to ensure that the third-party service providers they affiliate with properly appreciate the risks of their business and implement security measures, insurers will be less skeptical. This allows insurers to underwrite in a less rigorous or narrow manner.[76] Ultimately, this will provide

---

72. INS. DATA SEC. MODEL LAW § 4(A).

73. Nat'l Ass'n of Ins. Comm'rs, *Cybersecurity*, NAT'L ASS'N OF INS. COMM'RS & THE CTR. FOR INS. POL'Y & RES. (Apr. 30, 2018), http://www.naic.org/cipr_topics/topic_cyber_risk.htm [https://perma.cc/LH5X-2SYE] (noting that insurers writing cyber coverage will be interested in the risk-management techniques applied by the business to protect its network and its assets).

74. INS. DATA SEC. MODEL LAW § 4(A).

75. *See* Heft, *supra* note 10 ("Some insurers may fear being overwhelmed by a sudden aggregation of losses, in which a third-party service that works with a wide swath of businesses get hacked and leads to service failures for all of its users. This sort of systemic event could spell chaos for the insurance industry.").

76. *See* Jeff Sistrunk, *4 Key Cybersecurity Insurance Cases to Watch*, LAW360 (July 14, 2017, 7:01 PM), https://www.law360.com/articles/934228/4-

a more reasonable balance between companies and cybersecurity insurance providers, as the insurers will be more likely to expand their coverage knowing that companies are highly incentivized to protect their information in light of the clear legal consequences that companies now face.[77]

Finally, the Model Law that will aid in reshaping the cybersecurity insurer-policyholder relationship by requiring post-breach response plans and notification.[78] The law requires companies to establish an incident response plan to deal with breaches or threats of breaches, which provides companies with a detailed procedure for managing crisis.[79] Also, the investigation and notification requirements ensure that companies obtain as much information as possible about the breach event right away, which is crucial to minimizing further damage and learning from the breach for the purpose of strengthening the company's security measures.[80]

Ultimately, the post-breach response plans and investigation and notification requirements will be beneficial for two reasons. First, the investigation and notification requirements provide insurers with more actuarial data to examine in their risk assessment of applicants, which will lead to a greater gauge of companies' vulnerability to cyber attack. Secondly, the post-breach response plan helps policyholders identify the type of cyber attack and document its character to ensure that policyholders can provide proof to their insurers when it is time to file their claim.

---

key-cybersecurity-insurance-cases-to-watch [https://perma.cc/MS8T-Y6NP]. Some insurers already require compliance with a cybersecurity network, which serves as a prerequisite to coverage. *Id.* Thus, the Model Law will facilitate compliance with certain cyber policies, which will help eliminate coverage these types of coverage disputes. *See id.* The case of *Cottage Health v. Columbia Casualty Co.* "is notable because it marks the first time a court has been asked to interpret cyberinsurance policy language requiring the policyholder to comply with specified network security requirements . . . ." *See id.* In 2013, Cottage Health (Cottage), a non-profit network of six hospitals, suffered a data breach that lead to the public disclosure of medical records for 32,500 patients. *Id.* Cottage sought coverage from its insurer Columbia Casualty. However, Columbia Casualty invoked a policy exclusion and argued that Cottage failed to apply the security measures it promised when it sought coverage. *Id.*

77. *See id.*

78. *See* INS. DATA SEC. MODEL LAW §§ 4(H)–6.

79. *Id.* § 4(H).

80. *See id.* §§ 5–6.

Undoubtedly, all of the benefits that foster an improved cybersecurity insurer-policyholder relationship directly enhance the Model Law's ultimate goal of protecting consumer information. The more regulation required for proactive protection of cybersecurity information, the greater likelihood that companies can evade breaches, insurers can avoid making large payouts, and consumers can be confident that their information is in the hands of companies that are doing everything in their power to protect it.[81] Accordingly, based on the breadth of the data security requirements, and the nuanced drafting of the Model Law, it is clear that all parties involved in cybersecurity insurance will be put in a more favorable position; all that is left for the states to do is adopt the Model Law and watch the benefits accrue.

III. THE MODEL LAW: THE STRONGEST CYBERSECURITY LAW

A. Comparing Ohio's Cybersecurity Bill and the Model Law

An assessment of current and pending state cybersecurity legislation confirms that the Model Law is the next logical step to meet the goals that the states have started trying to achieve. Moreover, unlike various state laws, the Model Law imposes requirements with consequences for non-compliance, rather than mere "suggestions" to encourage companies to develop their cybersecurity departments. In order to truly highlight the strength of the Model Law's cybersecurity risk-management approach, it is appropriate to compare its contents to the Data Protection Act (the Act), a proposed cybersecurity bill in Ohio, which also employs a risk-management approach.[82]

On October 21, 2017, the Act was introduced in the Ohio State Senate and was designed to "encourage businesses to achieve a

---

81. *See* James R. Woods et al., *The Role of Cyberinsurance in Risk Management*, LAW360 (Apr. 7, 2016, 11:32 AM), https://www.law360.com/articles/780942/the-role-of-cyberinsurance-in-risk-management [https://perma.cc/6ZDQ-6U59] ("Companies with well-developed safeguards, including up-to-date written information security programs (WISPs) and data breach response plans (DBRPs), together with active board of director governance of cybersecurity risk, will enjoy broader cybersecurity coverage at lower premium costs.").

82. S.B. 220, 132nd Gen. Assemb. (Ohio 2017), https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-SB-220 [https://perma.cc/Z5DR-J278].

higher level of cybersecurity through voluntary action."[83] The Act specifies that:

> [A] covered entity's cybersecurity program shall.....[:] (1) Protect the security and confidentiality of the information; (2) Protect against any anticipated threats or hazards to the security or integrity of the information; [and] (3) Protect against unauthorized access to and acquisition of the information "[84]

The entity is rewarded for implementing this risk-based program because doing so creates "an affirmative defense to any cause of action sounding in tort that . . . alleges that the failure to implement reasonable information security controls resulted in a data breach concerning personal information."[85] Ultimately, in order to be eligible for this safe harbor, the entity's cybersecurity program must "reasonably comply" with one of the frameworks listed in the Act.[86]

Ohio's Act serves as an example of the type of well-meaning legislation often introduced in state legislatures to facilitate companies' implementation of cybersecurity standards.[87] However,

---

83. *Id.*

84. *Id.* ("'Covered entity' means a business that accesses, maintains, communicates, or processes personal information.....").

85. *Id.*

86. *Id.*

> The cybersecurity program reasonably complies with the current version of any of the following or any combination of the following, subject to divisions (A)(2) and (D) of this section: (a) The "framework for improving critical infrastructure cybersecurity" developed by the "national institute of standards and technology" (NIST); (b) "NIST special publication 800-171"; (c) "NIST special publications 800-53 and 800-53a"; (d) The "federal risk and authorization management program (FedRAMP) security assessment framework"; (e) The "center for internet security critical security controls for effective cyber defense"; (f) The "international organization for standardization/international electrotechnical commission 27000 family - information security management systems."

Id.

87. *See* Weiss, *supra* note 32.

> Last year at least 42 states introduced more than 240 bills or resolutions related to various cybersecurity issues, according to the National Conference of State Legislatures. And since the NYDFS rules took effect, financial regulators in Colorado and Vermont have followed New York's lead with cybersecurity regulations of their own.

despite an admirable effort, this Act lacks any meaningful punch. First, the bill does not *require* companies to implement a cybersecurity program or follow a risk-based framework.[88] If the goal of the bill is to encourage the adoption of a risk-based cybersecurity framework, then the most efficient way to do so would be to demand such a framework. A bill that merely provides benefits to a company for implementing standards that it should already be required to have—and is required to have in states such as New York—ultimately makes a miniscule impact in protecting sensitive information.[89] Additionally, the Act states that a covered entity must "reasonably comply" with a listed framework, which ultimately necessitates an interpretation of what exactly qualifies as reasonable compliance.[90]

All in all, Ohio's Act misses the point, as its underlying focus for enacting cybersecurity legislation appears to support the wishes of companies rather than consumers whose personal information is always ripe for attack. The legislators are focused on company liability and protecting businesses rather than paying closer attention to the issue of cybersecurity itself.[91] Of course, businesses should receive some protection when they exercise scrupulous care in taking proper steps to protect against cybersecurity events, but this is the last step in a multi-step mission. It is fundamental that states and other regulators ensure that company practices are as comprehensive as possible before rolling out protection from liability. If not, the result will be that companies who implement good, average, or even below average cybersecurity procedures will gain protection from liability for doing "something." In the event that occurs, consumers are in trouble.

Id.

88. *See* INS. DATA SEC. MODEL LAW §§ 4–6.

89. *See* COMP. § 500.02 ("Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity's Information Systems.").

90. Ickes Holt, *Is Ohio Getting its Cybersecurity Act Together?*, ICKES HOLT (Feb. 16, 2018), https://ickesholt.com/2018/02/16/ohio-getting-cybersecurity-act-together/ [https://perma.cc/S4KU-E9VB] ("What does 'substantial' mean? It is wholly subjective and it will take years in Ohio courts, if ever, to create a case law definition from a cybersecurity standpoint, we do not have years to shore up Ohio's networks.").

91. *Id.* ("A clear mandate would bring more clarity to questions of liability and presumably more businesses would adopt a risk-based framework in the face of a mandate. In the end, isn't more about security than liability?").

The Model Law addresses a chief flaw of the Ohio Act; the Model Law focuses on the dual purpose of protecting the consumer and providing incentives to companies for their diligence. Particularly, the Model Law is more concerned with the details of the companies' cybersecurity programs, as it requires the implementation of an information security program, which is aimed at protecting consumer information on a daily basis, and an incident response plan, which is activated in the event a breach occurs. Moreover, it imposes an ongoing obligation on licensees to monitor and adjust their cybersecurity programs upon changing conditions within the company.[92] This requirement is strictly enforced through an annual certification requirement.[93] Thus, the general theme is that the Model Law places its attention where Ohio's Act did not: on the implementation of the cybersecurity program. The Model Law ensures that companies remain engaged in installing cybersecurity measures because it mandates compliance.[94] At most, the Act ensures that companies "reasonably comply" with a named cybersecurity framework, but *only if* they want to receive the benefit of an affirmative defense in particular court proceedings.

B. Complete Compliance with the Model Law Should Serve as the Standard of Care for Businesses in Data Breach Lawsuits Brought by Consumers

Despite the Ohio Act's shortcomings, the Act is a trailblazer in its concept that compliance with particular cybersecurity frameworks should aid companies in a litigation setting.[95] While the Act did not institute a high enough standard for its companies to reach before being eligible to receive a safe harbor, the Model Law, in all its thoroughness, could serve as an appropriate standard of care for businesses in data breach lawsuits brought by consumers.[96] In other words, if the defendant business can show

---

92. *See* Rajesh De et al., *NAIC Adopts Insurances Data Security Model Law*, LEXOLOGY (Nov. 10, 2017), https://www.lexology.com/library/detail.aspx?g=b8d96b1b-f110-47d6-ad95-8405bccb7a36 [https://perma.cc/P87S-G5ZC].

93. *Id.*

94. *Id.*

95. *See* Holt, *supra* note 90.

96. David Forscey et al., *Cybersecurity Is the Next Frontier of State*

complete compliance with the Model Law, then the court should find that the business acted reasonably under the circumstances. By making the Model Law an industry standard and requiring *complete* compliance, businesses would have a clear view of exactly what would be required of them with regard to cybersecurity. Most importantly, customers would have the greatest assurance that companies are incentivized to protect their information. Companies are less apt to cut corners knowing that there is a realistic way to protect themselves from liability. Currently, companies have no such assurance. But, through the use of the Model Law as the standard of care, companies would be aware that a breach would not automatically result in insurmountable liability so long as the breach was one that even a Model Law-compliant cybersecurity program could not stop.

The Model Law's risk-management approach is viewed as a best practice to prevent, respond to, and mitigate cyber threats and, thus, it is appropriate to render it the industry custom.[97] However, in light of the recommendation that the Model Law serves as the standard of care for businesses in data breaches brought by consumers, it is important to underscore a significant aspect of company conduct that the Model Law does not address: data breach notification. Under the Model Law, companies are only required to notify the Insurance Commissioner of a particular state within seventy-two hours of a "cybersecurity event."[98] Thus, for this piece

---

Regulation, LAW360 (May 11, 2017, 1:26 PM), https://www.law360.com/articles/922786/cybersecurity-is-the-next-frontier-of-state-regulation [https://perma.cc/J6HW-X3GD].

> [I]t is also possible that the flexible "reasonableness" standards already implemented in 13 states could develop into a roughly similar cross-jurisdiction rule. This is already happening among federal agencies, where different regulators are beginning to coalesce around similar definitions of what constitutes prudent cybersecurity (e.g. adherence to the NIST Cybersecurity Framework).

Id.

97. Healy Clifford, *supra* note 21 ("It bears noting that many of the principles outlined in the Data Security Model are gaining wider acceptability as 'best practices' to prevent, respond to, and mitigate cyber threats domestically and internationally.").

98. Nathan K. Tenney, *Litigation Update: The Times They (May Be) A-Changin': State Legislators Now Have a Uniform Cybersecurity Law Framework to Consider After NAIC Adopts the Insurance Data Security Model Law*, KANE RUSSELL COLEMAN LOGAN (Jan. 8, 2018), https://www.krcl.com/articles/litigation-update/litigation-update-times-may-

of the cybersecurity puzzle, a respective state's breach notification law (and the applicable federal laws depending on the type of industry being regulated) would dictate the companies' obligations to notify consumers or other parties under a particular circumstance. Currently, there are fifty different state breach notification laws in the United States with varying requirements.[99] To offer a solution to this patchwork of state laws, the NAIC plans to develop a Model Breach Notification Law for states to adopt, which the association will work on in 2018.[100] With the success that the Model Law garnered, there is a strong reason to believe that the NAIC will produce a comprehensive Breach Notification Law for states to adopt, and also for courts to incorporate as part of the standard of care.

IV. UNITED STATES DEPARTMENT OF THE TREASURY'S QUALIFIED SUPPORT OF THE MODEL LAW

A. *The Model Law Is the Most Effective Way to Reach Functional Uniformity*

The Model Law has enjoyed strong state support since the NAIC announced its adoption in October of 2017, but one of the most influential comments on the Model Law came from the U.S. Treasury, which recognized the Model Law in its report on Asset Management in Insurance.[101] Specifically, the report endorsed adoption of the Model Law and "include[d] recommendations to the states to adopt uniform data security and breach notification legislation . . . ."[102] However, the report expressed skepticism

changin-state-legislators-now-uniform-cybersecurity-law-framework-consider-naic-adopts-insurance-data-security-model-law/ [https://perma.cc/M9KD-Z447].

99. Fran Faircloth & Colleen Theresa Brown, *Alabama Passes Data Breach Notification Law; Breach Laws Now on the Books in All 50 States*, SIDLEY (Mar. 30, 2018), https://datamatters.sidley.com/alabama-passes-data-breach-notification-law-breach-laws-now-books-50-states/ [https://perma.cc/6Z3Q-Y22L].

100. Press Release, *supra* note 1.

101. Gloria Gonzalez, *Treasury Recommends Revamping Federal Insurance Office, Adopting Uniform Cyber Rules*, BUS. INS. (Oct. 27, 2017, 10:56 AM), http://www.businessinsurance.com/article/20171027/NEWS06/912316842/Treasury-recommends-revamping-Federal-Insurance-Office,-adopting-uniform-cyber-r [https://perma.cc/SVP3-GMZ5].

102. Healy Clifford, *supra* note 21.

regarding the Model Law's ability to achieve uniformity,[103] and the U.S. Treasury ultimately recommended Congress "step in with legislation if a state legislative effort fails . . . ."[104] Thus, based on the report, the U.S. Treasury believes that five years is enough time to consummate uniform data security regulation amongst the states.[105] This has renewed the longstanding debate about which governmental entity is in the best position to resolve the issues related to cybersecurity and consumer protection.[106]

The states are far better suited to handle the cybersecurity insurance issues pertaining to data security, investigation, and notification of breach through their adoption of the Model Law rather than waiting for federal legislation that will likely be less comprehensive than current state laws.[107] First and foremost, cybersecurity legislation should remain a matter of state regulation because "it is important that states can experiment based on their own individual policy preferences." [108] Furthermore, in this instance, "[d]iverse state rules do not necessarily cause an undue burden."[109] Companies often complain about having to comply with a patchwork of state laws, but as stated previously, compliance with the Model Law could largely resolve the lack of uniformity by creating a de facto standard of care for breach data lawsuits brought by consumers. Because cybersecurity is entirely about reducing one's risk of exposure to data breach, it is proper to devise

---

103. Gonzalez, *supra* note 101 ("The Insurance Data Security Model Law will not necessarily result in nationally uniform insurance laws regarding data breach notification and data security."); *see also* Colleen Theresa Brown et al., *U.S. Treasury Expresses National Perspective in Response to NAIC Insurance Data Security Model Law*, SIDLEY (Dec. 7, 2017), http://data matters.sidley.com/u-s-treasury-expresses-national-perspective-response-naic -insurance-data-security-model-law/#page=1 [https://perma.cc/93SH-56WE].

104. Healy Clifford, *supra* note 21.

105. Gonzalez, *supra* note 101.

106. Ryan Hagemann, *Congress Overlooks Cyber-Security Strengths in State, Local Governments*, WATCHDOG (July 23, 2015), https://www. watchdog.org/opinion/congress-overlooks-cyber-security-strengths-in-state-local-governments/article_91160f66-0eda-5dfb-8aa6-586f5678b489.html [https://perma.cc/Y2FB-MKY3]; *see also* Charlie Mitchell, *State Officials, Small Retailers: We Were Left out of Data-Breach Legislation Compromise*, WASH. EXAMINER (Nov. 28, 2017, 12:01 AM), https://www.washington examiner.com/state-officials-small-retailers-we-were-left-out-of-data-breach-legislation-compromise [https://perma.cc/UAW4-8HYB].

107. Forscey, *supra* note 96.

108. *Id.*

109. *Id.*

a cross-jurisdiction reasonableness standard in defining what constitutes "prudent cybersecurity."[110]

Although the Model Law can serve as a starting point to defining "prudent cybersecurity," the development of an adequate breach notification law may take time. Currently, states are all over the map with respect to when a company must provide notification of a data breach, who should be notified, and how quickly it must be done.[111] For that reason, the NAIC will need to consult with its members from all states in crafting the appropriate Breach Notification Model Law. The organization has repeatedly shown promise in devising standards for the insurance industry, and these standards certainly can be expanded to businesses outside of the insurance context. Moreover, states such as New York—that developed the trailblazing DFS Regulation—have also proven that state experimentation can produce meaningful progress in a complex industry. Thus, given the progress of state legislatures and organizations such as the NAIC, states do not need federal assistance in this area; they simply need more time.[112]

---

110. Id.

111. Andrea O'Sullivan, *Would Data Breach Notification Laws Really Improve Cybersecurity?*, MERCATUS CTR.: GEO. MASON UNIV. (Sept. 26, 2017), https://www.mercatus.org/%5Bnode%3A%5D/commentary/would-data-breach-notification-laws-really-improve-cybersecurity [https://perma.cc/6UTH-FDJ9].

> Already, companies are governed by a patchwork of 48 different state and territorial data breach reporting rules. These range from fairly broad, as in Alaska's guidance to notify affected parties "without unreasonable delay," to California's relatively specific requirements for what and when companies need to bring victims in the loop.

Id.

112. States have recently expressed this sentiment in a letter written to the House Financial Services Committee leadership by thirty-two attorneys general who assert that "it would be greatly detrimental to have federal regulations that preempt data security and state data breach laws." *See* Elizabeth Snell, *Attorneys General Stress Need for State Data Breach Laws*, HEALTHIT SEC. (Mar. 28, 2018), https://healthitsecurity.com/news/attorneys-general-stress-need-for-state-data-breach-laws [https://perma.cc/DAH7-7LT3]. The letter raises concerns about the Data Acquisition and Technology Accountability and Security Act proposed by Congress on February 16, 2018, which would "totally preempt[] all state data breach and data security laws, including laws that require notice to consumers and state attorneys general of data breaches." *See* Mike Litt, *32 State Attorneys General to Congress: Don't Replace Our Stronger Privacy Laws!*, U.S. PIRG (Mar. 27, 2018),

The Model Law is the most effective way to reach *functional* uniformity, especially because the federal government has consistently demonstrated that it cannot even protect its own cyber network.[113] Particularly, several data security experts highlight the fact that despite "years of increasing spending and information sharing among agencies, the federal government's information security incidents continue to rise every year."[114] Therefore, they advise that the federal government "should refrain from imposing sweeping, expensive, top-down solutions that could increase rigidities of existing systems."[115] Ultimately, states have shown significantly greater progress than the federal government and should be left to continue the excellent regulatory work that they have started in the cybersecurity industry.[116]

---

https://uspirg.org/blogs/blog/usp/32-state-attorneys-general-congress-dont-replace-our-stronger-privacy-laws [https://perma.cc/58R2-DL8T]. Specifically, the states highlight the usefulness of state data breach notification in increasing transparency about data breaches over the last ten years based on the states' use of "information about where organizations have failed in their security measures" in order to create stronger requirements for companies. Snell, *supra* note 112. Regarding the proposed legislation, the states believe that the bill will reduce transparency because the Act only requires notification for "large, national scale breaches affecting 5,000 or more consumers and prevent[s] attorneys general from learning of or addressing breaches that have a smaller national scale but nonetheless victimize [their] state residents." *Id.* Ultimately, the states assert that federal legislation must ensure that state data breach laws are not preempted because "they are truly essential to safeguarding consumer information." *Id.*

113. O'Sullivan, *supra* note 111 ("[T]he federal government has an abysmal track with its own cybersecurity, and is hardly the entity that should be entrusted to singlehandedly solve our nation's security problems.").

114. Durado et al., *supra* note 62 ("The government is not in a credible position to help the private sector secure itself until it improves its own network security. After years of increasing spending and information sharing among agencies, the federal government's information security incidents continue to rise every year.").

115. *Id.*

> Cybersecurity policy should refrain from imposing sweeping, expensive, top-down solutions that could increase rigidities of existing systems. The federal government can better protect American information systems by shoring up its own network vulnerabilities, supporting strong encryption techniques, and reforming laws to encourage security research and reporting, so that the entities best positioned to do so can strengthen their own cybersecurity.

Id.

116. Litt, *supra* note 112.

> If these industries want a uniform standard, which is often the selling

Finally, the five-year timetable for uniformity is unreasonable in light of the novelty of the cybersecurity industry, which is currently suffering from a talent shortage in the cybersecurity workforce. One report indicated "the global cybersecurity workforce will have more than 1.5 million unfilled positions by 2020."[117] It is clear that companies need cybersecurity experts in order to properly implement, monitor, and adjust the cybersecurity programs mandated by the Model Law, and if these individuals cannot be found, then this significantly threatens the strength of companies' cybersecurity safeguards.[118] Moreover, even when companies can secure a sizeable team, they are often "too busy to invest time in continuing education to keep up with the latest threats," which is just as serious of a problem.[119] Thus, it is unrealistic for the federal government to expect uniform cybersecurity laws to be implemented within five years when the individuals who play the most significant role in cybersecurity are exceedingly unavailable for companies to hire.[120] These considerations, among others, must be

---

> point behind this and other bad federal breach bills . . . they could take the strongest state laws and apply them to all consumers across the country—they don't need Congress for that. This is simply an attempt to set weaker federal laws as the ceiling for what states can do to protect consumers.

Id.

117. Marc van Zadelhoff, *Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It*, HARV. BUS. R. (May 4, 2017), https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it [https://perma.cc/45Q7-TDCW].

118. Carson, *supra* note 13.

119. Jon Oltsik, *Cybersecurity Skills Shortage Creating Recruitment Chaos*, CSO (Nov. 28, 2017, 7:41 AM), https://www.csoonline.com/article/3238745/security/cybersecurity-skills-shortage-creating-recruitment-chaos.html [https://perma.cc/RS84-XNJW].

120. Jeff Kauflin, *The Fast-Growing Job with a Huge Skills Gap: Cyber Security*, FORBES (Mar. 16, 2017, 6:46 PM), https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#4e88e6f5163a [https://perma.cc/QH92-VJXH].

> The ISACA, a non-profit information security advocacy group, predicts there will be a global shortage of two million cyber security professionals by 2019. Every year in the U.S., 40,000 jobs for information security analysts go unfilled, and employers are struggling to fill 200,000 other cyber-security related roles, according to cyber security data tool CyberSeek. And for every ten cyber security job ads that appear on careers site Indeed, only seven people even click on one of the ads, let alone apply.

Id.

considered by the U.S. Treasury before recommending such an impractical uniformity timetable.

CONCLUSION

Cybersecurity is an increasingly timely and complex topic, and therefore, a rigid one-size-fits-all approach cannot remedy the cyber issues that arise for individuals and companies. Each day, technological advances provide opportunities to accomplish tasks that once appeared impossible. But while these newly developed tools can be used to promote positive outcomes for society, they can also be used to inflict considerable harm. Individuals have learned the hard way that the information they share online to accomplish mundane tasks such as purchasing products, participating in social media, or even applying for jobs does not always remain secure—not without extensive cybersecurity efforts by the companies that receive the information. Therefore, for better or for worse, the arduous duty lies with businesses to employ measures to protect the information and also to inform individuals in the event that information is wrongfully transmitted.

Until recently, most businesses did not properly fulfill their duties to protect their consumers' information due to a lack of knowledge about cybersecurity and minimal regulatory pressure to do so. Fortunately, today, the above reasons are no longer considered adequate excuses for inaction. Cyber breaches have forced businesses to recognize the danger that cyber attacks pose and to become educated on the subject; some are even acquiring cybersecurity insurance. Moreover, cybersecurity laws, such as the DFS Regulation and the Model Law, have required companies to implement measures to reduce the likelihood of cyber breaches. Ultimately, these laws, developed by *state* legislators, have sent a message to businesses throughout the United States that even the federal government has consistently failed to convey: cybersecurity is not simply *encouraged*, it is *required*. And if other states wish to convey the same message in the name of protecting consumers, they have a single task: adopt the Model Law.