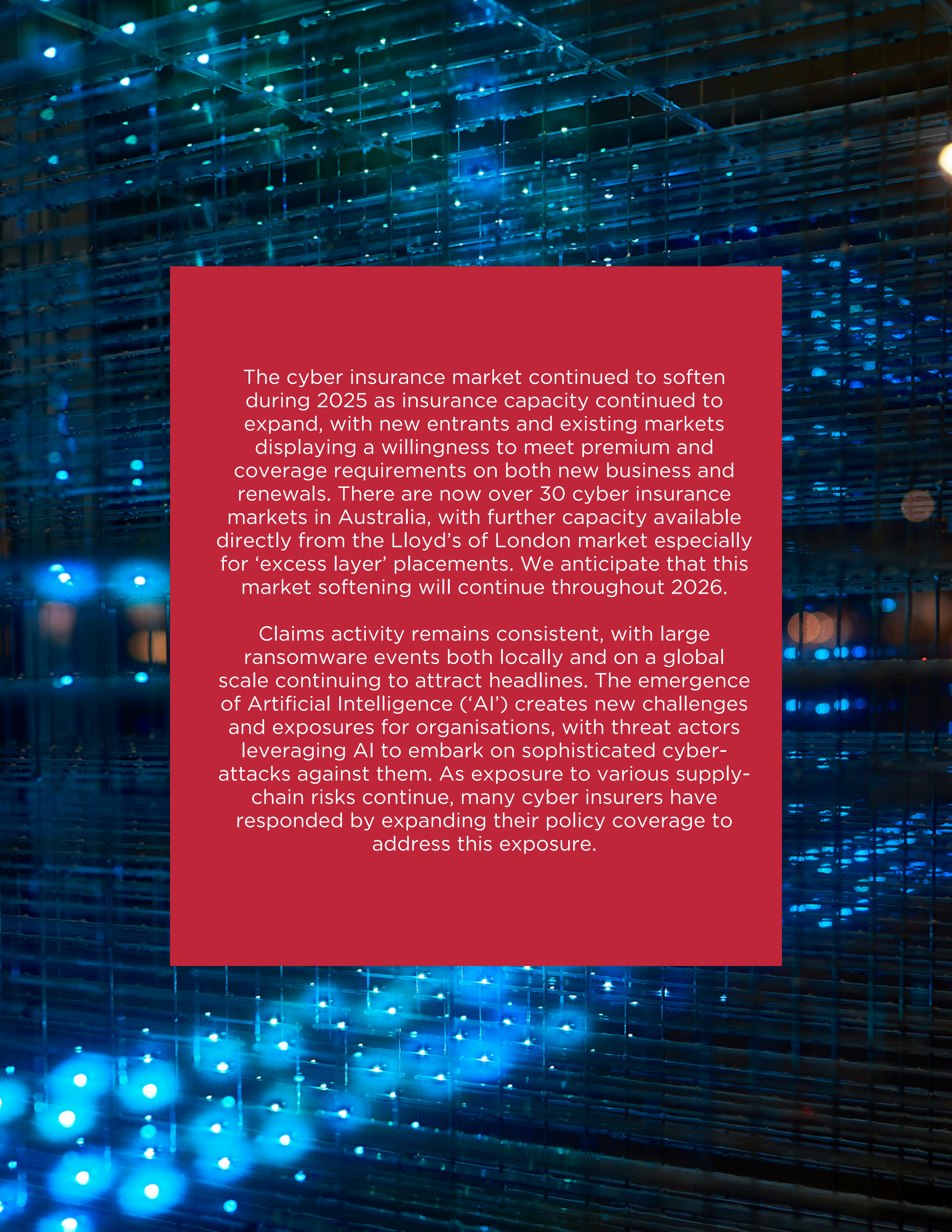
CYBER INSURANCE MARKET UPDATE 2026

ACP
AUSTBROKERS CYBER PRO



The cyber insurance market continued to soften during 2025 as insurance capacity continued to expand, with new entrants and existing markets displaying a willingness to meet premium and coverage requirements on both new business and renewals. There are now over 30 cyber insurance markets in Australia, with further capacity available directly from the Lloyd’s of London market especially for ‘excess layer’ placements. We anticipate that this market softening will continue throughout 2026.

Claims activity remains consistent, with large ransomware events both locally and on a global scale continuing to attract headlines. The emergence of Artificial Intelligence (‘AI’) creates new challenges and exposures for organisations, with threat actors leveraging AI to embark on sophisticated cyber-attacks against them. As exposure to various supply-chain risks continue, many cyber insurers have responded by expanding their policy coverage to address this exposure.

Premiums and Policy Coverage Trends

Cyber insurance premiums continued to decline throughout 2025, which looks likely to continue (albeit at a potentially slower pace) throughout 2026. During 2025, average premium reductions were in the 5% to 12% range, with even higher premium reductions being achieved on excess layer placements above locally placed primary limits for the larger corporate cyber insurance programs. These reductions resulted in many organisations taking the opportunity to use these premium savings to increase the limits of their current cyber programs to minimise potential underinsurance issues, in the event of a significant cyber incident.

More competitive pricing has also increased demand for cyber insurance in general. In particular, the cyber insurance take-up rate for SMEs continues to increase. However, clients need further education to increase their awareness of the cyber exposures that they face, to adequately address and insure this significant business risk.

With premiums decreasing and risk exposures increasing, specialist cyber insurance brokers are focussing on expanding coverage for their clients. Some of these policy enhancements include broader cyber-crime, responding to system failure, broader reputational harm coverage and business interruption cover for non-IT dependent situations. Insurers continue to be flexible with broker requests for policy enhancements if their clients can demonstrate strong cyber controls and processes within their business operations.

Underwriting Oversight

Whilst insurers are more flexible on pricing and coverage, they remain consistent in their underwriting approach including the requirement for clients to have key minimum-security standards in place, especially for larger organisations and higher-risk industries such as financial services, manufacturing, providers of logistics and technology firms.

Before providing *best in class* cyber insurance, insurers mandate that key controls and processes are in place. These include Multi Factor Authentication ('MFA') on remote access into networks and cloud-based email accounts, strong controls around privileged access, patch management policies, implementation of EDR solutions, staff cyber security awareness training including on the use of AI, strong back-up protocols, as well as quality-tested incident response & business continuity plans that address ransomware and supply chain exposures.

Even in the prevailing soft market, those organisations that fail to have adequate security controls and processes in place will struggle to purchase sufficient cyber insurance, leaving them in the hands of untested cyber insurers who can only provide inadequate coverage, leaving them exposed to uninsured losses when a cyber incident occurs.

Claim Trends & Regulatory Oversight

While the cost of cyber insurance continues to decrease, claims activity hasn't and remains consistent with previous years. Australian regulators continue to strengthen their oversight and scrutiny of the cyber risk landscape, highlighted by the recent introduction of mandatory reporting of ransomware payments for organisations with more than $3m in annual revenue.

Ransomware & Extortion

Cyber extortion claims have developed into two distinct paths; being volume-driven Ransomware-as-a-Service (RaaS) campaigns targeting SME businesses, and high-cost targeted intrusions aimed at the larger organisations.

Large organisations are increasingly resisting the pressure to pay ransoms. Several high-profile data exfiltration campaigns were largely unfruitful despite widely reported impacts on the victim organisations. Conversely with SMEs, as they tend to have less robust back-ups and recovery processes in place, they are easier to disrupt and therefore more likely to negotiate with, as well as pay a lower ransom amount to threat actors.

The main attack vectors are similar to previous years including remote access compromises and credential-based intrusions through VPNs and cloud gateways. Remote access and social engineering have effectively merged. Threat actors are increasingly obtaining access, not just by logging into a system but by convincing someone to provide it for them. Campaigns that blur these lines, such as impersonating SaaS support teams, or abusing help desk processes, are becoming increasingly common. Threat actors continue to exploit vulnerabilities such as unpatched CVEs and applications with weak authorisation methods.

Ransomware continues to be a main threat, not just for large organisations but also for SMEs. According to ransomware recovery first responder Coveware, 31% of organisations employing between 11 - 100 staff have been impacted by a ransomware event, compared to 38% for organisations with 101-1,000 employees. Healthcare, professional services, technology/software companies, manufacturers and logistics companies continue to be key targets for threat actors.

Supply Chain Risks & Breaches

Supply chain risks will continue to be a major cyber-risk exposure to businesses in 2026. Multi-party breaches, often involving Managed Service Providers (‘MSPs’), SaaS, cloud providers and third parties that can access systems, are a major concern for organisations, given the interconnectivity and reliability that technology plays in the function of most day-to-day business activities.

With the emergence of non-IT supply chain risk, organisations are increasingly concerned about how a cyber incident at a key customer or supplier can materially impact their own ability to maintain their business operations. Therefore, many cyber insurers have expanded their policy coverage to address this exposure.

Business Email Compromise (‘BEC’) & Funds Misdirection

Business Email Compromise (‘BEC’) including funds misdirection is an underlying threat to all Australian businesses. Whilst Multi Factor Authentication (‘MFA’) insurer-mandated requirements on cloud-based email networks such as Office365 have helped increase resilience in this area, threat actors continue to develop techniques to bypass such controls.

Phishing campaigns are becoming more difficult to identify, as cyber criminals continue to use AI to create AI-powered phishing campaigns that are highly adaptive and personalised to specific individuals within an organisation. Human error continues to be a driving factor for cyber breaches, with the majority of funds misdirection losses being caused by a breakdown in the organisation’s internal risk management process.

Regulatory Oversight

Australian regulators are intensifying their focus on how organisations implement cyber risk management. The Office of the Australian Information Commissioner (OAIC) and the Australian Securities and Investments Commission (ASIC) have increased enforcement activity and recent amendments to privacy laws now allow individuals to seek legal recourse for breaches caused by an organisation’s intentional or reckless conduct.

Since May 2025, mandatory reporting of ransomware payments have been in place for organisations with annual revenue above $3 million. We believe that regulatory scrutiny will continue to increase, with them taking action against those organisations that have a cyber incident and/or committed serious or repeated breaches, imposing significant fines and penalties where appropriate.

The Austbrokers Cyber Pro ('ACP') Approach

Despite the softer market conditions in the cyber insurance market, ACP's approach remains consistent. We continue to partner with our key insurers, being proven cyber insurance providers with a track record of pro-actively managing and paying claims. These insurers either subscribe to our exclusive 'broker-form' cyber policy wording, or agree to our enhanced cyber product endorsements, to ensure that clients have a broad cyber insurance program in place.

We continue to work with our incident response partners, all of whom are embedded into our cyber insurance product offering to ensure fast and efficient assistance at the time of a cyber incident. As a specialist cyber insurance broker, we not only place the cyber insurance, but more importantly we actively engage with the insurer, the incident response firm and other important vendors to assist the client at the time of a cyber incident, ensuring that claims are paid in a timely manner.

We work closely with our retail broker partners to assist their clients in understanding their cyber exposures, what cyber insurance actually covers (including case-studies based on previous cyber claims), leaving clients with peace of mind that they have a sound cyber insurance program in place.