



Report on the Cybersecurity Insurance Market

2025 REPORTING YEAR

Market Analysis and Threat Landscape Narrative

*For members and interested regulators of the **Property and Casualty Insurance (C) Committee** and the **Innovation, Cybersecurity, and Technology (H) Committee**.*

This report examines the U.S. cyber insurance market using data from the NAIC *Property & Casualty Annual Statement Cybersecurity Insurance Coverage Supplement* (Cyber Supplement) and alien surplus lines data from the NAIC International Insurers Department (IID). The Cyber Supplement retains the three-way primary (Part 2), excess (Part 3), and endorsement (Part 4) reporting structure adopted in 2024, which distinguishes stand-alone cyber policies from cyber written as an endorsement to another policy and preserves state-level transparency through Part 5. Section 1 presents the financial and statistical picture; Section 2 presents the threat environment through an underwriting lens; and Section 3 delivers a regulatory developments and supervisory outlook. NAIC Cyber Supplement and IID figures are NAIC data. All other statistics and incidents are drawn from the publicly available sources cited in the footnotes.

Section 1. The Cyber Insurance Market: Financials and Data

GLOBAL MARKET CONTEXT

Global cyber insurance premium surpassed \$16 billion in 2025, though growth was slower than in prior years, with much of the deceleration attributable to the decline in U.S. direct written premium amid intensifying competition and growing capacity.¹ The United States remains the world's largest cyber insurance market, accounting for more than half of global premium. Once U.S. exposures written in the Lloyd's market are included, the U.S. share is approximately 60%. International markets, particularly Europe, Latin America, and developed Asian small- and medium-sized enterprise markets are expected to gain a larger share of global premium over time.²

The global segment carries a stable outlook, supported by robust demand, favorable intermediate-term profitability, strengthening cyber hygiene, and continued reinsurance and alternative capital inflows. This is balanced against escalating ransomware, business email compromise, and funds transfer fraud, there's a recognizable concern about the impacts of systemic accumulation risk, artificial intelligence (AI)-enabled attacks, and geopolitical uncertainty.³

U.S. MARKET SIZE AND PREMIUM

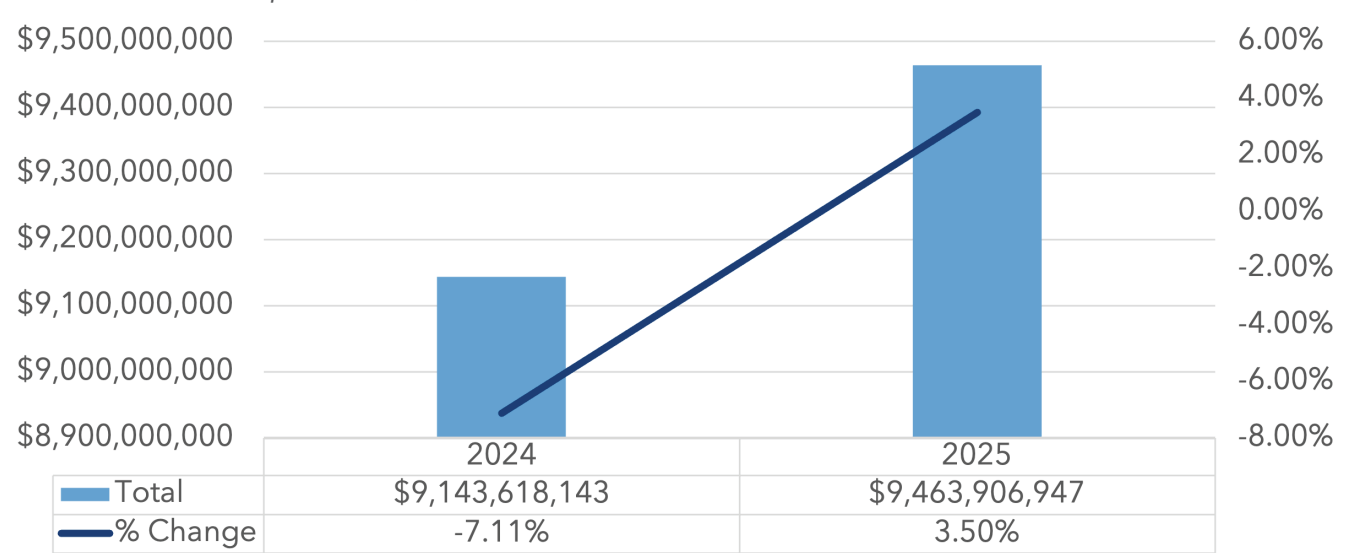
Total U.S. direct written premium, including alien surplus lines, reached approximately \$9.46 billion in 2025, an increase of about 3.5% from \$9.14 billion in 2024 and a return to modest growth after the first-ever contraction recorded the prior year. Domestic insurers wrote \$7.46 billion, while alien surplus lines carriers reporting through the IID wrote roughly \$2.0 billion. Since 2020, domestic premiums have grown from \$2.75 billion to \$7.46 billion, a compound annual growth rate of approximately 22%, though the trajectory has shifted from rapid, hard-market expansion toward a steadier, more disciplined growth pattern.

¹ AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

² AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

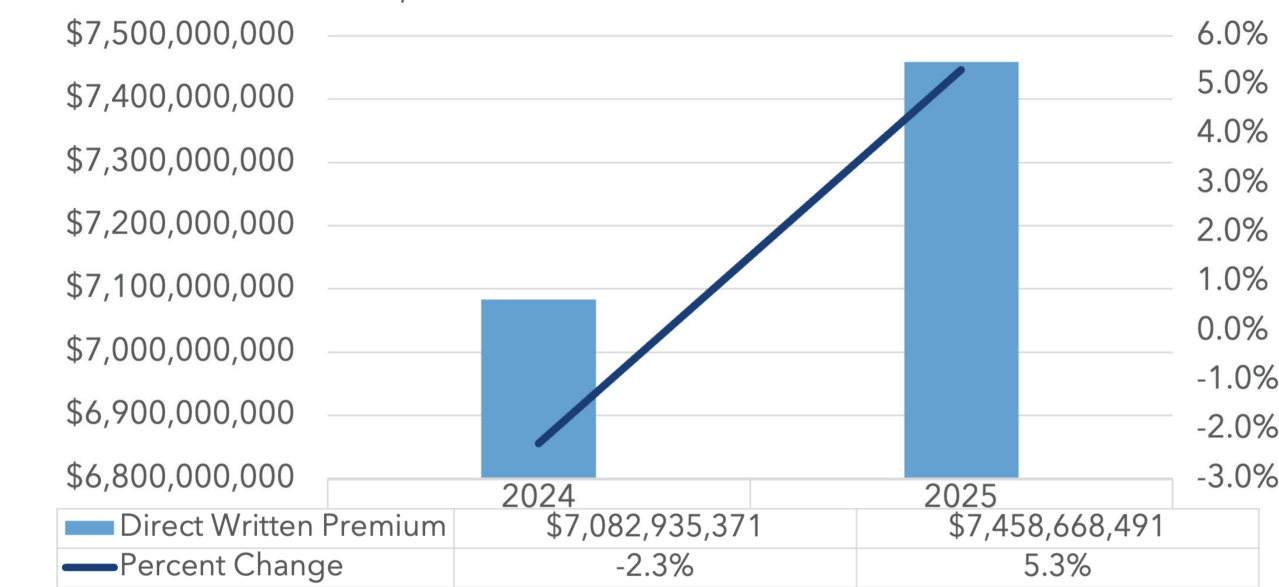
³ AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

FIGURE 1.
Direct Written Premium Showing Percent Change
(Includes Alien Surplus Lines)



U.S. cyber direct premiums reportedly rose to \$7.46 billion in 2025 from \$7.08 billion in 2024, a 5.3% increase. Continued rate decreases are expected to keep pressure on premium growth.⁴

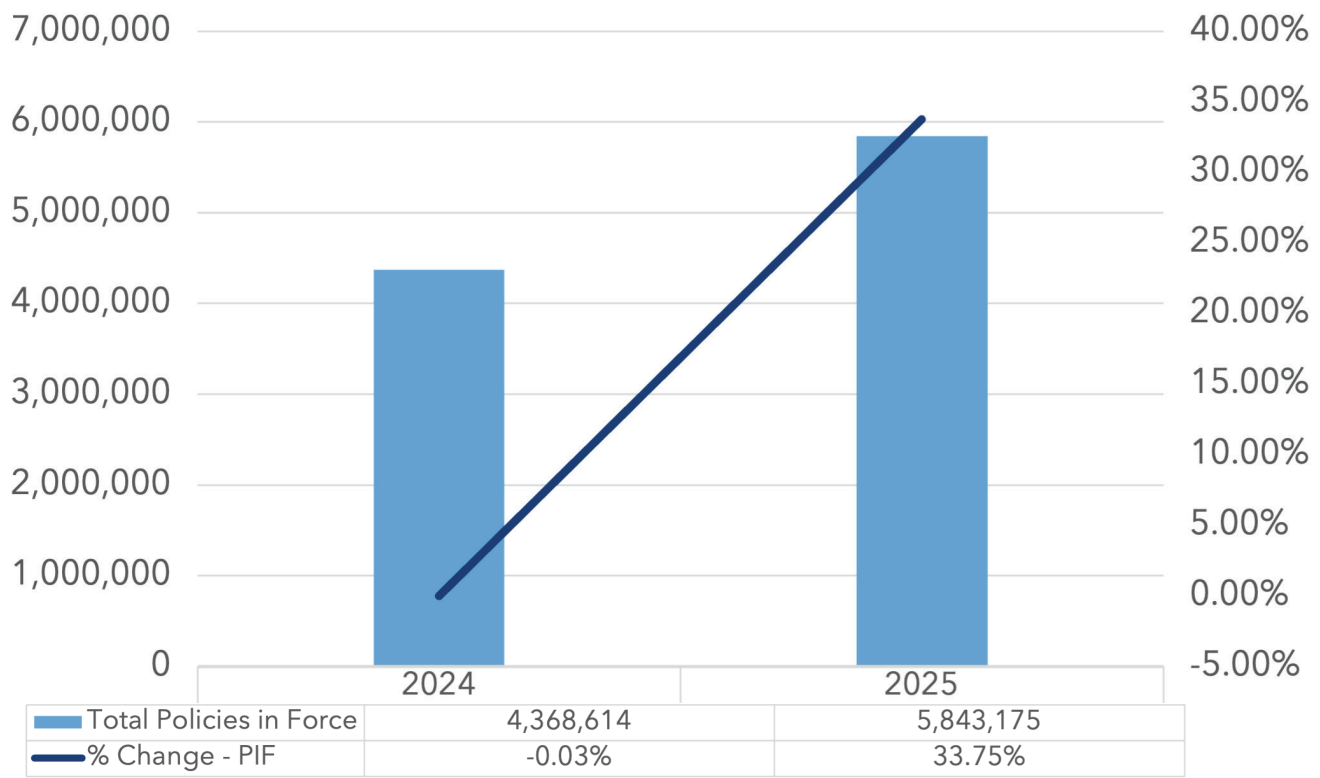
FIGURE 2.
Direct Written Premium Showing Percent Change
(Does Not Include Alien Surplus Lines)



⁴ AM Best, "U.S. Cyber: Premium Growth Lags Behind Cyber Threats,"
Best's Market Segment Report, June 2026 (BestLink data).
NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

POLICIES IN FORCE AND DISTRIBUTION BY POLICY TYPE

FIGURE 3.
Policies in Force Showing Percent Change



Domestic policies in force rose 33% to 5.84 million in 2025, while reported claims increased 20% to 56,323, more than six times the 2017 level. Endorsement policies are up 53.8%, primary up 13.6%, and excess policies are down 45.3%. Coverage premium is concentrated in primary policies, which account for approximately 64% of premium, with excess coverage at about 32% and endorsement coverage at approximately 4%. Endorsement coverage continues to generate the largest share of policy counts relative to premium, reflecting the widespread practice of bundling modest amounts of cyber protection into other commercial lines rather than purchasing dedicated coverage.

FIGURE 4.
Distribution of Direct Written Premium (2025)

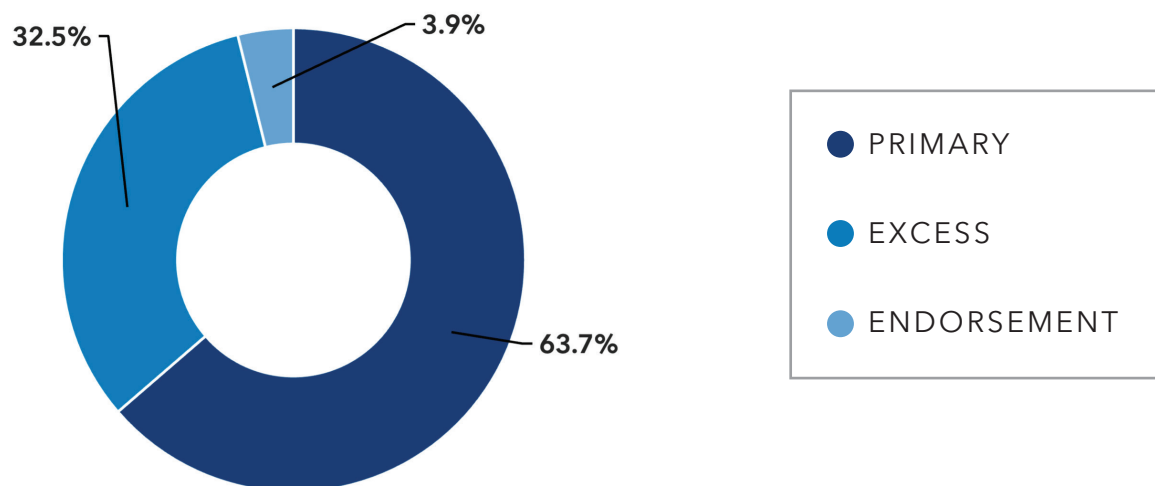
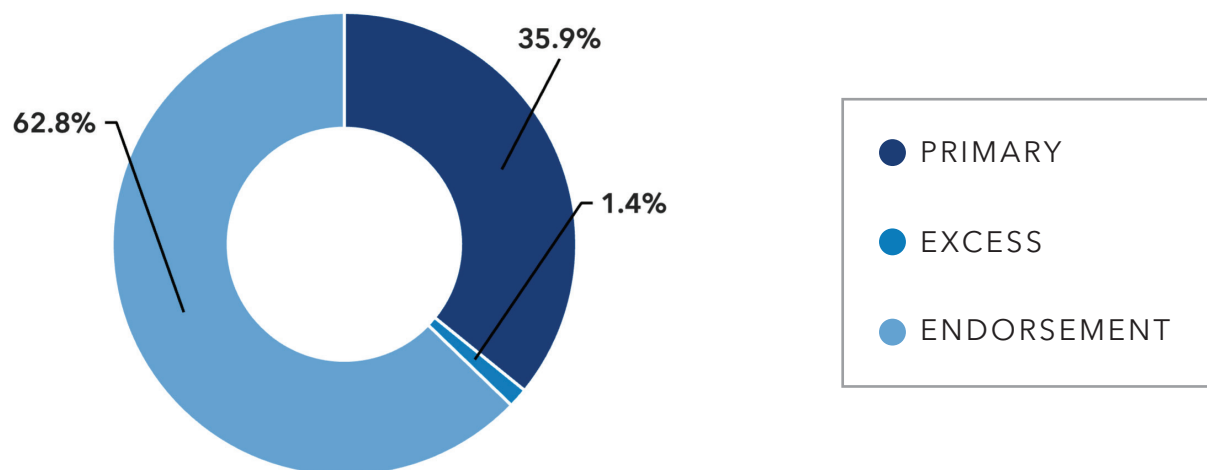


FIGURE 5.
Distribution of Policies in Force (2025)



More than 60% of U.S. cyber premium comes from primary cyber policies, yet the majority of policies are endorsements to other commercial policies. Endorsements are high-volume by count but generate low-premium, while primary and excess are low-volume by count but generate more premium.⁵ Large global specialty carriers lead the primary segment, with Chubb, Beazley, and Travelers at the top, and the 10 largest carrier groups controlling approximately 60% of primary premium.

⁵ AM Best, "U.S. Cyber: Premium Growth Lags Behind Cyber Threats," Best's Market Segment Report, June 2026 (BestLink data).

TABLE 1.
Top 20 Groups

2025 Rank	2024 Rank	Group Name	Direct Written Premium	Loss Ratio w/DCC	Market Share	Cumulative Market Share
1	1	Chubb Ltd Grp	\$629,201,236	58.81%	8.44%	8.44%
2	16	Beazley Grp	\$570,949,568	16.28%	7.65%	16.09%
3	2	St Paul Travelers Grp	\$543,864,601	58.26%	7.29%	23.38%
4	9	Sompo Grp	\$341,952,941	60.78%	4.58%	27.96%
5	4	Tokio Marine Holdings Inc GRP	\$319,281,234	56.60%	4.28%	32.24%
6	3	Fairfax Financial	\$301,192,570	53.62%	4.05%	36.29%
7	8	American Intrnl Grp	\$284,315,426	62.28%	3.97%	40.26%
8	6	Arch Ins Grp	\$268,150,877	41.60%	3.81%	44.07%
9	7	At Bay Speciality Ins Co	\$276,564,105	73.45%	3.60%	47.67%
10	10	Starr Grp	\$250,782,708	3.75%	3.36%	51.03%
11	17	QBE Ins Grp Ltd	\$231,214,119	74.42%	3.10%	54.13%
12	12	AXIS Capital Grp	\$230,866,128	61.73%	3.10%	57.23%
13	11	CNA INS Grp	\$212,411,370	59.51%	2.85%	60.08%
14	5	AXA INS Grp	\$204,474,929	72.29%	2.74%	62.82%
15	13	AmTrust Financial Serv Grp	\$200,803,833	60.28%	2.69%	65.51%
16	21	Intact Financial Grp	\$198,641,587	26.15%	2.66%	68.17%
17	14	Berkshire Hathaway	\$173,269,759	88.03%	2.32%	70.49%
18	15	Hartford Fire & Cas Grp	\$166,492,869	10.70%	2.23%	72.72%
19	18	Liberty Mut Grp	\$161,246,818	60.77%	2.16%	74.88%
20	19	Zurich Ins Grp	\$145,021,055	54.81%	1.94%	76.82%

A MARKET SPLITTING INTO TWO MARKETS

U.S. cyber is becoming two distinct sub-markets: a surplus lines market writing primary and excess cyber-specific policies and an admitted market focused on endorsements to other commercial policies. According to AM Best, surplus lines carriers now hold nearly two-thirds of all cyber premium, and their 2025 incurred loss and defense and cost containment (DCC) ratio (55.9) exceeded that of admitted carriers (50.2). Consecutive years of a higher surplus lines incurred ratio suggest these carriers are writing longer-tail business for which losses take longer to settle.⁶



⁶ AM Best, "U.S. Cyber: Premium Growth Lags Behind Cyber Threats," Best's Market Segment Report, June 2026 (BestLink data).

FIGURE 6.
Domestic Direct Written Premium

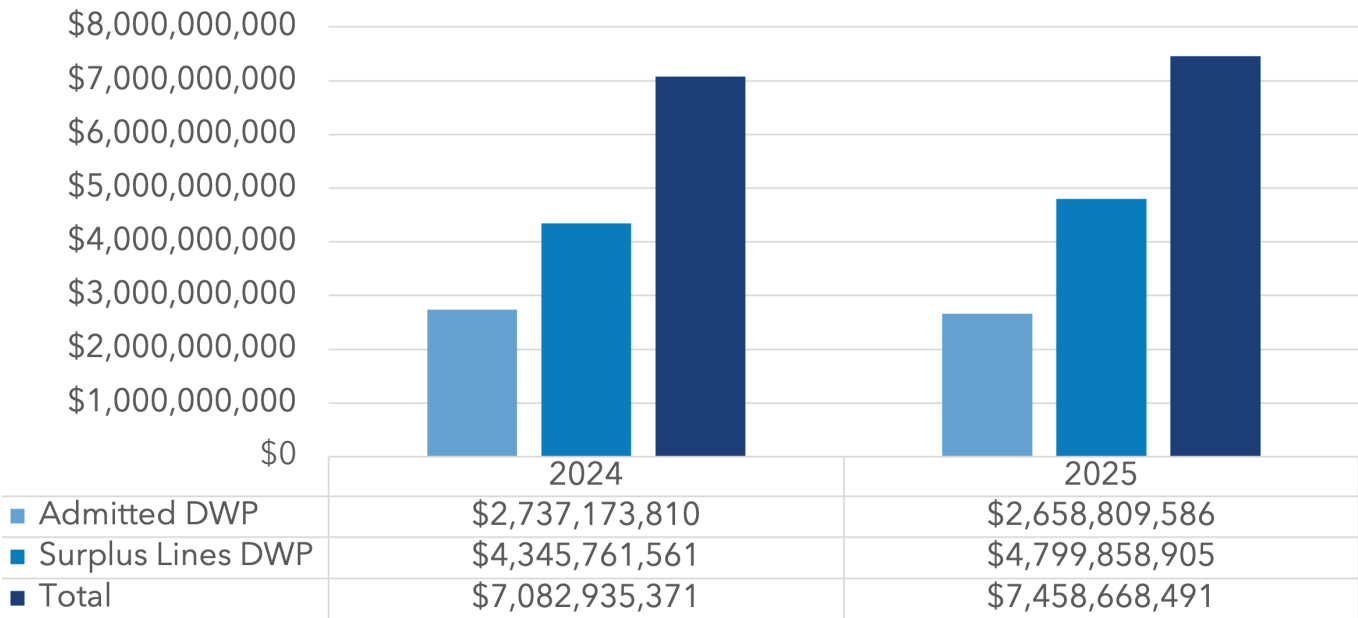
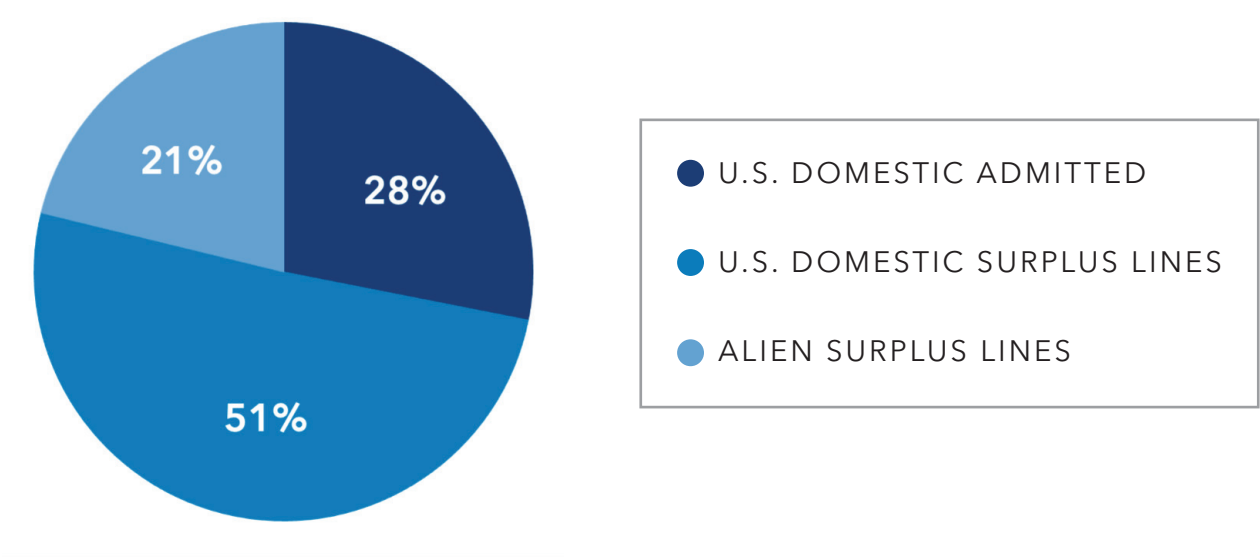


FIGURE 7.
Market Type Percentages

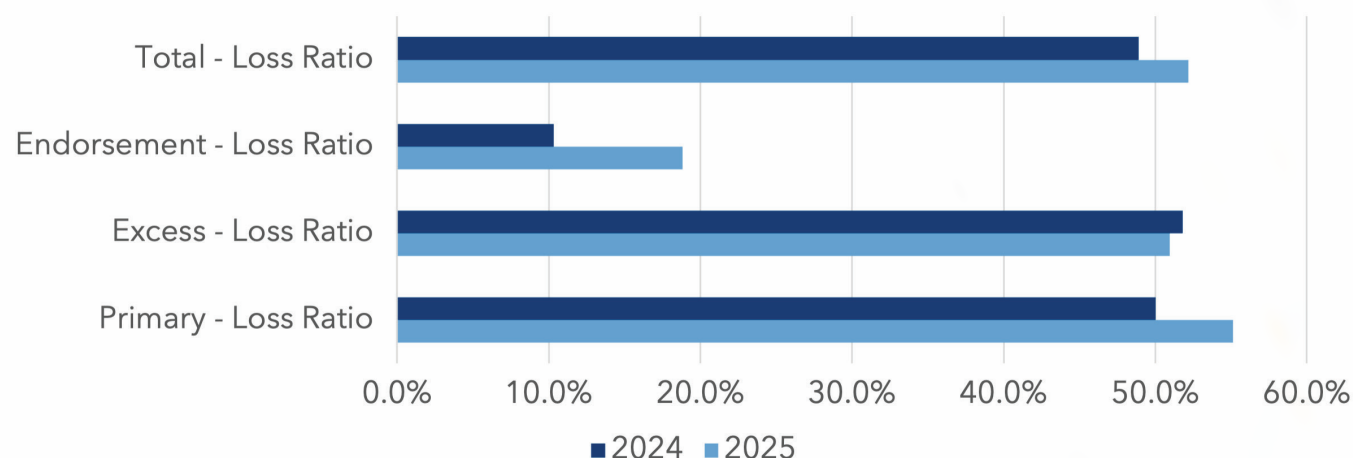


PROFITABILITY: LOSS RATIOS AND PRICING

The industry-wide cyber loss ratio rose to 53 in 2025 from 48.7 in 2024, the second consecutive annual increase and the highest level since the COVID-era ransomware spike. This deterioration is occurring as prices continue to fall. The first quarter of 2026 marked the eighth consecutive quarter of U.S. cyber rate cuts, with the fourth quarter of 2025 and the first quarter of 2026 the steepest of the cycle.

FIGURE 8.

Loss Ratios by Coverage Type



A rising loss ratio during an eighth straight quarter of rate reductions is the inverse of the 2021 hard market, when a ransomware surge produced an immediate price correction. The deterioration is concentrated in the primary book, where the loss and DCC ratio rose approximately 8 points to 57%, while the excess book improved slightly to 52%. Endorsement business, though small in premium, saw its ratio nearly double from 10.2% to 19.1%.

UNDERWRITING PERFORMANCE: CLAIMS SEVERITY AND FREQUENCY

Carrier-level claims data illuminate where aggregate severity is headed. Average claim severity for large businesses, those with \$1 billion or more in annual revenue, reached approximately \$4.4 million in 2025, up from roughly \$2.2 million in 2024 and representing a 586% increase since 2021, driven by rising business interruption expenses and the growing cost of data breach and privacy-related litigation.⁷ Middle-market severity rose more modestly, from about \$619,000 to \$759,000 year over year, while severity in the small- to mid-sized enterprise segment actually declined, from roughly \$215,000 in 2024 to about \$142,000 in 2025. Claim frequency for large accounts fell from about 15 claims per 100 cyber policies in 2024 to roughly 10 in 2025, and middle-market frequency also declined from about six to just over five claims per 100 policies.⁸

This combination of lower frequency but sharply higher severity at the top of the market might suggest that improved underwriting selection and security controls may be reducing the number of incidents reaching a claim, even as the incidents that do occur, particularly at large organizations, are becoming noticeably more expensive to resolve.

A broader global claims data set, drawn from more than 100,000 policyholders across the U.S., Canada, the United Kingdom (UK), Australia, and Germany, points to a related but distinct pattern at the smaller end of the market. Overall claims frequency rose 3% in 2025, while overall claims severity fell 19% to an average loss of \$116,000.⁹ Among the smaller accounts that make up the bulk of that book, more incidents are occurring, but the average cost of each is being contained. A pattern that contrasts with the sharply rising severity observed at the large-account level. Viewed together, the two data sets indicate that claims-cost pressure in the cyber line is concentrating at the top of the market even as smaller policyholders benefit from improving loss containment.

On ransomware economics specifically, initial ransom demands might have risen 47% year over year to an average of more than \$1 million. A record 86% of businesses that experienced a ransomware event reportedly refused to pay, a shift attributed to improved backup practices and incident-response readiness. Ransomware nonetheless remained the single costliest claim type by average severity, at \$269,000.¹⁰

⁷ Insurance Journal, "Chubb: Cyber Claim Severity Nearly Doubled for Large Businesses," March 30, 2026, reporting the Chubb 2026 Cyber Claims Report. insurancejournal.com/news/national/2026/03/30/863799.htm

⁸ Insurance Journal, "Chubb: Cyber Claim Severity Nearly Doubled for Large Businesses," March 30, 2026, reporting the Chubb 2026 Cyber Claims Report. insurancejournal.com/news/national/2026/03/30/863799.htm

⁹ Coalition, Inc., 2026 Cyber Claims Report, March 5, 2026 (based on 100,000+ global policyholders, calendar year 2025). coalitioninc.com/claims-report/2026

¹⁰ Coalition, Inc., 2026 Cyber Claims Report, March 5, 2026 (based on 100,000+ global policyholders, calendar year 2025). coalitioninc.com/claims-report/2026

CAPACITY: REINSURANCE, INSURANCE-LINKED SECURITIES, AND ALTERNATIVE CAPITAL

Capacity remains robust. Reinsurers continue to support primary insurers largely through proportional covers, with a notable recent shift toward non-proportional structures for greater tail protection, such as using excess-of-loss with lower attachment points and sliding-scale commissions.¹¹ The insurance-linked securities and catastrophe-bond markets deployed over \$1.3 billion in 144A cyber catastrophe (CAT) bonds in 2025, including a \$300 million PoleStar 2026-1 issuance and a \$150 million East Lane Re 2026-1 issuance.

MARKET INNOVATION: PARAMETRIC AND SYSTEMIC-RISK SOLUTIONS

Carriers are developing new products aimed at systemic and aggregation risk, particularly as businesses deepen their reliance on cloud infrastructure. In August 2026, a Parametric Cloud Outage Solution was launched that pays a predetermined amount when a defined cloud-service outage trigger is met, rather than relying on a traditional indemnity-based claims process. It features a two-hour waiting period, no monetary retention thereafter, a rapid payout process, and the option to be added as an endorsement to an existing cyber policy.¹² The scale of the underlying exposure is significant, considering global enterprise spending on cloud infrastructure services reached \$129 billion in the first quarter of 2026 alone, up 35% year over year and the fastest growth since 2021.¹³

¹¹ AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

¹² Insurance Journal, "AIG Starts Parametric Cloud Outage Solution," August 14, 2026; AIG press release, August 13, 2026. [insurancejournal.com/news/national/2026/08/14/881539.htm](https://www.insurancejournal.com/news/national/2026/08/14/881539.htm)

¹³ Synergy Research Group, global cloud infrastructure spending data, Q1 2026, as cited by AIG.

Section 2. The Cybersecurity

Threat Landscape

The evolving threat landscape is the mirror image of the underwriting and pricing decisions cyber insurers are, or should be, making. Every escalation described below translates into frequency, severity, or correlation pressure that the eighth consecutive quarter of rate cuts has yet to reflect.

A THREAT LANDSCAPE IN STRUCTURAL TRANSITION

The 2025 report characterized 2024 as a market inflection point, marked by the first-ever contraction in U.S. direct written premium (a 7.11% decline to \$9.14 billion) while claim counts rose nearly 40%.¹⁴ Entering 2026, the threat landscape has not stabilized; it has fundamentally shifted. The convergence of frontier artificial intelligence, maturing ransomware ecosystems, deepening third-party dependencies, and rising geopolitical cyber operations is compressing the time between vulnerability discovery and exploitation from years to hours, with mean time-to-exploit collapsing from 2.3 years in 2018 to roughly 10 hours in 2026.¹⁵

Cyber risk is evolving at the pace of machines, but remediation continues to lag because organizational processes are based on human speed. In the 2026 reporting period, only 26% of critical vulnerabilities in the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities Catalog were fully remediated, down from 38% the prior year, while median time to full remediation rose to 43 days from 32, and the median organization faced roughly 50% more critical vulnerabilities to patch.¹⁶

For the cyber insurance market, the operating environment itself is changing, with direct implications for underwriting, accumulation risk, policy wording, and regulatory monitoring. Even framed as a “\$15 billion market poised for further profitable growth,”¹⁷ cyber must be read against global cybercrime costs expected to reach \$14 trillion by 2028.¹⁸ Therefore, annual statement data must be interpreted against a threat environment that is larger, structurally faster, and more connected than the prior cycle.

¹⁴ NAIC, 2025 Report on the Cybersecurity Insurance Market.

¹⁵ CrowdStrike, Zero Day Clock data; “Five Steps for Frontier AI Security Readiness” (white paper), 2026.

¹⁶ Verizon, 2026 Data Breach Investigations Report (DBIR)

¹⁷ Munich Re, Global Cyber Risk and Insurance Survey 2026.

¹⁸ Financial Stability Institute / International Association of Insurance Supervisors, “Cyber Insurance Unpacked,” June 2026.

VOLUME, VELOCITY, AND LOSS MAGNITUDE

Cyber risk is now the leading global business concern, driven by heightened threat-actor capability, accelerating digitalization, and supply chain vulnerability. Global economic losses from cyber incidents are estimated at \$1 trillion to more than \$10 trillion annually, with one widely cited projection reaching \$12.2 trillion by 2031. Yet, only about 1% of global economic cyber losses are covered by insurance, underscoring the protection gap that conditions market demand.^{19 20}

U.S. reporting reinforces the scale. The FBI Internet Crime Complaint Center received 1,008,597 complaints in 2025, with reported losses exceeding \$20.877 billion, a 26% year-over-year increase, with cyber-enabled fraud alone accounting for 85% of total losses.²¹

The manner of initial compromise is also shifting. For the first time, exploitation of vulnerabilities became the most common initial access vector in confirmed breaches, rising from 20% to 31% and overtaking credential abuse, which fell to 13%. Breaches involving a third party increased 60% year over year to 48% of all breaches, consistent with an estimated fourfold rise in major supply-chain breaches over five years.²²

THE ARTIFICIAL INTELLIGENCE INFLECTION POINT

AI is reshaping both attack surfaces and defensive tooling, with material implications for cyber pricing and capacity. Arguably one of the most consequential developments of the year is the emergence of frontier AI models capable of autonomously identifying software vulnerabilities and generating working exploits at machine speed, described as a potential “step change” in cyber risk. In the weeks before the April 2026 announcement of the Mythos model, a frontier system scanned critical software infrastructure and identified thousands of previously unknown zero-day vulnerabilities across every major operating system and web browser, 99% of which remained unpatched at the time of disclosure.²³

¹⁹ *Cybersecurity Ventures, global cybercrime cost projections.*

²⁰ *Financial Stability Institute / International Association of Insurance Supervisors, “Cyber Insurance Unpacked,” June 2026.*

²¹ *FBI Internet Crime Complaint Center (IC3), 2025 Internet Crime Report.*

²² *Verizon, 2026 Data Breach Investigations Report (DBIR).*

²³ *Financial Stability Institute / International Association of Insurance Supervisors, “Cyber Insurance Unpacked,” June 2026.*

THE ARTIFICIAL INTELLIGENCE INFLECTION POINT *(continued)*

Underwriting implications:

AI-enabled adversary attacks rose 89% year over year, and zero-days exploited before disclosure rose 42% in 2025, while active exploitation increased a further 43% in the first quarter of 2026 alone.^{24 25} If AI democratizes offensive capability faster than defenders can patch, loss ratios may deteriorate, particularly for insureds relying on common software stacks.²⁶

Buyer sentiment confirms the significance of the issue. Seventy-one percent of C-level executives now cite AI as the most strategically relevant technology (up from 62% in 2024), yet 66% list data security and privacy as their top AI concern, and 62% cite cyberattacks specifically.²⁷

Not all assessments frame frontier AI as a cutoff. AI-driven vulnerability discovery could be characterized as a real step-function increase in speed, volume, and breadth, while cautioning against confusing acceleration with transformation. Most AI-discovered vulnerabilities fall into familiar classes that mature security programs already anticipate, leaving organizations with strong fundamentals better positioned to absorb the change.²⁸

AI is reshaping fraud and intrusion. In one industry study, 98% of insurers believed AI-powered editing tools are fueling an increase in digital insurance fraud; 99% reported encountering manipulated or AI-altered claims documentation; and only 32% felt very confident in their ability to detect deepfakes. Thirty-six percent of consumers, rising to 55% among Generation Z, said they would consider digitally altering a claim image or document even if doing so violated insurer rules.²⁹

²⁴ CrowdStrike, Zero Day Clock data; "Five Steps for Frontier AI Security Readiness" (white paper), 2026.

²⁵ Beazley Security, threat activity data, Q1 2026.

²⁶ National Bureau of Economic Research, Working Paper No. 31668.

²⁷ Munich Re, Global Cyber Risk and Insurance Survey 2026.

²⁸ Center for Internet Security, "Mythos Retold," April 2026.

²⁹ Verisk, 2026 State of Insurance Fraud Study, March 17, 2026. verisk.com/company/newsroom

RANSOMWARE: STEADY VOLUME, RISING SOPHISTICATION, CONCENTRATED ACTORS

Ransomware remains a dominant driver of insured cyber losses, but the 2026 picture is more nuanced than headline volume suggests. Volume has plateaued at a high level. In the first quarter of 2026, researchers tracked 2,135 publicly posted ransomware victims, essentially flat compared with 2,287 in the fourth quarter of 2025 and 2,063 in the first quarter of 2025—across 68 active groups.³⁰

Headline volume understates the loss dynamics beneath it. Ransomware rose to 48% of all breaches from 44%, even as a record 69% of victims declined to pay, and the median ransom paid fell 7% to \$139,875.³¹ The industry-wide cyber loss ratio rose to 53 in 2025 from 48.7 in 2024, the highest since the pandemic-era spike, and this deterioration occurred through an eighth consecutive quarter of rate decreases.³²

Global data corroborate a high plateau, with 2025 shaping up as a likely third consecutive record year for ransomware, attacks up more than 30% to 7,419 worldwide, with the U.S. accounting for roughly half, and major incidents at large UK retailers and manufacturers illustrating the operational-disruption exposure now central to cyber underwriting.³³

SOCIAL ENGINEERING, BUSINESS EMAIL COMPROMISE, AND DEEPPAKES

The human attack surface remains the most consistent entry point for loss. The human element was present in 62% of breaches in the 2026 reporting period, and human-driven incidents translate directly into the largest and most frequent claim categories.³⁴

Business email compromise (BEC) remains one of the costliest cyber-enabled crimes, accounting for more than \$3 billion in reported U.S. losses in 2025 across 24,768 complaints, second only to investment fraud. Social engineering is also evolving in its channels and methods. Voice and mobile-based attacks now produce simulated click rates roughly 40% higher than email phishing, while pretexting increasingly precedes ransomware and extortion.

³⁰ GuidePoint Security (GRIT), Q1 2026 Ransomware and Cyber Threat Insights.

³¹ Verizon, 2026 Data Breach Investigations Report (DBIR).

³² AM Best, "U.S. Cyber: Premium Growth Lags Behind Cyber Threats," Best's Market Segment Report, June 2026 (BestLink data).

³³ Comparitech ransomware tracking data, 2025, as cited in AM Best, Global, July 2026.

³⁴ Verizon, 2026 Data Breach Investigations Report (DBIR).

SOCIAL ENGINEERING, BUSINESS EMAIL COMPROMISE, AND DEEPFAKES *(continued)*

Coverage structure compounds exposure. Standard cyber policies frequently exclude, or sharply limit, social engineering and funds transfer fraud losses, often relying on a policyholder's separate crime coverage to respond, a structural gap between how organizations increasingly perceive their top cyber risk and how their insurance programs are actually built to respond.³⁵

Cyber-enabled fraud and phishing overtook ransomware as the top cyber risk concerning chief executives heading into 2026, with 73% of surveyed executives reporting that they or someone in their network had experienced cyber-enabled fraud in 2025. Chief information security officers (CISOs), by contrast, continue to rank ransomware first, followed by supply-chain disruption, a divergence attributed to CEOs prioritizing financial-loss prevention while security leaders remain focused on operational resilience.³⁶

Generative AI is lowering the barrier to entry and raising believability. More than 22,000 complaints with an AI nexus were received in 2025, with adjusted losses exceeding \$893 million.³⁷ Insurers are documenting coordinated deepfake fraud, including cases in which a phone-number-spoofing specialist works alongside a deepfake operator to simulate an internal executive call and trigger an employee action against the company.³⁸ These developments erode the traditional fraud indicators awareness training was built on and place renewed emphasis on payment verification and out-of-band authentication.

³⁵ Debevoise Data Blog, "Business Email Compromise: Reducing Risk and Litigation Exposure," June 19, 2026.

³⁶ World Economic Forum (with Accenture), *Global Cybersecurity Outlook 2026*, January 12, 2026. [weforum.org/publications/global-cybersecurity-outlook-2026](https://www.weforum.org/publications/global-cybersecurity-outlook-2026)

³⁷ FBI Internet Crime Complaint Center (IC3), *2025 Internet Crime Report*.

³⁸ AM Best, "U.S. Cyber: Premium Growth Lags Behind Cyber Threats," *Best's Market Segment Report*, June 2026 (BestLink data).

LARGE-SCALE DATA BREACH AND THIRD-PARTY VENDOR ACTIVITY

Large breaches involving insurance-adjacent organizations and their vendors remained a persistent feature of the landscape, illustrating how deeply exposed the industry's data ecosystem is to third-party and social-engineering risk. A major life insurer disclosed that an unauthorized party had accessed one of its agents' email accounts in December 2025 and later confirmed the account contained clients' names, addresses, Social Security numbers, driver's license numbers, financial account information, and medical and health insurance information, demonstrating how a single compromised agent credential can expose sensitive policyholder data well beyond a carrier's own core systems.³⁹

A health care revenue cycle and practice management software vendor processing more than \$70 billion in net health care charges annually disclosed a data center intrusion affecting 3,803,750 individuals, with exposed data including Social Security numbers, insurance policy numbers, and claims and benefits information. Because the vendor processes data on behalf of health care organizations, most affected patients had no direct relationship with it.⁴⁰ Separately, a publicly traded Medicare Advantage insurer disclosed that a threat actor used social engineering to compromise three non-managerial employee accounts, gaining potential access to personal and protected health information. A reminder that social engineering remains a primary entry point for attackers targeting insurance-adjacent organizations.⁴¹

THIRD-PARTY DEPENDENCY AND ACCUMULATION RISK

If the defining underwriting challenge of the prior cycle was ransomware frequency, the defining challenge of the current cycle is accumulation risk arising from shared digital dependencies. This is identified as the most pressing concern in cyber underwriting because a single event or vulnerability can trigger correlated losses across many policyholders simultaneously and because non-affirmative coverage and overlapping policies compound the exposure.⁴²

³⁹ PR Newswire, "New York Life Insurance Co. Data Breach," May 17, 2026;
Commonwealth of Massachusetts Notice of Data Breach filing, 2026.

⁴⁰ Bleeping Computer, "Unlimited Technology Systems breach impacts 3.8 million people," August 7, 2026.

⁴¹ The HIPAA Journal, "Clover Health Assessing Impact of Social
Engineering Incident," July 22, 2026; SecurityWeek, July 21, 2026.

⁴² Financial Stability Institute / International Association of Insurance
Supervisors, "Cyber Insurance Unpacked," June 2026.

THIRD-PARTY DEPENDENCY AND ACCUMULATION RISK

(continued)

The structural driver is concentration. More than three-quarters of companies rely on cloud services across most or all operations, yet only three providers account for over 60% of global cloud infrastructure, and each experienced a significant outage in 2025. A single point of failure at a dominant provider can generate simultaneous business interruption, data loss, and liability claims across a large share of an insurer's portfolio, extending to nth-party dependencies, where insureds have limited visibility. Recent outages at AWS, CrowdStrike, and CDK Global are live demonstrations of this systemic exposure.⁴³

GEOPOLITICAL AND STATE-SPONSORED OPERATIONS

Geopolitical instability is now a direct input to cyber demand and to tail risk, with strengthening demand linked to instability stemming from the Iran-U.S. conflict that began in February 2026 and a surge in cybercrime activity in the first months of operations, even as the direct loss impact remains difficult to measure.⁴⁴

On the exposure side, insurers' losses linked to state-backed operations are expected to be partly contained by war exclusions, which have been widely applied in cyber policies since 2023. Considerable uncertainty remains, however, because triggering an exclusion typically requires proving a link between the malicious act and a state-backed perpetrator, an evidentiary standard difficult to meet at machine speed and across obfuscated infrastructure. Nation-state actors, particularly those targeting file transfer software and managed service providers, continue to blur the line between espionage, disruption, and financially motivated crime.⁴⁵

War exclusion wording, attribution standards, and the treatment of "hostile cyber activity" below the threshold of armed conflict are becoming central to policy wording review. Divergent exclusion language across carriers is itself a source of coverage uncertainty that regulators could monitor for consumer protection and solvency implications.

SILENT CYBER AND SILENT ARTIFICIAL INTELLIGENCE

"Silent," or non-affirmative, cyber coverage for cyber losses unintentionally embedded in non-cyber policies remains a live concern despite years of tightening exclusions, as overlapping policies and non-affirmative coverage can compound accumulation risk precisely when a systemic event strikes. Gaps persist across property, marine, D&O, and general liability lines.⁴⁶

⁴³ AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

⁴⁴ AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

⁴⁵ Verizon, 2026 Data Breach Investigations Report (DBIR).

⁴⁶ Financial Stability Institute / International Association of Insurance Supervisors, "Cyber Insurance Unpacked," June 2026.

THE PROTECTION GAP AND SMALL- AND MEDIUM-SIZED ENTERPRISES

The protection gap remains the market's defining structural feature and its largest growth opportunity. Only about 1% of global economic cyber losses are insured, and small- and medium-sized enterprise penetration is estimated at just 10% to 20%.^{47 48} These businesses represent a significant area of potential growth, though the sheer number of small insureds also concentrates aggregation risk for carriers that write them at scale.

Small- and medium-sized enterprises are simultaneously the most exposed and the least protected. They typically lack mature controls, are increasingly targeted as digitalization and cloud adoption rise, and are frequently the entry point for supply chain compromise for larger organizations. Closing the gap will require sustained partnership among insurers, brokers, agents, and trade associations to raise awareness. Absent such effort, the market may need a "tipping point," such as a systemic event, to drive adoption.⁴⁹

QUANTUM ON THE HORIZON

Quantum computing represents a longer horizon but structurally significant threat that is already shaping present-day behavior. Threat actors are pursuing a "harvest now, decrypt later" strategy, exfiltrating encrypted data today in anticipation that future quantum capability will break the encryption protecting it. Cybersecurity industry reporting suggests, AI is already increasing threat actors' ability to break encryption, and this approach leaves victims unaware of a compromise until stolen data is used, extending the tail of cyber loss development.⁵⁰

For underwriters, the quantum horizon has three practical effects. First, it lengthens the effective tail of today's data breach claims because harvested data may surface as a loss years after the policy period. Second, it elevates the importance of post-quantum cryptography readiness and data retention practices as underwriting criteria. Third, it raises long-dated accumulation questions for insurers holding portfolios of long-tail liability exposure. While large-scale cryptographically relevant quantum computing is not yet operational, the harvesting behavior it incentivizes is a present-tense underwriting consideration.

⁴⁷ Financial Stability Institute / International Association of Insurance Supervisors, "Cyber Insurance Unpacked," June 2026.

⁴⁸ Swiss Re Institute, SME cyber-insurance penetration estimates.

⁴⁹ AM Best, "Global Cyber Insurance Market Segment Outlook," July 2026.

⁵⁰ AM Best, "U.S. Cyber: Premium Growth Lags Behind Cyber Threats," Best's Market Segment Report, June 2026 (BestLink data).

Section 3. Summary and Supervisory Outlook

Taken together, the 2025 Cyber Supplement data and the broader 2025–2026 threat landscape describe a market that remains large, profitable, and increasingly sophisticated, but one in which the direction of expected loss and the direction of realized price have diverged.

Domestic policies in force rose 33% to 5.84 million and reported claims increased 20% to 56,323, even as premium growth remained modest.

The financial picture in Section 1 and the threat picture in Section 2 describe the same phenomenon from two directions. Expected loss is rising, driven by faster exploitation, AI-enabled offense, third-party accumulation, and a lengthening tail from harvested data and third-party claims. Realized price, meanwhile, has fallen through an eighth consecutive quarter of rate decreases. The loss incurred and DCC ratio climbed to 53 precisely as the market softened, an inversion of the 2021 hard-market pattern in which deteriorating results and rising rates moved together. AM Best notes that this dynamic could test the adequacy of rates over the intermediate term, while maintaining a stable outlook on the segment.

Layered onto that base dynamic are several threat trends likely to intensify the pressure on rate adequacy: 1) sharply rising severity for large-account losses driven by business interruption and litigation costs, even as smaller accounts appear to be experiencing more contained severity alongside rising frequency; 2) a shift in executive concern toward cyber-enabled fraud, a category of loss that current cyber and crime policy structures often handle inconsistently; 3) the dual use rise of AI as both a fraud amplifier and a defensive and underwriting tool; and 4) persistent, well-documented protection gaps that leave meaningful exposure outside the insurance system altogether.