Markets in Focus

Q2 2024

CYBER

Market Update

CYBER INSURANCE MARKETPLACE

In the first quarter of 2024 (the most recent quarter for which data is available), cyber insurance premiums were 12 percent more likely to change than in the previous quarter. The size of premium reductions tapered off while the number of policies seeing decreases jumped by 8 percent. Ironically, the number of policies with increases grew by the same amount. The number of policies that saw increases of 10 percent or more doubled over the prior quarter.

Our data on cyber renewals through the second quarter is broadly consistent.

The cyber insurance marketplace remains healthy and competitive. Organizations that demonstrate good cyber hygiene and information governance practices can count on a rate reduction. Pricing for excess policies continues to be very soft.

Cyber insurers are hungry to write new business. One sign of that may be more liberal underwriting standards and a broader underwriting appetite. Anecdotally, we have seen more insurers be willing to consider insuring organizations that do not have all basic controls, such as multi-factor authentication, in place. Underwriters also remain open to enhancing coverage where doing so is necessary to win or retain business. We have also seen several insurers begin to write smaller and, in some cases, larger organizations than they were willing to consider in the past.

Barring any significant cyber events that impact insurers' cyber business profitability, we expect the current trends to continue through the third quarter.

The following survey response data from the Council of Insurance Agents & Brokers' Commercial Property/Casualty Market Report covering Q1 2024[1] reflects the trends for the first quarter:

CYBER PREMIUM PRICING

1	↓ Down more than 30%	0.00%
2	↓ Down 20% - 30%	0.00%
3	↓ Down 10% - 19%	0.00%
4	↓ Down 1% - 9%	40.00%
5	No Change	20.00%
6	↑ Up 1% - 9%	20.00%
7	↑ Up 10% - 19%	20.00%
8	↑ Up 20% - 29%	0.00%
9	↑ Up 30% - 50%	0.00%
10	↑ Up more than 50%	0.00%
N/A	Not Sure	0.00%

CYBER RISK ENVIRONMENT

The first half of 2024 has been eventful, with most headlines focused on large supply chain events.

In February, Change Healthcare suffered a ransomware attack that impacted healthcare providers and others, resulting in massive industry disruption. In June, cyber criminals launched a ransomware attack against CDK Global. CDK provides software to car dealers for dealership management, finance, and other aspects of their business. The attack crippled roughly 15,000 dealers in North America for two weeks. This trend has continued into the third quarter, with the CrowdStrike outage affecting computers using Microsoft Windows and CrowdStrike's Falcon cybersecurity product. Billions of dollars of insured losses have been forecast to arise from these events.

Data breaches remain a constant problem. The number of breaches in the first half of 2024 was 14 percent higher than during the same period in 2023.[1] Noteworthy breaches during 2Q2024 include Ticketmaster (560 million records), Advance Auto Parts (380 million records), AT&T (73 million records), and Dell Technologies (49 million records). The Financial Services, Healthcare, Professional Services, and Manufacturing industries were the hardest hit. The vast majority of breaches resulted from cyberattacks.

Ransomware attacks in the second quarter increased by 21.5 percent over the first quarter. The industries targeted most often are Manufacturing, Commercial Facilities, and Healthcare.[2] Sixty-six percent of attacks were directed against organizations with fewer than 1,000 employees.[3] Cyber criminals accomplished their attacks primarily by taking advantage of known software vulnerabilities and through phishing. The average ransom amount, $391,015, was slightly higher than that in the first quarter, but the median ransom, $170,000, decreased by 32 percent. Roughly one-third of victims paid ransoms.

The common thread running through the risk environment is that many events were preventable. While supply chain events are unpredictable, requiring basic cyber hygiene from vendors and ensuring that the organization is prepared for cyber events can limit the impact of events affecting supply chain partners. That same preparedness can make organizations resistant to cyberattacks that result in data breaches and to the disruption resulting from ransomware. Fortunately, cyber insurers can help. Insurers often offer free or discounted services to their insureds to improve their cyber risk posture.

Sources:

1 Identity Theft Resource Center. (n.d.) *Targeted Cyberattacks Fuel Massive Increase in Breach Victim Counts*. ID Theft Center. https://www.idtheftcenter.org/wp-content/uploads/2024/07/ITRC-H1-2024-Data-Breach-Analysis.pdf

2 IT ISAC. (2024, July 26). *Exploring the Depths: An Analysis of the 2023 Ransomware Landscape and Insights for 2024*. IT ISAC. https://www.it-isac.org/_files/ugd/473ff0_e276665f580f4001b21fb286ee9c7e27.pdf

3 Coveware. (2024, July 30). *Ransomware actors pivot away from major brands in Q2 2024*. Coveware. https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

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