A Brief History of the NAIC Insurance Data Security Model Law

Authored by ALFA International Attorney:

Meghan Ruesch
LEWIS WAGNER, LLP
Indianapolis, Indiana
mruesch@lewiswagner.com
A BRIEF HISTORY OF THE NAIC INSURANCE DATA SECURITY MODEL LAW

Author: Meghan Ruesch, Lewis Wagner, LLP

I. Introduction

In 2019, the concept of a “Cybersecurity Event” is not a foreign concept—the terms “hacking” and “data breach” have dominated the news over the past five years, though such events are almost so common place anymore that the news may only give a significant Cybersecurity Event a passing mention. Major data breaches have affected significant Fortune 500 companies like Equifax, Uber, Sony, Yahoo, Anthem, Target, Verizon…the list goes on. One way to fully appreciate and understand the significant likelihood and impact of a Cybersecurity Event is to just look at some of the numbers:

- In 2017, 147.9 million consumers were affected by the Equifax breach.
- In 2013, 3 billion customers were affected by the Yahoo breach.
- There are around 24,000 malicious mobile apps blocked every day.
- Between January 1, 2005 and April 18, 2018 there have been 8,854 recorded breaches.
- In 2018, the average ransomware attack cost a company $5 million.
- It takes organizations an average of 191 days to identify data breaches.
- 88% companies spent more than $1 million on preparing for the GDPR.
- 54% of companies experienced an industrial control system security incident.
• 61% of organizations have experienced an Internet of Things (IoT) security incident.

• The United States is the number one country for targeted cybersecurity attacks, accounting for 38% of attacks of the top ten attacked countries affected by targeted attacks between 2015 and 2017.¹

At the top of the list of industries targeted for cybersecurity attacks is the financial services and insurance industry. While, from a business perspective, it seems ever necessary that companies providing financial and insurance services implement internal cybersecurity standards, legislators and regulators are also taking note, and states are starting to implement regulations for cybersecurity requirements within the insurance industry. Many states that have started implementing such regulations have looked to (or are looking to) the National Association of Insurance Commissioners’ (“NAIC”) Insurance Data Security Model Law (“IDSML”) for guidance in implementing these regulations.²

This paper will provide a brief discussion of the history and development of the IDSML, and then provide a high-level overview of some of the key provisions of the IDSML. This will then look to some of the states that have already implemented cybersecurity regulations applying to the insurance industry, including those that have

---


² For your reference, a copy of the NAIC Insurance Data Security Model Law is attached to the end of this article.
adopted the IDSML specifically, before discussing the potential future impact the IDSML will have nationwide, and what that impact means for the insurance industry.

II. History of the NAIC Insurance Data Security Model Law

The IDSML was officially adopted by the NAIC’s Executive Committees on October 24, 2017. The purpose of the IDSML was to establish standards for data security, investigation, and notification requirements following a Cybersecurity Event for the insurance industry. The IDSML was the product of two years of development by the NAIC’s Innovation and Technology Task Force and Cybersecurity Working Group.

The provisions of the IDSML closely mirror New York’s cybersecurity regulations for financial services companies (including insurance entities) (23 N.Y.C.R.R. § 500), implemented by the New York State Department of Financial Services (DFS) in March 2017. Indeed, a drafting note from on working draft of the IDSML explicitly notes that compliance with the New York regulations will ensure compliance with the IDSML. The New York cybersecurity regulation established certain cybersecurity requirements for financial services companies, requiring that insurance and insurance-related companies (brokers, agents, adjusters, etc.) that are licensed in New York to assess their specific cyber risks and possible exposures, and to design a cybersecurity program to address such risk. While there were some limited exemptions to required compliance with these

---

regulations, the regulations would span a vast majority of insurance and insurance-related entities licensed in New York. The final deadline for “covered entities” to transition to full compliance with the New York regulations was on March 1, 2019. The regulations also have ongoing compliance requirements, many of which are also present in the ISDML.4

The foundation for the IDSML also stems from several NAIC materials, including the NAIC Principles for Effective Cybersecurity Insurance Regulatory Guidance, adopted in April 2015.5 This document set forth twelve (12) guiding principles for state insurance regulators, insurers, and insurance-related entities to consider in assessing and implementing cybersecurity measures in their firm. Another document that was instructive in the development of the IDSML was the NAIC Road Map for Cybersecurity Consumer Protections, which contained recommendations and a “bill of rights” for insurance consumers regarding the protection of their personal and financial information.6 Considering the necessity for all insurance and financial institutions to implement cybersecurity measures from both the consumer and industry perspective guided the NAIC in developing the IDSML.

III. Key Provisions in the NAIC Insurance Data Security Model Law

---

The IDSML applies to all “licensees” doing business in the state to develop, implement, and maintain a comprehensive, written information security program. The IDSML also establishes specific requirements imposed on “licensees” for responding to a Cybersecurity Event. The following will identify some of the key provisions of the IDSML regarding the entities that the regulations apply to; the specific requirements for the implementation of the mandatory information security program; and the obligations imposed on an entity in responding to a Cybersecurity Event.

Who/What does the IDSML Apply to?

The IDSML provides, at its most general level, “The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees.”

What is significant here is that the IDSML only applies to “Licensees,” which is defined in Section 3 of the act to include “any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State.” The definition of “Licensees” specifically excludes “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.”

Section 9 of the IDSML identifies certain exemptions from compliance with the laws, including the following:
(1) A Licensee with fewer than ten employees;

(2) A Licensee subject to HIPAA, which are required to maintain a HIPAA-compliant Information Security Program (maintenance of a HIPAA-compliant program will be deemed to be in compliance with the IDSML); and

(3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, to the extent that they are covered by the Licensee’s Information Security Program.

The IDSML applies to the protection of “Nonpublic Information,” which is defined, in general, as any information that is not “Publicly Available Information,” and is considered either (1) the Licensee’s “business information;” (2) personal identifying information of a “Consumer” (including Social Security numbers; driver’s license numbers; bank account, credit card, debit card information; security codes/access codes/passwords; or biometric information); and (3) personal health information.

The IDSML also applies to the protection of “Information Systems,” which is defined to include industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

What is required for the Information Security Program?

---

7 Defined as “any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public.”
Section 4 of the IDSML sets for the specific requirements for a Licensee’s development and implementation of an Information Security Program, stating as follows:

Commensurate 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 by the Licensee or in the Licensee’s possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive written Information Security Program based on the Licensee’s Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee’s Information System.

Section 4 provides for the following specific actions in developing, implementing, and maintaining the Information Security Program:

1. Risk Assessment: The ISDML requires that a Licensee designate one or more employees, an affiliate, or outside vendor to be responsible for the Information Security Program. Such designee is required to identify “reasonably foreseeable internal or external threats” to the Licensee’s Nonpublic Information or Information Systems, and the security of such information and systems that are accessible to third-party vendors. They must also assess the likelihood and potential damage of these threats, and the sufficiency of current security controls in place to protect Nonpublic Information and Information Systems. They must also implement information safeguards to manage these threats, and at least annually, assess the effectiveness of the safeguards’ key controls, systems, and procedures.

2. Risk Management: Based on the Risk Assessment, the Licensee must design its Information Security Program to mitigate identified risks, in a manner commensurate with the size of the Licensee, the sensitivity of the Nonpublic Information, and access of such information to Third-Party Vendors. The Licensee
then must implement appropriate security measures, as provided in a list of eleven (11) enumerated security measures. The Risk Management provision also requires the Licensee stay informed of emerging cybersecurity threats and vulnerabilities on an ongoing basis, and to conduct ongoing awareness training to personnel.

3. Oversight by Board of Directors: The IDSML requires an entity's Board of Directors (if such a Board exists) to develop, implement, and maintain an Information Security Program, and to prepare a written report regarding the status and any issues pertaining to the Information Security Program annually. This is a unique development in imposing traditional C-Suite duties and oversight on the Board of Directors, and imposes an affirmative duty on the Board to take an active role in an organization's cybersecurity and data management.

4. Oversight of Third-Party Service Provider Arrangements: This section requires Licensees to exercise due diligence in choosing Third-Party Service Providers, and to require that Third-Party Service Providers similarly implement and maintain adequate security measures to protect Nonpublic Information and Information Systems.

5. Program Adjustments: The IDSML requires Licensees to continuously monitor and update its Information Security Program to respond to relevant changes in technology or changes in the nature of the information and systems that the business maintains.
6. Incident Response Plan: One of the most significant parts of the Information Security Program is the development and establishment of a written incident response plan designed to promptly respond to and recover from a Cybersecurity Event. The Incident Response Plan must address the following eight (8) issues: (a) the internal process for responding to a Cybersecurity Event; (b) the goals of the incident response plan; (c) the definition of clear roles, responsibilities and levels of decision-making authority; (d) external and internal communications and information sharing; (e) identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls; (f) documentation and reporting regarding Cybersecurity Events and related incident response activities; and (g) the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

7. Annual Certification to State Commissioner: The IDSML requires annual certification of compliance with the IDSML to the appropriate state commissioner or agency.

What is required to respond to a Cybersecurity Event?

While Section 4 addresses preventative measures in addressing possible Cybersecurity Events, Sections 5 and 6 address what responsive measures an organization must take in responding to a Cybersecurity Event.
Section 5 establishes specific requirements for the Investigation of a Cybersecurity Event. It requires that Licensees, upon discovery that a Cybersecurity Event occurred or might have occurred, to conduct a “prompt investigation,” during which the Licensee (or a designated outside vendor) to at a minimum determine (1) whether a Cybersecurity Event occurred; (2) the nature and scope of the Cybersecurity Event; (3) what Nonpublic Information might have been impacted; and (4) reasonable measures to restore security of compromised Information Systems. This section also requires a Licensee to maintain records of a Cybersecurity Event for at least five years.

Section 6 establishes and outlines requirements for Notification of a Cybersecurity Event. Upon determination that a Cybersecurity Event has occurred, the IDSML requires that a Licensee notify the commissioner of the regulating insurance department of a state within 72 hours of such determination to either: (1) the Commissioner of in the Licensee’s state of domicile/home state; or (2) the Commissioner of another state if the Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in the state, and the Commissioner of that state (a) requires notice of a Cybersecurity Event as a matter of state or federal law; or (b) the Cybersecurity Event has a reasonable likelihood of materially harming any consumer in the state or any material part of the Licensee’s normal operation(s).

Under the IDSML notice requirements, the Licensee must provide the Commissioner of whatever states it reports to as much information concerning the Cybersecurity Event as possible, and imposes a continuing reporting obligation on the
Licensee as more information becomes available. The IDSML identifies thirteen specific points of information that should be noticed to the Commissioner in the course of the Licensee’s investigation.

The IDSML also requires that a Licensee notify consumers of a Cybersecurity Event in accordance with applicable state consumer data breach notification laws. For Cybersecurity Events involving Third-Party Service Providers, the IDSML requires Licensees to treat such Cybersecurity Events as if experienced by the Licensee itself, provided that the agreement between the Licensee and Third-Party Service Provider delegates investigation and notification obligations between the two parties.

The ISDML includes a specific requirement that reinsurers notify its ceding insurers of a Cybersecurity Event, and then obligates the ceding insurers to notify potentially affected consumers of the Cybersecurity Event as required by either state consumer notification laws, or as required by the ISDML. Finally, the ISDML requires insurers that experience a Cybersecurity Event to notify producers of record of such an event, but only to the extent of potentially affected consumers.

**Anything else worth noting?**

Two additional noteworthy provisions of the ISDML:

1. The IDSML specifically states that it may not be construed to create or imply a private cause of action for violation of its provisions, but nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.
2. The IDSML imposes a duty on the Commissioner or Department of Insurance to keep any Nonpublic Information or materials it receives from a Licensee in the wake of a Cybersecurity Event confidential, and protects such Commissioner (and its employees, agents, etc.) who reviews such information from having to testify in any private civil action concerning any confidential information.

3. The IDSML includes a section for “Penalties,” where by a state may impose penalties commensurate with the state’s general penalty statute on any violation of the IDSML’s provisions.

IV. State Adoptions and the Future of the Insurance Data Security Model Law

As with any model law drafted by the NAIC, the IDSML is not binding—it is a model law, providing recommended language and standards that states might adopt. Since its adoption in October 2017, three states have adopted the IDSML, or a similarly-modeled set of regulations: South Carolina (adopted May 9, 2018; eff. Jan. 1, 2019); Ohio (adopted Dec. 19, 2018); and Michigan (adopted Dec. 28, 2018). While the statutes adopted by these three states significantly model the IDSML, there are some nuances, the most significant being certain changes in the Ohio statute. Specifically, the Ohio law

---

9
10
specifically creates an affirmative defense for insurance company’s against torts alleging the insurer lacked reasonable cybersecurity measures, if the company “satisfied” the provisions of the new law. The Ohio statutes also amends the definition of a cybersecurity event to incidents causing unauthorized access or misuse of information that “has a reasonable likelihood of materially harming” consumers residing in the state or the Licensee’s normal operations. This phrase requiring “material harm” does not exist in the IDSML. The Michigan statute also deviates slightly from the IDSML, and provides for a 10-day notice requirement, as opposed to the 72-hour notification requirement of the IDSML and other states.

Although over 18 months have passed since the adoption of the NAIC IDSML and, at least as of the date of my writing this, only three states have adopted similar regulations, it is not inconceivable that more states will follow, and in quick order. At least four jurisdictions (Rhode Island, Vermont, Louisiana, and the District of Columbia) have proposed similar laws in their legislation.

V. Conclusion

The passage of regulations like the IDSML in most states will have a significant impact on the insurance industry. Organizations impacted by these regulations, if they have not done so already, should begin preparing their organizations (and any entities with which they work that might be subject to such regulations) to anticipate compliance
with state regulations early. The current IDSML provides the best source of guidance for state regulations that will likely be implemented in more and more states in the near future. Organizations should begin its risk assessment and risk management activities. They should also start evaluating third-party service providers, and implementing appropriate actions at all relevant levels of the organization to support necessary security measures. While it seems that appropriate security measures for insurance companies and related organizations will have some universality, in truth, the needs of each organization will vary based on the size of the company, the nature of the insurance being written (P&C vs. LH&A in particular), and the specific requirements for each state that company is a Licensee. With the ever-evolving implementation of federal and international regulations regarding cybersecurity, it is not inconceivable that the IDSML will impact laws in all fifty states. Ultimately, while time will tell how much traction the IDSML makes across the country, insurers should begin preparing to comply now to be ahead of the curve.