

NAIC Cyber Model Law Support Program

As of October 24, 2017, the National Association of Insurance Commissioners (NAIC) approved a model law that directly impacts a licensee. “Licensee” means any Person 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 or a Licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction

In an effort to meet the needs of the insurance sector, HEMISPHERE Cyber Risk Management, LLC (HEMISPHERE) has designed a packaged solution tailored for licensees to meet these new requirements.

Each licensee is required under this model law to have a written information security program that describes the business processes of protecting non-public information such as social security numbers, driver’s license numbers, financial account numbers, security codes, passwords, or even biometrics.

The written program must be accompanied by a risk assessment that defines who is responsible for the information security program (internal resource or outsourced), properly identify threats that may result in the unauthorized or unapproved release of non-public information held by the licensee, conduct a damage assessment, review the sufficiency of any existing or proposed policies & procedures, and evaluate the effectiveness of the licensee’s ability to detect, prevent, and respond to an cyber incident through both technical and operational mechanisms.

As of 2015, there were approximately 1.07 million insurance agents. Many of these agents rely upon having free antivirus software and generally are self-reliant in managing their client’s non-public records. Statistically, over 60% of small business owners close down after a cyber incident.

HEMISPHERE has worked closely with the NAIC’s Cyber Working Group and understands the stated goals and objectives of this model law. With the launch of recent cybersecurity requirements from the State of New York’s Insurance Commissioner, the regulatory landscape is becoming increasing more complicated to independently manage. Our NAIC Model Law Support Program is designed to rapidly enable adherence while simultaneously transferring the risk of operating and managing an information security program.

When business owners hear “cybersecurity” they generally believe it is very costly. HEMISPHERE specializes in helping small and medium size business owners across the United States address cyber risk in the most cost effective means available on the market today.

Call us for a free consultation today at (703) 881-7785 or email us at contact@hemispherecyber.com.



Your Gateway To Cyber Risk Management

www.hemispherecyber.com

Insurance Cyber Risk Solutions



- ⇒ Easy to implement
- ⇒ Actionable
- ⇒ Lowers your operations cost
- ⇒ Improves your risk surface

HEMISPHERE’s robust framework positions our clients for success. We accomplish this by applying lessons learned from other’s mistakes. This enables reductions in your total cost of ownership and enhancing operational fidelity.



**Making Cyber Risk
“Operationally Relevant”**

Implementing Cyber Risk Management as a “Cost-Avoidance” Mechanism



Your Gateway To Cyber Risk Management

www.hemispherecyber.com

NAIC Cyber Model Law Support Program

To meet the needs of the insurance sector, HEMISPHERE has designed assessment and monitoring solutions that allow licensees to focus on their business operations.



Today’s business environments can no longer afford to focus on trying to defend against highly organized, well-funded, and highly skilled adversaries by simply using antivirus and perimeter defense techniques. Providing higher assurances of operational fidelity can only be achieved through a strategy ensuring you have the capability to identify, protect, detect, respond and recover.

Service	Traditional Assessment	HEMISPHERE
Pre-Site Analysis	X	X
Onsite Technical Assessment to identify gaps when measured against NAIC Model Law	X	X
Vulnerability Scan (Nessus)	X	X
Business Risk Analysis of scan results		X
Certificate of Assessment		X
Legal/Litigation Exposure Analysis		X
3rd Party Business Partner Risk—SLA and T&C gap analysis*		X
Cost-Benefit Analysis to determine “reasonableness”		X
Provide Policy and Procedure templates with easy to understand video instruction for each		X
Formal Debrief to Ensure Knowledge Transfer with C-Suite		X
Managed Detection and Response Solutions		X

* SLA—Service Level Agreements T&C—Terms and Conditions

Our clients consistently see reductions in operations cost when using our resources when compared to attempting similar capabilities on their own.