Ensuring Insurer Security: Where the Iowa Data Security Act Falls Short

Grace L. Vorbrich[*]

ABSTRACT: Cybercrime is on the rise, especially for the insurance industry, which collects massive amounts of sensitive data. In response, the National Association of Insurance Commissioners adopted the Model Insurance Data Security Act. This model law provides that state-licensed insurers must conduct a risk assessment as well as implement appropriate security measures, and it lays out when insurers must report data breaches to state insurance commissioners or consumers. As states have implemented their own versions of an Insurance Data Security Act, they have often modified it to make compliance easier for insurers, but in doing so have weakened its safeguards. Iowa's Insurance Data Security Act broadened exemptions for small insurers significantly, creating a gap in privacy protection that leaves many consumers vulnerable to data breaches. This Note argues that Iowa should close this gap by amending the law to narrow the exemptions back to the model law's original scope and help small insurers bear the significant costs of compliance by providing data privacy consultations, education, and/or lobbing the National Association of Insurance Commissioners to provide these necessary resources.

INTRODUCTION 1504

I. WHAT IS A DATA BREACH AND WHY SHOULD INSURERS BE WORRIED? 1505

II. U.S. DATA PRIVACY REGULATION, THE NAIC, AND THE MODEL DATA SECURITY ACT 1508
A. PRINCIPLES OF U.S. PRIVACY REGULATION 1508
B. HISTORY OF INSURANCE REGULATION AND THE NAIC 1510
C. THE NAIC MODEL DATA SECURITY ACT 1511

[*] J.D. Candidate, The University of Iowa College of Law, 2023; B.A. in Linguistics and International Studies, minor in Legal Studies, Northwestern University, 2017. My sincerest thanks to the *Iowa Law Review* writers and editors who helped make this Note possible; to my parents for supporting me in all my educational endeavors; and to my husband, Steven, for his encouragement and for answering my endless questions about coding and software.

D. STATE VARIATIONS ON THE MODEL ACT 1516

III. AN EXPANSIVE EXEMPTION 1519

IV. PROVIDING CONSUMER SECURITY AND INSURER SUPPORT 1526

CONCLUSION 1529

INTRODUCTION

In April 2021, Iowa passed the Insurance Data Security Act ("IDSA").[1] The IDSA requires state-licensed insurers to develop, implement, and maintain a comprehensive written information security program, as well as plan for, manage, and notify authorities of data breaches that compromise sensitive customer information.[2] Thus, Iowa became the nineteenth state to pass some version of the Model Insurance Data Security Act ("Model Act") promulgated by the National Association of Insurance Commissioners ("NAIC").[3]

States that have passed versions of the Model Act have each modified it somewhat, particularly in the areas of the small business exemption, required timeframe for notification of a breach, and penalties imposed.[4] The IDSA is no exception, with exemptions for employers with fewer than twenty employees, less than $5 million in gross annual revenue, or less than $10 million in year-end total assets.[5] But Iowa's expanded exemption provision is misguided given the equal vulnerability of small insurers to data breaches. It also leaves few insurers actually covered by the law and otherwise leaves insurance customers vulnerable to having their data exposed.

This Note argues that Iowa should modify the IDSA to narrow exemptions back to the standard set in the Model Act and the state insurance commissioner should provide resources and support to help smaller insurers comply. Part I describes the threat posed to insurers by data breaches. Part II provides a brief history of U.S. privacy law and insurance regulation, before describing the provisions of the Model Act and the ways various states have implemented it. Part III presents the problems with an expanded exemption that includes more small insurers when small insurers make up a substantial portion of the industry and are equally vulnerable to data breaches. Part IV argues for revising the IDSA to conform to the exception originally proposed in the Model Act

1. Jason Oliveri, *Iowa Becomes the Latest State to Adopt the NAIC Model Cybersecurity Law*, JD SUPRA (May 12, 2021), https://www.jdsupra.com/legalnews/iowa-becomes-the-latest-state-to-adopt-1325431 [https://perma.cc/6NFS-VGCB].

2. Insurance Data Security Act, IOWA CODE §§ 507F.1–507F.16 (2022).

3. *See* PRACTICAL LAW DATA PRIVACY & CYBERSECURITY, NAIC MODEL DATA SECURITY LAW AND STATE-SPECIFIC IMPLEMENTATIONS (2022), Westlaw W-020-5945.

4. *Id.*

5. § 507F.4(1)(b)(1).

and additionally providing compliance support to help ease the substantial burden on insurers to update and maintain strong privacy protections.

I. WHAT IS A DATA BREACH AND WHY SHOULD INSURERS BE WORRIED?

Before addressing the implications and requirements of the IDSA and other data privacy laws generally, it is helpful to understand why these laws are needed in the first place. Cybercrime is a growing threat with losses totaling $6.9 billion in 2021 (up approximately sixty percent from the prior year).[6] Bad actors breach targets by using various types of malware, including viruses, spyware, and ransomware.[7] Viruses—the most common form of malware—consist of code that attaches itself to the code of an otherwise innocent program and waits for a user or automated process to run that program, at which point the virus spreads and causes damage by corrupting files and locking out users.[8] Spyware is designed to hide in the background on a computer and collect sensitive information without the user's knowledge.[9] Ransomware is used to lock users out of their own information and force them to pay the hacker ransom money to regain access.[10]

Human employees are usually the weakest link when hackers deploy malware; phishing attacks are a common example of this weakness.[11] Typically, the hacker sends an email to an employee that appears to come from an innocent source.[12] When the employee clicks on the seemingly legitimate link or attachment, they may be prompted to enter their log-in information, thus giving that information to the hacker, or the malicious code may start to run immediately.[13] Thus, even sophisticated software will not necessarily prevent an attack without adequate employee training.

Insurers are a prime target for data breaches due to the large volume of sensitive data they collect.[14] Recent, high-profile examples include the breaches

---

6. DEP'T OF JUST., FED. BUREAU OF INVESTIGATION, FEDERAL BUREAU OF INVESTIGATION: INTERNET CRIME REPORT 2021, at 7 (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf [https://perma.cc/4FD5-W83U].

7. Cyber Edu, *What Is Malware?: Malware Defined, Explained, and Explored*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/malware [https://perma.cc/J3GM-UXWR].

8. *Id.*

9. *Id.*

10. *Id.*

11. ROBERT CIESLA, ENCRYPTION FOR ORGANIZATIONS AND INDIVIDUALS: BASICS OF CONTEMPORARY AND QUANTUM CRYPTOGRAPHY 94–96 (Celestin Suresh John, Rita Fernando & Divya Modi eds., 2020).

12. *Id.*; *see Strengthen Your Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity [https://perma.cc/CN2V-MQE4].

13. CIESLA, *supra* note 11, at 94–96; *see Strengthen your Cybersecurity*, *supra* note 12.

14. Tal Vegvizer, *Cybersecurity Threats in the Insurance Industry*, ALM: PROPERTYCASUALTY360 (Jan. 29, 2018), https://www.propertycasualty360.com/2018/01/29/cybersecurity-threats-in-the-insurance-industry [https://perma.cc/5RLB-XD7R]; *see Cybersecurity*, NAIC: CTR. FOR INS. POL'Y & RSCH. (July 9, 2022), https://content.naic.org/cipr_topics/topic_cybersecurity.htm [https://perma.cc/SS88-J7LE].

at Nationwide Mutual in 2012,[15] Anthem in 2015,[16] CareFirst BlueCross BlueShield in 2014 (and again in 2018),[17] and CNA Financial in 2021.[18] In the attack on CNA Financial, the hackers accessed the names and Social Security numbers of more than seventy-five thousand employees, contractors, and policyholders.[19] Information collected by insurers includes not only the kinds of traditional data, such as demographic information, medical history, behavioral data, and type and features of property, which are gathered from customers to select a policy; but it also includes big data.[20] Insurers have increasingly turned to big data to aid in underwriting, rating, marketing, and claim settlement.[21] Big data is typified by the "3Vs"—volume, variety, and velocity.[22] This means that the datasets are large (often comprised of multiple terabytes—the equivalent of over 620,000 pictures[23]), include different types of data (both structured data, or data in defined fields, and unstructured data such as social media posts, recorded interviews, pictures, or satellite images), and are generated at a high rate.[24] Insurers may collect this highly granular data from a variety of sources. One source is consumer devices, such as smart home technology or wearable devices that track physical activity.[25] Another is

15. Kevin McCoy, *Nationwide Mutual Insurance Agrees to $5.5M Settlement Over Data Breach*, USA TODAY (Aug. 9, 2017, 3:47 PM), https://www.usatoday.com/story/money/2017/08/09/nationwide-mutual-insurance-agrees-5-5-m-settlement-over-data-breach/552687001 [https://perma.cc/LQS7-UZTL].

16. Marianne Kolbasuk McGee, *A New In-Depth Analysis of Anthem Breach*, BANK INFO. SEC. (Jan. 10, 2017), https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627 [https://perma.cc/2JYR-Y7ZS].

17. Jessica Davis, *CareFirst Breached Again, Notifying 6,800 Members of Phishing Attack*, HIMSS MEDIA: HEALTHCARE IT NEWS (Apr. 2, 2018, 1:56 PM), https://www.healthcareitnews.com/news/carefirst-breached-again-notifying-6800-members-phishing-attack [https://perma.cc/5V3H-43PN].

18. Kartikay Mehrotra & William Turton, *CNA Financial Paid $40 Million in Ransom After March Cyberattack*, BLOOMBERG (May 20, 2021, 2:57 PM), https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack [https://perma.cc/X6C4-QGRZ].

19. Robert Channick, *CNA Cyberattack in March Exposed Personal Information of More than 75,000 People, Filings Reveal*, CHI. TRIB. (Nov. 2, 2021, 11:38 AM), https://www.chicagotribune.com/business/ct-biz-cna-cyberattack-exposed-personal-information-20211102-2jle5opb65hczlpz6tifik6n2a-story.html [https://perma.cc/8F6B-CFWS].

20. INT'L ASS'N OF INS. SUPERVISORS, ISSUES PAPER ON THE USE OF BIG DATA ANALYTICS IN INSURANCE 14, 40 (2020), https://www.iaisweb.org/uploads/2022/01/200319-Issues-Paper-on-Use-of-Big-Data-Analytics-in-Insurance-FINAL.pdf [https://perma.cc/LZ89-BGAP].

21. *Big Data*, NAIC: CTR. FOR INS. POL'Y & RSCH. (May 27, 2021), https://content.naic.org/cipr_topics/topic_big_data.htm [https://perma.cc/4THW-EPKL].

22. OECD, THE IMPACT OF BIG DATA AND ARTIFICIAL INTELLIGENCE (AI) IN THE INSURANCE SECTOR 10 (2020), https://www.oecd.org/finance/The-Impact-Big-Data-AI-Insurance-Sector.pdf [https://perma.cc/6FPD-8HFQ].

23. Brady Gavin, *How Big Are Gigabytes, Terabytes, and Petabytes?*, HOW-TO GEEK (May 25, 2018, 10:24 AM), https://www.howtogeek.com/353116/how-big-are-gigabytes-terabytes-and-petabytes [https://perma.cc/B2W5-5EPQ].

24. OECD, *supra* note 22, at 10; *Big Data*, *supra* note 21.

25. INT'L ASS'N OF INS. SUPERVISORS, *supra* note 20, at 25.

insurer-provided devices or apps, such as those that track driving behavior.[26] Yet another source is from third parties, such as internet providers, search engine providers, and social media platforms.[27]

In addition to being at risk of a data breach themselves, insurance companies provide insurance against cybersecurity risk for other businesses as well. However, they have struggled to craft appropriate coverage and pricing based on often-scarce actuarial data and a lack of standardization across the industry.[28] The number of cyber policies in force increased by sixty percent from 2016 to 2019, while the cost of premiums increased by seventy-four percent in 2021 alone.[29] One issue in crafting appropriate coverage is the lack of standardized terminology.[30] For example, it is difficult to predict whether coverage would apply under traditional exclusions for war and terrorism, when hackers may be affiliated or covertly sponsored by a foreign government and also motivated by personal financial gain.[31] Lawsuits over what is or is not covered are common.[32] Another issue that affects pricing is the lack of actuarial data normally used by insurers to accurately underwrite policies using predictive models.[33] Many hacks go unreported if they are not required to be disclosed by law—for example, if they are unrelated to consumer data.[34]

Such cyber insurance may also do more harm than good. Covered organizations may develop a false sense of security and fail to keep up adequate security measures and trainings, and insurers may encourage quick payouts in ransomware attacks to avoid more costly remediation efforts.[35] Hackers are aware of these factors and specifically target insured organizations, demanding even higher ransoms.[36] The average ransomware payments are

26. *Id.*

27. *Id.* at 38–39.

28. Jayleen R. Heft, *7 Challenges Insurers Face in the Cyber Insurance Market*, ALM: PROPERTYCASUALTY360 (Mar. 8, 2017), https://www.propertycasualty360.com/2017/03/08/7-challenges-insurers-face-in-the-cyber-insurance-market [https://perma.cc/5HN6-8AHS].

29. Peter Karalis, *Analysis: Not All's Fair in Cyber War (For Insurers or Insureds)*, BLOOMBERG L. (June 14, 2021, 4:00 AM), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-not-alls-fair-in-cyber-war-for-insurers-or-insureds [https://perma.cc/2MP4-J86X]; Jake Holland, *Cyber Insurance Policies Grow Pricey Amid Rising Hacks, Lawsuits*, BLOOMBERG L. (May 31, 2022, 4:31 AM), https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/X8TAoPBO000000?bna_news_filter=privacy-and-data-security#jcite [https://perma.cc/NLF7-7GVJ].

30. Heft, *supra* note 28.

31. Karalis, *supra* note 29; *see* Heft, *supra* note 28.

32. Holland, *supra* note 29.

33. Heft, *supra* note 28.

34. *Id.*

35. Rob Shavell, *Why "Ransomware Insurance" Causes Healthcare Industry to Overlook Deeper, Underlying Security Issues*, CPO MAG. (Sept. 2, 2021), https://www.cpomagazine.com/cyber-security/why-ransomware-insurance-causes-healthcare-industry-to-overlook-deeper-underlying-security-issues [https://perma.cc/27AU-9TCB].

36. *Id.*

between ten million and fifteen million dollars.[37] Insurers increasingly require companies to enact a broad array of security measures and data breach recovery plans.[38] Thus, insurance companies have an interest in keeping up with trends and best practices in cybersecurity beyond merely protecting themselves. Knowledge of these best practices is key to crafting effective and profitable cybersecurity insurance policies for purchase by others.

II. U.S. DATA PRIVACY REGULATION, THE NAIC, AND THE MODEL DATA SECURITY ACT

A. PRINCIPLES OF U.S. PRIVACY REGULATION

The United States has historically taken a minimalist approach to privacy regulation.[39] Unlike the European Union, where privacy and personal data protection are considered human rights, the United States Constitution merely creates "zone[s] of privacy" protected against government intrusion by the First, Third, Fourth, Fifth, and Ninth Amendments.[40] "[T]he protection of personal information is primarily motivated by the protection of liberty," and personal privacy interests are balanced against commerce and state security interests.[41] As a result, "[p]rivacy is protected in the US by means of a patchwork quilt made up of common law, federal legislation, the US Constitution, state law, and certain state constitutions."[42] The resulting laws are also primarily sector-specific.[43] The broadest examples of federal law that protects personal privacy are the Federal Trade Commission Act ("FTCA") and the Fair Credit Reporting Act ("FCRA").[44] Other notable sector-specific laws include the Health Insurance Portability and Accountability Act ("HIPAA"),[45] Gramm-

37. Mehrotra & Turton, *supra* note 18.

38. Holland, s*upra* note 29.

39. Emmanuel Pernot-Leplay, *EU Influence on Data Privacy Laws: Is the US Approach Converging with the EU Model?*, 18 COLO. TECH. L.J. 25, 34–36 (2020).

40. McKenzie L. Kuhn, Note, *147 Million Social Security Numbers for Sale: Developing Data Protection Legislation After Mass Cybersecurity Breaches*, 104 IOWA L. REV. 417, 423 (2018) (citing Griswold v. Connecticut, 381 U.S. 479, 484 (1965)); *see* Pernot-Leplay, *supra* note 39, at 35.

41. Pernot-Leplay, *supra* note 39, at 36.

42. Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 360 (2005).

43. Kuhn, *supra* note 40, at 421.

44. Federal Trade Commission Act § 5, 15 U.S.C. § 45 (2018) (creating a right of action against persons or entities who violate a written privacy policy); Fair Credit Reporting Act § 602, 15 U.S.C. § 1681 (requiring credit reporting agencies to maintain accurate consumer information and protecting against misuse of that information).

45. Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d (establishing standards for the use and disclosure of personal health information by certain medical care providers, insurers, and other entities, and providing civil and criminal penalties for violations).

Leach-Bliley Act ("GLBA"),[46] Family Educational Rights and Privacy Act,[47] and Children's Online Privacy Protection Act.[48] U.S. privacy regulation is therefore constructed in a piecemeal fashion, sector by sector.

In recent years, as concern over data security has grown, some attempts at comprehensive federal privacy regulation have taken shape. The Cybersecurity and Infrastructure Security Agency ("CISA") was formed in 2018 as a division of the Department of Homeland Security.[49] In March 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") into law.[50] CIRCIA requires covered entities to report certain cyber incidents to CISA within seventy-two hours and report ransomware payments within twenty-four hours.[51] CIRCIA itself does not specify precisely what types of entities and cyber incidents are covered, but instead leaves these determinations up to CISA rulemaking authority.[52] Prior executive directives have deemed the financial services sector, including insurance, to fall under the umbrella of critical infrastructure, so it is likely that insurers would be covered entities under CIRCIA.[53] The legislature is currently considering another data privacy bill, the American Data Privacy and Protection Act, which would provide a comprehensive framework for data collection and retention and empower the Federal Trade Commission ("FTC") to issue regulations regarding data security requirements.[54] The bill would preempt most state law, but it is applicable to

46. Gramm-Leach-Bliley Act, 15 U.S.C. § 6801(a)–(b) (requiring financial institutions to explain their information-sharing practices to customers and protect customers' sensitive data).

47. Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (protecting the privacy of student education records and giving parents of children under eighteen the right to inspect and request corrects to those records).

48. Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501–6505 (regulating the collection of personal information by website operators whose services are directed at children under thirteen or who have actual knowledge that they are collecting personal information from children under thirteen).

49. Bastien Inzaurralde, *The Cybersecurity 202: Trump Set to Make a New DHS Agency the Top Federal Cyber Cop*, WASH. POST (Nov. 16, 2018, 7:34 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/11/16/the-cybersecurity-202-trump-set-to-make-a-new-dhs-agency-the-top-federal-cyber-cop/5bedb9a71b326b39290548 67 [https://perma.cc/H5XF-64PY].

50. *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/circia [https://perma.cc/6U2P-Q9SR].

51. Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, § 103, 136 Stat. 49, 1038.

52. *Id.*

53. Press Release, The White House: Off. of the Press Sec'y, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/PH29-9DVL]; *see Financial Services Sector*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/financial-services-sector [https://perma.cc/F3FG-ZUWB].

54. *See generally* American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) (proposing a comprehensive data collection and retention framework).

only large data collectors and exempts small and mid-size businesses and those that comply with other federal privacy laws.[55] For the moment, the vast majority of business—including most insurers—must primarily look to state rather than federal law.

B. HISTORY OF INSURANCE REGULATION AND THE NAIC

Insurance regulation in the United States is primarily enacted by the states.[56] In the 1868 U.S. Supreme Court case *Paul v. Virginia*, the insurance industry had sought to federalize regulation in order to create uniformity in its regulatory obligations, but the legal challenge failed and the Court affirmed the power of the states to continue regulating the industry.[57] State insurance "regulation was fairly comprehensive" by 1944 when "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."[58] Despite this, insurance regulation has remained with the states due to the passage of the McCarran-Ferguson Act in 1945, which "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."[59] Today, state governments each include an insurance regulatory department within their executive branch.[60] These departments are headed by a commissioner or director of insurance and have broad powers delegated by the legislature.[61] The commissioners are typically appointed by the governor, but are elected by the people in a minority of states.[62]

The National Association of Insurance Commissioners was founded shortly after the decision in *Paul*, with nineteen of the thirty-six state insurance regulators meeting to discuss the need for uniformity in insurance regulation.[63] It was the NAIC that proposed what would become the McCarran–Ferguson Act and, following its passage, ensured that no federal intervention would occur by drafting model laws for passage by the states.[64] Fundamental tensions exist in the NAIC's very existence—its "goal of uniform, nationalized regulation

55. *See id.* §§ 2(17), 209.

56. M. Bob Kao, *Regulating the Cybersecurity of Insurance Companies in the United States*, 21 TRANSACTIONS: TENN. J. BUS. L. 11, 18 (2019).

57. *Id.* at 17; Susan Randall, *Insurance Regulation in the United States: Regulatory Federalism and the National Association of Insurance Commissioners*, 26 FLA. ST. U. L. REV. 625, 630–31 (1999).

58. Kao, *supra* note 56, at 17 (quoting Randall, *supra* note 57, at 632); *see* McCarran-Ferguson Act, 15 U.S.C. § 1011 (1945).

59. Kao, *supra* note 56, at 18.

60. *Id.*

61. *Id.*

62. *Id.*

63. Randall, *supra* note 57, at 629–32.

64. *Id.* at 633–34.

is facially inconsistent with the preservation of autonomous regulation by the states," which it also seeks to promote.[65] It has classified itself as both "a group of public officials imbued with the public trust" and "an instrumentality of the states."[66] But "it is clear that the NAIC is a private . . . entity," as it has no binding power on the legislature or industry and is entirely self-governing.[67] Furthermore, though the NAIC plays a central role in insurance regulation, it is considered by many to be part of and act at the behest of the insurance industry.[68] Both states and insurers pay fees to the NAIC for providing training programs, distributing industry publications, and maintaining a centralized filing database, among other services.[69] While fees paid by the states compose less than two percent of the NAIC 2021 budget, fees from insurers compose 27.7 percent, making them the largest single category of revenue.[70]

C. THE NAIC MODEL DATA SECURITY ACT

In December 2016, New York became the first state to enact cybersecurity regulations for insurers.[71] These regulations would go on to heavily influence the Model Data Security Act.[72] The New York Department of Financial Services ("NYDFS") released new regulations ("NYDFS Regulation") requiring covered entities to conduct risk assessments and implement cybersecurity programs "to protect the confidentiality, integrity and availability of" their information systems.[73] Covered entities include insurers, but also banks and other financial institutions.[74] Entities with fewer than ten employees (including contractors), "less than $5,000,000 in gross annual revenue in each of the last 3 fiscal years from New York business operations," or "less than $10,000,000 in year-end total assets" are exempt.[75]

The NYDFS Regulation requires covered entities to appoint a Chief Information Security Officer to "oversee[] and implement[] the covered entity's cybersecurity program and enforc[e] its cybersecurity policy," as well as "report in writing at least annually to the covered entity's board of directors or equivalent governing body."[76] When a Cybersecurity Event occurs, the Covered Entity must notify the Superintendent of Financial Services within

65. *Id.* at 635.

66. *Id.* at 638 (footnote omitted).

67. *Id.* at 638–39.

68. *Id.* at 639–40.

69. *See* NAT'L ASS'N OF INS. COMM'RS, 2021 NAIC BUDGET 1–2 (2020), https://content.naic.org/sites/default/files/inline-files/Approved_NAIC_2021_Budget_1.pdf [https://perma.cc/VG72-Q7V3].

70. *Id.* at 15, 25, 28.

71. Kao, *supra* note 56, at 19–20.

72. *Id.* at 20.

73. N.Y. COMP. CODES R. & REGS. Tit. 23, § 500.2(a)–(b) (2021).

74. *Id.* § 500.1(c).

75. *Id.* § 500.19(a).

76. *Id.* § 500.4(a)–(b).

seventy-two hours after determining that such an event has occurred.[77] The NYDFS Regulation defines a Cybersecurity Event 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."[78] The Covered Entity must also submit annual reports to the superintendent certifying its compliance with the provisions of the regulation.[79] Other provisions of the NYDFS Regulation include maintaining audit trails to reconstruct financial transactions after a loss of access,[80] requiring Third Party Service Providers to adhere to minimum cybersecurity practices,[81] implementing a data retention policy,[82] and requiring encryption of Nonpublic Information to the extent feasible.[83] Though the regulations were initially criticized as inflexible and overly broad, they were significantly less stringent than what was initially proposed.[84] Nevertheless, the NAIC borrowed heavily from the NYDFS Regulation in crafting the Model Act.[85]

In October 2017, the NAIC adopted the Model Act, which serves as a guideline for states in adopting their own legislation.[86] The Model Act deviates from the NYDFS Regulation in certain notification requirements and in that its definition of Cybersecurity Event only applies to insurers.[87] The Model Act defines Cybersecurity Event as "an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System."[88] However, it exempts "unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization" or where "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."[89] This exemption effectively excludes ransomware attacks from the scope of Cybersecurity Events, since attackers need not unencrypt, use, or release information in order to hold it hostage for payment. And while information may be "returned" in that it is rendered accessible to the insurer again, it would be nearly impossible to determine whether the hacker had kept a copy. These exemptions narrow the scope of both who the law applies

77. *Id.* § 500.17(a).
78. *Id.* § 500.1(d) (emphasis added).
79. *Id.* § 500.17(b).
80. *Id.* § 500.6(a)(2).
81. *Id.* § 500.11(a)(2).
82. *Id.* § 500.13.
83. *Id.* § 500.15.
84. Kao, *supra* note 56, at 20, 22–28.
85. *Id.* at 20.
86. *Id.* at 28.
87. *Id.* at 28–32.
88. INS. DATA SEC. MODEL L. § 3(D) (NAT'L ASS'N OF INS. COMM'RS 2017).
89. *Id.*

to and under what circumstances they must take action, making it considerably less stringent as compared to the NYDFS Regulation.

While encryption, or the process of using an algorithm to transform plaintext into an unintelligible string of characters, is thought of as "the bedrock of cyber security," it is not foolproof.[90] Several methods exist to decrypt encrypted data without needing the key.[91] These may be harder or easier depending on the password strength requirements or the chosen hashing algorithm.[92] A hashing algorithm is the one-way function used to encrypt data.[93] Not all hashing algorithms are equally resistant to decryption, and all may be accompanied by additional methods of randomization to make the dataset's security more robust.[94] As written, the definition of Cybersecurity Event with the exemption for situations where Encrypted Nonpublic Information is acquired without the key fails to account for a situation in which an initial attack captures encrypted data alone but a subsequent attack accesses the key.[95] Most concerningly, the additional exemption for a situation where the information is returned and not released appears to exclude ransomware attacks altogether. In a ransomware attack, hackers need not decrypt or release the data; they merely encrypt it themselves such that the victim loses access and must pay to have it decrypted so they can resume normal business operations.[96] And once they pay and the data is "returned," it may be impossible to tell whether the hackers kept a copy until some later harm results.[97]

Aside from these crucial differences, the rest of the NAIC Model Act is substantially similar to the NYDFS Regulation. It defines Nonpublic Information as any information fitting under one of three categories. The first category is "[b]usiness related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to . . . the Licensee."[98] The second is the combination of information that can be used to identify a Consumer along with "(a) Social Security number, (b) Driver's license number or non-driver identification card number, (c) Account number, credit or debit card number, (d) Any security code, access code or password that would permit access to a Consumer's

90. Kao, *supra* note 56, at 29; CHRIS JAIKARAN, CONG. RSCH. SERV., R44642, ENCRYPTION: FREQUENTLY ASKED QUESTIONS 2, 7–8 (2016).

91. *See* JAIKARAN, *supra* note 90, at 8; CIESLA, *supra* note 11, at 76–91.

92. CIESLA, *supra* note 11, at 76–91 (describing various forms of cyberattacks and their drawbacks and advantages).

93. *Id.* at 41–42.

94. *Id.* at 43–47.

95. Kao, *supra* note 56, at 30–31.

96. CIESLA, *supra* note 11, at 100–01.

97. Kao, *supra* note 56, at 31.

98. INS. DATA SEC. MODEL L. § 3(K)(1) (NAT'L ASS'N OF INS. COMM'RS 2017).

financial account, or (e) Biometric records."[99] The last category is "information . . . except age or gender . . . created by or derived from a health care provider or a Consumer and that relates to [health conditions or health care of the Consumer]."[100] This definition mirrors that of the NYDFS Regulation except for the substitution of "Consumer" for "individual."[101] This change limits the scope of the Model Act to only those people who do business with the insurer, rather than keeping the broad range of the NYDFS regulation which would protect others who do not own a policy, but whose information has been packaged and sold as part of a big data dataset to be used for marketing or underwriting purposes.

The Model Act is also similar to the NYDS Regulation in its provisions for the implementation of an information security program and risk assessment. The information security program under the Model Act is to be "[c]ommensurate with the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used."[102] In completing their risk assessment, the Licensee must designate someone to be responsible for the information security program, identify internal and external security threats and assess their potential for damage, and assess current safeguards and implement new ones as necessary.[103] This provision is important because it requires insurers to be proactive about their security and implement preventative measures, rather than merely focusing on the required response once a breach has occurred. The provision's requirements also scale with the size and complexity of the insurer's business. This allows, by default, a great deal of flexibility and discretion for those governed by the law.

The investigation and notification requirements following a Cybersecurity Event provide more specific guidance than those of the NYDFS Regulation.[104] It sets out minimum determinations to be made during the investigation into an incident, including "whether a Cybersecurity Event has occurred," "the nature and scope of the Cybersecurity Event," and "any Nonpublic Information that may have been involved."[105] The Licensee must undertake "reasonable measures to restore the security of the Information Systems compromised."[106] The Licensee must also take the same steps to investigate any potential data breach in systems maintained by a Third Party Service Provider.[107] Notification must occur within the same seventy-two hour

99. *Id.* § 3(K)(2).
100. *Id.* § 3(K)(3).
101. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.1(g).
102. INS. DATA SEC. MODEL L. § 4(A) (NAT'L ASS'N OF INS. COMM'RS 2017).
103. *Id.* § 4(C).
104. Kao, *supra* note 56, at 32.
105. INS. DATA SEC. MODEL L. § 5(B)(1)–(3) (NAT'L ASS'N OF INS. COMM'RS 2017).
106. *Id.* § 5(B)(4).
107. *Id.* § 5(C).

window.[108] However, under the Model Act, notification need only occur if the Licensee falls under one of two categories.[109] First, the Licensee must notify the relevant state insurance regulator if it is domiciled in the state.[110] Second, the Licensee must notify the state regulator if it reasonably believes the Nonpublic Information of 250 or more state residents has been affected and (1) notice of the breach is otherwise required by law or (2) there is a reasonable likelihood that a state consumer or a material part of the Licensee's normal operations will be materially harmed.[111] The information provided in the notification includes information about the breach, such as how it occurred and was discovered, the specific types of information acquired, how long the system was compromised, and the number of consumers affected.[112] It also includes a description of any remediation efforts and whether the breach has been reported to law enforcement or any information recovered.[113]

Like the NYDFS Regulation, the NAIC Model Act provides exemptions for "Licensee[s] with fewer than ten employees."[114] Unlike the NYDFS Regulation however, the Model Act does not include an exemption for Licensees with less than $5 million in gross annual revenue or less than $10 million in year-end total assets.[115] This difference in exemptions likely stems from the fact that the NYDFS Regulation applied to a variety of financial institutions, while the Model Act only covers insurers. Additionally, in tabletop exercises conducted by the NAIC to assess insurer's cyberattack response protocols, the NAIC found that while large insurers had some response systems in place, small, regional insurers were totally unprepared. This likely led to the Model Act's more comprehensive coverage.[116]

The Model Act also provides an exemption from section 4 of the Act—including the information security program, risk assessment, incident response plan, and annual certification requirements—for Licensees who are covered by and comply with HIPAA.[117] Lastly, there is an exemption from section 4 if they are already covered by the Information Security Program of another Licensee.[118] The Model Act provides for penalties in accordance with a general

108. *Id.* § 6(A).
109. *Id.*
110. *Id.* § 6(A)(1).
111. *Id.* § 6(A)(2).
112. *Id.* § 6(B).
113. *Id.*
114. *Id.* § 9(A)(1).
115. *Compare id.* § 9, *with* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19(a).
116. The Regulators, *Cybersecurity's Impact on the Insurance Industry. A Conversation with South Carolina Insurance Director Ray Farmer* (Sept. 2021) (accessed on Spotify).
117. INS. DATA SEC. MODEL L. § 9(A)(2) (NAT'L ASS'N OF INS. COMM'RS 2017).
118. *Id.* § 9(A)(3).

penalty statute of the relevant state, but it expressly does not create a private cause of action for violation or curtail any existing right of action.[119]

D. STATE VARIATIONS ON THE MODEL ACT

Since its adoption by the NAIC in late 2017, twenty-one states have enacted a version of the Insurance Data Security Act.[120] South Carolina was the first to do so in May 2018, with the law becoming effective January 1, 2019.[121] South Carolina's Insurance Data Security Act tracks closely with the Model Act.[122] Following South Carolina's lead in 2018 were Michigan and Ohio.[123] In 2019, Alabama, Connecticut, Delaware, Mississippi, and New Hampshire all passed their own Insurance Data Security Acts.[124] Indiana, Louisiana, and Virginia followed suit in 2020;[125] and Hawaii, Maine, Minnesota, North Dakota, Tennessee, Wisconsin, and Iowa did the same in 2021.[126] Since Iowa's adoption of the Act, Kentucky, Maryland, and Vermont

---

119. *Id.* §§ 2(B), 10.

120. PRACTICAL LAW DATA PRIVACY & CYBERSECURITY, *supra* note 3.

121. S.C. CODE ANN. §§ 38–99–10 to 38–99–100 (2019); *see* PRACTICAL LAW DATA PRIVACY & CYBERSECURITY, *supra* note 3.

122. *Compare* S.C. CODE ANN. §§ 38–99–10 to 38–99–100, *with* INS. DATA SEC. MODEL L. (NAT'L ASS'N OF INS. COMM'RS 2017).

123. Katherine Doty Hanniford, *Michigan Enacts Insurance Data Security Model Law*, JD SUPRA (Jan. 8, 2019), https://www.jdsupra.com/legalnews/michigan-enacts-insurance-data-security-83105 [https://perma.cc/U9YZ-4ZHV]; Robert J. Hanna & Daniel L. Schiau II, *Client Alerts: Ohio Joins Growing Trend Requiring Cybersecurity Standards and Reporting Obligations for Insurance Industry*, TUCKER ELLIS LLP (Feb. 2019), https://www.tuckerellis.com/alerts/ohio-joins-growing-trend-requiring-cybersecurity-standards-and-reporting-obligations-for-insurance-industry [https://perma.cc/LA5L-ZY8E].

124. J. Paul Zimmerman, *Alabama Passes Insurance Data Security Law*, CHRISTIAN SMALL (June 7, 2019), https://csattorneys.com/2019/06/07/alabama-passes-insurance-data-security-law [https://perma.cc/6KSE-RN9P]; Theodore P. Augustinos & Ben FrazziniKendrick, *Connecticut Adopts Insurance Data Security Law*, LOCKE LORD (Aug. 5, 2019), https://www.lockelord.com/newsandevents/publications/2019/08/connecticut-adopts-insurance-data-security-law [https://perma.cc/7SWW-WB4M]; *Insurance Data Security Act Signed into Law*, DELAWARE.GOV (Aug. 1, 2019), https://news.delaware.gov/2019/08/01/insurance-data-security-act-signed-into-law [https://perma.cc/KMG8-SN96]; PRAC. L. DATA PRIV. ADVISOR, MISSISSIPPI PASSES INSURANCE DATA SECURITY LAW (2019), Westlaw W-019-8862; *New Hampshire Governor Signs Insurance Data Security Law*, HUNTON ANDREWS KURTH (Aug. 6, 2019), https://www.huntonprivacyblog.com/2019/08/06/new-hampshire-governor-signs-insurance-data-security-law [https://perma.cc/TUD8-YBSS].

125. PRAC. L. DATA PRIV. ADVISOR, INDIANA ENACTS INSURANCE DATA SECURITY LAW (2020), Westlaw W-024-6269; PRAC. L. DATA PRIV. ADVISOR, LOUISIANA ENACTS INSURANCE DATA SECURITY LAW (2020), Westlaw W-026-1112; *The Virginia Insurance Data Security Act – What You Need to Know*, MCGUIREWOODS (May 22, 2020), https://www.passwordprotectedlaw.com/2020/05/virginia-insurance [https://perma.cc/3HMM-Y97F].

126. PRAC. L. DATA PRIV. ADVISOR, HAWAII AND MINNESOTA ENACT INSURANCE DATA SECURITY LAWS (2021), Westlaw W-031-7166; Deborah George, *Maine and North Dakota Are Latest States to Adopt the NAIC Data Security Model Law*, NAT'L L. REV. (Apr. 15, 2021), https://www.natlawreview.com/article/maine-and-north-dakota-are-latest-states-to-adopt-naic-data-security-model-law [https://perma.cc/DP6B-XNKW]; PRAC. L. DATA PRIV. ADVISOR, TENNESSEE ENACTS INSURANCE DATA SECURITY LAW (2021), Westlaw W-030-9810; Sadia Mirza & Ronald Raether, *Wisconsin*

have adopted versions as well.[127] The fast pace of adoption is due to a U.S. Treasury report which "urged prompt action by states to adopt the model law within five years. If the model was not adopted and implemented, the Treasury recommended that Congress act by passing legislation setting forth uniform requirements for insurer data security."[128]

Most states have varied the model law somehow, several in significant ways, in response to local industry lobbying.[129] The most common deviations from the Model Act involve definitions, notification requirements, and exemptions. One common deviation is defining Nonpublic Information to include only consumer information and not business-related information.[130] Big data collections purchased by insurers would fall into a gray area under these laws, since the individuals whose information the datasets are comprised of are not direct consumers of the insurer, but had their data collected by a third party. Other deviations also deal with notification requirements. Some states' laws provide that licensees domiciled in the state need only notify the commissioner when the breach will cause material harm or when it involves 250 state residents and notification to another authority is required.[131] Some provide that licensees that insure consumers accessing their services from an independent insurance producer must notify applicable producers by the time they notify affected consumers.[132] Several states extend the notification timeline (most commonly to three business days, but in some jurisdictions up

Enacts Insurance Data Security Law Requiring Notification of Cybersecurity Incidents to Insurance Commissioner Within Three Business Days, JD SUPRA (Nov. 30, 2021), https://www.jdsupra.com/legalnews/wisconsin-enacts-insurance-data-4570843 [https://perma.cc/B8QD-TQAQ]; Oliveri, *supra* note 1.

127. *Two States Enact Insurance Data Security Laws*, HUNTON ANDREWS KURTH (May 4, 2022), https://www.huntonprivacyblog.com/2022/05/04/two-states-enact-insurance-data-security-laws [https://perma.cc/2FK7-YQU7]; *Vermont Enacts Insurance Data Security Law*, HUNTON ANDREWS KURTH (June 9, 2022), https://www.huntonprivacyblog.com/2022/06/09/vermont-enacts-insurance-data-security-law [https://perma.cc/5FX9-38FF].

128. *Privacy Regulatory Trends: Your Guide to the NAIC Insurance Data Security Model Law*, RADARFIRST (2022), https://www.radarfirst.com/blog/privacy-regulatory-trends-guide-to-naic-insurance-data-security-model-law [https://perma.cc/7QPM-XU7D].

129. *See* Kuhn, *supra* note 40, at 419; Kao, *supra* note 56, at 35–36.

130. ALA. CODE § 27-62-3 (2019); DEL. CODE ANN. tit. 18, § 8603 (West 2019); MISS. CODE ANN. § 83-5-805 (West 2019); N.H. REV. STAT. ANN. § 420-P:3 (2020); IND. CODE ANN. § 27-2-27-12 (West 2020); LA. STAT. ANN. § 22:2503 (2020); HAW. REV. STAT. ANN. § 431:3B-101 (West 2021); MINN. STAT. ANN. § 60A.985 (West 2022); N.D. CENT. CODE ANN. § 26.1-02.2-01 (West 2021); WIS. STAT. ANN. § 601.95 (West 2021).

131. MICH. COMP. LAWS ANN. § 500.559 (West 2021); OHIO REV. CODE ANN. § 3965.04 (West 2019); ALA. CODE § 27-62-6; DEL. CODE ANN. tit. 18, § 8606 (West); MISS. CODE ANN. § 83-5-811 (West); N.H. REV. STAT. ANN. § 420-P:6; IND. CODE ANN. § 27-2-27-21 (West); N.D. CENT. CODE ANN. § 26.1-02.2-05 (West); TENN. CODE ANN. § 56-2-1006 (West 2021); WIS. STAT. ANN. § 601.954(1) (West).

132. MICH. COMP. LAWS ANN. § 500.559; OHIO REV. CODE ANN. § 3965.04; ALA. CODE § 27-62-6; CONN. GEN. STAT. ANN. § 38a-38 (West 2021); DEL. CODE ANN. tit. 18, § 8606; MISS. CODE ANN. § 83-5-811; N.D. CENT. CODE ANN. § 26.1-02.2-05; TENN. CODE ANN. § 56-2-1006; WIS. STAT. ANN. § 601.954(1).

to ten business days).[133] Common exemptions not present in the Model Act that states have incorporated include an exemption for licensees that comply with the GLBA,[134] an exemption for licensees with less than $5 million in gross annual revenue or less than $10 million in year-end total assets,[135] and increasing the number of employees and contractors that qualify a licensee for the small business exemption (most commonly to twenty-five, but in some jurisdictions up to fifty).[136]

These variations predominantly serve to ease the compliance burden on insurers. This is achieved by decreasing the amount of information that needs to be protected, decreasing the circumstances in which notification is necessary, and removing some insurers from needing to comply with the law at all. However, in doing so, they leave more information and consumers vulnerable and give the insurance commissioner less information about the state of data security in the industry. Other notable variations exist in many states' versions of the Model Act, which similarly serve to make the law less onerous for insurers.[137] Although these alterations make things easier for insurers, they also lower the bar of heightened security the law is meant to impose. These

133. MICH. COMP. LAWS ANN. § 500.559; MINN. STAT. ANN. § 60A.9853; OHIO REV. CODE ANN. § 3965.04; ALA. CODE § 27-62-6; CONN. GEN. STAT. ANN. § 38a-38; DEL. CODE ANN. tit. 18, § 8606; MISS. CODE ANN. § 83-5-811; N.H. REV. STAT. ANN. § 420-P:6; IND. CODE ANN. § 27-2-27-21; LA. STAT. ANN. § 22:2506; VA. CODE ANN. § 38.2-625 (West 2020); HAW. REV. STAT. § 431:3B-302; ME. REV. STAT. ANN. tit. 24-A, § 2266 (2021); N.D. CENT. CODE ANN. § 26.1-02.2-05; TENN. CODE ANN. § 56-2-1006; WIS. STAT. § 601.954.

134. ALA. CODE § 27-62-9; MISS. CODE ANN. § 83-5-817; N.H. REV. STAT. ANN. § 420-P:9; IND. CODE ANN. § 27-2-27-26; LA. STAT. ANN. § 22:2509; VA. CODE ANN. § 38.2-629; ME. REV. STAT. ANN. tit. 24-A, § 2269; MINN. STAT. ANN. § 60A.9856; WIS. STAT. § 601.951.

135. OHIO REV. CODE ANN. § 3965.07; ALA. CODE § 27-62-9; MISS. CODE ANN. § 83-5-817; IND. CODE ANN. § 27-2-27-26; LA. STAT. ANN. § 22:2509; N.D. CENT. CODE ANN. § 26.1-02.2-08; TENN. CODE ANN. § 56-2-1009; WIS. STAT. § 601.952.

136. DEL. CODE ANN. tit. 18, § 8609 (fifteen employees); OHIO REV. CODE ANN. § 3965.07 (twenty employees); N.H. REV. STAT. ANN. § 420-P:9 (twenty employees); MICH. COMP. LAWS ANN. § 500.565 (twenty-five employees); ALA. CODE § 27-62-9 (twenty-five employees); LA. STAT. ANN. § 22:2509 (twenty-five employees); MINN. STAT. ANN. § 60A.9856 (twenty-five employees); N.D. CENT. CODE ANN. § 26.1-02.2-08 (twenty-five employees); TENN. CODE ANN § 56-2-1009 (twenty-five employees); MISS. CODE ANN. § 83-5-817 (fifty employees); IND. CODE ANN. § 27-2-27-26 (fifty employees); WIS. STAT. § 601.952 (fifty employees).

137. One variation implemented by some states is excluding the Model Act's provision regarding due diligence and security testing procedures for externally developed applications. *See* ALA. CODE § 27-62-4(d)(2)(e); MISS. CODE ANN. § 83-5-807; N.H. REV. STAT. ANN. § 420-P:4; MINN. STAT. ANN. § 60A.9851; N.D. CENT. CODE ANN. § 26.1-02.2-03; WIS. STAT. § 601.952. Some states also create a broader standard for what constitutes an authorized individual. *See* OHIO REV. CODE ANN. § 3965.01; DEL. CODE ANN. tit. 18, § 8603; IND. CODE ANN. § 27-2-27-2; VA. CODE ANN. § 38.2-621; ME. REV. STAT. ANN. tit. 24-A, § 2263. And some states have enacted a specific consumer data breach notification regime for licensees rather than referencing the state's existing data breach notification laws. *See* MICH. COMP. LAWS ANN. § 500.561; DEL. CODE ANN. tit. 18, § 8606; MINN. STAT. ANN. § 60A.9853; TENN. CODE. ANN. § 56-2-1006.

variations have also added complexity for multi-state insurers and hindered the Model Act's stated goals of providing uniform standards for all insurers.[138]

III. AN EXPANSIVE EXEMPTION

Iowa Governor Kim Reynolds signed the IDSA into law on April 30, 2021.[139] The Act became effective January 1, 2022.[140] Like other states, Iowa's law is largely consistent with the Model Act but carves out significant differences. The ostensible purpose of these deviations is to ease the burden on insurance providers—primarily small providers. However, they come at the cost of less data security.

Before analyzing Iowa's IDSA, it is helpful to survey the preexisting privacy laws in Iowa. Title 16, chapter 715C of the Iowa Code sets forth requirements for notification of affected individuals after a data breach.[141] All fifty states and the District of Columbia have enacted some form of data breach notification law.[142] Iowa's law provides that a person who owns or licenses computerized data must give notice to a consumer "in the most expeditious manner possible and without unreasonable delay" following a breach of "computerized data that includes a consumer's personal information that is used in the course of the person's business."[143] A breach of security has occurred if there has been an "unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information."[144] The person is excused from giving notice if they determine there is "no reasonable likelihood of financial harm to the consumers" as a result of the breach.[145] They may also be excused if they comply with other, stricter notification requirements including the GLBA and HIPAA.[146]

Iowa's data breach law is broadly applicable to all those who collect computerized data but concerns only the necessary response following a breach of information.[147] Iowa's student online privacy law, on the other hand, is tailored to a specific sector but concerns the means of safeguarding information in the first place.[148] Title 7, section 279.71 of the Iowa Code

138. *See generally* Trevor Meers, *The Wild West of Data Breach Notifications*, IOWA LAW., Mar. 2021, at 13 (discussing the complexities of complying with notification requirements after a data breach).

139. Oliveri, *supra* note 1.

140. *Id.*

141. IOWA CODE §§ 715C.1–715C.2.

142. Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 816.

143. §§ 715C.2(1), 715C.2(8).

144. *Id.* § 715C.1(1).

145. *Id.* § 715C.2(6).

146. *Id.* § 715C.2(7)(c)–(d).

147. *Id.* § 715C.2.

148. *Id.* § 279.71.

specifically protects student online personal information.[149] It prohibits online service providers who know their services are used in kindergarten through twelfth grade education from engaging in targeted advertising, amassing a unique, identifiable profile on a student, selling or renting a student's information, or disclosing covered information except in some narrow, specified circumstances.[150] Iowa is one of many states that passed legislation modelled on California's Student Online Personal Information Protection Act ("SOPIPA").[151] When passed, these laws were a significant step forward from the total lack of prior regulation.[152] However, in 2019, the Parent Coalition for Student Privacy gave Iowa a D+ in protecting student privacy, primarily due to section 279.71's failure to require transparency about the uses of data collected or provide a clear enforcement mechanism.[153]

The IDSA was thus not the first foray into privacy regulation for the Iowa Legislature. But its prior attempts with sections 715C and 279.71 were by no means rigorous, comprehensive, or innovative. Since the passage of the IDSA, the Iowa House passed H.F. 2506, which would have given Iowa consumers the right to know what information was being collected about them and request that it be deleted.[154] But that bill died in committee and was opposed by consumer groups, who argued that the bill's industry-friendly provisions and exemptions fell short of true reform.[155] With only two regulations on the books—a post hoc breach notification law and a narrowly tailored protection for schoolchildren—Iowa is solidly middle-of-the-pack when it comes to data security.[156] The current regulatory landscape does not indicate that the legislature is either familiar with the intricacies of data privacy nor eager to be on the forefront of such regulation. This is similarly illustrated by the ways in

149. *Id.*

150. *Id.*

151. PARENT COAL. FOR STUDENT PRIV. & THE NETWORK FOR PUB. EDUC., THE STATE STUDENT PRIVACY REPORT CARD: GRADING THE STATES ON PROTECTING STUDENT DATA PRIVACY 8 (2019), https://www.studentprivacymatters.org/wp-content/uploads/2019/01/The-2019-State-Student-Privacy-Report-Card.pdf [https://perma.cc/WU58-VSMD].

152. *Id.*

153. *Id.* at 4, 11, 21.

154. H.F. 2506, 89th Gen. Assemb. § 3 (Iowa 2022); *see* Jake Holland, *Iowa House OK's Consumer Privacy Bill with Month Left in Session*, BLOOMBERG L. (Mar. 15, 2022, 10:07 AM), https://news.bloomberglaw.com/tech-and-telecom-law/iowa-house-oks-consumer-privacy-bill-with-month-left-in-session [https://perma.cc/FNT8-GHNJ].

155. *Iowa House Bill 2506*, LEGISCAN, https://legiscan.com/IA/bill/HF2506/2021 [https://perma.cc/FNJ2-4WJK] (providing that the bill "died in committee"); Letter from Consumer Reports et al. to Pat Grassley, Speaker, Iowa H.R. & Jennifer Konfrst, Minority Leader, Iowa H.R. (Mar. 8, 2022), https://advocacy.consumerreports.org/wp-content/uploads/2022/03/Group-Letter-HF-2506-oppose.pdf [https://perma.cc/X4UQ-EZMX].

156. *Compare* IOWA CODE §§ 715C.1–715C.2, *and id.* § 279.71, *with* 815 ILL. COMP. STAT. ANN. 530/1–530/50 (West 2020), *and* 105 ILL. COMP. STAT. ANN. 85/1–85/99 (West 2021), *and* 820 ILL. COMP. STAT. ANN. 55/1–55/20 (West 2019), *and* 740 ILL. COMP. STAT. ANN. 14/1–14/99 (West 2008).

which the legislature slackened the already reasonably permissive requirements of the Model Act in crafting the IDSA.[157]

First, the IDSA pushes back deadlines for licensees.[158] The timeline for sending notification to the insurance commissioner is extended to three business days, rather than seventy-two hours.[159] Every hour counts in an area as fast-paced as cybersecurity, where those carrying out attacks act without any constraints. Earlier notification of the commissioner means an earlier ability to notify other insurers in the event of a coordinated attack on multiple institutions. It also means the insurance commissioner and the state can step in earlier to enforce a uniform approach to (non)payment in ransomware attacks or to furnish resources to stop the hacker who may have ongoing access and continue to wreak havoc within the system.

Bills considered at the federal level regarding notification of cybersecurity attacks on key infrastructure institutions—including insurers[160]—have seventy-two hours as the maximum timeline considered.[161] The seventy-two hour timeframe has even been endorsed by some in the financial sector as striking the right balance between the interests of financial institutions and the government.[162] Three business days, on the other hand, does not require a sufficient level of urgency in responding to a serious data breach. The IDSA also pushes back the deadline by which licensees must send a certificate of compliance with the law to the insurance commissioner, giving them until April 15, rather than February 15, of each year.[163] But with the ever-increasing number of data security incidents per year, insurers should be pressured to update their systems and complete their risk assessments in as timely a manner as possible. The inherent tradeoff of giving insurers more time in both of these circumstances is the heightened risk of harm and extent of potential fallout.

Secondly, the IDSA expands the small business exception. Thus, rather than excluding only licensees with fewer than ten employees or those that comply with the provisions of HIPAA, the IDSA exempts licensees with fewer than twenty employees, less than $5 million in gross annual revenue, or less

157. *See supra* Section II.C.

158. *Compare* IOWA CODE § 507F.7, *with* INS. DATA SEC. MODEL L. § 6(A) (NAT'L ASS'N OF INS. COMM'RS COMM'RS 2017).

159. *Compare* IOWA CODE § 507F.7, *with* INS. DATA SEC. MODEL L. § 6(A) (NAT'L ASS'N OF INS. COMM'RS 2017).

160. *Financial Services Sector*, *supra* note 53.

161. Michael Kans, *Congress Debates Cyber Incident Reporting Deadlines in the NDAA*, JUST SEC. (Oct. 26, 2021), https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa [https://perma.cc/UF6X-GM6Y].

162. *Id.*

163. *Compare* IOWA CODE § 507F.4(8), *with* INS. DATA SEC. MODEL L. § 4(I) (NAT'L ASS'N OF INS. COMM'RS 2017).

than $10 million in year-end total assets.[164] Like other states then,[165] Iowa has imported additional exemption provisions from the NYDFS Regulation that were explicitly removed by the NAIC when crafting the Model Act.[166] Additionally, the IDFS exempts licensees that comply with HIPAA or with the GLBA.[167] Notably, it exempts these licensees from the entire Act, unlike the Model Act's HIPAA exemption, which only exempts licensees from the section 4 information security program, risk assessment, incident response plan, and annual certification requirements.[168]

HIPAA, which applies to all health insurance providers, provides for the protection of personally identifiable health information.[169] It requires the Department of Health and Human Services to promulgate a national security standard for such health information.[170] Similar to the mandates of the IDSA, those standards include conducting a risk assessment and implementing security programs based on the size and complexity of the entity.[171] Because HIPAA only protects health information—information that relates to the "physical or mental health . . . of an individual, the provision of health care to an individual, or . . . payment for the provision of health care"[172]—other information, such as location data collected from wearable devices, is not covered. HIPAA's guidelines for protecting health information are slightly more detailed and extensive, but still comparable to those of section 4 of the IDSA. Despite this, breaches at hospitals and medical centers continue to be on the rise.[173] One thing HIPAA does have that the IDSA clearly lacks, on the other hand, is an enforcement mechanism.[174] Unlike violations of the IDSA, violations of HIPAA are subject to civil penalties of up to $50,000 per violation.[175] Therefore, while not a substantially higher bar, HIPAA does have more compliance incentives. Still, exempting insurers subject to HIPAA from

164. IOWA CODE § 507F.4(1)(b)(1)(a)–(c).

165. *See* OHIO REV. CODE ANN. § 3965.07; ALA. CODE § 27-62-9; MISS. CODE ANN. § 83-5-817; IND. CODE ANN. § 27-2-27-26; LA. STAT. ANN. § 22:2509; N.D. CENT. CODE ANN. § 26.1-02.2-08; TENN. CODE ANN. § 56-2-1009; WIS. STAT. ANN. § 601.951.

166. *See* INS. DATA SEC. MODEL L. § 9 (NAT'L ASS'N OF INS. COMM'RS 2017); N.Y. COMP. CODES R. & REGS. tit. 23, § 500.19(a).

167. IOWA CODE § 507F.13.

168. *Compare id.*, *with* INS. DATA SEC. MODEL L. § 9(A)(2) (NAT'L ASS'N OF INS. COMM'RS 2017).

169. GUIDE TO MEDICAL PRIVACY AND HIPAA § 500 (Joan M. Flynn ed., 2010), Westlaw.

170. *Id.*

171. *Id.*; 45 C.F.R. § 164.306 (2021).

172. 42 U.S.C. § 1320d(4)(B).

173. *See generally* Jessica Davis, *Update: The 10 Biggest Healthcare Data Breaches of 2020, So Far*, HEALTH IT SEC.: XTELLIGENT HEALTHCARE MEDIA (July 8, 2020), https://healthitsecurity.com/news/the-10-biggest-healthcare-data-breaches-of-2020-so-far [https://perma.cc/UP6L-4DL8] (describing recent data breaches in the healthcare industry).

174. *Compare* 42 U.S.C. § 1320d-6, *with* IOWA CODE § 507F.

175. *See* 42 U.S.C. § 1320d-6.

the entire IDSA rather than just section 4 deprives the insurance commissioner of the complete picture regarding cybersecurity threats to the industry.

The GLBA addresses the security of consumer financial information and applies only to insurance agencies whose customers purchase insurance products "for personal, family, or household purposes."[176] A number of insurers will clearly already comply with the GLBA, and thus be taken completely out of the IDSA's purview. The GLBA requires covered entities to disclose to consumers "the policies that the institution maintains to protect the confidentiality and security of nonpublic personal information"[177] and delegates more specific rulemaking to other agencies.[178] Regulation to "establish appropriate standards . . . to insure the security and confidentiality of customer records and information"[179] as it relates to insurers is delegated to the state authorities, and the FTC has declined to exercise jurisdiction in this area.[180] The state has thus exempted GLBA-compliant insurers from its regulation, but it is responsible for establishing the very measures that those insurers must take to be GLBA-compliant. Nor is there any reason why the standards for insurers who would fall under the GLBA (whose customers purchase insurance products "for personal, family, or household purposes")[181] should be different than those of other insurers. At best, this exemption leads to needless complexity and confusion. At worst, it leaves individual insurance consumers (as opposed to corporate or business consumers) more vulnerable to having their personal data stolen because their insurer did not have appropriate safeguards.

The biggest problem with exemptions for small insurers is that small insurers are a group that is no less vulnerable to data breaches than large insurers. In 2020, just under half of reported data breaches targeted small businesses.[182] That number is down from previous years, when small business made up over half of data breach victims.[183] Additionally, small businesses

176. *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FED. TRADE COMM'N. (July 2002), https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm [https://perma.cc/U7AN-RNQD].

177. 15 U.S.C. § 6803(c)(3).

178. *Id.* § 6804.

179. *Id.* § 6801(b).

180. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462, 82,484 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

181. *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, *supra* note 176.

182. VERIZON, 2021 DATA BREACH INVESTIGATIONS REPORT 89 (2021), https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf [https://perma.cc/B5J8-2FEC] [hereinafter Verizon, 2021 Report].

183. VERIZON, 2018 DATA BREACH INVESTIGATIONS REPORT 5 (11th ed. 2018), https://www.verizon.com/business/resources/reports/DBIR_2018_Report.pdf [https://perma.cc/NH7Q-VTMG].

generally took longer to discover the breaches than larger businesses did.[184] Thus, small insurers are clearly no less a target for hackers than large insurers are. As small businesses with fewer resources, small insurers may already have less sophisticated web applications or security protocols than large insurers, which leaves them more susceptible to being breached successfully. Without the IDSA providing an incentive to prioritize more comprehensive security measures, small insurers are left in a continued state of vulnerability—as are their customers.

In the Iowa market specifically, there are roughly two hundred insurance companies domiciled in Iowa and over one thousand more carriers that operate in the state.[185] There is no publicly available data on how many of those employ fewer than twenty people, but in the Iowa finance and insurance industry as a whole, there are just under three thousand of such businesses.[186] Across all industries, over ninety-nine percent of Iowa businesses are classified as small businesses.[187] Of the top insurers in each subsector of the insurance industry, none of them have more than twenty percent of the national market share, and most have less than ten percent, meaning that smaller insurers cover a larger share of policyholders than in a more monopolistic market.[188] It can therefore be extrapolated that the exemption will cover more than a mere handful of insurers, and the number of policyholders whose information is left vulnerable could be quite high. The exemption thus practically consumes the rule. The IDSA cannot succeed in its goal of protecting consumer data when it covers few insurers and leaves the rest to continue with suboptimal security procedures and little pressure to change them.

Looking to the metric of insurers with less than $5 million in gross annual revenue or less than $10 million in year-end total assets, similar problems become apparent. Based on the annual financial statements filed by Iowa-domiciled insurers with the Iowa Insurance Division, roughly twenty-five percent appear to be exempt under the IDSA thresholds.[189] That is in spite of the solvency requirements placed on insurers by law. Insurers must comply with risk-based capital requirements developed by the NAIC, which set minimum capital requirements based on type of insurance offered, the size of

184. Verizon, 2021 Report, *supra* note 182, at 89–90.

185. *Iowa Insurance Industry at a Glance*, IOWA INS. INST. (Mar. 8, 2021), https://www.iowainsorg/iowa-insurance-industry-at-a-glance [https://perma.cc/6VNW-26AK].

186. U.S. SMALL BUS. ADMIN. OFF. OF ADVOC., 2020 SMALL BUSINESS PROFILE 68 (2020), https://cdn.advocacy.sba.gov/wp-content/uploads/2020/06/04143025/2020-Small-Business-Economic-Profile-IA.pdf [https://perma.cc/RY7V-QAPR].

187. *Id.* at 65.

188. *Major Players—Rankings by Line*, INS. INFO. INST. (2022), https://www.iii.org/publications/a-firm-foundation-how-insurance-supports-the-economy/driving-economic-progress/major-players-rankings-by-line [https://perma.cc/X7B7-78AE].

189. *See Financial Statements*, IOWA INS. DIV. (2022), https://iid.iowa.gov/financial-statements [https://perma.cc/8JBM-J2MF] (providing the most recently "file[d] financial statements" for "insurance companies domiciled in Iowa").

the insurer, and "the inherent riskiness of its financial assets and operations."[190] Thus, the $10 million in year-end total assets figure, at least, does not simply reflect licensee size. It also reflects capital requirements based on policy risk. Accordingly, this exemption does not relieve smaller insurers with fewer resources from the IDSA requirements, as was presumably its purpose. Rather, it exempts insurers with policies that fit under a certain risk portfolio.

The reasons for providing a small business exemption in the first place are straight-forward. Implementing data security compliance measures is expensive. "For mid-tier licensees, the average cost to implement any information security program will be between $33,000 and $54,000."[191] Additionally, many small insurers would likely need to hire outside contractors or new technical staff to ensure the constant maintenance of security systems. The average salary of an entry-level cybersecurity analyst in Iowa is $70,093.[192] Costs for outside security monitoring services vary, but "over half of companies spend a minimum of 1,200 hours per year on maintaining compliance."[193] Insurers must also bear the cost of providing company devices if they were not doing so previously. With the increased prevalence of work-from-home during the COVID-19 pandemic, ensuring that employees work from company-provided devices rather than personal ones is crucial to maintaining an adequate security barrier.[194] In the financial and insurance industries, the vast majority of breaches are due to internal errors, such as an employee sending an email with sensitive information to the wrong person or external phishing attacks that trick employees into giving up their credential information.[195] Protecting against these kinds of attacks requires constant training programs and employee-awareness programs to combat them. All this adds up to a huge increase in time, money, and resources for small insurers in order to comply with the IDSA.

Insurers were already attempting to cut costs prior to the pandemic, but that need has only been exacerbated since.[196] Across North America, sixty-

190. *Risk-Based Capital*, NAIC (June 24, 2020), https://content.naic.org/cipr_topics/topic_riskbased_capital.htm [https://perma.cc/K9QT-6ZNV]; *see* IOWA CODE § 522.

191. Zachary B. Randolph, Note, *Are You in Good Hands: South Carolina's New Data Security Act and Whether It Does Enough to Protect Insurance Consumers*, 71 S.C. L. REV. 999, 1021 (2020).

192. *Entry Level Cyber Security Analyst Salary in Iowa*, SALARY.COM (2022), https://www.salary.com/research/salary/posting/entry-level-cyber-security-analyst-salary/ia [https://perma.cc/9GJU-9ERW].

193. Ericka Chickowski, *Compliance Costs Are Eating Security Budgets*, SEC. BOULEVARD (June 2, 2020), https://securityboulevard.com/2020/06/compliance-costs-are-eating-security-budgets [https://perma.cc/C5HP-QQPE].

194. Hervé Debar, *Cybersecurity: High Costs for Companies*, THE CONVERSATION (Feb. 3, 2019, 2:12 PM), https://theconversation.com/cybersecurity-high-costs-for-companies-110807 [https://perma.cc/7K34-NZUW].

195. Verizon, 2021 Report, *supra* note 182, at 75.

196. Gary Shaw & Neal Baumann, *2021 Insurance Outlook: Accelerating Recovery from the Pandemic While Pivoting to Thrive*, DELOITTE INSIGHTS (Dec. 3, 2020), https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/insurance-industry-outlook-2021.html/#technology-could-play-a-crucial [https://perma.cc/J24L-G8ML].

eight percent of respondents to a Deloitte survey indicated their organizations would cut costs between eleven percent and twenty percent over the next year and a half.[197] Even in the midst of ramping up the use of artificial intelligence and remote claims handling, twenty-seven percent of total survey respondents indicated they expected no change in spending on cybersecurity and twenty-two percent indicated they expected to cut cybersecurity spending.[198]

Clearly, the costs of compliance add up quickly. But the costs of a data breach are significantly higher, often in the millions of dollars.[199] Without incentives to upgrade their security protocols, small insurers remain vulnerable, as do their customers. Complete exemption from the provisions of the IDSA is not the solution—particularly when the Model Act, an act crafted by a body made up of insurance commissioners and heavily influenced by the insurance industry, provided a narrower exemption with an overall less stringent standard for data privacy than the NYDFS on which it was based.

IV. PROVIDING CONSUMER SECURITY AND INSURER SUPPORT

So how can Iowa improve the IDSA so that it functions in its purpose of protecting the private data of more than merely a fraction of insurers and their consumers? And can it do so in a way that is still responsive to the demands this puts on small businesses? The Iowa Legislature should amend the IDSA to bring the exemptions back into conformity with the Model Act. First, the exemptions for insurers with less than $5 million in gross annual revenue and less than $10 million in year-end total assets should be eliminated, and the exemption for insurers with fewer than twenty employees should be brought down to insurers with fewer than ten employees.[200] These changes would narrow the small business exemption to a reasonable level and protect far more businesses and consumers from the massive harms caused by data breaches and the failure to quickly react to them.

Second, the legislature should consider eliminating the exemption for insurers that comply with the GLBA. Hewing as closely as possible to the Model Act promotes uniformity—a crucial goal of the NAIC which has been undermined by the way states have implemented the Act. It would also create a clearer and more uniform standard for Iowa insurers, since the standards insurers must comply with under the GLBA are already promulgated by state regulators.

Third, the legislature should also revise the notification timeline back to seventy-two hours rather than three business days. A seventy-two hour deadline is still reasonably manageable for insurers while promoting a sufficiently urgent

197. *Id.*

198. *Id.*

199. *See supra* Part I.

200. *Compare* INS. DATA SEC. MODEL L. § 9(A)(1) (NAT'L ASS'N OF INS. COMM'RS 2017) (exempting businesses with fewer than ten employees), *with* IOWA CODE § 507F.4(1)(b)(1) (exempting businesses with fewer than twenty employees).

response to the serious threat data breaches pose. Even though the law went into effect January 1, 2022, licensees have a year to comply with its requirements.[201] The sooner a revision is implemented, the less need there would be for a further grace period for licensees who were formerly exempt.

Some states may have been reacting to pressure from constituents when they eased up requirements or expanded exemptions in their versions of the Model Act. In Iowa, however, there is little evidence that that is the case. Most individual Iowans have likely never heard of the law since there was negligible news coverage or public outreach communication from legislators about it.[202] Lobbyists from the insurance sector were all either for the bill or undecided on it.[203] During voting in both the Iowa house and senate, no substantive discussion was had nor did any representative raise criticisms or questions about the bill.[204] Representative Chris Hall alluded to "adjustments and improvements" that had been made to the bill by the Information Technology committee since it was submitted by the Iowa Insurance Division, but there was no further discussion of those changes among the whole body.[205]

Even if changes were made at the behest of the insurance lobby, Iowa is in a position to hold insurers to a high standard rather than cave to their demands. Iowa's low one percent premium tax and general low cost of doing business are big draws for many insurance agencies.[206] Des Moines in particular markets itself as the insurance capital of the United States.[207] Insurance contributes over ten percent of the state's GDP, the highest percentage of any state.[208] And the industry is only growing, having done so by forty-five percent

201. IOWA CODE § 507F.4(9).

202. *See generally, e.g.*, *State Representative Garrett Gobble*, FACEBOOK, https://www.facebook.com/gobbleforiowahouse [https://perma.cc/E5H9-FSRP] (showing that State House Representative Gobble posted multiple times but never mentioned the bill near March 9, 2021); *Dave Williams, Iowa House*, FACEBOOK, https://www.facebook.com/DaveIowaHouse [https://perma.cc/E327-73XJ] (showing the State House Representative Williams posted multiple times but never mentioned the bill around March 12, 2021); *"Insurance Data Security Act,"* DES MOINES REG., https://www.desmoinesregister.com/search/?q=%22insurance+data+security+act%22 [https://perma.cc/KE8D-5PER] (demonstrating absence of results for articles about the Act).

203. *See Lobbyist Declarations*, THE IOWA LEGISLATURE, https://www.legis.iowa.gov/lobbyist/reports/declarations?ga=89&ba=HSB198 [https://perma.cc/63G6-H8CT].

204. *House Video (2021-03-09)*, THE IOWA LEGISLATURE, https://www.legis.iowa.gov/dashboard?view=video&chamber=H&clip=h20210309022336437&offset=6309&bill=HF%20719&dt=2021-03-09 [https://perma.cc/L3ZJ-ASH6]; *Senate Video (2021-04-07)*, THE IOWA LEGISLATURE, https://www.legis.iowa.gov/dashboard?view=video&chamber=S&clip=s20210407122035117&offset=9416&bill=HF%20719&dt=2021-04-07 [https://perma.cc/5V7X-RZD3].

205. *House Video (2021-03-09)*, *supra* note 204.

206. *The Insurance Capital of the U.S.? Look to Des Moines*, CO (2022), https://www.uschamber.com/co/good-company/growth-studio/des-moines-iowa-insurance [https://perma.cc/YT2U-XPC2].

207. *Id.*; *see Insurance & Financial Services*, GREATER DES MOINES P'SHIP (2022), https://www.dsmpartnership.com/growing-business-here/key-industries/insurance–financial-services [https://perma.cc/9XCK-W5TG].

208. *Iowa Insurance Industry at a Glance*, *supra* note 185.

in the last five years.[209] The financial benefits of operating in Iowa can therefore act as a counterbalance to the comparative onerousness of privacy regulation as compared to other states. Additionally, the Global Insurance Accelerator Program hosted annually in Des Moines is a mentorship program designed to assist insurance technology startups.[210] Many of these startups are data aggregators.[211] They provide just the sort of big data that is concerning for privacy activists and makes companies prime targets for hackers.[212] Thus the centrality of the insurance industry in Iowa, as well as the existing financial incentives to operate there, give Iowa both the right and the obligation to mandate comprehensive data security laws for the industry.

To help ameliorate the costs and research associated with bringing insurers into compliance, the state should also provide technical consultations and information sessions for insurers. These could be done through the Iowa insurance commissioner's office or be subsidized through private-party data compliance service providers. Better yet, the NAIC, with its significant resources pooled from both the nationwide insurance industry and the states, could create educational programs to assist small insurers at no cost. Given that providing similar educational resources is a primary component of the NAIC's work, they are perhaps best poised to fill this gap. Such a program run by the NAIC would benefit not just insurers in Iowa, but insurers across the country. Since Iowa is a major center of the insurance industry, it should have the lobbying power to convince the NAIC to implement such training programs. And with a nationally available compliance training program already in place, more states are likely to keep to the original exemptions and not attempt to expand them. This, again, would promote the uniformity and clarity that were original goals of the Model Act and of the NAIC as an organization.

Whether run by the NAIC or the insurance commissioner, compliance assistance and education would enable small insurers to fully meet the demands of the IDSA without needing to invest as much money in hiring their own technical consultants. While this would not eliminate necessary costs, it would lower them and justify the narrowing of the exemption. Further compliance guidance is also helpful in light of the flexibility of the statute itself. Good privacy laws are adaptive, meaning they establish standards rather than prescribing a particular technological requirement.[213] The rapid pace of technological advancement means that it is unrealistic to expect legislatures

209. *Id.*

210. *See Innovation and Acceleration for a Trillion Dollar Industry. Be a Part of the Insurance Industry's Accelerator*, GLOBAL INS. ACCELERATOR, https://www.globalinsuranceaccelerator.com [https://perma.cc/NCK8-JFJ2].

211. *See Once an Alumni, Always an Alumni!: Global Insurance Accelerator Portfolio of Cohort Companies.*, GLOBAL INS. ACCELERATOR, https://www.globalinsuranceaccelerator.com/portfolio [https://perma.cc/W7A7-AX57].

212. *See supra* Part I.

213. Kosseff, *supra* note 142, at 828.

to keep up with specific best practices.[214] Instead, it is more advantageous to have specific rulemaking authority delegated to another authority in a better position to act quickly.[215] The IDSA sets such flexible standards by stating that the licensee's security program be "[c]ommensurate with the size and complexity of a licensee[] [and] the nature and scope of a licensee's activities."[216] But it leaves determinations up to the licensees to "[i]dentif[y] reasonably foreseeable . . . threats" and "[a]ssess[] the sufficiency of [their] policies, procedures, information systems, and other safeguards."[217] Further guidance from the insurance commissioner or the NAIC would assist insurers in meeting these standards, provide certainty and predictability, and generally make implementing the necessary security measures more straightforward.

CONCLUSION

Cybercrime and security are pressing issues, especially for industries such as insurance that collect massive amounts of sensitive data. Recognizing this and the general lack of comprehensive privacy regulation in the United States, the NAIC took an important step in drafting the Model Act. However, the variance in the laws that states have actually implemented has lowered the bar that insurers must meet in protecting sensitive data. Iowa's law is no different, having broadened exemptions that make the law inapplicable to many insurers. This leaves a significant number of Iowans vulnerable to having their data infiltrated by bad actors. Iowa must use its position as a national hub of the insurance industry to take the lead on privacy issues. The Iowa Legislature should amend the law to narrow the exemptions back to the scope originally contemplated in the Model Act. And to compensate for concerns regarding compliance costs for small insurers, the state should provide cybersecurity assistance consultations and education or press the NAIC to do so.

214. *Id.*
215. *Id.*
216. IOWA CODE § 507F.4(1)(a).
217. *Id.* § 507F.4(3)(b), (d).