NAIC Insurance Data Security Model Law

This whitepaper presents an in-depth examination of the NAIC Insurance Data Security Model Law, aimed at guiding insurance entities through the complexities of maintaining robust data security frameworks. It outlines the critical requirements and best practices for protecting sensitive nonpublic information, ensuring compliance with evolving regulatory landscapes.

Authored by
Eevabits

Introduction

The NAIC Insurance Data Security Model Law presents a framework to enhance data security in the insurance sector, emphasizing the need to protect consumer information and maintain data integrity and confidentiality. It requires insurance entities to establish comprehensive Information Security Programs (ISPs), conduct thorough investigations in response to cybersecurity incidents, and maintain transparent communication with both authorities and consumers. The law accentuates the responsibility of licensees to safeguard nonpublic information, undertake consistent risk assessments, and comply with the specified enforcement, exemptions, and penalties, ensuring effective compliance.

The NAIC Insurance Data Security Model Law was developed by the National Association of Insurance Commissioners (NAIC), which is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories. This Model Law was adopted by the NAIC in October 2017 during the NAIC's Executive (EX) Committee and Plenary meeting.

Since its adoption, the Model Law has started to be enacted by states across the U.S. Each state has the discretion to adopt the Model Law entirely or implement it with state-specific variations. As of January of 2024, 23 states have implemented the Model Law. Other states have engaged in related activities that reflect the principles of the Model Law, though they may not have adopted it in its entirety.

The future of the NAIC Insurance Data Security Model Law looks to be one of increasing relevance and adoption. As cybersecurity threats continue to evolve, states are likely to look to the Model Law for guidance in strengthening their regulations and protections around insurance data security. We can anticipate that more states will adopt or adapt the Model Law in the coming years, and it will serve as a critical foundation for industry-wide best practices in data security and consumer protection.

Developing a Comprehensive Information Security Program

An effective Information Security Program (ISP) is grounded in established security frameworks such as the NIST Security Framework, ISO 27001, or CIS 20, each offering structured approaches to cybersecurity risk management. In alignment with the NAIC Insurance Data Security Model Law, the following specific controls and automated processes are vital:

Identification:
Implement automated systems to inventory data assets and analyze existing access controls. Utilize content classification, Optical Character Recognition (OCR), and metadata scanning to pinpoint sensitive data, its size, and age, establishing data ownership based on user interaction with data assets.

Review:
Automate entitlement and data reviews in collaboration with identified Data Owners, enabling continuous auditing and refinement of access controls across the organization.

Define Standards:
Establish permission standards for both unstructured and structured data assets, outlining how data is shared and accessed, and defining controlled access protocols for users and administrators.

Audit:
Maintain systems capable of auditing user activities on data assets, encompassing all forms of data interaction, including modifications and permission changes.

Threat Identification:
Employ behavior tracking systems to detect potential malicious activities at any stage of an attack, from reconnaissance to exfiltration or data destruction.

Data In-Motion:
Manage the movement of data across the organization's network, utilizing data labeling to enforce movement policies or encryption at gateway points such as SharePoint Online, email systems, and endpoint workstations, including USB drive transfers.

By integrating these mechanisms into an ISP, insurance entities can ensure adherence to the NAIC Insurance Data Security Model Law, building a robust defense against cyber threats. This approach not only protects sensitive consumer information but also strengthens trust and integrity within the insurance industry, adapting to the evolving landscape of cybersecurity risks.

Key Takeaways

- **Automated Inventory and classification**
- **Continuous Auditing through Entitlement Reviews**
- **Establishing Permission Standards**
- **Proactive Threat Identification**
- **Data In-Motion Security**
- **Strategic Risk Management**

Strategic Risk Management within Information Security Programs

Risk Management is the cornerstone of a robust Information Security Program (ISP). An effective ISP is tailored to the organization's unique landscape, systematically addressing the multifaceted nature of cybersecurity risks. It is a continuous strategic process that involves assessing, mitigating, and monitoring risks, with a particular focus on safeguarding Nonpublic Information from emerging and evolving threats.

Assessing Risk:

Creating an effective Information Security Program (ISP) requires a proactive and systematic approach to risk assessment. This critical process is essential for understanding and mitigating potential threats to an organization's data integrity and confidentiality. Far from being a singular task, it's an ongoing effort that strengthens the ISP and enables it to evolve alongside the ever changing threat landscape that the insurance sector faces.

Proactive Oversight and Access Governance

The process begins by assigning a dedicated team or individual the responsibility of managing the Risk Assessment. This crucial role goes beyond mere identification of threats; it includes formulating and managing risk mitigation strategies. A deep understanding of the organization's structure, its data assets, and the supporting information systems is fundamental. A key aspect of this role is overseeing access controls, ensuring that only authorized individuals can access sensitive data, thereby reducing the risk of unauthorized disclosure.

Identifying Threats and Protecting Sensitive Data

It is vital to scrutinize data access levels to prevent excessive access rights, such as data being accessible by unauthorized departments, or worse, the entire domain through open access settings. Additionally, the exposure of sensitive data due to external access by third parties not governed by IT or through anonymous links significantly elevates the risk profile. Simultaneously, sensitive data that resides in unsecured locations or is subject to access risks calls for immediate attention. Equally important is the management of data retention; specifically, the oversight of stale data which, if left unchecked, increases the daily risk exposure and the overall liability should a compromise occur. These elements combined represent a spectrum of threats that must be identified and managed to protect sensitive data effectively.

Analyzing the Likelihood and Impact of Risk

The process of analyzing the impact of potential vulnerabilities hinges on understanding both the sensitivity of the data and the environment in which it resides. For high-impact data, such as personally identifiable information or trade secrets, its exposure can have severe repercussions. Likelihood analysis involves evaluating the conditions that increase the chance of a breach, with particular attention to access risks. For example, data stored on file servers with open access settings is particularly vulnerable, as it is exposed to the entire domain. In the scenario of a ransomware attack, such data is more likely to be compromised due to its accessibility.

This comprehensive risk assessment concludes with prioritized actions to mitigate identified risks satisfying NAIC requirements and solidifying the organization's overall information security posture.

Key Takeaways

- **Ongoing Risk Assessments**
- **Identifying and Managing Threats of Sensitive Data**
- **Analyzing Likelihood and Impact**
- **Quick Mitigation Wins Yields the Best Results**

Mitigating Risk:

Mitigation is a pivotal phase in Risk Management that focuses on minimizing the potential impact of identified risks. The first step is to prioritize risks, focusing on 'quick wins'—those mitigations that can be achieved swiftly and with minimal effort but have a significant positive effect on security. This tactic not only fortifies the organization's defense against the most immediate threats but also provides visible improvements that can enhance stakeholder confidence.

Start with a plan:

In planning the mitigation objectives, it's critical to devise a comprehensive strategy that details the action items, resource allocations, milestones, and responsible parties. This plan acts as a roadmap, guiding the execution phase and ensuring that each mitigation effort is systematically approached and tracked. Effective planning also involves forecasting potential roadblocks and planning contingencies for them.

Stay close to the business:

The role of Permission Entitlement and Data Reviews becomes an essential collaborative effort between IT and key business users. These reviews are crucial in not only reinforcing access controls but also in safeguarding business processes from disruptions during remediation efforts. In conjunction with regular communication, which is vital to successful mitigation, these reviews ensure transparency and align security initiatives with business objectives. Educating stakeholders about the impact of each mitigation action helps integrate security measures seamlessly into business operations, thereby enhancing the organization's resilience and ensuring that security enhancements are made without compromising business functionality.

Put your efforts to work:

Execution of the mitigation plan requires disciplined implementation and a keen eye for detail to ensure that all measures are enacted as intended. It's during this stage that the theoretical planning is put to the test, and adjustments may be required to address any unforeseen challenges.

Keep an eye on things:

Finally, support and maintenance are crucial once the mitigation strategies are in place. Continuous review and adaptation of the strategies are necessary to cater to the evolving threat landscape and the changing needs of the business. This includes regular updates to security protocols, refresher on access governance, and re-evaluation of the risk priorities. Robust support ensures that the mitigation measures not only remain effective but also improve over time.

Key Takeaways

- **Prioritization of Risk**
- **Strategic Mitigation Planning**
- **Collaboration Between IT and Business Units**
- **Educating Stakeholders**
- **Disciplined Execution**
- **Continuous Support and Process Improvement**

Mitigating Risk:

Monitoring risk is an ongoing and dynamic component of an Information Security Program that ensures the continued effectiveness of risk management strategies. It involves constant vigilance through continuous monitoring of the IT environment to detect any unusual activity that could indicate a threat, such as ransomware or other malicious software. This process includes regular audit activities to examine user behavior, looking for deviations from established access control standards and checking for misconfigurations, like unintentionally granted open access, which could lead to data breaches.

Auditing extends to the oversight of sensitive business accounts within critical departments such as HR, Legal, Finance, and Accounting. These accounts often have elevated access to sensitive data and require close scrutiny to detect any inappropriate access patterns or transactions. Monitoring the placement, movement, and access of sensitive data helps in identifying unauthorized data handling or data leakage.

Administrator accounts, given their broad privileges, are also under tight surveillance to detect any abuse of rights or potential inside threats. By keeping a close watch on these accounts, organizations can quickly respond to any red flags that surface, thereby maintaining a robust security posture and reinforcing the culture of compliance and vigilance across the business.

By maintaining rigorous monitoring protocols, organizations can detect, analyze, and respond to risks in real-time, preserving the integrity of their Information Security Programs. This continuous process not only safeguards against current threats but also prepares the enterprise for future challenges, reinforcing a culture of proactive security and resilience.

Key Takeaways

- **Regular Audits and User Behavior Analysis**
- **Focused Oversight on Sensitive & Privileged Accounts**
- **Monitor Data Access and Movement**

Information Security Program Oversight

The governance of an Information Security Program (ISP) is paramount, often falling under the purview of the Board of Directors. Their role involves ensuring the establishment, execution, and ongoing refinement of the ISP, setting a tone at the top that prioritizes cybersecurity within the organization's culture. This oversight is critical in aligning the ISP with the strategic direction of the company and ensuring that cybersecurity is not an IT issue alone but a board-level concern.

Furthermore, the board mandates an annual review of the ISP, assessing its effectiveness and compliance with relevant acts and regulations. This encompasses a review of risk assessments, risk management strategies, relationships with third-party service providers, and the efficacy of response plans to cybersecurity events. Such comprehensive reporting fosters transparency and accountability, encouraging a proactive stance on potential security challenges.

Within this structure, the board requires not just reports, but insightful analysis and strategic responses from management. This enables informed decision-making and resource allocation to bolster the ISP, ensuring it remains robust in the face of evolving cyber threats and aligns with the organization's risk appetite and regulatory obligations.

Key Takeaways

- **Strategic Alignment with Company Goals**
- **Annual Review and Compliance**
- **Transparency and Accountability**
- **Insightful Analysis and Strategic Response**

A Commitment to Robust Data Security

The NAIC Insurance Data Security Model Law outlines a future-proof framework to enhance data security in the insurance sector. This legislation mandates comprehensive Information Security Programs (ISPs) to protect consumer information and maintain the integrity and confidentiality of data. Insurers are compelled to establish ISPs, perform thorough cybersecurity incident investigations, and uphold transparent communication with authorities and consumers. Adherence to this law ensures the safeguarding of nonpublic information and the consistent evaluation and mitigation of risks, fostering a culture of compliance.

Eevabits, with its comprehensive suite of services including Data Risk & Security Assessments, stands ready to assist organizations in not only conducting thorough assessments but also in developing and maintaining robust Information Security Programs.

Eevabits distinguishes itself as a trusted advisor, leveraging its partnership with Netwrix and grounded in industry best practices, to help businesses navigate and fortify their data security postures. With a focus on safeguarding sensitive data and ensuring compliance with evolving regulations, Eevabits provides customized, proactive solutions. This partnership ensures that the steps from assessment to continuous monitoring and risk mitigation are not just strategic actions but also practical and actionable pathways to strengthen an organization's resilience against cybersecurity threats.