SECURITY COMPASS WHITEPAPER

Insurance Data Security Model Law

What It Means for Software Security

Security Compass

In light of multiple high-profile data breaches leading to the compromise of sensitive personal information, the National Association of Insurance Commissioners (NAIC) drafted and adopted the Insurance Data Security Model Law in collaboration with the insurance industry, consumer representatives, and state insurance regulators. In this whitepaper, we are exploring the requirements and adoption of this law across different states in the U.S.

Rising number of data breaches in the insurance industry

Insurance companies handle large amounts of extremely sensitive data. This Personally Identifiable Information (PII) can be used by criminals for identity theft and insurance fraud. It is no surprise that insurance companies are a lucrative target of hackers.

While large organizations are prime targets, any organization processing PII is a target. The criminals that attacked UConn Health stole "only" 326,000 records; not an insignificant number. In addition to loss of customer confidence, reputation, and lawsuits, these organizations face financial penalties from regulators. Hacks have even been reported to result in loss of life.

The insurance industry has long been acquainted with stringent regulations. In recent years, this has included regulatory requirements for cybersecurity. While much attention is given to HIPAA in the U.S., the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, and GDPR in Europe, there are additional regulatory requirements directly from insurance regulators.

Growing security recommendations from NAIC

In 2014, in response to increasing cybersecurity threats, the NAIC formed a Cybersecurity Working Group to identify and recommend regulatory priorities and activities. In 2015, NAIC published its *"Principles for Effective Cybersecurity."* The principles described the responsibilities of state insurance regulators to ensure the protection of PII collected by the regulators and insurers operating in their states.

It recognized that *"a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations."*

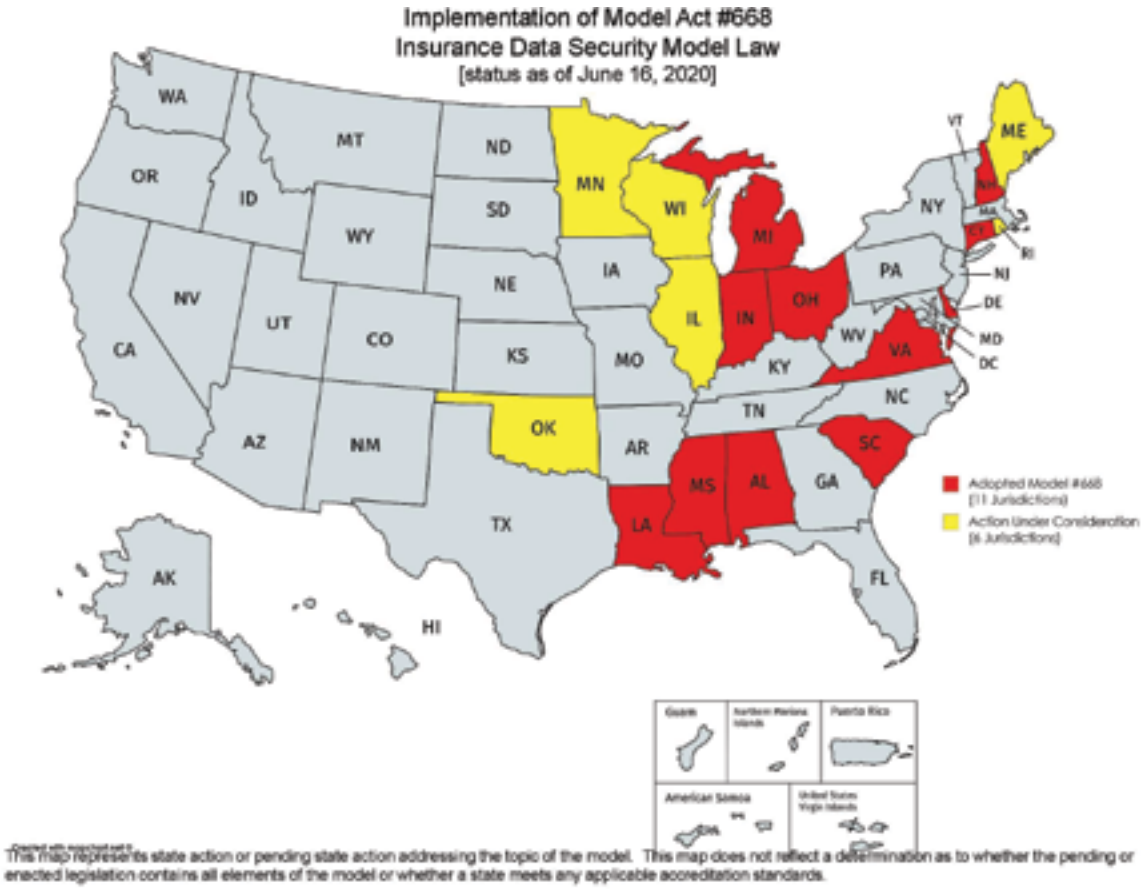

Image source: The NAIC Insurance Data Security Model Law, State Legislative Brief

Implementation of the Insurance Data Security Model Law

In 2017, NAIC approved the Insurance Data Security Model law. As of June 2020, the law had been adopted by 11 states and was under consideration in six others.

The U.S. Treasury Department has encouraged all states to adopt it within the next five years "or the administration will ask Congress to preempt the states." When adopted, the Data Security Model Law requires regulated entities to:

1. Protect the security and confidentiality of nonpublic information and the security of the information system;

2. Protect against any threats or hazards to the security or integrity of nonpublic information and the information system;

3. Protect against unauthorized access to or use of nonpublic information, and minimize the likelihood of harm to any consumer; and

4. Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

Requirement: Information Security Program

The Data Security Model Law, like HIPAA, offers general guidance rather than specific controls. Its primary requirement is that organizations licensed by the state to operate in the insurance industry ("licensees") develop, implement, and maintain an information security program.

The details of the information security program are not prescribed, as not all organizations manage the same types or volume of PII. Instead, the Law requires the program be "commensurate with the size and complexity of the Licensee…."

Requirement: Risk Assessment

Instead, similar to HIPAA, the law requires each organization to conduct risk assessments to identify "reasonably foreseeable internal or external threats" then build policies and controls to mitigate risk from those threats.

What defines a "reasonably foreseeable internal or external threat"? One could argue strongly that threats that have been known to result in successful breaches would be minimally reasonable. For example, since weak passwords and brute force attacks have been used successfully in the past, these should logically be enumerated threats. Likewise, poor cloud bucket configurations have resulted in breaches.

In other words, "reasonably foreseeable" threats are not unique to a specific application and identifying them should not require extraordinary security expertise. The Model Law does not require ISO 27001 or NIST 800-53 certification, nor does it require modeling specific tactics, techniques, and procedures used by likely adversaries as called out in the MITRE ATT&CK Framework (all of which would be extremely burdensome to smaller Licensees and not "commensurate with the size and complexity of the Licensee…"). Reasonably foreseeable threats are those inherent to a technology stack and deployment environment.

Requirement: Risk Management

Awareness of risks and threats is an obvious first step in a security program, as is a plan to mitigate those risks and threats. The Insurance Data Security Model Law therefore requires licensees to have a risk management program "to mitigate the identified risks, commensurate with the size and complexity of the Licensee's activities." This would include practices such as requiring strong passwords or password resets after multiple failed login attempts to mitigate the threat of brute force attacks mentioned above.

In this section the Model Law is more specific, calling out over a dozen activities and controls for cyber and physical security. Again, the Model Law does not require activities and controls that would be burdensome to smaller organizations. These include:

- Access controls on systems managing sensitive information to block unauthorized individuals from seeing PII, and consider using multi-factor authentication
- Restrict access to physical locations where sensitive information is maintained
- Encrypt sensitive data in transit
- Encrypt sensitive data at rest on portable computing and storage devices
- Maintain audit trails for investigating security events

Requirement: Adopt Secure Development Practices

Not all organizations subject to the Model Law have in-house development teams. Those that do, however, are required to adopt secure development practices and procedures for testing the security of externally developed applications. This requirement aligns well with risk assessments and controls but is specific to application security.

The Model Law does not provide specific activities or controls for the secure development program. It should, obviously, include a risk assessment to identify "reasonably foreseeable internal or external threats," controls to mitigate those threats and risks, and testing to validate that the controls were implemented correctly.

Requirement: Include Cybersecurity Risk in an Enterprise Risk Management Process

Having programs in place to identify risk and apply controls is the overriding goal of the Model Law. However, it also recognizes the need to maintain a reporting requirement that can be used to monitor the program's status.

Requirement: Cybersecurity Awareness Training

Many attacks today do not require sophisticated hacking skills. It is far easier for an attacker to trick an employee to disclose credentials or click on a link to launch a ransomware attack. These attacks are simple to launch and can target entry-level employees as well as senior executives.

Evolving regulatory landscape for data security

This new law for the insurance industry is not the only legislative trend affecting companies in the insurance markets. The New York Department of Financial Services issued 23 NYCRR Part 500 in 2017 to establish cybersecurity guidance for financial services companies operating in the state, including insurance companies. This, too, requires covered entities to create and maintain risk assessments and cybersecurity policies for secure software development in addition to information, network, and physical security. Likewise, multiple actions against organizations have occurred under Section 5 of the US Federal Trade Commission Act under States' "mini FTC Acts" for failure to maintain "reasonable security."

Reasonable security need not be burdensome for software development and security teams. It requires organizations to have visibility to likely threats and risks which result from the technology stack and deployment environments of their applications. Identifying these through automated threat modeling, mapping controls to each identified threat, and validating the correct implementation of those controls form the basis for a secure development program.

Security Compass

Go Fast. Stay Safe.

Security Compass, a leading provider of cybersecurity solutions and advisory services, enables organizations to adopt Balanced Development Automation for rapid and secure application development. With their flagship product, SD Elements, the company helps automate significant portions of proactive manual processes for security and compliance that improves time to market for new technology. In addition, they offer advisory services on howorganizations can embrace emerging technologies like cloud to strengthen their security posture. Security Compass is the trusted solution provider to leading financial organizations, technology enablers, and renowned global brands. The company is headquartered in Toronto, with offices in the U.S. and India. Follow Security Compass on Twitter @securitycompass or visit them at securitycompass.com to learn more.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
USA 94108

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001