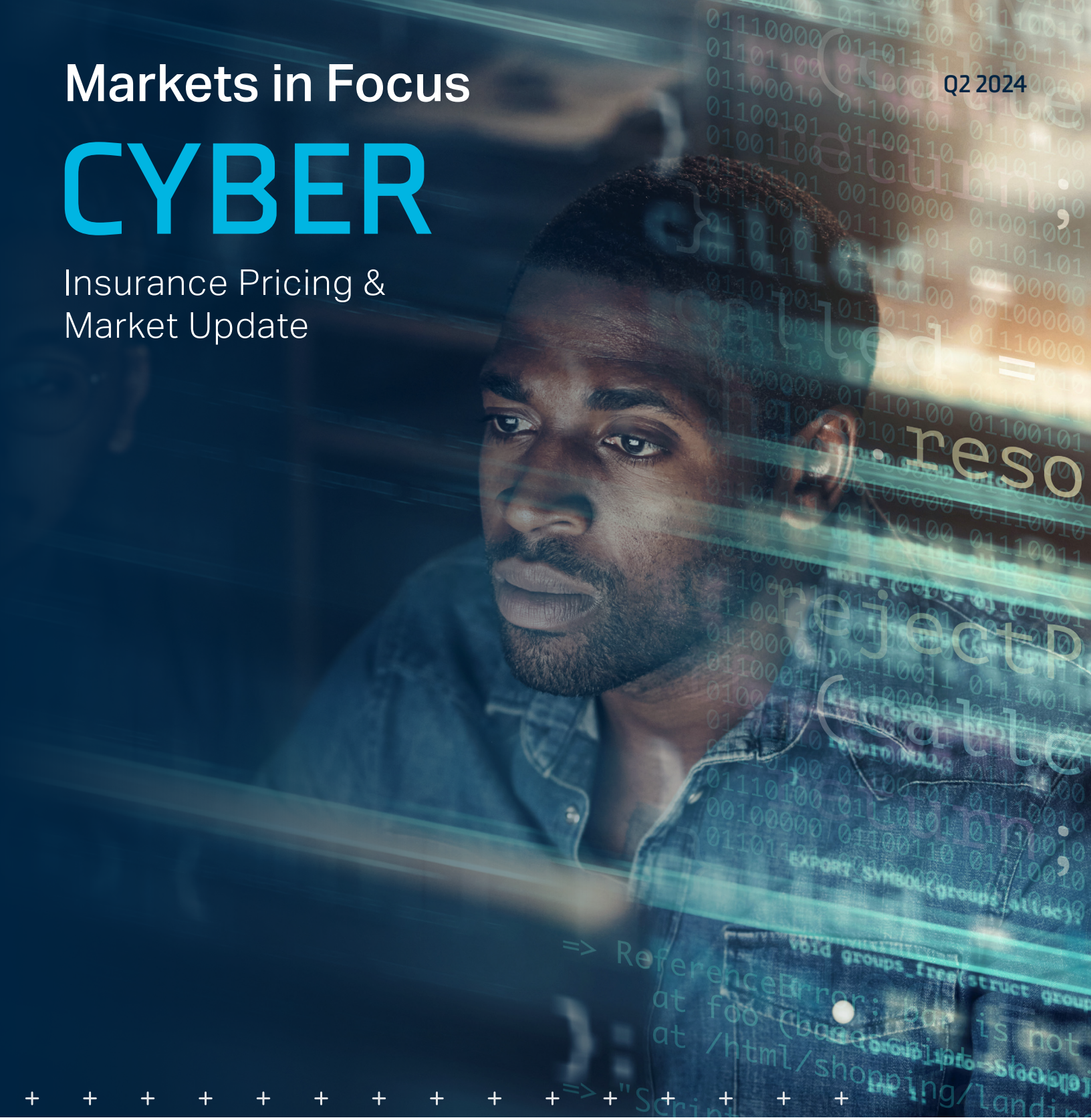
Markets in Focus

Q2 2024

CYBER

Insurance Pricing & Market Update



CYBER INSURANCE MARKETPLACE

The insurance market trends in the last quarter of 2023 continued into the first quarter of 2024. Overall, we categorize the market as stable.

The cyber insurance market continues to offer ample capacity, a positive sign of the market's health. This is partly due to many insurers' favorable reinsurance renewal in January. Pricing for cyber policies remains aggressive. Premium reductions were the norm rather than the exception throughout the first quarter. Decreases of 5% or more were common for policies providing only cyber coverage. Decreases were smaller for policies that contain errors and omissions (E&O) coverage, such as technology E&O.

The following survey response data from the Council of Insurance Agents & Brokers' Commercial Property/Casualty Market Report for Q4 2023[1] reflects trends that continued into the first quarter:

CYBER PREMIUM PRICING

1	↓ Down more than 30%	0.00%
2	↓ Down 20% - 30%	0.00%
3	↓ Down 10% - 19%	2.27%
4	↓ Down 1% - 9%	29.55%
5	No Change	31.82%
6	↑ Up 1% - 9%	22.73%
7	↑ Up 10% - 19%	9.09%
8	↑ Up 20% - 29%	0.00%
9	↑ Up 30% - 50%	0.00%
10	↑ Up more than 50%	0.00%
N/A	Not Sure	4.55%

These pricing trends are poised to continue into the second quarter. Many insurers have growth goals that can only be met by keeping their existing cyber business and writing new policies. That bodes well for an ongoing competitive marketplace. However, some insurers believe that the current rate environment is not sustainable. They think the current claims environment and emerging risks will likely produce insured losses that will force insurers to raise premiums. Whether that prediction is prophetic remains to be seen.

We have not seen cyber insurers attempt to impose new restrictions on coverage during the first quarter. Insurers remain willing to consider modifications and expansions of coverage when necessary to address an organization's actual needs.

Insurers' underwriting standards remained unchanged in the first quarter, reflecting the industry's commitment to robust risk management. Cyber underwriters continue to demand basic levels of cyber hygiene, including multifactor authentication, endpoint detection and response tools, employee cybersecurity training, and non-networked backups. There is a heightened focus on the need for maintaining a cyber business continuity plan. This requirement is driven by concerns about prolonged operational disruption. While it may be possible to find coverage for organizations without all the desired controls, they are likely to face fewer insurers willing to provide coverage, and the policies may be more expensive and have more coverage restrictions.

CYBER RISK ENVIRONMENT

While ransomware continues to be a significant cause of insured losses, the year 2024 could mark a pivotal shift, with privacy events and litigation potentially taking the forefront, underscoring the urgency of the situation.

2022 saw a dramatic rise in class action lawsuits alleging that online tracking technologies (pixels, cookies, etc.) improperly sent website visitors' personal information to third parties such as Meta and Google. Healthcare companies were hit particularly hard. That wave of litigation continued to build in the first quarter 2024. These cases are expensive to defend and require expertise with the relevant technologies and privacy laws. Several have resulted in multi-million dollar settlements, including one in the first quarter of 2024. Many more settlements are likely. Cyber insurers worry that the number of losses could affect their profitability. That could lead insurers to firm up pricing or even increase premiums. Insurers whose policies. exclude claims for the wrongful collection of data are using those exclusions to avoid covering settlements and, in some cases, the cost to defend the suits.

In February of this year, Change Healthcare announced that it was the victim of a cyber attack and had shut down its systems to prevent the attack from spreading. Change provides electronic infrastructure for payments and other matters to healthcare providers, pharmacies, and other healthcare businesses. Change is widely used in the industry, and its shutdown prevented its customers from issuing bills, receiving payments, issuing electronic prescriptions, and performing many other functions. This one event is having ripple effects throughout the healthcare industry and producing business interruption and other losses that will be covered under cyber policies. It has led to a renewed focus on the risk of attacks on supply chain vendors across all industries.

For more on cyber supply chain, read our latest publication on managing cyber supply chain risk.

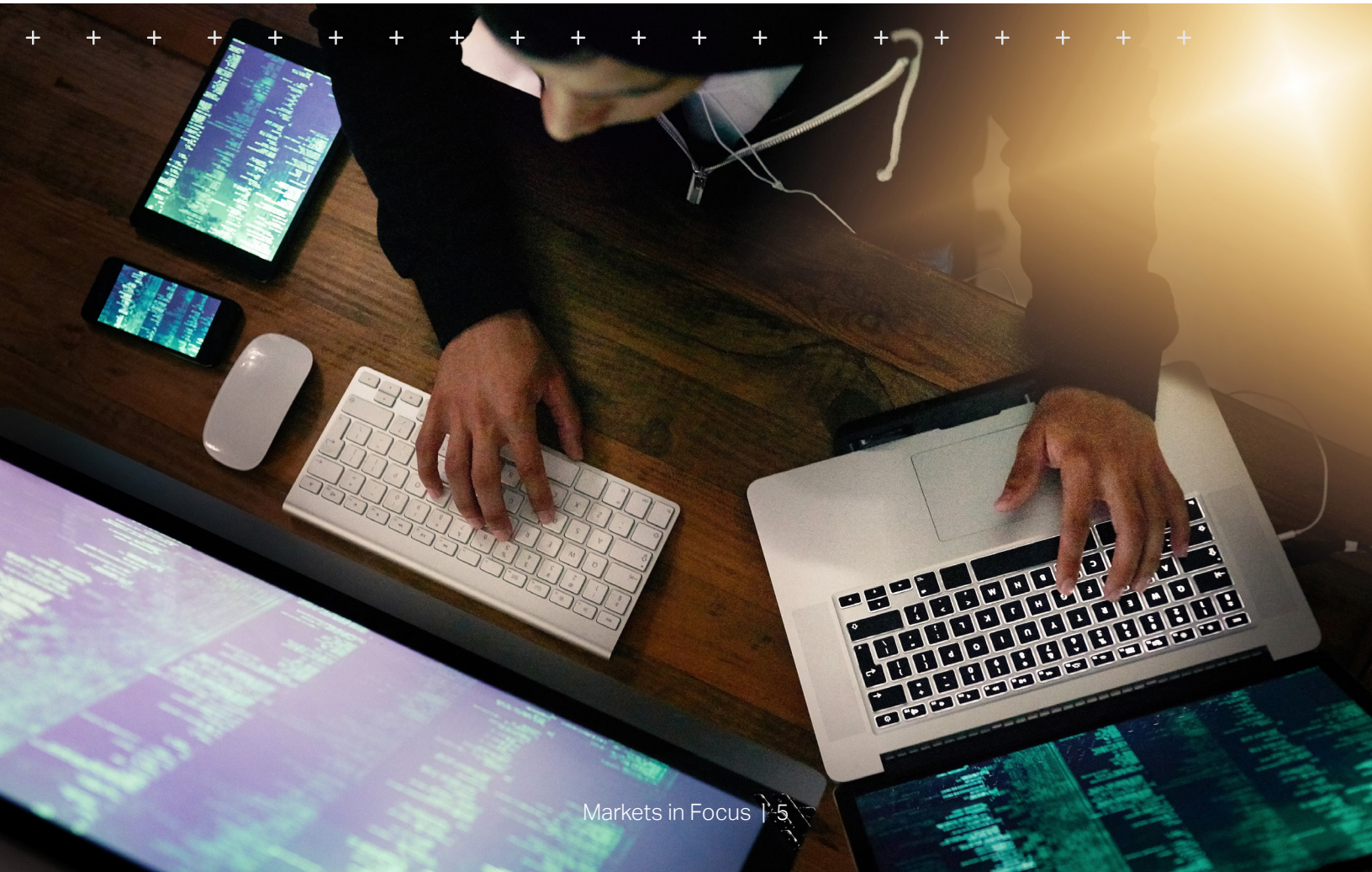
Other significant sources of privacy-related losses that continued in the first quarter include litigation based on collecting biometric information (principally in Illinois, though Washington and Texas have also enacted legislation in this area). We continue to monitor state biometric privacy legislation due to the dramatic impact of the Illinois BIPA law.

Data breaches, perhaps the archetypal cyber event, continued during the first quarter.

Other data breaches continue to result from ransomware threat actors stealing protected or confidential information to increase their ability to extract large ransoms.

Whether these and other events lead cyber insurers to change the underwriting and pricing of cyber policies will become apparent over time. Today, insurers are taking a wait-and-see approach. None are signaling that significant changes are coming, though many believe premium reductions could taper off in the third or fourth quarter of the year.

Source:
1. CIAB. (2024, February 21). Commercial Property/Casualty Market Index Q4/2023. CIAB. https://www.ciab.com/download/42254/?tstv=1708621180



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

EMPLOYEE BENEFITS BLOG

FOR ANY QUESTIONS, PLEASE REACH OUT TO:

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