DIGEST

The digest printed below was prepared by House Legislative Services. It constitutes no part of the legislative instrument. The keyword, one-liner, abstract, and digest do not constitute part of the law or proof or indicia of legislative intent. [R.S. 1:13(B) and 24:177(E)]

HB 614 Original 2020 Regular Session Seabaugh

Abstract: Establishes the "Insurance Data Security Law".

Proposed law enacts the Insurance Data Security Law to establish standards for data security and for the investigation of and notification to the commissioner of a cybersecurity event applicable to licensees of the Department of Insurance.

Proposed law defines "authorized individual", "consumer", "cybersecurity event", "encrypted", "information security program", "information system", "licensee", "multi-factor authentication", "nonpublic information", "person", "publicly available information", "risk assessment", and "third-party service provider".

Proposed law requires a licensee to develop, implement, and maintain a comprehensive, written information security program which satisfies the criteria required by proposed law and does all of the following:

(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.

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

Proposed law requires a licensee to conduct a risk assessment that meets the criteria specified in proposed law, design an information security program to mitigate the identified risks, and implement appropriate security measures.

Proposed law provides for the duties of the licensee's board of directors.

Proposed law provides for the duties of a licensee with regard to third-party service providers.

Proposed law requires the licensee to monitor, evaluate, and adjust, as appropriate, the information

security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to information, and the licensee's own changing business arrangements.

Proposed law requires each licensee to establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity, or availability of nonpublic information in its possession, the licensee's information systems, or the continuing functionality of any aspect of the licensee's business or operations and establishes the minimum requirements of the response plan.

Proposed law requires a licensee which learns that a cybersecurity event has or may have occurred, or an outside vendor or service provider designated to act on behalf of the licensee, to conduct a prompt investigation and provides for the requirements of the investigation and subsequent documentation.

Proposed law provides for the notification duties of a licensee once there is a determination that a cybersecurity event has occurred.

Proposed law authorizes the commissioner to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any violation of proposed law and to take any action that is necessary or appropriate to enforce the provisions of proposed law whenever the commissioner has reason to believe that a licensee has been or is engaged in a violation of proposed law.

Proposed law provides for the confidentiality of any documents, materials, or other information in the control or possession of the commissioner that are furnished by a licensee or an employee or agent acting on behalf of a licensee pursuant to proposed law, including an exemption to the Public Records Law.

Proposed law requiring a licensee to develop, implement, and maintain a comprehensive, written information security program does not apply to a licensee who is any of the following:

(1) Having fewer than 10 employees including independent contractors.

(2) Establishing and maintaining an information security program pursuant to the federal Health Insurance Portability and Accountability Act.

(3) An employee, agent, representative, or designee of a licensee, who is also a licensee, to the extent that the employee, agent, representative, or designee is covered by the information security program of the other licensee.

Proposed law authorizes the commissioner to do any of the following in the event of a violation of proposed law:

(1) Suspend, revoke, or refuse to renew the certificate of authority or license of any insurer,

person, or entity.

(2) Levy a fine not to exceed $1,000 for each violation per insurer, person, or entity, up to $100,000 aggregate for all violations in a calendar year per insurer, person, or entity.

(3) Order any insurer, person, or entity to cease and desist any action that violates any provision of proposed law.

(Amends R.S. 44:4.1(B)(11); Adds R.S. 22:2501-2510)