Cybersecurity for Insurers: Squaring Safety With Service

A report by the
Insurance Information Institute,
in partnership with Fenix24

INSURANCE INFORMATION INSTITUTE

Affiliated with The Institutes

FENIX 24

Insurers occupy a paradoxical position in the cybersecurity landscape. While they assess cyber risk for policyholders, establish security requirements as conditions of coverage, and respond when incidents occur, they also are high-value targets due to the sensitive data they maintain and their systemic economic importance.

The cyber insurance market is growing. It reached $15.3 billion in 2024 and was projected to reach $16.3 billion in 2025 (Munich Re, 2025). While ransomware remains the leading cause of insured cyber losses, it accounted for only 19 percent of reported cyber claims in 2023, with 56 percent originating from business email compromise or funds transfer fraud.

According to NetDiligence (2025), business interruption accounts for about half of the $1 million average cost associated with ransomware incidents.

In light of this growth and evolution, the Insurance Information Institute (Triple-I), in partnership with Fenix24, conducted a series of conversations with insurance industry executives to share their insights on cybersecurity. Questions were designed to align with best practices, regulatory requirements, and security controls commonly required in cyber insurance underwriting.

Preparation Over Perfection

While these conversations were not academically rigorous, several consistent themes unified them. Most significantly, participants agreed on the need for systematic preparation; attention to changing conditions and threats; and continuous improvement in the absence of any single “perfect solution”.

The cyber challenge faced by any business – insurers or their policyholders – is in balancing performance and user experience with security. You could build a completely secure system, if it was completely walled off from any human or external network interaction. Clearly, that would not be useful.

Cyber risk must be thoughtfully addressed in ways that facilitate safe transactions without adding excessive friction to customer experience.

Immutable Backups

An “immutable backup” is a file that cannot be altered, protecting data against human error or malicious action. It should be part of any cyber resilience strategy. Most insurers interviewed said they implement immutable backups across critical system categories, including cloud data repositories, databases, email systems, file servers, foundational infrastructure, network configurations, and SaaS applications, but there is no universally accepted definition for an immutable backup. This can pose problems for insurers and their clients alike.

Most interviewees also reported meeting their established Recovery Time Objectives (RTO) for Tier 0 and Tier 1 systems. Such tests often are performed under ideal circumstances, calibrated to a single system. Best practices recommend testing across full network recovery scenarios. In IT security, Tier 0 is the highest, most restricted tier. It consists of core systems, like Active Directory domain controllers, identity management systems, and privileged accounts that grant administrative control over the entire network. Tier 1 includes systems that are business critical but not as foundational as Tier 0 assets.

Credentials and Access Management

All insurers in the discussions said they use corporate password vaults and demonstrate strong password complexity practices, with user passwords averaging more than 13 characters. However, several implement domain-joined SaaS accounts, creating single-point-of-failure vulnerabilities. Best practice favors using segmented identity architectures that reduce systemwide exposure.

All respondents said they require multi-factor authenticator applications or hardware tokens for administrative accounts, though some still allow confirmation methods like SMS messages, phones calls, email, and device push prompts. These methods are significantly stronger than not requiring MFA, but all have inherent limitations that are often exploited during security events.

Browsing Controls: Attack Surface Management

Most participants said they permit multiple web browsers across their environment, which can provide additional attack surfaces, requiring management, patching, and security configuration. However, most also implement Domain Name System (DNS) filtering at the network perimeter and block peer-to-peer file transfer websites and web-based e-mail systems. This reduces the ability of threat actors to reach their systems and is a good example of balancing security and performance.

Some companies use “split tunneling” – whereby employee Internet browsing occurs outside VPN encryption protection, potentially exposing employees to phishing, malware, and man-in-the-middle attacks. (Shea, 2020). Split tunneling improves user experience, but it can create additional exposure and reduce the accuracy of forensic investigations after a security incident. There is no single “right” approach, but it is essential to understand and mitigate the risks in whichever one your organization chooses.

Patching and Risk Management

All participants said they conduct penetration testing -- including Help Desk social engineering scenarios to help prevent cybercrime groups like Scattered Spider from talking their way into password resets (CISA, 2025). These practices reflect recognition that testing human defenses is just as important as testing technical ones.

All participants maintain automated patch-deployment systems, and approximately half of the participants deploy security patches monthly. In contemporary threat environments, adversaries often exploit newly disclosed vulnerabilities within hours or days of public disclosure. Best practice increasingly favors accelerated patch cycles, supported by tested emergency patching procedures. Governance structures should enable rapid decision-making when zero-day vulnerabilities emerge, balancing operational stability against escalating risk.

Conclusions and Recommendations

Insurers face the same cybersecurity adversaries as organizations across other sectors: Sophisticated threat actors target backups, exploit credential weaknesses, and move laterally through networks faster than most networks can react.

Demonstrating security practices that meet or exceed the standards they require from vendors and policyholders is critically important to meet regulators' expectations and promote public trust.

The difference between resilience and disaster lies not in perfect prevention but in systematic preparation, validated recovery capabilities, and organizational commitment to continuous security improvement. Organizations that prioritize recovery capabilities, conduct realistic testing, address identified gaps systematically, and maintain commitment to continuous improvement position themselves to withstand contemporary cyber threats.

Citations

CISA. (2025). Scattered Spider. *Cybersecurity Advisory*.

Marsh (2025). US cyber insurance market update: Rates decrease, threats evolve. *Insights*.

Munich Re. (2025). Cyber insurance: Risks and trends 2025. *Insights*.

NetDiligence. (2025). *Cyber Claims Study 2024*.

Shea, S. (2020). Is VPN split tunneling worth the security risks? *TechTarget Search Security*.

About Fenix24

As the world's leading breach recovery company, Fenix24 possesses unparalleled understanding of tactics employed by modern threat actors. The organization operates as the "world's first civilian cybersecurity force," comprising four specialized operational units: Fenix24™ (ransomware rapid response), Athena7™ (security assessments and planning), Grypho5™ (security-based management), and Argos99™ (data and infrastructure insights).

Fenix24 has developed Securitas Summa, the industry's only cyber resilience program that assures recoverability through integration of automated infrastructure mapping, managed protection, hardening and assessment, and battle-tested ransomware recovery into a unified defense platform. Learn more.

About Insurance Information Institute

The Insurance Information Institute (Triple-I) is a nonprofit research and communications organization supported by the insurance industry. Triple-I provides definitive insurance information for all audiences, serving as the insurance industry's trusted voice delivering expert data, analysis, and perspective on relevant issues. Learn more.