Markets in Focus
Cyber

MARKET UPDATE

SECOND QUARTER
2026

Cyber
Snapshot

CYBER INSURANCE MARKET

+ Capacity remains plentiful; new entrants continue to enter the market
+ Sustained soft market conditions with continued pricing moderation
+ Cyber remains one of the most competitive insurance lines
+ Well-controlled risks are being rewarded with favorable pricing
+ Market stability is expected to continue through 2026

RISK ENVIRONMENT

+ Intrusions can progress in minutes or seconds
+ Data exfiltration can begin almost immediately after access
+ Defenders must shift to real-time detection and response capabilities

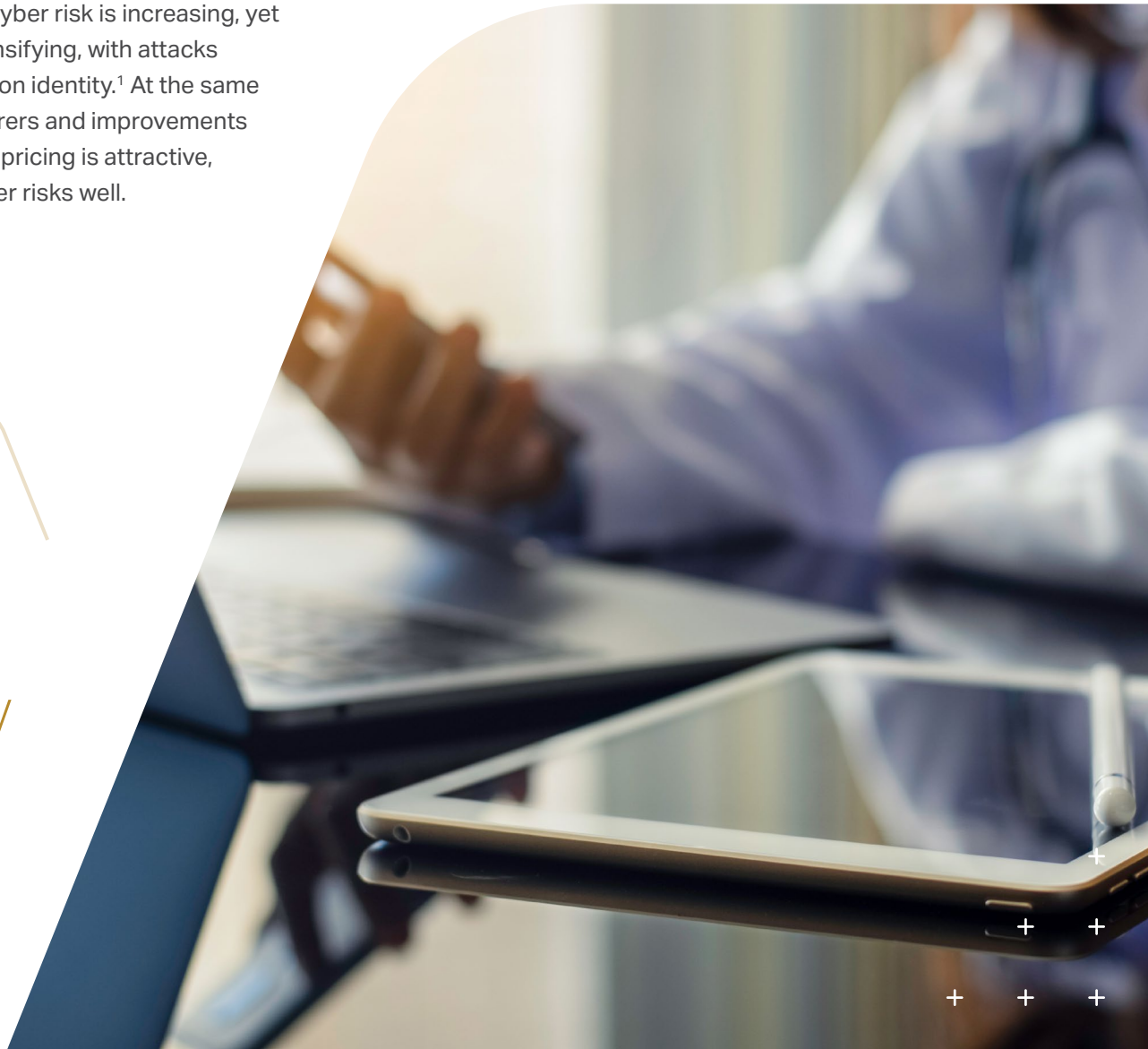
COVERAGE & INSURANCE TRENDS

+ **Cyber & Tech E&O:** Coverage remains broadly intact
+ **Other financial lines:** Early-stage AI exclusions emerging
+ Coverage gaps may develop outside cyber policies
+ Organizations should review total risk across all policies, not just cyber
+ Loss is shifting from ransom to regulatory, legal, and reputational exposure

Executive Summary

The cyber landscape in the first part of 2026 is paradoxical: cyber risk is increasing, yet insurance conditions remain favorable. Threat activity is intensifying, with attacks becoming faster, more automated, and increasingly focused on identity.[1] At the same time, because of continuing competition between cyber insurers and improvements in cybersecurity by insureds, insurance remains plentiful and pricing is attractive, particularly for those companies that are managing their cyber risks well.

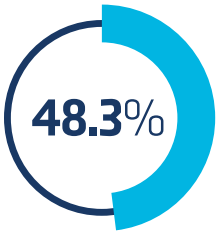
> Threat activity is intensifying, with attacks becoming faster, more automated, and increasingly focused on identity.



Insurance
Market Outlook

Cyber Insurance Marketplace

The cyber insurance market remains broadly competitive. Organizations' cyber hygiene has improved to the point that insurers see cyber insurance as a profitable line of business. Capacity is plentiful, which has prolonged the soft market and continued the trend of premium moderation. We do not anticipate a significant change in the market for the remainder of 2026.



In Q1 2026, 48.3% of respondents reported cyber pricing down 1–9%, 37.9% reported no change, and only 3.4% reported increases of 1–9%.

First Quarter Cyber Pricing Trend Summary

	CYBER
DOWN MORE THAN 30%	0.0%
DOWN 20–30%	0.0%
DOWN 10–19%	10.3%
DOWN 1–9%	48.3%
NO CHANGE	37.9%
UP 1–9%	3.4%
UP 10–19%	0.0%
UP 20–29%	0.0%
UP 30–50%	0.0%
UP MORE THAN 50%	0.0%
NOT SURE	0.1%

Source: CIAB Commercial Property/Casualty Market Index Q1 2026[2]

Insurance Trends

AI Exposures Push Policy Boundaries

Organizations often ask whether losses involving artificial intelligence are covered. The good news is that cyber and technology E&O policies do not limit coverage in any way. The same is not necessarily true for other financial lines policies. A small number of insurers have begun to attach exclusions of varying breadth to D&O, employment practices liability, crime, and other financial lines policies. It remains to be seen whether competitive pressures affect how often those exclusions are used and whether the exclusions proliferate in the industry.

AI Coverage Landscape

CYBER & TECHNOLOGY E&O

No explicit AI exclusions

Coverage generally applies

Claims treated as standard technology losses

MARKET POSITION: Stable, broad, and largely unchanged

FINANCIAL LINES

Emerging AI exclusions

Varying breadth and scope

Not yet standard

AFFECTED LINES: D&O, EPL, and Crime

MARKET POSITION: Evolving and fragmented

INSIGHTS

While cyber policies remain consistent, financial lines insurers are beginning to test AI-specific exclusions. Adoption remains limited, but competitive dynamics will determine whether these exclusions expand or recede.

Industry **Trends**

Cyberattack Vectors are Changing

Historically, threat actors have introduced malware, including ransomware, to compromise computer systems and electronic data. While this is still happening, today, criminals are increasingly focused on compromising user identities rather than exploiting system vulnerabilities. Using stolen credentials makes it far easier to access a victim's systems and harder to detect unauthorized access. Credential theft and abuse of authentic access paths are now central to many intrusions.[3] Strong identity governance is essential to resist these attacks.

> Cyber intrusions are increasingly driven by stolen identities, making identity governance a front-line defense.

The Ransomware Scourge Continues

23%
OF RANSOMWARE ATTACKS RESULTED IN PAYMENT IN Q1 2026

15%
RANSOMS INCREASED BY 15% FROM Q4 2025

In the first quarter of 2026 ransoms were paid in only 23% of attacks.[4] While that is good news, the average ransom was $680,081, a 15% increase over the average in Q4 2025.[5] Today, attackers are prioritizing data theft as the basis for extortion. Such theft took place in 77% of attacks in 2025.[6] This shift changes the nature of loss toward legal, regulatory, and reputational consequences tied to data exposure.

Supply Chain Risk Continues to Grow

Organizations are increasingly affected by cyber incidents involving vendors and service providers. An attack on a vendor that affects an organization's ability to conduct business can do great damage to its financial performance and reputation. The same is true of a cyberattack against an organization that affects its vendors. A clear example is the Jaguar Land Rover cyber incident in 2025, which forced production to shut down for several weeks.[7] The disruption affected thousands of suppliers and partners that were temporarily unable to do business with the company.

> Cyber risk is no longer contained within a single organization — vendor incidents can quickly become ecosystem-wide business disruptions.

Cyber
Risk Environment

Attacks Are Faster and More Automated

Cyberattacks now progress at a speed that makes detection and response extremely difficult. The average time between initial compromise and lateral movement has fallen dramatically, with some incidents unfolding in minutes or even seconds. In documented cases, attackers have begun exfiltrating data within minutes of access.[8]

The window between initial compromise, lateral movement, and data exfiltration has compressed dramatically, **with some attacks progressing in minutes or even seconds**.

This speed gives threat actors time to steal or corrupt data and damage computer systems before the attack is discovered and a patch is created and applied. The compression of timelines increases the importance of rapid detection and response.

Artificial Intelligence Is Amplifying Threat Activity

AI is now a vital tool for threat actors to mount and scale cyberattacks. Its uses include creating phishing emails, deepfakes used in social engineering attacks, and developing malware. Perhaps the most stunning example is a cyber espionage attack launched against 30 global targets by Chinese hackers in September 2025. The attack was carried out by AI agents instead of by the hackers themselves, and was successful in some instances.[9] AI-enabled attacks increased significantly in 2025.[10]

> AI is not just improving attacker efficiency — it is helping threat actors scale and automate complex operations.

Source Information

1. Mayers, A., Rodriguez, C., and Meyers, J. (2026). *2026 Global Threat Report: Year of the Evasive Adversary*. CrowdStrike. https://www.crowdstrike.com/en-us/global-threat-report/

2. Vasile, N., and West, Z. (2026, February 18). *Q4 2025 Showed Very Soft Market Conditions, According to The Council's P&C Market Survey*. Council of Insurance Agents & Brokers. https://www.ciab.com/resources/news-release-q4-2025-showed-very-soft-market-conditions-according-to-the-councils-p-c-market-survey/

3. Mayers, A., Rodriguez, C., and Meyers, J. (2026). *2026 Global Threat Report: Year of the Evasive Adversary*. CrowdStrike. https://www.crowdstrike.com/en-us/global-threat-report/

4. Coveware. (2026, April 30). *Patch management goes from hard, to ludicrous in the agentic AI era.* Coveware. https://www.coveware.com/blog/2026/4/27/patch-management-goes-from-hard-to-ludicrous-in-the-agentic-ai-era

5. Coveware. (2026, April 30).

6. Sadayappan, B., et al. (2026, March 16). *Ransomware Under Pressure: Tactics, Techniques, and Procedures in a Shifting Threat Landscape*. Google Threat Intelligence. https://cloud.google.com/blog/topics/threat-intelligence/ransomware-ttps-shifting-threat-landscape

7. Cyber Monitoring Centre. (2025, October). *Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident*. CMC. https://cybermonitoringcentre.com/2025/10/22/cyber-monitoring-centre-statement-on-the-jaguar-land-rovercyber-incident-october-2025/#)

8. Mayers, A., Rodriguez, C., and Meyers, J. (2026). *2026 Global Threat Report: Year of the Evasive Adversary*. CrowdStrike. https://www.crowdstrike.com/en-us/global-threat-report/

9. Lakshmanan, R. (2025, November 14). *Chinese Hackers Use Anthropic's AI to Launch Automated Cyber Espionage Campaign*. The Hacker News. https://thehackernews.com/2025/11/chinese-hackers-use-anthropics-ai-to.html

10. Mayers, A., Rodriguez, C., and Meyers, J. (2026). *2026 Global Threat Report: Year of the Evasive Adversary*. CrowdStrike. https://www.crowdstrike.com/en-us/global-threat-report/

Markets in Focus
Contributors

TIM BURKE
EVP, Head of Cyber / Commercial E&O

WILLIAM BOECK
EVP, Cyber Product Leader

ANGELA THOMPSON
Marketing Strategist, Market Intelligence & Insights

BRIAN SPINNER
Marketing Specialist, Market Intelligence & Insights

FOR ANY QUESTIONS, PLEASE REACH OUT TO:

TIM BURKE
EVP, Head of Cyber / Commercial E&O
tim.burke@imacorp.com

NPN 1316541 | IMA, Inc dba IMA Insurance Services
California Lic #0H64724

CT-MIF-IMA-C-060926