Crowe Horwath

Q&A

What's the Risk?

Navigating the NAIC's Insurance Data Security Model Law

With the passage of the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law (Model Law) in October 2017, insurers will need to develop, implement, and maintain a comprehensive written information security program that includes data security, investigation, and notification of breaches. The program, which should be part of the insurer's enterprise risk management process, must cover administrative, technical, and physical safeguards.

Although individual states may include compliance exceptions to the Model Law's guidelines for maintaining an information security program, insurers can begin using the Model Law as a standard to develop a compliant cybersecurity program.

Insurers of all sizes must review the NAIC's recommendations for cybersecurity. Hackers breached 54 percent of small- and midsize-businesses in the U.S. between September 2016 and September 2017.[1] In addition, 61 percent of small- and midsize businesses have fallen victim to a cyberattack in the past 12 months.[2]

Here are seven of the most important questions insurers are asking about the Model Law. The answers describe what insurers need to do now to facilitate the security of critical customer data.

1. What's the importance of performing a risk assessment?

The Model Law requirements are clear, but what the new standard does not provide are the detailed steps insurers need to take to achieve compliance. In fact, insurers must tailor their information security programs to their organizations. Each insurer's risk tolerance and business activities are unique, so the onus is on the insurer to assess its capabilities, strengths, and weaknesses, and then to identify areas of vulnerability and noncompliance. A risk assessment is the first step in identifying compliance gaps and developing the road map that will close those gaps.

A risk assessment helps insurers identify their sensitive assets, true risks, and the effectiveness of their controls. Cybersecurity is an investment, and an assessment helps insurers optimize their investments around compliance efforts.

2. May I just check the boxes and be in compliance with the Model Law?

Focusing on checking off the boxes rather than creating a culture of compliance that is implemented over time means an organization might not be able to take advantage of some cybersecurity benefits.

A cultural adaptation to the Model Law establishes that stakeholders are held accountable for compliance and that all employees understand their responsibilities in facilitating consistent compliance. Not only does this type of culture support compliance, it also prepares the organization to adapt to changes in the Model Law and address future cybersecurity threats.

3. I'm a smaller insurer. How can I comply?

Although exemptions are available for very small insurers, the majority of insurers must comply with the Model Law standards. The standards are based on the size and complexity of an insurer's activities, including its use of third-party service providers.

Because small- and midsize insurers typically lack the cybersecurity resources of larger organizations, they will need to weave cybersecurity compliance into existing priorities and initiatives or hire a third party to develop, implement, and maintain the program.

The Model Law allows insurers to delegate their information security program development or the management of the plan to a third party. In this situation, the insurer must designate at least one internal employee to be responsible for the program.

4. How should employees outside of IT participate in cybersecurity management?

Cybersecurity is not just an IT issue. The Model Law requires that insurers provide employees throughout the organization with cybersecurity awareness training. In fact, 54 percent of cyberattacks are due to employee or contractor negligence.[3]

The more employees understand cybersecurity and their roles in protecting the insurer, the more successful an organization will be in carrying out its program. Getting employees up to speed will require cybersecurity awareness training to reflect new risks. Communicating that cybersecurity is not only a compliance matter but an enterprise imperative and that employee actions can put the insurer at risk will help build awareness of the importance of cybersecurity across the organization.

The Model Law requires written attestation of compliance. Whether an insurer maintains the program internally or uses a third party, it needs to be able to relay the status of information security in a manner the board and senior leaders can understand.

Technology often is necessary to protect an organization from cyberthreats, but ultimately people are the key to success or failure of the information security program.

5. We use a large number of third-party providers. How can we verify they are compliant?

The Model Law requires that insurers apply due diligence in selecting third-party service providers – an important point when considering that 43 percent of cyberattacks are caused by third parties.[4] An insurer must require that third-party providers implement measures to protect and secure their information systems because the insurer is liable and must take full responsibility for any breaches.

Verifying compliance of third parties involves multiple activities that include identifying third parties with access to sensitive information, assessing their risk level, and determining the effectiveness of their programs.

6. What are the requirements for the incident response plan?

The Model Law requires a written incident response plan that includes certain criteria, such as the internal process for responding to a cybersecurity event, clear roles and responsibilities, and remediation. There are also requirements for external and internal communications and information sharing with regulators and law enforcement.

It is not enough to have a written plan: Insurers should test incident response capabilities periodically as well. Without testing, insurers will not truly know if they are capable of responding efficiently to thwart an attack, stem the damage, or fully comply with the timeliness of reporting requirements.

7. How often do I need to address cybersecurity compliance?

The Model Law states that insurers must provide annual certifications of compliance. This certification requires periodic reviews to assess the effectiveness of the controls, systems, and procedures of their information security programs. However, insurers should deploy technology or use a third party to log and monitor their cybersecurity activities for threats and vulnerabilities.

It also is important to keep employees aware and diligent through ongoing training and role-based instruction.

Conclusion

Crowe Horwath LLP can help your organization comply with the NAIC Insurance Data Security Model Law. We can assess your current state with our two-day health check and develop a road map that helps align your information security program with your business model, resources, and desired future state.

Crowe Horwath

Learn More

For more information on NAIC Insurance Data Security Model Law offerings from Crowe, contact:

Glenn Saslow, Partner
+1 860 470 2103
glenn.saslow@crowehorwath.com

Troy La Huis, Principal
+1 616 233 5571
troy.lahuis@crowehorwath.com

---

1 Ponemon Institute, "The 2017 State of SMB Cybersecurity" infographic, September 2017.

2 Ibid.

3 Ibid.

4 Ibid.

crowehorwath.com