CYBER INSURANCE

MARKET UPDATE 2024

ACP
AUSTBROKERS CYBER PRO

The cyber insurance market entered a period of stability throughout 2023 and that looks set to continue into 2024. The main driving factor behind this is the increase in capacity entering into the market, through both local and offshore providers. Increased rates over the last few years, along with more stringent underwriting requirements and an improvement in many organisation's cyber controls has driven additional capacity. Despite this, claims activity remains consistent, especially in relation to ransomware events. Recent and ongoing changes to legislation coupled with an increasingly stringent regulatory environment means the risk profile continues to increase. Many insurers with large cyber portfolios now have the ability to sustain larger losses, however those new entrants into the cyber market will likely need to proceed with caution.

Claim Trends

Claim trends continue to be mostly in line with prior years, however the second half of 2023 saw a significant increase in ransomware activity against Australian organisations.

Ransomware Activity

Sophisticated ransomware attacks continue to occur, however recent data suggests threat actors are finding it more difficult to extract ransom payments from organisations. According to Covewave, a ransomware incident response firm, Q4 2023 saw only 29% of victims paying a ransom, which was a record low. Organisations continue to grow their resilience, including their ability to recover from an incident. Whilst the attacks can still be destructive, the continued exfiltration of sensitive data from organisations by threat actors continues to persist and adds pressure on victim organisations to pay, with threat actors leaking data on the dark web and their leak sites if payments are not made.

The attack vectors are consistent with previous years and include brute force RDP attacks, Common Vulnerability & Exposures ('CVE') and increasingly sophisticated social engineering campaigns. From an industry perspective, manufacturing and logistics, along with financial and professional service firms continue to be targeted. In recent times, technology companies, particularly managed service providers have seen a substantial increase in ransomware activity, which is a cause for concern given their interconnectivity with the organisations they serve.

Business Email Compromise ('BEC')

Business Email Compromise ('BEC') continues to be a significant threat to many organisations. It continues to be a major concern for SME organisations. The introduction of Multi Factor Authentication ('MFA') requirements by insurers on cloud-based email networks, such as Office365, has helped increase resilience in this area, however threat actors are now beginning to bypass MFA and are continuing to develop their social engineering skill sets, with the assistance of Artificial Intelligence ('AI'). Recently, an overseas finance worker was scammed into paying a significant sum of money to threat actors via a deepfake video call that used AI copies of their colleagues. This area continues to be challenging for organisations and insurers, especially if the insurer is providing cover for funds transfer losses.

Government Response to the Privacy Act Review

The Government provided their responses to the Privacy Act Review Report which contained 116 proposals. The Government agrees to 38 proposals and agrees in principal with 68 of the proposals. This indicates the Government's intention to progress long awaited reforms of Australia's privacy laws.

Some of the key takeaways include the increasing protections requiring organisations to handle individuals personal information in line with community standards, enhanced requirements around the security and destruction of information (once it is no longer required), increased penalties along with strengthening enforcement powers for the OAIC and considerations in relation to modifying the employee records exemption and removal of the small business exemption that currently exist within the Privacy Act.

The potential removal of the small business exemption under the Privacy Act, which was agreed to in principal, potentially means millions of small businesses will be required to adhere to the Privacy Act. Consultation with small businesses and their representatives are underway to understand the impact of this change.

In short, sweeping changes are coming to the way organisations in Australia are required to collect, handle and use information they receive from their customers and stronger regulatory oversight and action means an increased risk for organisations who cannot demonstrate strong procedures, processes and controls. Cyber risk for 2024 and beyond will continue to be a key topic of discussion at board level for all organisations.

Key Themes for 2024

Rates have Stabilised

After an extremely difficult cyber insurance market, 2023 saw rates in the cyber insurance market stabilise. Q2 of 2023 saw rates only increasing on average by around 11%, whilst in Q3 2023, this dropped even further to only 4%. By the end of 2023 and into 2024, rates are now somewhat flat, with rollover rates on renewals (depending on industry, controls and revenue) being achieved in some cases. Importantly, the significant rate increases seen throughout 2021 & 2022 have subsided which is pleasing news for organisations looking to renew or purchase cyber insurance for the first time. We believe this trend will continue into 2024, however we remain cautious given the consistent claims activity we continue to see in the market.

Additional Capacity within the Market

Rate stability is mainly due to additional capacity entering into the Australian cyber insurance market. With higher rates and an increasing trend of organisations investing in cyber security controls and processes, insurers have been more willing to deploy capacity and write business, including new entrants into the market from both local and offshore providers.

Most insurance providers are now able to offer $10m limits, with some providers able to provide even more capacity. Those organisations purchasing excess layer programs are seeing significant competition, which in some cases is leading to savings on those layers. Whilst historical markets have larger premium pools now, ensuring they can sustain larger losses, new entrants will ultimately need to proceed with caution to ensure they are able to become sustainable providers within the market.

Demand for Cyber Insurance Continues to Increase

This trend has continued throughout 2023 and will no doubt continue into 2024 as cyber risk continues to be at the forefront of boards and organisations in general. Driving this is also cost savings on other lines, such as professional indemnity and directors and officers insurance, where such savings are being redeployed by organisations to purchase cyber insurance for the first time, or increase their existing policy limits at renewal time.

Given the penetration rate remains low when compared to other insurance lines, education and explaining the tangible benefits of a cyber insurance policy, including the incident response services that come with the policy remain key to increasing buyers within the market.

Underwriting Scrutiny

Underwriting remains rigorous, particularly in the corporate sector, with insurers continuing to expect minimum security standards such as Multi Factor Authentication ('MFA') on remote access into networks and cloud based email accounts, strong controls around privileged access, patch management policies, the implementation of EDR solutions, cyber security awareness training for all staff, strong backup protocols and testing, along with detailed and tested incident response and business continuity plans addressing ransomware incidents.

Insurers continue to focus on understanding how prepared an organisation is in relation to dealing with a ransomware event as they understand these events continue to be costly, in particular in relation to the first party coverage sections of the policy. Insurers also remain concerned around the types of data being held and how it is being secured within organisations, given the increase in regulatory oversight and community expectations in this area.

Those organisations who continue to demonstrate strong cyber hygiene are once again achieving the most favourable outcomes from a premium and coverage perspective as it allows their brokers to create competition within the market and then leverage this to drive down premium cost and enhance aspects of cover.