NAIC Data Security Model Law

Description

In October 2017, the NAIC adopted the Insurance Data Security Model Law. 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. A licensee is defined as a person or entity licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State.

The Data Security Model Law requires licensees to perform the following:

Information Security Program â?? A documented program designed to protect the security of nonpublic information and the security of the Information System. The program should also reevaluate a schedule for retention and destruction of n and of destruction of nonpublic information when no longer needed.

Risk Assessment â?? The Risk Assessment Identifies foreseeable internal or external threats to the security of nonpublic information and information systems and assess the likelihood and potential damage of these threats. The licensee should implement safeguards and assess the effectiveness on an annual basis.

Risk Management â?? Based on the Risk Assessment, the Information Security Program should be designed to mitigate the identified risks, including its use of Third Party Service Providers. The following security measures should be considered when designing your program:

- Access Controls
- Systems and Data Inventory
- Physical Security
- Encryption of Data
- Transmission over external networks and on mobile devices
- Application Security
- Multi-Factor Authentication
- Testing and monitoring of systems
- Audit Trails
- Disaster Recovery
- Secure Disposal

Oversight by Board of Directors â?? If the Licensee has a board of directors, the board must require the development, implementation and maintenance of a Information Security Program. The Licenseeâ??s executive management must report in writing at least annually the overall status of the

Information Security Program, compliance with the Act, cybersecurity events or violations to the Program and recommendations.

Oversight by Third-party Service Providers â?? A Licensee shall exercise due diligence when selecting a Third-Party Service Provider. The Third-Party Service Provider is required to implement administrative, technical and physical measures to protect and secure Information Systems and nonpublic information.

Program Adjustments â?? The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its nonpublic information and business arrangements.

Incident Response Plan â?? A written incident response plan is designed to promptly respond to, and recover from any Cybersecurity Event that compromises the confidentiality, integrity or availability of nonpublic information or Information System. The plan should address the following areas:

- Internal response process
- Goals of the incident response plan
- Definition of clear roles and responsibilities
- External and internal communications and information sharing
- Identification of requirements for the remediation of any identified weaknesses
- Documentation and reporting regarding Cybersecurity Events
- Evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

Annual Certification â?? Each year, by February 15, each domestic insurer is required to submit to the Commissioner a written certification of compliance with the NAIC Model.

Investigation

The NAIC model requires licensees to investigate potential Cybersecurity Events promptly. At a minimum, the investigation by the Licensee or its outside vendor is required to determine the following information as possible:

- Determine whether a Cybersecurity Event has occurred;
- Assess the nature and scope of the Cybersecurity Event;
- Nonpublic Information that may have been affected; and
- Reasonable measures to restore security of the compromised Information Systems in the Cybersecurity Event

Notification

Licensees are required to notify the Commissioner as promptly as possible but no later than 72 hours from determining that a Cybersecurity Event has occurred when either of the following criteria has been met:

- This State is the Licenseeâ??s state of domicile

- The Licensee believes that the nonpublic information involved is of 250 or more Consumers residing in this State and either requires notice to government agency or has a likelihood of materially harming and consumer residing in the State or any material part of the normal operation of the Licensee.
- The Licensee shall provide as much information as possible and obligation to update the Commissioner. The NAIC has identified 13 points required to be in the notification.
- Licensee shall comply with the Stateâ??s law as it relates to notifying consumers of a Cybersecurity event.
- Licensees are required to treat events that have occurred at Third Party Service Providers as their own.
- Reinsurers must provide notice to insurers of Cybersecurity Events and insurers are required to notify producers of record of Cybersecurity Events.
- The law was recently passed in South Carolina with Rhode Island, Nevada and Vermont looking to pass similar laws.

Raja Paranjothi, CISA

Raja is currently a Principal with Oread Risk & Advisory. Raja has 20 years of experience providing client and consulting services with expertise in IT Security, Risk Assessments, HIPAA assessments, PCI, IT audits, IT Governance and Compliance and SOC reports. Earlier in his career, Raja led the Business & Technology Risk Services practice at CBIZ and Mayer Hoffman McCann and was also a senior management consultant for Ernst & Young and Deloitte. Raja serves a variety of clients within multiple industries including financial institutions, healthcare companies, technology companies, etc.

Category

1. Cybersecurity

Tags

1. featured

Date Created
2018/08/06
Author
vltaexaminer