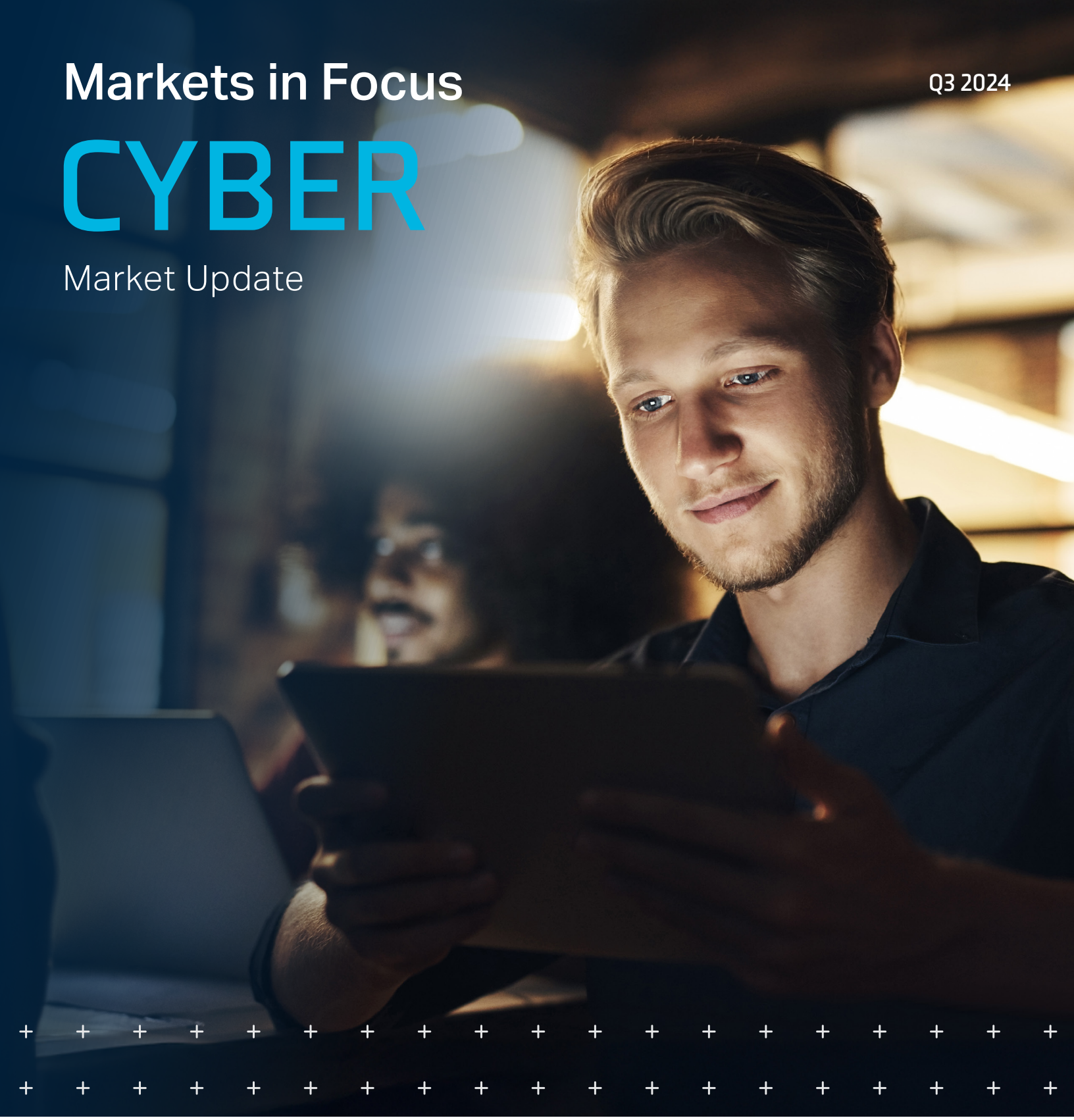
Markets in Focus

Q3 2024

CYBER

Market Update



CYBER INSURANCE MARKETPLACE

The cyber insurance marketplace was strong throughout the third quarter of 2024. Formidable competition existed between insurers to write new business. Cyber insurance premium decreases were the norm.

Insurers continue to be very interested in writing cyber policies. Capacity remains plentiful. Cyber MGAs continue to form and expand, which signifies the health of the market and the industry-wide desire to innovate in the cyber insurance space.

Cyber insurers were largely uninterested in expanding coverage in the third quarter. Ransomware and privacy claims outside the realm of data breaches continue to produce significant losses, so insurers were hesitant to change policy terms in ways that could increase losses. Insurers were willing to expand coverage on a case-by-case basis to win or retain business.

Insurers have taken steps to limit their exposure to certain types of claims. For example, in 2024 some insurers that have covered claims for the wrongful collection of data have put sublimits of $100,000 on that coverage. This is largely due to the growth of pixel litigation.[2] Class actions are being filed against organizations using online tracking technologies such as the Meta pixel that track the movement of website visitors on the site in order to show them personalized ads. Those lawsuits have proved to be expensive to defend and resolve. Healthcare organizations have been hit particularly hard.

We did not see any changes to underwriting standards in the third quarter. Insurers continue to require organizations to have basic cybersecurity controls in place to qualify for broad cyber coverage. While standards haven't changed, insurers are reacting to developments in the risk environment. One example is the questions being asked about the CrowdStrike outage.

The latest data from the Council of Insurance Agents & Brokers for the second quarter confirms the state of the marketplace.[1] Unlike the first quarter, where the number of premium increases and decreases were equal, the second quarter saw nearly twice as many decreases as there were increases.

CYBER PREMIUM PRICING

1	↓ Down more than 30%	0.00%
2	↓ Down 20% - 30%	2.44%
3	↓ Down 10% - 19%	4.88%
4	↓ Down 1% - 9%	34.15%
5	No Change	31.71%
6	↑ Up 1% - 9%	19.51%
7	↑ Up 10% - 19%	2.44%
8	↑ Up 20% - 29%	0.00%
9	↑ Up 30% - 50%	0.00%
10	↑ Up more than 50%	0.00%
N/A	Not Sure	4.88%

Source: CIAB Q2 2024 P/C Market Survey

The most forward-thinking insurers and MGAs are investing heavily in providing cyber risk management services. Those extend beyond free services and resources many other insurers offer and are similar to what an insured might receive from well-known third-party providers. Many of these services are of very high quality and quite reasonably priced for the value given.

CYBER RISK ENVIRONMENT

After the ransomware attacks on Change Healthcare and CDK Global and their knock-on effects on thousands of customers in the first half of the year, everyone hoped the third quarter would be relatively quiet. However, that hope was dashed quickly.

On July 19, 2024, a defective software update to CrowdStrike's Falcon Sensor product resulted in computers running Microsoft Windows failing to start up. The problem affected companies around the world. An early estimate of the resulting financial losses calculated them at $5.4 billion.[3] Insured losses were estimated to be between $300 million and $1 billion.[4]

In addition to the losses it caused, the CrowdStrike event was significant because there was nothing Falcon users could have done to protect themselves from the defective update. Moreover, the resulting losses would not be covered under all cyber policies. A well-crafted policy with broad system failure coverage can respond, though. For cyber insurance purposes, system failure arises when a computer system becomes unusable because of events listed in the policy. Better policies expand coverage beyond the list in the policy.

The ransomware scourge persisted in the third quarter. According to the latest quarterly report from Coveware, a ransomware incident response firm, reported that the average ransom payment increased to $479,237, a 23% increase over the average for the second quarter.[5] The median payment grew by 18% to $200,000. Phishing was the leading means of attack. Data theft took place in 76% of attacks. Healthcare, consumer services, and public sector organizations accounted for 44% of all attacks. Over 77% of attacks were directed against organizations with fewer than 1,000 employees. 37% affected organizations having 100 employees or less.

Data breaches, of course, continued in the third quarter. The good news is that the number is down from the first and second quarters.[6]

Sources:

1 The Council of Insurance Agents & Brokers. (2024). *The Council Commercial Property/Casualty Market Survey Q2 2024*. https://www.ciab.com/download/45285/?tmstv=1724084884

2 Jesse, E., & Weaver, H. (2024, August 14). *Tracking your cyber coverage: Pixel and other privacy- ... Tracking your Cyber Coverage: Pixel and Other Privacy-Related Litigation.* https://www.americanbar.org/groups/litigation/resources/newsletters/insurance-coverage/pixel-and-other-privacy-related-litigation

3 Parametrix. (2024). *CrowdStrike's Impact on the Fortune 500: An Impact Analysis.* Parametrix Insurance. https://cdn.prod.website-files.com/64b69422439318309c9f1e44/66a24d5478783782964c1f6f_CrowdStrikes%20Impact%20on%20the%20Fortune%20500_%202024%20_Parametrix%20Analysis.pdf

4 GuyCarpenter. (2024, August 1). *A CLOSER LOOK: UNVEILING THE GLOBAL IMPACT OF CROWDSTRIKE EVENT*. https://www.guycarp.com/content/dam/guycarp-rebrand/insights-images/2024/07/2024-8-1-Unveiling-the-Global-Impact-of-CrowdStrike-Event.pdf

5 Siegel, B. (2024, November 1). *Law enforcement doxxing raises risk profile for threat actors.* Coveware. https://www.coveware.com/blog/2024/11/1/law-enforcement-doxxing-raises-risk-profile-for-threat-actors

6 Identity Theft Resource Center. (2024). *Supply Chain Attacks Roar Back in Q3; Mega-Breaches Drive Increase in Victim*. https://www.idtheftcenter.org/wp-content/uploads/2024/10/ITRC-Q3-2024-Data-Breach-Analysis-1.pdf on page 2

MARKETS IN FOCUS CONTRIBUTORS

WILLIAM BOECK | *EVP, Cyber Product Leader*

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

KEEP READING

PREVIOUS EDITION

GENERAL EDITION

CYBER RISKS IN FOCUS

INSURANCE INSIGHTS

HR INSIGHTS

FOR ANY QUESTIONS, PLEASE REACH OUT TO:

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