Focus Report

2026 Midyear Cyber Market Outlook

IOA

INSURANCE OFFICE OF AMERICA

ioausa.com

INSURANCE OFFICE OF AMERICA

Cyber Continues on Path to Maturity, Adjusts To AI Risks

Cyber insurers have reached a point where capacity is strong, risks are understood, and coverage largely reflects a "get what you pay for" approach. At midyear 2026, the cyber insurance market remains stable and reflects a maturity in carrier understanding of the intricacies of risk and a balance between premiums and potential losses. Cyber insurance capacity is plentiful, and there are no blanket restrictions on limits of coverage. In fact, achieving necessary limits is not difficult for accounts that demonstrate solid cyber hygiene.

The primary area of concern is companies' tendency to underinsure. We see an ongoing mismatch between corporate worries about cyberattacks and their actions to defend against those attacks—in terms of both security and insurance.

AT A GLANCE

- Cyber insurance remains in a period of overall stability, with premiums reflecting both overall losses across the market as well as cybersecurity efforts by coverage applicants.
- Concern persists over companies' lack of adequate limits, with many going bare or relying on lower-cost endorsements that offer some, but not enough, coverage.
- Fears over artificial intelligence coverage gaps seem to be overblown, with most policies offering at least some protection.

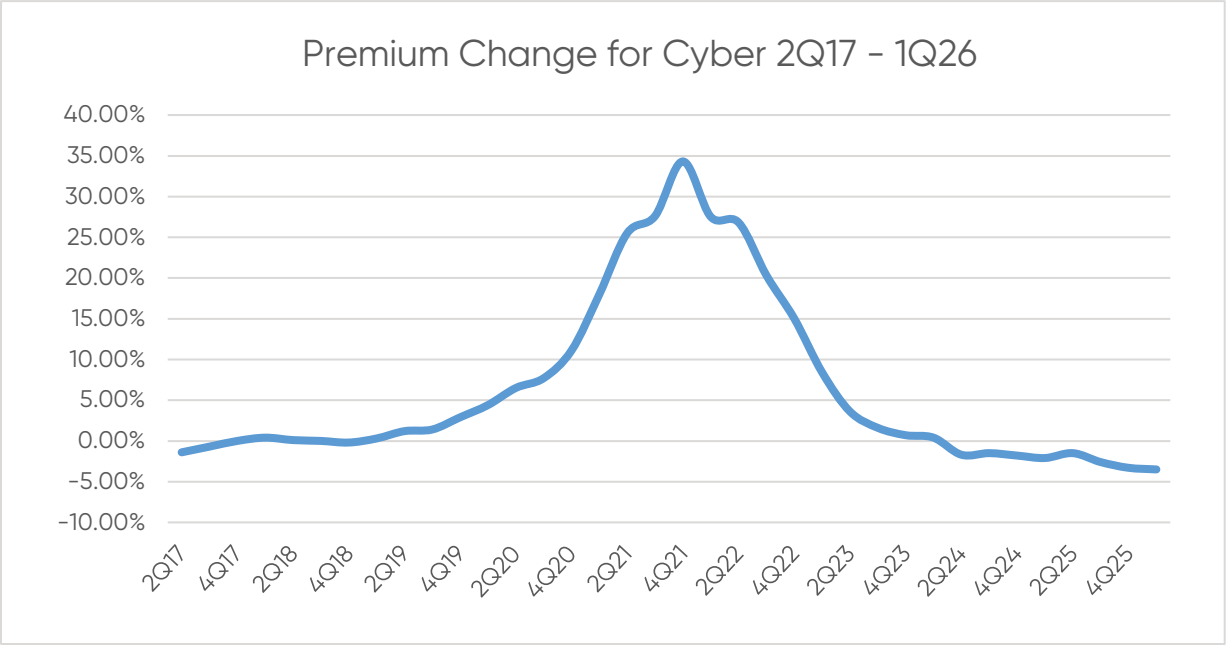
CYBER RATES AND TRENDS

Though fourth-quarter 2025 claims rose significantly in frequency, severity was mixed, with an overall decrease in use of full limits since 2021. Business interruption and litigation over privacy breaches are notable areas of claims activity, while tail risk is rising as an exposure. Chubb's 2026 Cyber Claims Report cites a litigation-first reflex—where claims and legal action come "within days" of or "shortly after" an incident—as a source of significant loss costs. According to NetDiligence's 2025 Cyber Claims Study, the average incident cost for small to medium enterprises (<$2B annual revenue) when business interruption occurred was 650% greater than claims without interruption.

Even though overall cyber insurance rates decreased in Q4 2025, we are seeing a rationalization of premium costs that reflects broad losses in the line but also favorable pricing and terms for accounts with aggressive cyber-control protocols. Pricing pressure appears to be concentrated in large and complex risks more so than for smaller accounts.

Many accounts are experiencing lower retentions, and some sublimits are being eased. This may reflect to some degree competition in the excess market.

FIGURE 1 - AVERAGE CYBER RATES CONTINUE TO FALL



SOURCE: COUNCIL OF INSURANCE AGENTS & BROKERS

Traditionally conservative carriers are deploying broader terms, reducing underwriting friction, and offering higher available limits as insurers pursue portfolio growth and demonstrate greater comfort with this segment's risk profile.

Improved terms frequently include lower retentions and expanded social engineering coverage, with limits in some cases returning to $1 million or greater for insureds able to demonstrate strong cybercrime controls and payment authentication procedures.

We are keeping watch on rates, however, since they are so responsive to litigation severity. While frequency in lower-cost claims can be absorbed with current capacity, a spike in payouts could undo the current equilibrium.

Uptake of cyber insurance continues to be lower than businesses' estimation of the threat, with 89% of C-level executives feeling their companies are inadequately protected, according to Munich Re's Global Cyber Risk and Insurance Survey 2026. Even those with cyber insurance are concerned that a contained event might challenge their policy's limits or response. This is often due to a lack of understanding of policy terms and exclusions. Ironically, Beazley's Spotlight on Cyber Threat & Tech Advances 2026 report shows that 78% of business leaders are confident they could recover from an attack and 82% say they are prepared for cyberrisk.

AI COVERAGE IS PRETTY STANDARD BUT DESERVES CAUTION

There has been much talk over the past couple of years about coverage for artificial intelligence based cyber losses. Our take is that AI exposures remain broadly insurable, though the market is becoming more nuanced as organizations embed AI deeper into business operations and customer-facing services.

Underwriters are paying closer attention to how AI is developed, deployed, monitored, and governed. Expect careful consideration of language models, automation, or AI-assisted decision-making to influence client outcomes or operational risk.

At the same time, the regulatory and liability landscape surrounding AI continues to evolve rapidly. In response, carriers are refining their approach through targeted underwriting, supplemental AI-specific diligence, and affirmative endorsements intended to clarify coverage intent while establishing defined parameters around emerging exposures. These evolving coverages are designed to expand protection thoughtfully while addressing concerns related to governance, transparency, data usage, intellectual property, and human oversight. Organizations leveraging AI at scale should expect increased underwriting scrutiny in these areas.

What we are seeing is more affirmative AI language in endorsements. These affirmative coverages include data poisoning attacks, data recovery expenses, machine-learning wrongful acts, and European Union fines and penalties. We strongly recommend AI affirmative coverage if any of the following are true in your business:

- AI influences decisions with legal, financial, or safety impact.
- AI outputs are relied upon by customers or third parties.
- Training data or outputs create intellectual property or privacy exposure.
- Existing policies contain AI exclusions or ambiguity.

TOP CYBER VULNERABILITIES

- **Ransomware**—Cyber criminals have shifted from encryption/lockdown of data to theft and threat of data sales, making backup files less effective in ignoring extortion demands.
- **Rapidity of exfiltration**—Attackers can move from attempt to success in minutes.
- **Sophistication of impersonations**—Artificial intelligence is making it easier to fake voicemails, invoices, emails, rerouting instructions, and other official communications in order to fraudulently cause the transfer of assets or goods.
- **Human error**—Behind most cyber failures is a human who clicked on a link, gave out information or improperly used it on an app, or lost a device that wasn't properly secured. Training and testing are having a hard time keeping up with sneak attacks and staff mistakes.
- **Internet of things**—Use of internet-connected devices for primary operational functions and storage or transfer of proprietary data has increased vulnerable attack surfaces beyond what many companies can defend. Investment in strong enough cybersecurity is a budgetary challenge.

GAPS IN COVERAGE PERSIST

We noted in our annual report last fall that some policyholders think they are okay regarding cyber insurance because they added a cyber endorsement to their package policy, but we warned that these endorsements fall short of a stand-alone policy due to their restrictive wording and lower limits of coverage.

This problem still exists, and important protections for invoice manipulation, deception of a vendor or client, and contingent business interruption due to a crucial partner's downtime caused by a cyber event are usually not covered by endorsements. Also commonly not offered in endorsements are reputational loss, cryptocurrency loss, dependent system failures, and risk mitigation services.

Stand-alone cyber policies have grown notably in terms of services—beyond coverage for losses. These cyberrisk control perks and crisis response offerings are making cyber insurers part of a holistic cyberrisk management team more than just a financial backstop. That is a significant added value that endorsements don't typically provide.

TEAMWORK AND SUPPORT

Even simple steps can vastly improve cybersecurity. Personnel efforts top the list. Employee training on phishing, impersonation, and AI use, along with implementing network access controls, such as multifactor authentication and dual approvals for money or data transfer and system entry authorization, can make a huge difference in hacker success. Immediately deploying software patches is another effort that closes criminal ingress portals.

Cyber insurance applications should be treated as underwriting representations. Inaccurate, incomplete, or misleading information identified during a claim investigation can lead to coverage disputes, denial of claims, or policy rescission.

We can help you review your policies and your business contracts for insurance coverage issues so you understand what risks you are undertaking or retaining and so you can see options for financial protection. IOA also offers claims advocacy services so, if there is a claim, you have support.

AI CONSIDERATIONS TO DISCUSS WITH YOUR BROKER

1. Do you use AI or machine-learning tools in production?
2. Does any AI system generate outputs that customers, employees, or third parties rely on?
3. Could incorrect, biased, or misleading AI outputs cause financial loss, legal claims, or reputational harm?
4. What types of data are used by your AI systems?
5. Are AI tools developed in house, purchased from vendors, or embedded in platforms you rely on?
6. What coverage exists in your general liability and crime products?
7. What limits make sense for your company?

ABOUT INSURANCE OFFICE OF AMERICA

Insurance Office of America (IOA) is one of the largest privately held independent insurance brokerages in the United States. Founded in 1988, IOA has more than 1,500 associates located in over 60 offices in the U. S., and it is a recognized leader in providing property and casualty, employee benefits, and personal lines insurance and risk management solutions.

For more information, visit ioausa.com.

We focus on your risk so you can focus on your dreams.

INSURANCE OFFICE OF AMERICA

ioausa.com

26-0065