2026 Cyber Insurance Market Outlook

Gallagher

Introduction

As we reflect on the developments in the cyber insurance market in 2025, it is clear that the insurance industry continues to evolve rapidly in response to complex and emerging threats, regulatory changes, advancements in technology and evolving underwriting requirements. Today's cyber insurance market is a robust one and is projected to grow significantly. However, it is a market not without its challenges: Increased capacity has led to declining rates overall, most recently in the single digits. We are noting greater underwriting scrutiny in certain industry sectors, such as healthcare, where rate increases have occurred. While these trends seem poised to continue into 2026, the underwriting community has been continually reminded of the potential of systemic risks. Recent cloud outages and supply chain attacks have fueled this concern and have pushed the marketplace to an inflection point. Our 2026 Cyber Market Outlook outlines key trends and expectations for the cyber insurance market in the coming year and beyond, focusing on cyber claims trends, underwriting posture, reinsurance influence, privacy regulation and the growing influence of artificial intelligence (AI).

Authors:

John Farley, Managing Director, US Cyber Practice

Dan Burke, Senior Vice President, US Cyber Practice

The Current State

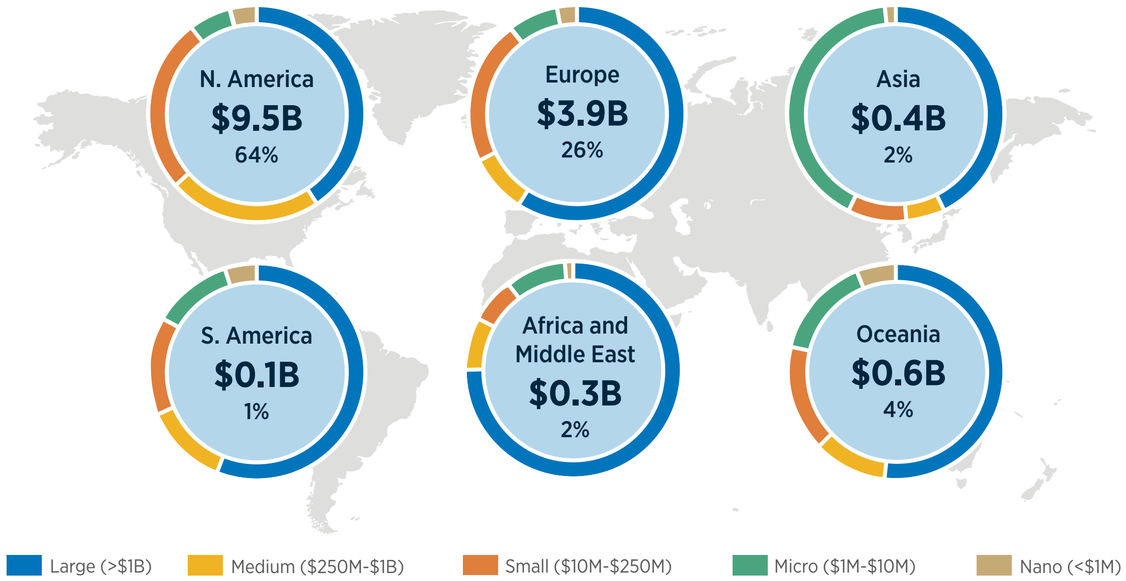
Global Cyber Insurance Market

Since the hardening of the cyber insurance market in early 2021, the global cyber insurance market has seen significant growth in gross written premiums GWPs. Demand for cyber insurance remains robust across geographies. Most forecasts for future growth agree that the 2025 market size of $16 to $20 billion could reasonably scale to $30 to $50 billion by 2030.[1]

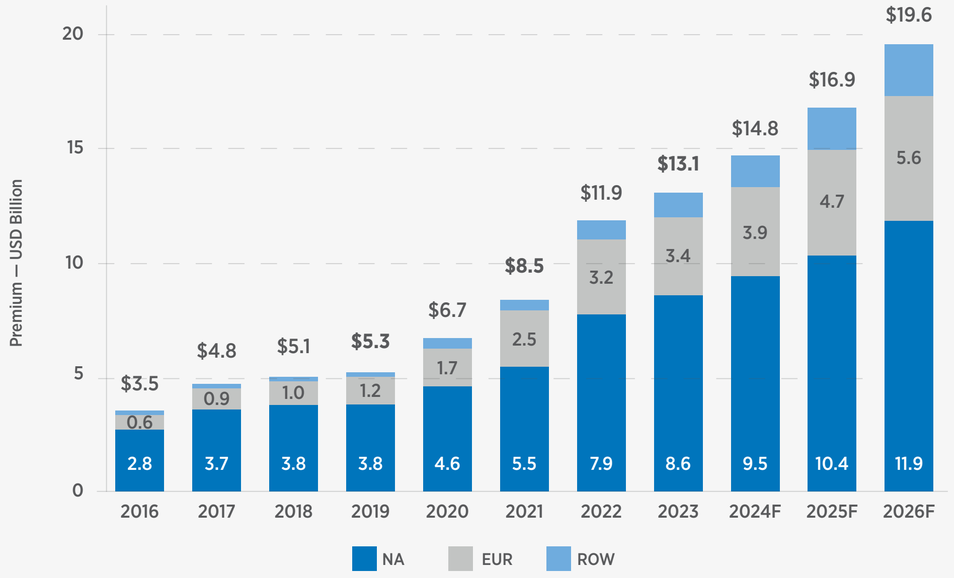
Higher growth rates in some longer-term outlooks reflect anticipated acceleration from AI risks, quantum computing threats and supply chain vulnerabilities. From a regional perspective, we expect North America to continue to dominate, with 60%-70% market share. Asia-Pacific is expected to see the highest growth due to rapid digitization and emerging regulations.

Cyber Market Spread and Growth Expectations

Gallagher Re Cyber Industry Database



Global Market Estimates



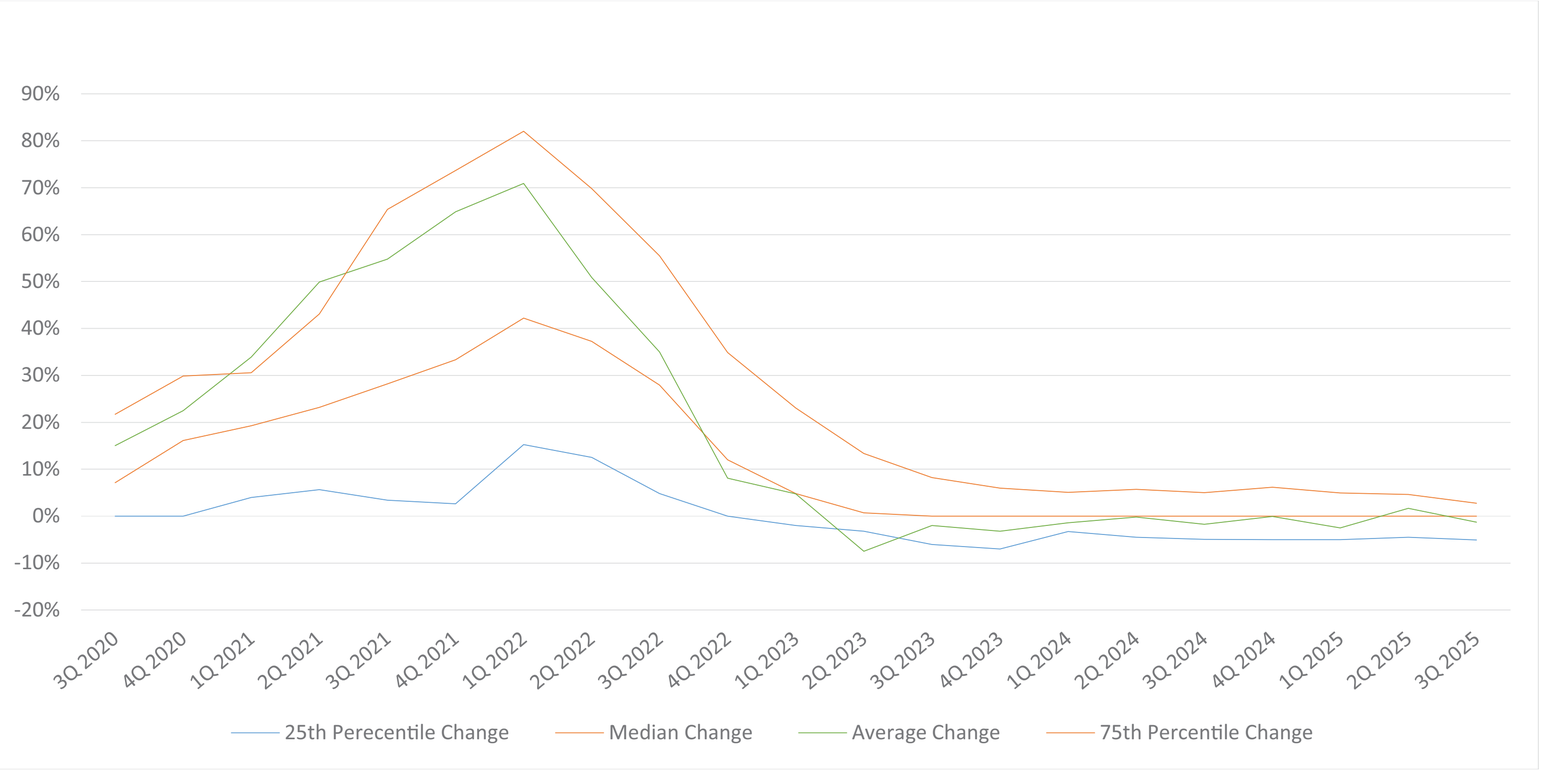
US Insurance market

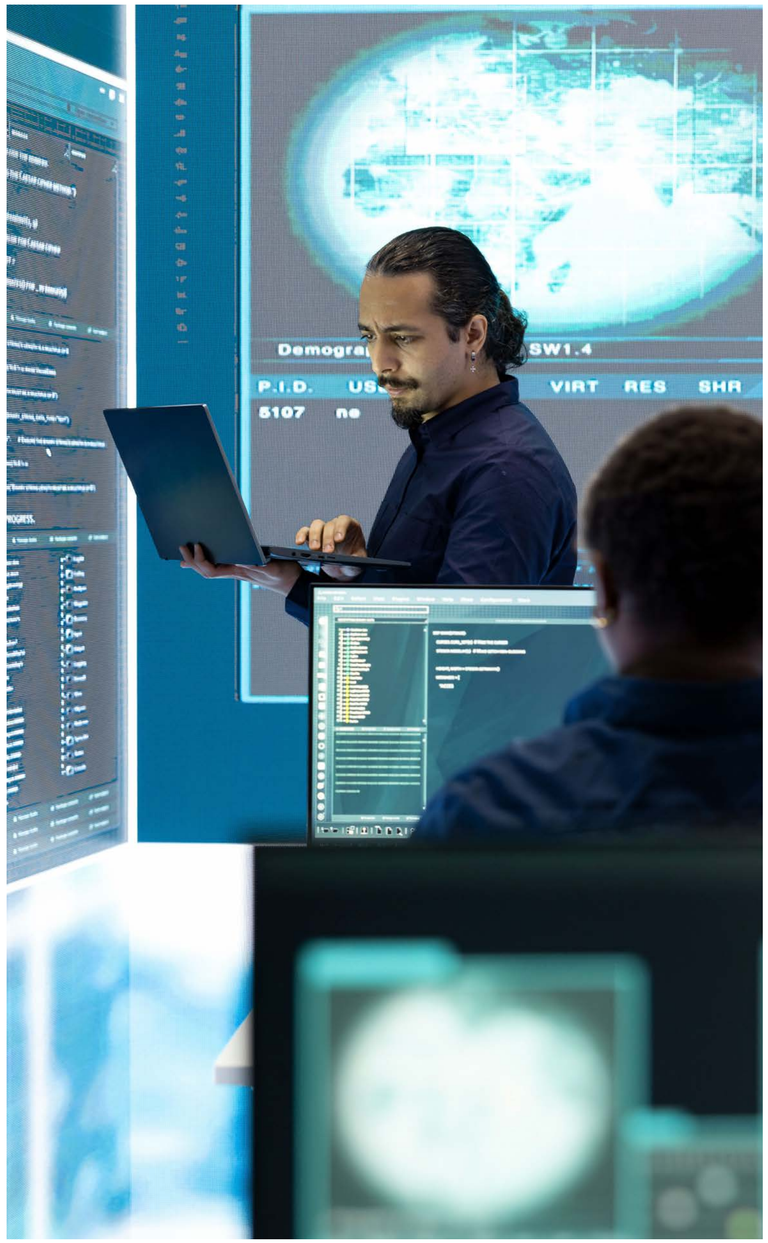
The cyber insurance marketplace continues to evolve to reflect concerns around new threats and advancements in technology. The softening market conditions that began three years ago mostly stabilized through 2025. Generally, cyber insurance buyers are experiencing flat prices. While we expect these trends to continue into at least the first half of 2026, we do note that the experience of our clients is industry specific.

The healthcare industry is an example of where competition is less fierce due to the claims environment, and that lack of competition is driving cyber insurance pricing slightly higher. At least one major carrier is taking a cautious approach to the healthcare sector, where rates have increased in single-digit percentages. Whether this is a bellwether to signs that the market may be reversing course remains to be seen.

Overall, cyber insurance pricing has retreated from the highs of the most recent hard market to levels more comparable to the very beginning of the hard market cycle in the first half of 2021. We attribute this to the market dynamics of carrier competition, as underwriters feel the pressure of lofty growth goals.

Cyber — Median, Average & 75th Percentile Over Time





Reinsurance market

Reinsurance continues to be a cornerstone, driving the growth and expansion of the cyber insurance marketplace by providing financial stability, risk-sharing mechanisms and capacity-building for insurers. The influx of capacity into the cyber insurance market that has precipitated the current competitive market conditions is driven by innovation in the cyber reinsurance market, including:

Insurance-Linked Securities (ILS): These instruments enable the transfer of cyber risk from insurers to capital markets, diversifying exposure across multiple investors.

Proportional Reinsurance Transactions: These agreements allow insurers to share a proportional amount of premiums and losses with reinsurers, effectively spreading risk.

Parametric Reinsurance: Payouts are triggered based on predefined parameters, such as outage duration as opposed to actual losses, to streamline claim adjudication.

Catastrophic Bonds (CAT Bonds): Designed to trigger payouts after extreme cyber events, these bonds are backed by capital markets, providing a robust safety net for insurers.

By leveraging these risk transfer mechanisms, cyber insurance carriers can offload a portion of their risk exposure to the broader capital markets, enhancing their ability to manage large-scale cyberthreats.

Moreover, the integration of advanced technologies, such as artificial intelligence and machine learning, into loss modeling and risk assessment processes could further enhance the efficiency and accuracy of reinsurance solutions. These technologies can analyze vast amounts of data to identify emerging trends and vulnerabilities, enabling more proactive risk management strategies.

The reinsurance market's role in the cyber insurance sector is not just about providing capacity but also about driving innovation and collaboration to address one of the most pressing challenges of the digital age.

Cyber Threat Landscape

According to the U.S. House Committee on Homeland Security,[2] the average cost of a data breach in the US was $10 million in 2025. Notable threat actor groups included:

DPRK Remote IT Workers: Nation-state actors associated with the Democratic People's Republic of Korea (DPRK) deployed undercover IT workers to infiltrate US companies by obtaining remote IT jobs.

Scattered Spider: A criminal organization used ransomware and data theft extortion schemes to launch financially motivated attacks on major global organizations.

Interlock: A threat actor who launched high-profile attacks against victims in the government and manufacturing sectors.

Salt Typhoon: Nation-state actors associated with China infiltrated backdoors at major US telecommunications companies and internet service providers.

Ransomware

Cyber claims trends in 2025 followed a similar pattern as previous years, with ransomware continuing to plague businesses of all sizes and industries. However, the tactics of threat actors have changed — moving from encrypting data to simply exfiltrating it.

Threat actors have leaned into the adage that data is more valuable to the company it was stolen from as opposed to a third party on the black market. Instead of extorting companies for payments to decrypt data, threat actors have resorted to threats of simply publishing sensitive data if extortion payments are not made. On a positive note, we are seeing a notable decline in the number of victims that agree to pay, and those that do are paying lesser amounts. Various studies show only 28% to 32% of victims paid ransoms in 2025, down from 37% in 2024.[3] When paid, average ransoms range from $1.2 to $1.8 million, a 10% drop from 2024.[4]

Various studies show only

28% to 32%

of victims paid ransoms in 2025, down from

37% in 2024.[3]

Supply Chain Attacks

Cyber incidents involving key players in the supply chain continued in 2025, and we see this as a persistent threat moving forward. Supply chain attacks typically target technology vendors and managed service providers. By infiltrating one of these providers, threat actors can impact all of the customers of the technology or managed service providers — creating potentially thousands of victims by launching a single attack.

In 2025, we've seen attacks launched against software-as-a-service (SaaS) companies, cloud providers and code repository companies — with a focus on compromising software updates, API integrations and authentication tokens.

These attacks highlight the importance of vendor risk management and implementing proper controls to assess the cybersecurity of your vendors as well as the business impact of an outage at key third-party vendors.

Non-Breach Privacy Violations

Perhaps one of the most alarming cyber claim trends involves losses related to website pixel tracking. We note a significant rise in litigation based on allegations around noncompliance with a variety of both recently evolving state privacy laws and decades-old laws, including California's Invasion of Privacy Act (1967), the Federal Wiretap Act (1968) and the Video Privacy Protection Act (1988). The plaintiff's bar has been adept at leveraging these statutes to launch class actions and mass arbitration demands — pursuing settlements and statutory penalties ranging from $250 to $10,000 per violation.[5]

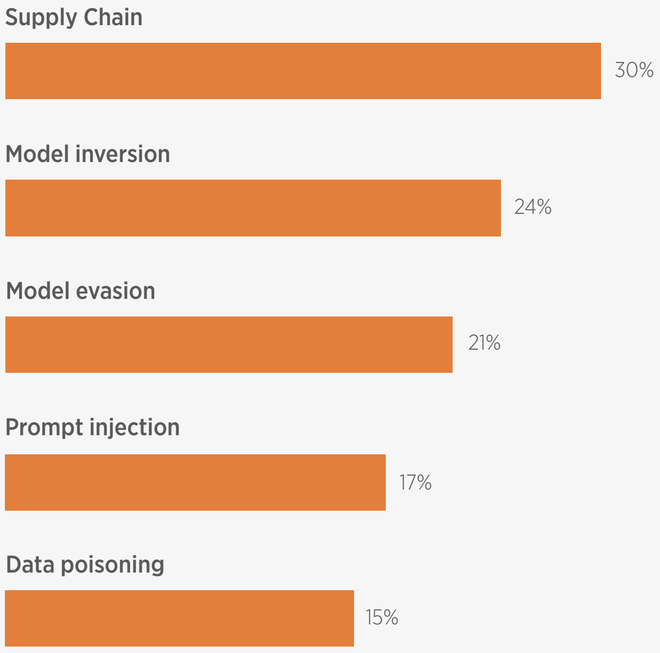
These claims have hit a broad swath of industries, including technology, healthcare, financial services and consumer-facing retail companies. Proper mitigation of this risk includes coordination between multiple stakeholders within a company — from legal and IT to marketing and product development teams.

Artificial Intelligence Claims

We are also beginning to see increasing evidence of AI-driven cyber losses. According to the 2025 IBM-Ponemon Cost of a Data Breach Report, several organizations are now reporting security incidents involving AI models and applications.

Supply chain compromise was the most common cause of incidents.

From organizations that reported a security incident involving an AI model or application; more than one response permitted



Source: IBM-Ponemon 2025 Cost of a Data Breach Report

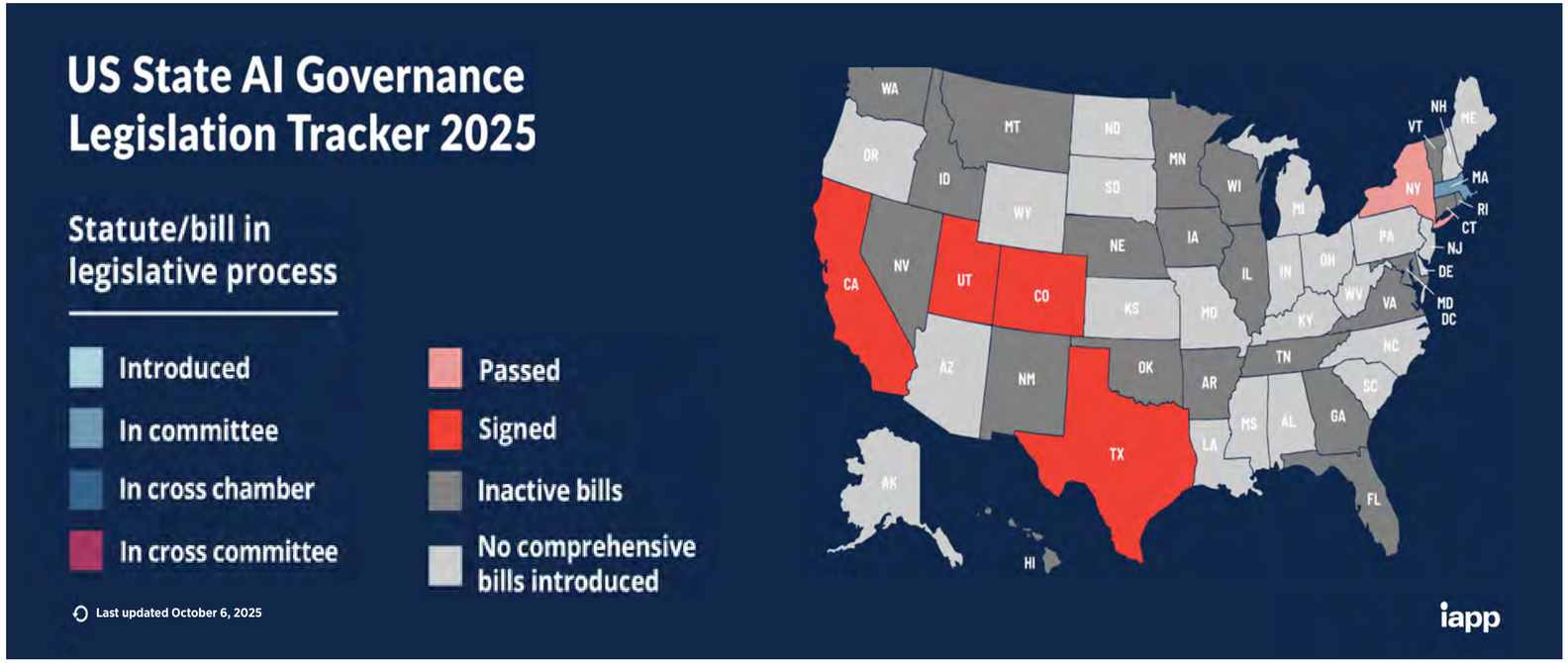
Regulatory Risk Landscape

The US cybersecurity regulatory landscape remains fragmented and complex. Federal executive orders, state-driven legislative action and industry-specific requirements continue to impose a dizzying array of obligations upon organizations.

At the federal level, threats against critical infrastructure remain a top priority. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which imposes a 72-hour incident reporting mandate, is slated to go into effect in May 2026.[6] Various executive orders reflect a focus on foreign cyberthreats and securing software in the supply chain through voluntary NIST-led guidance.

At the state level, 200 cybersecurity bills were introduced in 2025.[7] They generally focused on data breach notification, ransomware defense, critical infrastructure protections and privacy protections around the use of various tracking technologies. Enforcement is ramping up, with penalties for noncompliance and regulations that allow for private rights of action against organizations that fail to comply.

Regulation around the use of artificial intelligence remains nascent and decentralized. Tensions are emerging between a federal approach emphasizing innovation and the state's focus around risk mitigation specific to protections of basic human rights, transparency and explainability of large learning models. Many organizations are looking to NIST's AI Risk Management Framework[8] as the cornerstone to embedding AI risk management into enterprise risk management programs.



Looking Ahead to 2026

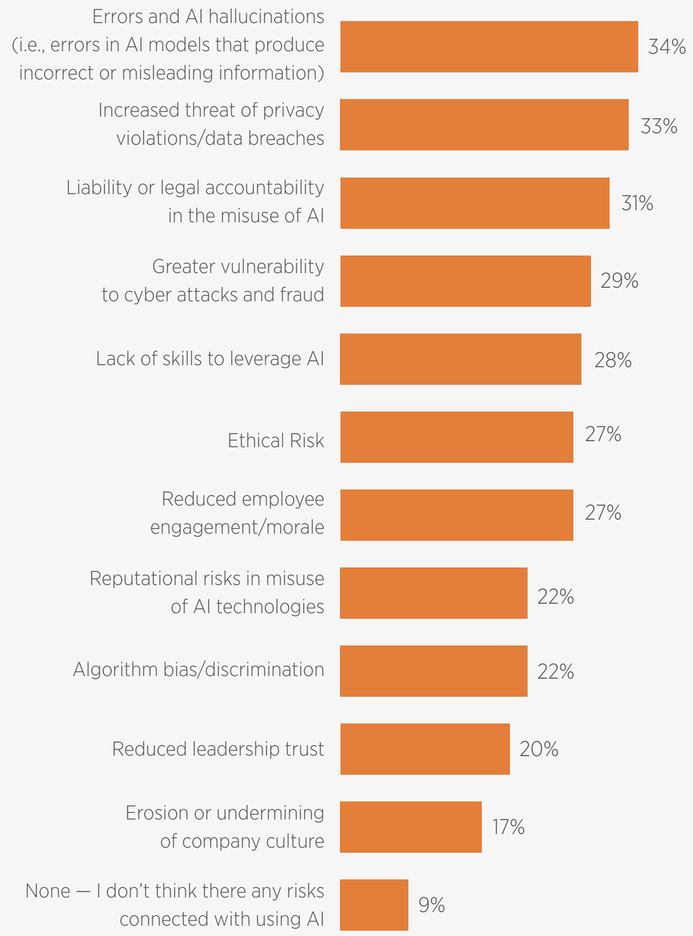
The cyber insurance market could hardly be described as predictable. As noted in this outlook previously, the current state of cyber is impacted by the reinsurance market and an influx of capacity in recent years, the competition between insurance carriers, and the rapidly adapting threat landscape. As we look to 2026, here are some areas that we expect to impact the cyber insurance market.

Artificial Intelligence (AI)

The sudden onset of AI-based attacks has driven the immediate need for more advanced cyber defense strategies. In fact, concerns were clearly revealed in Gallagher's 2025 Attitudes to AI Adoption and Risk Global Survey:

> Despite the benefits, business leaders are increasingly mindful of the risks of AI use in their business.

Perceived Risks With Using AI in the Business



Source: "Attitudes to AI Adoption and Risk Global Survey," *Arthur J. Gallagher & Co.*, 2025.

We expect more focus from underwriters in 2026 around AI risk management frameworks. These will be expected of both AI developers and adopters and will likely include:

1. Establishing Robust Governance Frameworks
2. Implement Transparent and Explainable AI Models
3. Explainable AI (XAI) techniques
4. Ensure Data Quality and Bias Mitigation
5. Enhance Security Measures
6. Adopt Ethical AI Principles
7. Consider New AI Leadership Roles: The Chief AI Officer
8. Revise Cyber Incident Response plans: The AI Incident Response Plan

Deepfake Technology and Social Engineering

Deepfake attacks use AI-generated audio, video or images to impersonate trusted individuals with alarming realism. These attacks are increasingly weaponized in phishing campaigns, where threat actors mimic executives or vendors to trick employees into authorizing payments or sharing sensitive data. Unlike traditional phishing, deepfakes exploit visual and auditory trust, making detection difficult and amplifying social engineering risks. As tools become more accessible, organizations face heightened exposure to financial fraud and reputational damage.

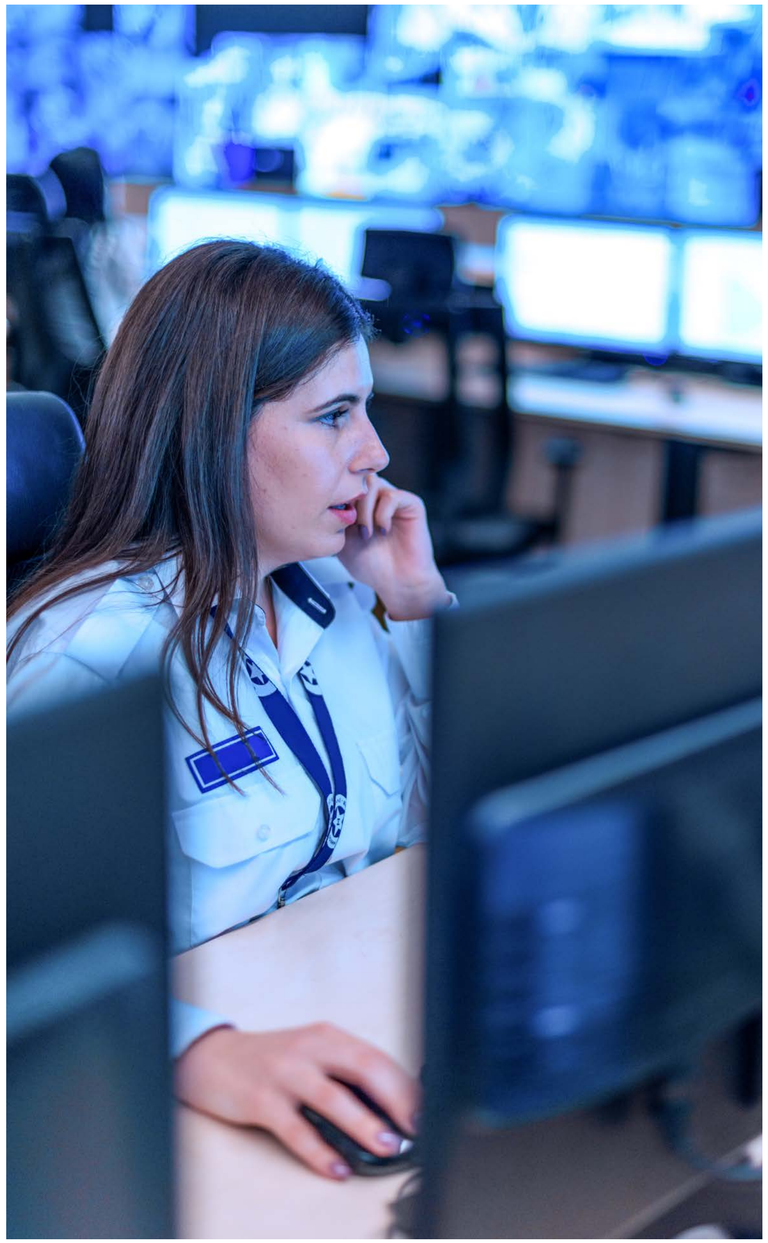
Social engineering attacks continue to be a boon for threat actors. Phishing/spoofing attacks topped the list of complaints reported to the FBI's IC3 division, with 193,407 complaints reported in 2024.[9] Total wire fraud losses in 2024 exceeded $109 million.[10] Given the low cost of entry to create these deepfake phishing campaigns and the success seen by threat actors in the past, we expect this attack vector to continue to be a prominent source of cyber risk in 2026.

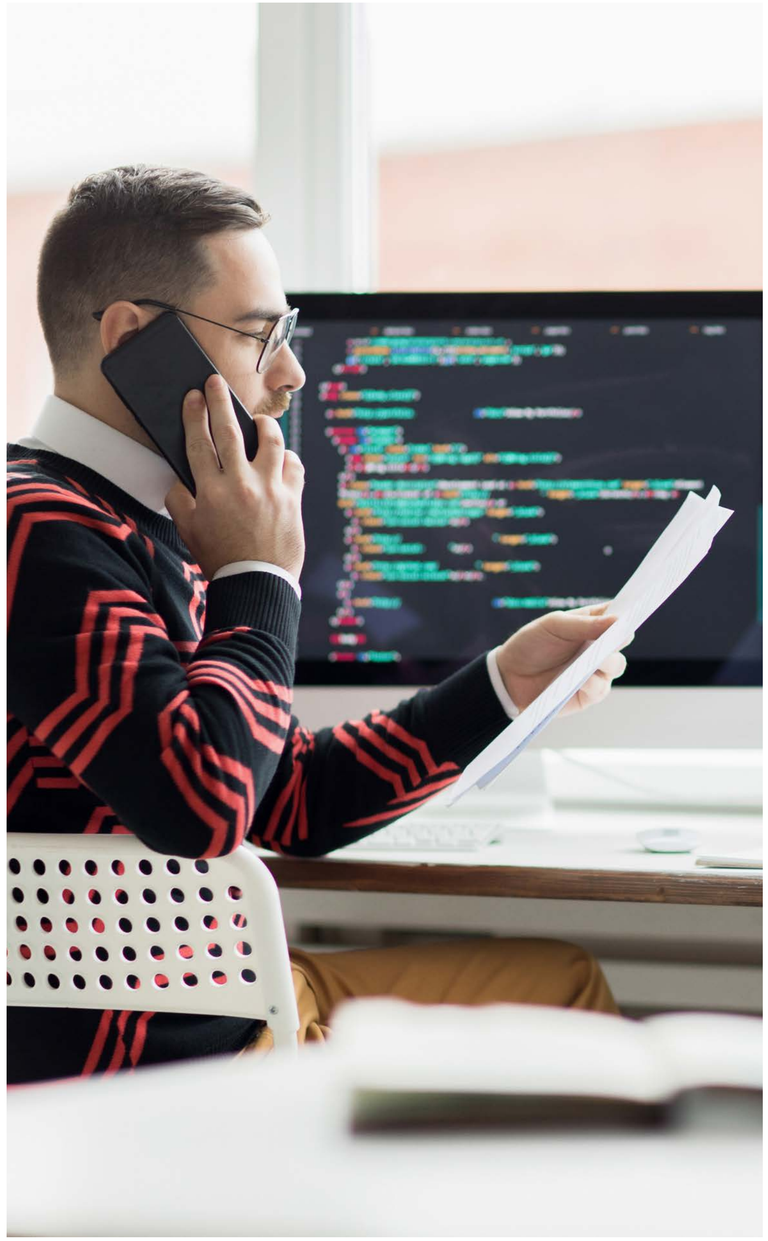
Insurance Coverage

Amidst the competitive environment, carriers are grappling with policy wording as they relate to a few key exposures:

Cyber risk in the supply chain

2025 saw several high-profile incidents involving cyber attacks on key software providers in the supply chain as well as system failure for two global cloud providers within days of one another. While none of these incidents led to a dreaded "systemic" cyber event, carriers are modifying policy language to reflect concerns. Carriers offering coverage for contingent business interruption losses may require an insured to have a written contract with the vendor that is impacted by the supply chain loss. Without it, exclusionary language may be imposed. Further, some carriers are limiting contingent business interruption coverage for losses sustained by IT vendors, with losses incurred by non-IT vendors excluded. Finally, cyber insurance buyers should pay attention to time element coverage wording, including "waiting period," "qualifying period" and "period of interruption." These terms, and the way they are specifically defined, can significantly impact recovery for costs related to business interruption and extra expenses.





Non-breach privacy claims

Underwriters are also cautious to cover non-breach privacy claims. Claims related to wrongful data collection, especially involving website tracking technologies and biometric data, are becoming more prevalent. These allegations are rooted in various state laws that continue to evolve, some of which permit private rights of action. Many carriers are excluding coverage, while others are willing to provide cover subject to certain underwriting requirements being met. We are seeing a few underwriters utilize new scanning technology to measure risk related to data collection and sharing practices.

Generative Artificial Intelligence

The widespread adoption of generative artificial intelligence (AI) tools is expected to continue accelerating through 2026. This trend has already prompted underwriters to take note of the AI usage risks as claims are emerging. Currently, there are over 200 active legal cases involving artificial intelligence and machine learning, stemming from data bias, intellectual property and trademark infringement, privacy liability, discrimination and regulatory risks. These risks extend beyond cyber insurance and into established lines of coverage, including employment practices liability, product liability, Errors & Omissions, medical malpractice and others. Although there is still uncertainty regarding how AI-related risks will be covered or excluded across various coverage lines, the cyber insurance market is beginning to adapt to these evolving exposures. For instance, at least one insurer has introduced a stand-alone AI policy, while others are issuing endorsements to cover costs associated with retraining large learning models. In 2026, we anticipate that a growing number of insurers will offer AI-related loss coverage, catering to both AI platform providers and the organizations utilizing these technologies. We expect significant negotiations around how ‘loss’ is defined within these new coverage grants.

Conclusion

Our 2026 Cyber Insurance Market Outlook highlights the dynamic and rapidly evolving nature of the cyber insurance industry, shaped by emerging threats, technological advancements, regulatory changes and shifting underwriting practices. While a mostly buyer-friendly environment, challenges such as systemic risks, ransomware, supply chain vulnerabilities and non-breach privacy violations persist. The cyber insurance market is at a critical juncture, balancing growth opportunities with the need to address emerging cyber risks and ever-evolving regulatory challenges that require a variety of compliance obligations. The outlook underscores the importance of collaboration, innovation and adaptability in shaping the future of cyber insurance. As the industry moves into 2026, insurers are expected to refine policy language, address AI-related exposures and focus on proactive risk management strategies to mitigate the impact of deepfake technology, social engineering and supply chain disruptions.

SOURCES

1. Primary Research Firms:
   - "Cybersecurity Insurance Market by Offering, Coverage, Type, Provider Type, and Vertical — Global Forecast to 2030," *MarketsandMarkets*, July 2025.
   - "Cybersecurity Insurance Market — Growth, Trends, COVID-19 Impact, and Forecasts (2025-2030)," *Mordor Intelligence*, June 2025.
   - "Cyber Insurance Market Size, Share & COVID-19 Impact Analysis Source," *Fortune Business Insights*, 2025.
   - "Cyber Insurance Market by Component, Deployment Mode, Organization Size, Industry Vertical: Global Opportunity Analysis and Industry Forecast, 2023-2032," *Allied Market Research,* 2025.
   - "Cyber Insurance Market: Global Industry Trends, Share, Size, Growth, Opportunity and Forecast 2025-2033," *IMARC Group*, September 2025.
   - "Global Cyber Security Insurance Market: Industry Analysis and Forecast (2024-2030)," *Maximize Market Research*, August 2025.
   - "Cyber Insurance: Risks and Trends 2025," *Munich Re,* April 2025.
   - "Cyber Insurance: A Maturing Market Faces New Challenges," *S&P Global Ratings,* mid-2025.
2. https://homeland.house.gov/wp-content/uploads/2025/10/Cyber-Threat-Snapshot.pdf
3. Coveware Ransomware Market Reports (Q1–Q3 2025 updates.
4. Multiple sources: Sophos State of Ransomware 2025; Coveware Q2 2025 Ransomware; Deepstrike.io; GetAstra 100+ Ransomware Attack Statistics; Exabeam Ransomware Statistics 2025.
5. "A Guide to Website Tracking for Nonprofits," *AJG United States.*
6. https://news.bloomberglaw.com/privacy-and-data-security/cyber-agency-pushes-data-breach-reporting-final-rule-to-2026
7. "Cybersecurity 2025 Legislation."
8. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.600-1.pdf
9. https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

AJG.com **The Gallagher Way.** Since 1927.

Gallagher