The Expanding Security Risks and Trends that Are Changing the Insurance Industry
Exploring Cyber Risk Vulnerability Management Solutions
Table of Contents

- Executive Summary 1
- Cyber Risk Trends and Challenges 2
  - Weaponizing Vulnerabilities 2
  - Insurtech and Digital Transformation – The Expanding Attack Surface 2
  - The NAIC Data Security Model 3
  - Board-Level Attestation and Accountability are Clearly Stated 3
  - South Carolina’s Insurance Data Security Act 3
- The RiskSense Solution 4
  - Vulnerability Data Management and Prioritization 4
  - Built-In Intelligence for Vulnerability and Threats 4
  - Attack Validation Services 5
  - RiskSense RS3 Security Score Reports 5
- Next Steps 6
Executive Summary

Cyber risk is a growing concern for today’s insurance entities. Hostile intruders and adversaries are increasingly weaponizing vulnerabilities and using insurance markets to gain personally identifiable data with high ‘sell’ value.

Insurance companies are also adopting a variety of new digital transformation solutions, including intelligent sensors for homes and automobiles, and other IoT devices. They are also broadening their product lines with a growing service and partner ecosystem and emerging InsurTech providers. Although these new technologies are enabling insurance entities to modernize their engagement with existing customers and expand into new markets, they are also greatly expanding the vulnerability attack surface.

Identifying and prioritizing the massive amount of potential cyber risks is a serious challenge for IT organizations. The sober reality is that the current standard of vulnerability remediation action based on criticality is not enough, the run rate of vulnerabilities is growing, and security teams can no longer rely on this heuristic approach to ensure they are addressing organizational cyber risk. Just as insurance products are leveraging enhanced analytics and up-to-the-moment risk and data assessments, cybersecurity teams also need a faster way to prioritize the vulnerability management actions that really can make a measurable difference in protecting the confidentiality of consumer data.

This document will examine the cyber risk trends that are of concern to the insurance industry, and introduce the RiskSense solution designed to address these challenges.
Cyber Risk Trends and Challenges

Weaponizing Vulnerabilities

The insurance industry is increasingly under attack from a variety of hostile intruders, and hackers are relentlessly exploiting common vulnerabilities. The latency between known vulnerability, exploit, and weaponized exploit is shrinking. Some software vendors are releasing patches with more frequency to ward off this activity, while other vendors still struggle. RiskSense has determined that this process of releasing security patches often takes upwards of 108 days. Determining vulnerability prioritization has to consider weaponization, especially when managing sensitive customer information.

Thousands of new cyber risk vulnerabilities are disclosed to insurance firms every year, and knowing which ones must be immediately patched or mitigated has become a major challenge for security teams. Fixing thousands of vulnerabilities is not even possible for most organizations. Insurance entities need to make sure they are fixing the right vulnerabilities, at the right time. The reality is that vulnerability prioritization and weaponization prediction require significant time, along with extensive data and domain expertise, beyond the skillsets of most corporate security teams.

As an example, digital sensor technologies and other telematic data capture devices can record driving patterns and provide the ability to track a driver's on-road behavior. The use of this technology is enabling the introduction of usage-based insurance (UBI) policies, also known as pay as you drive (PAYD) or pay how you drive (PHYD). The costs charged to consumers are dependent upon type of vehicle used, driving behavior, mileage, and geographical location. UBI has gained a lot of traction in the insurance industry, because it has the potential to generate substantial benefits of reducing policy administration and claims costs, while enabling personalized risk-based policy pricing.

Many other areas within policy and claims insurance are branching out to adopt usage-based technology. Although all of these new technologies are revolutionizing the insurance industry, they are also dramatically increasing the attack surface for these companies and the likelihood of cyber attacks. Customers' private data is vulnerable to exposure in an industry that already has one of the highest cyber breach incidents. While each individual carrier is forging its own path toward the future, the segmented vendor technology that supports the company's vision can quickly weaken their profitability and reputation. This is especially true if the vendor is unable to deliver patches for vulnerabilities ahead of exploit weaponization, and the connected services and partners are leaving themselves open with less than ideal vulnerability management.

Insurtech and Digital Transformation – The Expanding Attack Surface

Insurtech refers to the technology innovations poised to increase operational efficiency and drive digital transformation in the insurance industry. The emergence of insurtech innovations and the increasing number of companies associated with this segment is putting pressure on the traditional carriers. New relationships and speed to market are focused on the overdue need for innovation and technology improvements to keep up with customer demands.

The past use of environments that were monolithic, contained, and fully controlled by the insurance companies is no longer. As they move forward, carriers face a more complex life cycle of threats and vulnerabilities as they adopt new technology features and business models.
The NAIC Data Security Model

To combat the mounting cyber breaches in the insurance industry, The National Association of Insurance Commissioners (NAIC) released its Insurance Data Security Model in October of 2017, to provide best-practice cybersecurity guidelines for all insurance companies. The Model guides insurance organizations to create and conduct:

1.) Regular, planned cybersecurity testing;
2.) Board-level involvement and responsibility with a company’s information security program; and
3.) Incident response plans for specific breach notification procedures.

Although the Model is not enforceable at the national level, and no state or territory can be compelled to adopt it, the Model does become binding when it is officially adopted by each state’s regulated jurisdiction.

Board-Level Attestation and Accountability are Clearly Stated

What stands out in the NAIC Data Security Model guidelines is the clear direction that an insurance company’s board of directors becomes directly accountable for the oversight of the cybersecurity program and all of its activities and results. Executive leadership and senior management are made solely responsible for all program governance activities and compliance reporting. Responsibilities include yearly attestation as to the regulated entity’s cybersecurity programs maintenance, compliance status, and any “material matters related to the Information Security program.” These consist of events such as non-compliant testing results and any identified violations. The insurance company’s board of directors and executive leadership may delegate these responsibilities, but there is no mistaking who is held accountable. This pragmatic approach to accountability is long overdue and offers real benefits in the form of increased attention by the corporate citizenry. It will, however, put a burden on the carrier’s security and IT teams as they will need to provide understandable metrics on how they are addressing cyber risk to non-technical executives. This is something that continues to be difficult, regardless of industry.

South Carolina’s Insurance Data Security Act

South Carolina was the first state to adopt the NAIC Data Security Model on May 1, 2018, referred to as the ‘Insurance Data Security Act’. Among its many requirements, the Act creates rules for South Carolina licensees (defined as insurers, agents, and other licensed entities) regarding data security, investigation, and notification of a breach. It requires licensees to:

• Protect consumer information by safeguarding individual insurance policyholders’ personal information;
• Establish data security standards to mitigate the potential damage of a data breach;
• Develop, implement, and maintain a secure information security program, investigate any cybersecurity events, and notify the South Carolina Department of Insurance (SCDOI) of such events immediately; and
• Report a cybersecurity event to the department within 72 hours of the event occurring.

The NAIC is strongly encouraging all other states to follow South Carolina’s lead, enacting their own versions of the Data Security Model within the next three years. It’s clear there is pressure to have other states adopt these guidelines.
The RiskSense Solution

RiskSense has developed an innovative solution which enables insurance entities to modernize their cyber risk management activities. RiskSense’s game-changing approach to cybersecurity leverages intelligence-driven risk analytics to reveal cyber risk across a growing attack surface, quickly guide remediation, and monitor the results.

Key capabilities and benefits of the RiskSense solution include:

**Vulnerability Data Management and Prioritization**

Vulnerability scanning is time-consuming and requires expert analysis to identify next the best remediation actions. RiskSense significantly reduces the time it takes to digest and apply vulnerability scan results. Automated risk analysis of the vulnerability, criticality of exposed systems to the business, and current threat and vulnerability intelligence must happen to provide clear direction for patch coordination. A comprehensive view of IT cyber risk is obtained and can be used to guide specific security goals across departments, divisions, or types of systems. The platform provides a level of visibility that allows security departments to significantly reduce their attack surface, and makes security and IT departments more effective in protecting their business. Hours spent in this continuous activity of data management, researching findings, and vulnerability and threat intelligence gathering are provided through the RiskSense solution, delivering true risk-based vulnerability management.

**Built-In Intelligence for Vulnerability and Threats**

One of the guidelines of the NAIC Data Security Model is to provide ongoing threat and vulnerability intelligence. RiskSense has this capability built into the platform, automatically correlating and providing analysis of the most likely attacks. The RiskSense system is the most comprehensive in the industry, going beyond the standard US NVD database, using methodologies such as sourcing feeds from other countries, the vendor community, and from its own security analysts with deep knowledge providing penetration testing, writing exploits and providing best practice guidance to the industry. The numbers game of just patching vulnerabilities without context simply does not yield the results organizations need to see from a risk perspective. Bringing vulnerability data together with the context of what’s exposed within the carrier and what’s an active topic or exploit within threat intelligence is necessary. With over 100 sources of intelligence and deep-analytics, RiskSense delivers context clarity focused on what is most important to the organization.
**Attack Validation Services**

RiskSense Attack Validation Services (AI-assisted penetration testing) looks at all network, web applications, connected platforms, and devices across the organization. Deeply experienced pen testers/security analysts provide assessments that uncover vulnerabilities beyond automated penetration testing results. From critical enterprise environments, operational technology, and experience with Internet of Things (IoT) and connected devices, the service delivers exceptional results. Findings are shared with customers in near-real time through the RiskSense platform, enabling a carrier’s IT and security teams to take decisive actions immediately. This modern method of customer involvement reduces the time it takes to digest and delegate tasks to remediate the uncovered finding.

**RiskSense RS³ Security Score Reports**

With the new deadline for 72-hour breach notification looming, evidence that an organization is taking the best actions to protect and reduce cyber exposure will be needed. Executives and board members can no longer expect that an organization can address 100% of its IT vulnerabilities, because the environment and vulnerability landscape is too varied and the rate of exploits is growing too fast. The RiskSense RS³ Security Score allow organizations to track improvements, see how remediation is reducing their exposure, and identify where they are prone to risk. It enables them to set guidelines based on business sensitivity for different asset types, divisions, or systems associated with key growth initiatives. Much like a credit score, it can be used to reflect the achievement and progress toward an organization’s personalized security goals.
Next Steps

As the insurance industry adopts new technologies and IoT devices to support and grow their businesses, modernizing vulnerability management is a key requirement to stay ahead of cyber risk. The expanding attack surface is a reality. Digital transformation initiatives and growing cyber ecosystems make prime targets for weaponized vulnerabilities. Critical personally identifiable data is attractive to adversaries, and the growing segmentation of this market provides many different avenues to for them to automate their exploitation attempts.

RiskSense precision vulnerability and risk management delivers the most informed risk-based prioritization for maximizing the effectiveness of remediation resources. It identifies meaningful security weaknesses, improves IT collaboration, and provides immediate delivery of exposure findings through this cloud-delivered solution. Cyber risk is personalized, organizations can control and manage their security goals, validate their attack surface exposure, and in minutes, act to defend against weaponized exploits.

About RiskSense

RiskSense®, Inc. provides vulnerability prioritization and management to measure and control cybersecurity risk. The cloud-based RiskSense platform uses a foundation of risk-based scoring, analytics, and technology-accelerated pen testing to identify critical security weaknesses with corresponding remediation action plans, dramatically improving security and IT team efficiency and effectiveness. The RiskSense Platform® embodies the expertise and intimate knowledge gained from real world experience in defending critical networks from the world’s most dangerous cyber adversaries. As part of a team that collaborated with the U.S. Department of Defense and U.S. Intelligence Community, RiskSense founders developed Computational Analysis of Cyber Terrorism against the U.S. (CACTUS), Support Vectors Intrusion Detection, Behavior Risk Analysis of Vicious Executables (BRAVE), and the Strike Team Program.