Markets in Focus

Q3 2025

CYBER

Market Update

IMA

CYBER INSURANCE MARKETPLACE

Abundant cyber insurance capacity persisted throughout the first half of 2025. Cyber continues to be a profitable insurance line, and insurers are focusing on growing their cyber books. Insurers are backing an ever-increasing number of cyber MGAs that usually focus on small and middle market organizations.

Insurers continue to innovate with respect to coverage. Several insurers have released new policy forms in 2025 that broaden coverage, address a few pain points, and add features that will be popular with insureds. Nevertheless, insurers are tightening up language around third-party risk exposures, especially when it comes to vendor responsibilities, data handling, and breach response.

Insurers also continue to invest in providing meaningful risk control services. These can be truly beneficial for organizations that take advantage of them.

Premium decreases are still possible for organizations that embrace practices to manage their privacy and cybersecurity risks. The size of decreases has moderated, though; now they are typically limited to 10% or less.

All of this paints a picture of a healthy cyber insurance marketplace for insurers and for buyers. It speaks well for the industry that this is the case in the face of a challenging risk environment.

CYBER PREMIUM PRICING

The following survey response data from the Council of Insurance Agents & Brokers' Commercial Property/Casualty Market Report covering Q2 2025. Cyber premiums fell an average of 1.5%.[1]

1	**Down more than 30%**	0.00%
2	**Down 20% - 30%**	0.00%
3	**Down 10% to 19%**	3.00%
4	**Down 1% to 9%**	47.0%
5	**No Change**	31.0%
6	**Up 1% to 9%**	11.0%
7	**Up 10% to 19%**	0.00%
8	**Up 20% to 29%**	3.00%
9	**Up 30% to 50%**	0.00%
10	**Up more than 50%**	0.00%
N/A	**Not Sure**	5.00%

CYBER RISK ENVIRONMENT

Ransomware

As is so often the case, ransomware was a dominant trend in the first half of 2025. In the second quarter alone, the average ransom paid increased by more than 100% to $1.13 million.[2] That number isn't the result of a few big ransoms being paid. The median ransom also increased by 100% to $400,000. A third of all attacks were against organizations with fewer than 100 employees or less, and another third against those with 101 to 1,000 employees.[3] 74% of all attacks involved the theft of data from victims. The good news is that only 26% of ransomware attacks in 2Q2025 resulted in ransom payments—a reflection of growing resilience on the part of organizations.

The role of third parties in high-profile ransomware attacks is significant. Threat actors are compromising vendors as a means to get inside the IT systems of their intended victims. An attack in May against a well-known cryptocurrency exchange is a good example. The exchange used IT vendors outside the U.S. In an unusual turn of events, instead of hacking into the vendors' computer systems, the threat actor simply bribed the vendors' employees to give them information about the exchange's customers that was then used to trick those customers into sending funds to the threat actor.

Supply Chain Attacks

Attacks on supply chain vendors continue to produce significant disruptions and losses for their customers. In June, a cyberattack impacted a large food wholesale distributor of food supplies to grocery stores across the U.S., and to many regional and local natural foods grocers. The company reported that the attack would likely have a significant financial impact, including reduced sales, increased operational costs, and expenses related to investigating and fixing the breach.[4] The cascading effects of such were immediate. Disruptions left store shelves empty and affected businesses relying on the company to supply goods for sale. The disruptions continued throughout July and into August.

Emerging Threats

New attack vectors continue to emerge. GPS spoofing—as seen with the May 2025 grounding of MSC Antonia in the Red Sea—shows how cyber threats extend beyond traditional IT systems. Spoofing occurs when a fake GPS signal is broadcast to a receiver, tricking it into believing it's in a location other than its actual position. This can disrupt navigation systems, misdirect vehicles, and even manipulate location-based applications.[5]

Sources:

1 Vasile, N. and West, Z. (2025, August 13). Commercial Property/ Casualty Market Index Q2/2025. CIAB. https://www.ciab.com/resources/q2-2025-p-c-market-survey/

2 Coveware. (2025, July 23). Targeted social engineering is en vogue as ransom payment sizes increase. Coveware. https://www.coveware.com/blog/2025/7/21/targeted-social-engineering-is-en-vogue-as-ransom-payment-sizes-increase

3 Id.

4 Geller, Eric. (2025, June 27). United Natural Foods says cyberattack will reduce quarterly earnings. Cybersecurity Dive. https://www.cybersecuritydive.com/news/unfi-cyberattack-reduce-quarterly-earnings/751849/

5 McAfee. (2025). What is GPS spoofing?. McAfee. https://www.mcafee.com/learn/what-is-gps-spoofing/

MARKETS IN FOCUS CONTRIBUTORS

TIM BURKE | *Executive Vice President, Head of Cyber | Commercial E&O*

WILLIAM BOECK | *Executive Vice President, Cyber Product Leader*

ANGELA THOMPSON | *Marketing Strategist, Market Intelligence & Insights*

BRIAN SPINNER | *Senior Marketing Coordinator, Market Intelligence & Insights*

KEEP READING

MARKETS IN FOCUS

INSURANCE INSIGHTS

HR INSIGHTS

FOR ANY QUESTIONS, PLEASE REACH OUT TO:

TIM BURKE
Executive Vice President, Head of Cyber | Commercial E&O
tim.burke@imacorp.com