eSENTIRE

CHECKLIST

Cyber Risk in the Insurance Sector

How eSentire helps your organization map your security program against the NAIC Insurance Data Security Model

As part of the insurance industry and its supporting ecosystem, a combination of business factors and security vulnerabilities increase your cyber risk and make your organization a high-profile and lucrative target for ransomware gangs and other bad actors fuelling the cybercrime economy:

- The application and claims processes require insurance carriers, agents, and brokerages to manage an unparalleled volume of valuable PII, financial accounting details, and protected healthcare information (PHI).
- The shift to online or app-based customer self-service and even live-data tracking technology deployed on hybrid cloud platforms and legacy back-end infrastructure creates new potential exploitation opportunities and increases the attack surface.
- Criminals view the insurance industry as weakly defended targets and understand how to attack you with proven methods that lead to massive ransomware outages, public exposure, and crippling reputational damage.
- Attackers intentionally exfiltrate client data from your business and then use that stolen policyholder information to identify your lucrative customers, create lures guaranteed to ensnare their targets, and even negotiate ransoms that fall within the client's coverage.

Where Every Insurer Should Start: Using the NAIC Insurance Data Security Model Law as a Guide

The National Association of Insurance Commissioners (NAIC) drafted the Insurance Data Security Model Law in reaction to data breaches involving large insurers. Following this effort from the NAIC, several states adopted and put into effect laws to formalize insurance data security protections for all insurance licensees.

While the purpose of the NAIC Model Law is to establish standards for data security and breach notification for licensees, it also serves as a good framework to start from as your organization looks to develop an end-to-end cybersecurity and incident response plan that will ensure data security and prevent business disruption. eSentire has broken down the NAIC guide to provide tangible recommendations that can be leveraged as a Cyber Risk checklist in terms of service integration and adoption by insurers.

Core Components of the NAIC Model Law

Information Security Program	eSentire Support
Risk assessment Perform a vulnerability assessment of possible threats to the security of your information systems and data. You should assess the risk of these threats to your business and policyholders. Are your cybersecurity measures sufficient, and do you have a framework for recovery in the event of a breach?	✔ Managed Vulnerability Scanning ✔ Managed Risk Services for security strategy development, penetration testing and Security Incident Response Planning
Risk management Design your cybersecurity strategy to mitigate the vulnerabilities and risks identified. Implement the proper cybersecurity measures and periodically reevaluate your risk and attack surface vulnerabilities. Implement regular Security Awareness Training and phishing testing for your staff.	✔ Managed Phishing and Security Awareness Training ✔ Virtual CISO executive support in proactive cyber roadmap development
Oversight by a board of directors The board of directors should require that an organization implement and maintain a cybersecurity strategy. This should include reporting and an annual review of the program.	✔ Documented security operations processes ✔ Operational and executive level reporting
Address third-party service provider risk Insurers need to be aware of the risks that third parties and supply chain partners may pose if they are handling or storing sensitive data. You should choose providers that are trusted, and they should be required to implement data security safeguards of their own.	✔ Adherence to compliance requirements ✔ Third party risk security assessments ✔ Compromise assessment services
Monitoring and Adjusting Your organization should monitor and perform ongoing adjustments to your cybersecurity strategy as technology changes and new threats develop.	✔ 24/7 Security Event Monitoring, Threat Hunting and Response with Multi-Signal Managed Detection and Response ✔ Security Advisories and Threat Response Unit Intel Reporting
Incident response planning Perform security incident response planning that includes: • Incident Response Life Cycle Planning • Incident Response Policy Development	✔ Emergency Incident Response Services ✔ Incident Response Retainer offering with 4-hour remote threat suppression SLA ✔ Security Incident Response Planning services

Investigation, Incident Recovery, and Determination of Extent

If your organization experiences a cybersecurity breach, an incident response provider should determine:

- Whether a cybersecurity event has occurred
- The full extent of compromised assets and determine root cause
- The appropriate steps to return to service

Notification of a Cybersecurity Event

Know and understand what stakeholders need to be notified in the event of a breach:

- State(s) government
- Insurance commissioner(s)
- Affected customers and policyholders
- Third parties and supply chain partners

How eSentire Can Help

We are recognized globally as the Authority in Managed Detection and Response because we hunt, investigate, and stop known and unknown cyber threats before they become business disrupting events. We were founded in 2001 to secure the environments of the world's most targeted industry - financial services. Over the last two decades we have scaled our cybersecurity services offering to hunt and disrupt threats across every industry on a global scale. With two 24/7 Security Operations Centers, hundreds of cyber experts, and 1000+ customers, across 70+ countries, we have demonstrated the ability to Own the R in MDR with a Mean Time to Contain of 15 minutes. While many companies focus on detection, we recognize that there is no end to cyber risk. Preventative technologies will be bypassed, and defenses will fail. That's why eSentire prioritizes Response. Our MDR is really MDR3 - Response, Remediation and Results.

We proudly protect some of the leading insurance-related companies. We would welcome the opportunity to outline how we can help defend your firm with advanced detection, 24/7 threat hunting, deep investigation, and end-to-end coverage that protects your organization and policyholders.

Our cybersecurity services include:

Managed Risk Services

Strategic services including Security Assessments, Managed Phishing and Security Awareness Training and Managed Vulnerability Scanning to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

Managed Detection and Response

By combining our cutting-edge XDR platform, 24/7 threat hunting and security operations leadership, we hunt and disrupt known and unknown threats before they impact your business.

Digital Forensics and Incident Response

Battle-tested Incident Commander level expertise driving emergency Incident Response, Security Incident Response Planning services and delivering an industry-leading 4-hour remote threat suppression SLA with our IR Retainer offering.

Reach out to learn more.

Get Started

If you're experiencing a security incident or breach contact us  **1-866-579-2200**

eSentire

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1000+ organizations in 70+ countries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Thre at Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.