Focus Report

2026 Cyber Market Outlook

INSURANCE OFFICE OF AMERICA

ioausa.com

INSURANCE OFFICE OF AMERICA

Premiums Drop as AI, Hostile Nation-States, and Gaps in Coverage Present Substantial Risk

Cyber claim severity is down in 2025 as is the frequency of large cyber claims. As a result, average cyber insurance rates continue their decrease. Premiums dropped again in third-quarter 2025, by 2.6%, according to the Council of Insurance Agents & Brokers' Q3 2025 survey. In the previous quarter, only 14% of respondents indicated they saw premium increases.

AT A GLANCE

- Overall, the cyber insurance market is in a period of stability. Insurance companies are reducing premiums for known, high-quality accounts, and they're providing coverage terms that support and reward solid cyber risk management.
- Companies that practice even the most basic cyber hygiene—multifactor authentication, recordkeeping, patch/software updates, and employee training, for example—can usually find cyber insurance at a manageable price point.
- A significant concern, however, is the gap in protection clients have when gaining low-limit, broadly generalized coverage through a policy endorsement rather than buying a tailored, stand-alone policy.

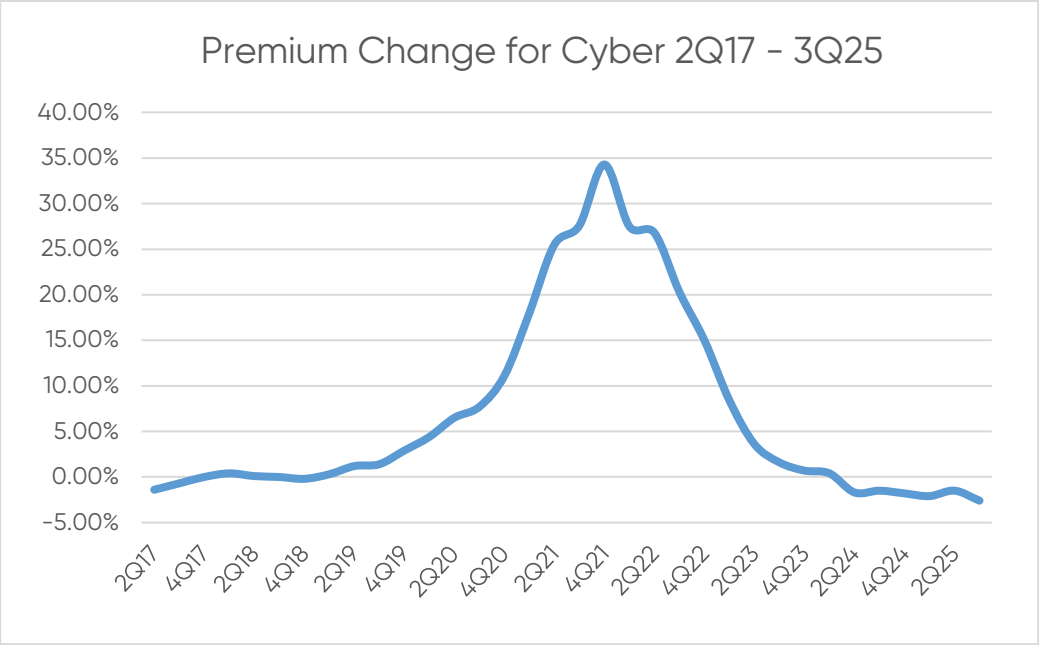
Brokers in the survey said there is ample capacity, and we concur that capacity is expanding in some classes of business. Where we were able to get only $2 million to $3 million before in single-insurer limits, we can now get to $5 million before adding on a layer.

Cyber insurance mandates are fairly common now. Companies in government and defense sectors as well as the financial services industry often require contractors to obtain minimum cyber insurance terms and limits.

While insurance prices are down, cyber criminal activity is up, so businesses must keep up their defenses. Identifying vulnerabilities, closing gateways to attacks, and knowing how to respond when an attempted incursion is underway or a breach happens are part and parcel of company risk management. And insurers expect—even demand—such capabilities, so it's crucial to train staff to prevent incursions such as phishing, unauthorized system access, impersonation, and monitoring for attacks. Minimum acceptable standards in today's business environment are strong password policies (that expire every 90 days), encryption for data (while at rest and in transit), and multifactor authentication.

The primary cyber concerns are artificial intelligence, cyber liability lawsuits, and cyberattacks or failures that cause massive systemic disruptions. Coverage exclusions may exist for attacks by malign nation-states or terrorist cells, and cyber endorsements tacked on to other policies in lieu of purchasing tailored, stand-alone cyber insurance may leave significant coverage gaps.

FIGURE 1 - CYBER PREMIUMS HIT RECORD LOW



SOURCE: COUNCIL OF INSURANCE AGENTS & BROKERS

THE RISING ROLE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence (AI) is the most daunting problem facing cybersecurity personnel these days. It is increasing the:

- Number of simultaneous pathways into systems
- Speed of attacks
- Rapidity of data exfiltration
- Ease of attack, even by low-skill hackers
- Persistence of intrusion attempts

AI is also enabling autonomous malware that modifies code in real time to outwit cybersecurity barriers.

Almost no insurers have language defining and limiting AI coverage, so there can be confusion and disputes about insurance for AI-based events. Though the lack of AI wording might not exclude coverage on a policy, if the proximate cause of an incident is related to AI, it's unclear how carriers will respond or decide which insuring agreement covering such incidents would apply. Claims could be drawn out.

Ransomware as a Service

Ransomware remains a growing cyber risk for organizations. With the rise of artificial intelligence, it has become much easier to create and deploy ransomware—malicious software that locks owners out of their systems, paralyzes their data, or readies that data for publication on the dark web until a demand is met.

Ransomware as a service (RaaS) is a cottage industry populated by skilled hackers who, for a fee, aid low-skill hackers in formulating and propagating attacks. RaaS providers know how to avoid detection, so shutting down their operations is difficult.

The GuidePoint Research and Intelligence Team report from Q3 2025 says the number of ransomware groups is at an all-time high of 77%, up 57% from the same period last year.

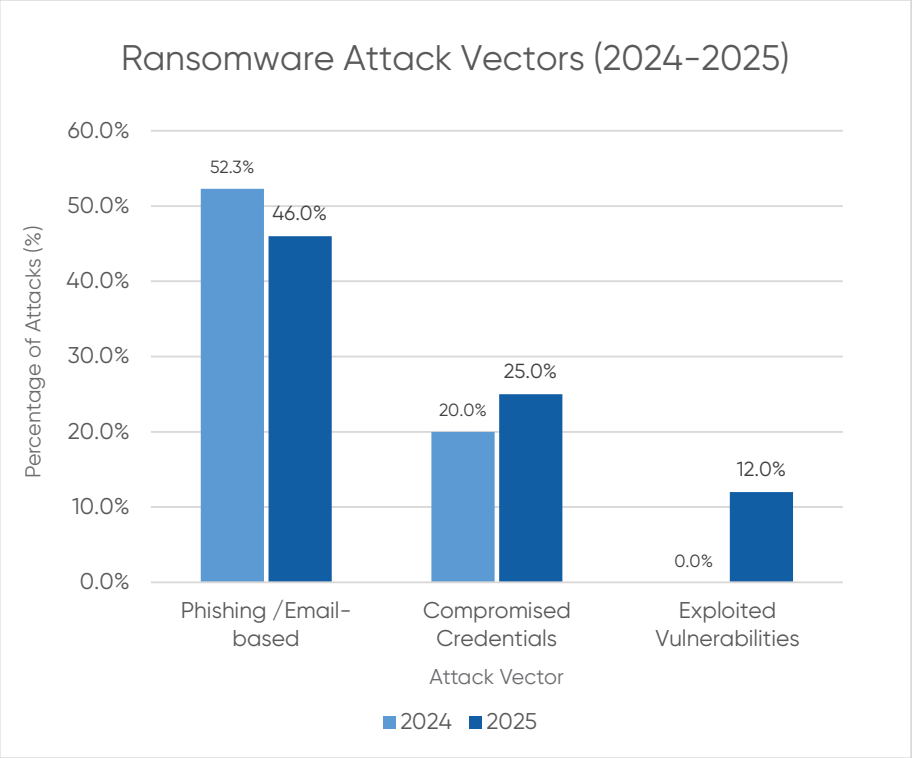
Hornetsecurity reports that 24% of organizations it surveyed this year said they were attacked by ransomware, up from 18.6% last year, reversing a downward trend seen in 2023 and 2024. Hornetsecurity cites AI automation as the driver of the uptick.

The good news is that 62% of organizations in the Hornetsecurity survey said they have implemented immutable backups, which can't be locked or modified by ransomware, and 82% said they have a cyber disaster recovery plan in place.

A business may ask, "Why buy ransomware or cyber extortion insurance if I have air-gapped my computers so crucial backups are not connected to the internet?" The answer is that cyber ransom demands may include threats to publish data instead of simply locking or encrypting it. Insurers are willing, with the right policy in


vPROJECT ANN Xv ADVANCED ARTIFICIAL NEURAL NETWORK FOR SPEACIAL PURPOSES
vPreferences
vSSystem
001v110_
001v110_
001v110
011v110_
001v110_
001v110_
001v110
011v110_

FIGURE 2 - HOW RANSOMWARE HACKERS GET IN



SOURCE: HORNETSECURITY RANSOMWARE IMPACT REPORT

place, to cover such demands, and they're watching the dark web to make sure hackers don't release the data once the ransom is paid. Oddly enough, hackers usually honor their promises.

Nearly all cyber incidents involve some type of human error, so it's vital to teach network users to spot and avoid intrusion attempts. Training can include familiarity with how the normal flow of requests works, what employees can do if they get a suspicious email, and whom to call to confirm validity of any requests for money or system access. Unfortunately, the Hornetsecurity survey indicates a decline in the number of organizations honing employee cyber-awareness skills, which bodes ill for the future.

Speed of Attack and Data Exfiltration by AI

The speed at which cyber criminals can move from attack to mission completion is rendering the traditional model of cybersecurity obsolete. Artificial intelligence has automated cyberattacks, allowing hackers to achieve goals in under an hour—from infiltration attempt to full exfiltration of data. That means organizations that use typical detect and patch methods may find themselves grossly outmatched by the scale and pace of hostile activity. Palo Alto Networks suggests four must-have defenses:

- AI-powered detection, which identifies anomalies and potential attacks in real time
- Zero-trust architecture, which requires verification for every request for system access
- Automated defense responses, which can shut down an attack before a human can respond
- Extended detection and response (XDR), which tracks threats across systems and endpoints, since hackers typically target more than one attack surface in an infiltration attempt

CYBER LIABILITY LAWSUIT TRENDS

Though overall cyber claim frequency and severity are down, there are hot spots organizations should be aware of.

Class actions

Class actions over data breaches and privacy violations have surged, particularly as a result of data privacy laws. Allianz Commercial reported in its recent Cyber Security Resilience 2025 report that about 1,500 data privacy lawsuits were filed in 2024 in the United States alone. Moreover, law firm Jackson Lewis says there are more class actions over small and midsize data breaches.

Not All (Cyber) Policies Are Created Equal

Cyber Coverage – Endorsement vs. Stand-alone Policy

WHY THIS MATTERS

Many feel at ease by being able to say, "Yes, I have cyber," when in actuality they have very limited coverage. They assume adding a cyber endorsement to their package policy is enough, but the reality is that endorsements often leave critical gaps.

BOTTOM LINE

Endorsements are entry-level protection, suitable for small businesses with minimal cyber exposure, and even then, it might not be enough. For any company handling sensitive data, conducting online transactions, or relying on IT systems, a stand-alone policy is strongly recommended.

HOW DOES YOUR POLICY COMPARE?

Cyber Endorsement
(Add-on to Package Policy)

PROS

- **Convenient:** Added to existing policy
- **Lower cost:** Typically $100–$500 annually
- **Meets baseline:** Basic coverage for small exposures

CONS

- **Low limits:** Usually $50,000–$250,000
- **Limited scope:** Often covers only breach notification and some legal defense
- **Excludes major risks:** Ransomware, business interruption, social engineering, regulatory fines
- **Help:** Offers minimal risk management resources

Stand-alone Cyber Policy

PROS

- **Higher limits:** $1 million–$10 million or more
- **Comprehensive coverage:**
  - Ransomware/extortion
  - Business interruption
  - Social engineering fraud
  - Regulatory fines and penalties
  - Invoice manipulation
- **Post-breach aid:** Incident response team, forensic services, and breach coaches
- **Prevention:** Access to cybersecurity tools and training

CONS

- **Higher premium:** $1,000–$10,000+ depending on revenue and risk profile
- **More complicated:** Separate underwriting process

Accessibility

Digital accessibility is another area of heightened action. UsableNet's Midyear ADA Lawsuit Report projects a 20% increase in accessibility lawsuits nationwide for 2025. It cites reduced federal enforcement and a shift to state courts that are more plaintiff-friendly, noting the popularity of New York and Florida in particular. E-commerce, at 69% of accessibility lawsuits, is far and away the most targeted sector, with the food service industry coming in a distant second at 18% and all others sharing the remaining 12%.

We also are still seeing plenty of nuisance accessibility claims, where plaintiffs demand low-level money from organizations, knowing that such cases are often cheaper to settle than to fight. Demonstrating due diligence in consistently tracking and addressing issues is key to defense of these types of claims.

Wrongful Collection and Processing of Data

Common website and business practices are now a source of cyber liability claims. This includes things like pixel tracking, sharing collected data without user consent, and failing to inform users that their data is being collected or how the data may be used. Any of these practices may violate various privacy laws. Biometric system access technologies, keystroke monitoring, website tracking, and session replay scripts all have been the basis of privacy lawsuits.

Biometric restrictions are going to be on the increase in policies, so companies need to make sure they have coverage if they use biometrics. Currently 24 states (plus some local jurisdictions) have laws regulating the collection and use of biometric data. Illinois allows people to sue the company directly for a violation. The rest must rely on the state attorneys general to bring suit. Some cyber carriers offer limited coverage, some provide defense only, and some flat out refuse to offer coverage. Work with your broker on both risk management and the fullest insurance protection.

Vendor Breaches

Vendor and cloud provider failures are rising as an exposure. SecurityScorecard's 2025 "Global Third Party Breach Report" says there was a 6.5% increase in breaches from 2023 to 2024, with IT service, cloud platform, and software solution providers being the most frequently compromised and file transfer software being the most exploited vector (or pathway into systems).

Organizations should have airtight contracts that put the loss-cost onus on at-fault vendors, and they should expect underwriters to inquire about vendor loss-prevention protocols.

Delayed Discovery of Attack

When there is a delay in detecting a cyberbreach, loss exposures can be compounded. The following failures take the longest to detect and can usher in the most harm, according to IBM's "Cost of a Data Breach Report 2025":

- **Shadow AI**—where employees or external users use AI in an unsanctioned way that compromises data security
- **Malicious insiders**—where employees either allow hackers in or implant code/exfiltrate data themselves
- **Accidental credential compromise**—where system access is granted through carelessness or trickery
- **Partner/vendor breach**—where an organization's system is infiltrated through a partner or vendor's system

Some insurers are limiting or excluding coverage when security requirements are not met, such as in the case of not installing patches, not training employees, and not adequately guarding system access, according to Red Dog Security. Organizations should be diligent in ensuring they avoid taking on hidden risk in their vendor and partner contracts. Such risks might not be covered in either party's cyber insurance policy.

Nation-State/War Exclusions

Since the 2023 *Merck & Co. v. ACE Am. Ins. Co.* decision in Merck's favor, which declared ACE had to cover Merck for the NotPetya attack since, historically, the war exclusion clause had not been applied "outside of a clear war or concerted military action," Lloyd's of London and other insurers have clearly stipulated that state-backed cyberattacks would be excluded from coverage.

Nonetheless, ambiguity in insurance contracts persists. That is partly because hostile states outsource their dirty business to criminal groups and partly because economic profiteering by hostile states may not rise to the definition of "war." The costs of investigating and fighting a nation-state/war exclusion can be high. Very tight language regarding such an exclusion is a goal.

If the criminal actor is on a list of terrorist groups or hostile nation-states, no negotiations or payments are legal, leaving the victim high and dry. Good negotiations with the insurance company may yield creative solutions on the first-party side of coverage, gaining some business interruption help. But it's not a solution to get data back or cover full loss costs. We are following legislative attempts to address terrorist and hostile-state cyberattacks and will keep clients apprised as developments arise.

ON THE HORIZON

Risks

Aggregation of service providers combined with the large number of businesses depending on that small group creates a systemic risk that could lead to calamity. Of note are the healthcare industry, financial services, the energy grid, communications, and transportation, which have outsized, critical vulnerabilities. Over-reliance on single points of failure—along with the potential for a global systemic cyber event, whether due to an attack or a multisystem disaster—represent two of the biggest concerns for the cyber insurance industry and organizations across the board.

Remember that the widespread AWS failure in October 2025 and the 2024 Crowdstrike-based crash were not cyberattacks. They were software failures on the part of two of the global cyber lynchpins. Coding or system bugs that cause business interruption are often not included in an organization's cyber insurance policy or, if they have been added by forward-thinking enterprises, are often subject to highly restrictive sublimits. Costs may include compensation to harmed customers, lost revenue, and remediation of each machine affected. Those whose cyber insurance policies cover only malicious attacks could find themselves with heavy uninsured losses.

Worse, cyber insurers do not yet share a standardized definition of "systemic," so claims may be disputed and payments unsettled while courts sort out what ambiguously worded policies mean.

Regulatory

In the case of a widespread nation-state attack, it remains unclear what kind of coverage would be available, especially with cyber insurers increasingly excluding government-backed attacks. Calls persist for some kind of national cyber insurance backstop, à la the Terrorism Risk Insurance Act, and IOA will continue watching for progress in this area.

Funding for the Cybersecurity and Infrastructure Security Agency (CISA) is in jeopardy of substantial cuts. We are keeping abreast of budget developments here because cybersecurity information sharing is protected under that program and, without it, such cooperation could be undone. A loss of that private-public partnership could make it harder to identify and defend against cyber threats.

What You Can Do

Customization is key so that your company secures the coverage and limits for exposures you're most concerned about.

You also need to review contracts so you don't take on uncovered liabilities and do meet contractual obligations for cyber insurance. Working with government entities and financial institutions could require specific cyber policies and high limits.

Continued vigilance is needed because threat actors are getting smarter and their expanded use of AI (DarkGPT) is raising new concerns.

You should have an incident response plan (which we can help build or improve), and you should implement minimum acceptable standards that underwriters now require, such as multifactor authentication, encryption, and a 90-day patching cadence, among others.

IOA stands ready to advise and assist your business in finding the best risk avoidance and recovery solutions for your cyber needs.

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 1,400 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 www.ioausa.com.

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

INSURANCE OFFICE OF AMERICA

ioausa.com

25-0101