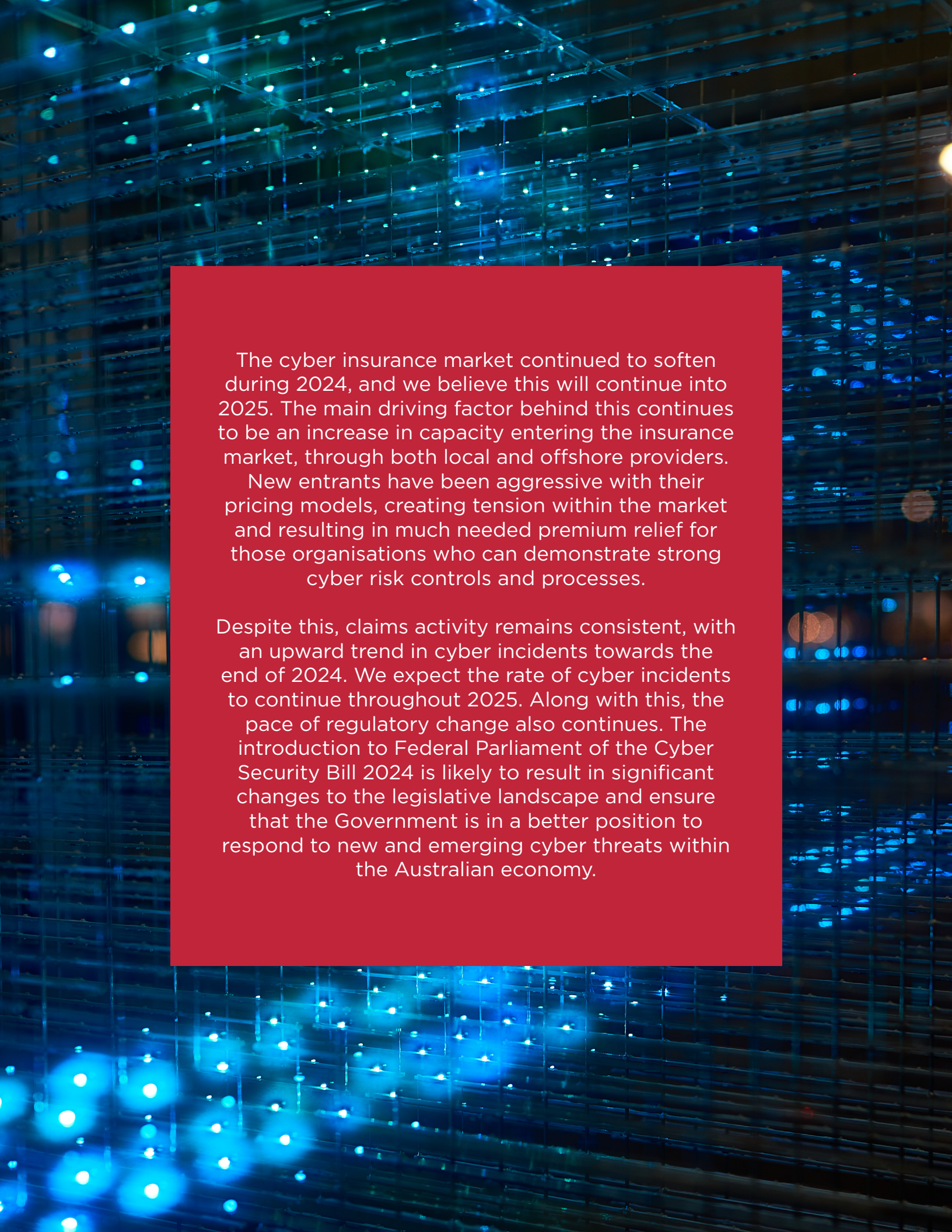
CYBER INSURANCE MARKET UPDATE 2025

ACP
AUSTBROKERS CYBER PRO



The cyber insurance market continued to soften during 2024, and we believe this will continue into 2025. The main driving factor behind this continues to be an increase in capacity entering the insurance market, through both local and offshore providers. New entrants have been aggressive with their pricing models, creating tension within the market and resulting in much needed premium relief for those organisations who can demonstrate strong cyber risk controls and processes.

Despite this, claims activity remains consistent, with an upward trend in cyber incidents towards the end of 2024. We expect the rate of cyber incidents to continue throughout 2025. Along with this, the pace of regulatory change also continues. The introduction to Federal Parliament of the Cyber Security Bill 2024 is likely to result in significant changes to the legislative landscape and ensure that the Government is in a better position to respond to new and emerging cyber threats within the Australian economy.

Claim Trends for 2025

Business Email Compromise ('BEC') & Funds Misdirection

Business Email Compromise ('BEC') is always a significant threat to all 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 continue to develop techniques to bypass this control. There has recently been an increase in funds misdirection fraud as the result of BEC events, with organisations in Australia losing hundreds of millions of dollars per annum due to these incidents.

Phishing scams are becoming more difficult to spot as cyber criminals continue to use Artificial Intelligence ('AI') to create AI powered phishing campaigns that are highly adaptive and personalised to specific individuals within an organisation. Along with MFA, organisations should ensure that email authentication protocols are set up correctly and that comprehensive cyber security awareness (including phishing simulation) training is conducted on a regular basis for all employees.

Supply Chain Risks & Breaches

Supply chain risks were a major issue in 2024, and this looks set to continue into 2025 and beyond. These multi-party breaches, often involving Managed Service Providers ('MSPs'), SaaS, cloud providers and third parties that access systems, can cause major concerns for organisations given the interconnectivity and reliability that technology plays in the function of day to day business activities.

This raises the important issue of how to protect supply chains. Organisations need to ensure that adequate due diligence is being undertaken, along with ongoing reviews of security and access controls, for those parties they are sharing information or systems with. Strong contractual terms can be critical in protecting organisations in these situations. Organisations must also be prepared for technology downtime; by ensuring they can perform critical business functions by reverting to manual operations during digital outages. This all leads to an uptick in organisations preparing, testing and responding to such events through simulated tabletop exercises to ensure their procedures are robust and senior executives are prepared and confident in their abilities to navigate supply chain incidents of scale.

Ransomware Threats

Sophisticated ransomware attacks continue to be a serious threat for organisations. There was an uplift in ransomware towards the end of 2024 and ransomware is likely to stay consistent as one of the key threats to organisations in the future.

The downfall of Lockbit 3.0 has seen the emergence of new threat actor groups, including Akira and RansomHub with the attack vectors somewhat consistent as in previous years. These vectors include VPN compromise, where some threat actors are exploiting a vulnerability/unpatched CVE, along with brute forcing accounts on appliances without multi-factor authentication enabled, while others are weaponising legitimate stolen or leaked credentials that are scraped weeks or months in advance by infostealers.

Ransomware continues to be a threat not just for large organisations, but also for SME organisations. Data by Coveware suggest towards the back end of 2024, 35% of ransomware events impacted those organisations with 11-100 staff, whilst 40% of attacks impacted those organisations with between 101-1000 staff. Healthcare, professional services, technology and software services and manufacturing and logistics continue to be key targets for threat actors, but what is clear is that no organisation, no matter what industry they operate in, is immune from these threats.

Key Themes in 2025

Continuation of the Softening Market

Soft market conditions are likely to persist throughout 2025. 2024 saw reductions in premiums of between 5% - 11% on average throughout the year and something similar is expected to continue in 2025. With such soft market conditions, experienced brokers should be negotiating additional policy coverages, to ensure broader coverage outcomes can be achieved for organisations, but this is dependent on insurers being comfortable with an organisation's cyber risk controls and processes.

Capacity Continues to Enter the Market

The soft market conditions are mainly due to additional capacity which continues to enter the Australian market. Over the last few years, several Australian-based insurers and underwriting agencies have expanded to include cyber insurance as part of their suite of product offerings. In addition, specialist cyber insurance underwriting agencies have set up locally, creating additional competition and increased capacity, leading to a buyers' market.

Whilst this has assisted the SME market, it has also ensured positive outcomes for larger organisations, especially those wishing to buy additional capacity and increase their cyber insurance limit. Competition for excess layers has been fierce leading to positive outcomes in this space.

It is important that adequate due diligence is undertaken on any new capacity, especially on a primary placement. Considerations include the strength of the capacity's wording and their ability to manage and handle claims effectively.

Regulatory Change to Continue

The introduction to Federal Parliament of the Cyber Security Bill 2024 was a significant milestone for the Government. Some of the key features of the Bill include, but are not limited to:

- Granting ministerial powers to mandate security standards for smart devices.
- Introducing mandatory reporting of ransomware and cyber extortion payments, which is likely to apply to organisations with turnover greater than $3m.
- Introducing a limited use obligation on cyber incident information voluntarily reported to the National Cyber Security Coordinator.
- Establishing a Cyber Incident Review Board to conduct post-incident reviews into significant cyber security incidents.

On November 29, 2024, the Privacy and Other Legislation Amendment Bill 2024 was passed by both Houses of Parliament, which was the first step on legislative changes in response to the Attorney General's Privacy Act Review Report. Some of the key features here, include but are not limited to:

- A new cause of action in tort for serious invasions of privacy.
- Lower thresholds in relation to civil penalties that will apply proportionately with the seriousness of the interference with privacy.
- Enhanced powers for the OAIC, including the power to issue infringement and compliance notices.

It is clear that these reforms will increase obligations on organisations in Australia and potentially open up significant regulatory and litigation risk. This may also have a material impact on third party coverage sections under cyber insurance policies, along with how organisations and their insurers respond to a cyber incident. Organisations must understand the impact of any legislative changes to ensure they are complying with their responsibilities.

Underwriting Oversight

Underwriting remains mostly in line with previous years with most insurers still requiring standard cyber security controls and processes to be enacted by organisations. Such standards include 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 and supply chain incidents.

Insurers have increased their focus on supply chain risk in their underwriting and following the Crowdstrike incident, many insurers are now becoming more cautious in providing blanket systems failure coverage within their policy wordings, and those that do may have certain carve-backs which limit the coverage available.

What is clear is that with softer market conditions, those organisations who continue to demonstrate strong cyber hygiene are achieving favourable outcomes from a premium and coverage perspective, with some organisations using the savings achieved at renewal time to increase their cyber insurance limits.