Dickie McCamey
ATTORNEYS AT LAW

3/22/2016 | Articles

NAIC Cybersecurity Task Force Model Law

The Cybersecurity Task Force of the National Association of Insurance Commissioners (NAIC) has proposed a comprehensive Model Law designed to regulate licensed insurers' handling of electronic data and investigation of breaches in electronic data security. Comments on the proposed model law are due by March 23.

Written Information Security Program

The Model Law requires licensed insurers to prepare written information security programs designed to protect personal information collected by the insurer. The plan, the Model Law suggests, should be proportional to the characteristics of the licensed insurer including the scope of the insurer's activities and the sensitivity of the consumer information collected.

Insurers are required to designate employees who can perform data risk assessment, i.e., identification of potential threats as well as the potential for damage from these threats. The Model Law suggests that insurers develop standards and methods from the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST).

The Model Law requires the insurers' board of directors to monitor security programs and to receive reports at least annually to determine the status of the insurer's security plan and compliance with the Model Law. Recognizing the involvement of third-party service providers, the Model Law mandates that insurers “select and retain third-party service providers that are capable of maintaining appropriate safeguards for the personal information at issue.” The law also mandates that the third-party providers "implement and maintain appropriate safeguards for the personal information at issue” (including those described above under “Implementation of a Written Information Security Program”) and “allow licensee or its agents to perform cybersecurity audits.”

Consumer Rights

The Model Law requires that insurers disclose to consumers the types of personal information collected and stored by the insurer and any third-party service providers involved. Insurers must make the policy available on its website and furnish hard copies of the policy on consumer requests.

After a security breach, the Model Law requires insurers to notify affected consumers no later than 60 days following notice of or identification of the breach. In what may turn out to be a murky area, notification is not required if the data in question is encrypted or the breach is not reasonably likely to cause substantial harm or inconvenience. Insurers are also required to offer to pay affected consumers for 12 months of identity theft protection.

There are additional notification requirements. Insurers must advise without delay law enforcement organizations, the insurance commissioner, payment card networks, and for certain breaches consumer reporting agencies. Notice to the commissioner must take place within five calendar days of discovering a breach. The insurer is also required to provide the commissioner with any draft written communications to consumers regarding an identified breach.

Oversight by Insurance Commissioners

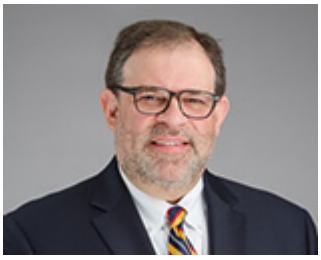
If the insurance commissioner has reason to believe that an insurer has violated the Model Law, the commissioner has hearing and subpoena power and can make a finding whether insurer has engaged in conduct breaching the Model Law. The commissioner also has power to issue cease and desist rulings based upon such findings and may also order monetary penalties.

The Model Law provides for a $500 penalty per violation up to a maximum aggregate of $10,000. For violation of commissioners' cease and desist orders, the Model Law calls for a penalty of $10,000 for each violation and possible suspension and revocation of the insurer's license. The Model Law allows for penalties of $50,000 for violations which occur with such frequency as to be determined to be a business practice.

Confidentiality

Presumably to encourage reporting under the Model Law, it provides that any information in the control or possession of a department of insurance furnished by a licensee shall be confidential and is not subject to open records laws or subpoena, thereby protecting the confidentiality and privileged nature of consumer information.

Whether the Model Law proceeds, and how it proceeds after the comment period, depends on whether the law receives majority support from within the NAIC following the comment period.



Charles E. Haddick, Jr.
717-731-4800
chaddick@dmclaw.com
@cjhinsurancelaw
blog: badfaithadvisor.com

© 2024 Dickie, McCamey & Chilcote, P.C. All rights reserved.