Insurance Council of Australia

24 February 2026

Senator Deborah O'Neill
Chair
Parliamentary Joint Committee on Corporations and Financial Services

Via upload

Dear Chair

Small business insurance – cyber insurance

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to provide a submission on behalf of our members on this important topic.

The Insurance Council is the representative body for the general insurance industry of Australia. Our members represent approximately 85 per cent of total premium income written by private sector general insurers and provide a range of general insurance products including small business insurance products.

This submission is one of a series of submissions the Insurance Council will be providing to the Committee's inquiry and focusses on cyber insurance.

What is cyber insurance

Cyber insurance, which is a relatively novel product, provides coverage to businesses for liability relating to cyber threats. Cyber insurance generally includes what is known as first-party cover and third-party cover.

First-party cover protects a business against the immediate expenses incurred to survive a cyber incident, including immediate incident response and hardening defenses against a future attack. It may also cover business interruption costs, recovery of data, crisis management, and public relations expenses and in some cases, cyber extortion.

Third-party cover protects a business against liabilities to others because of a cyber-attack. The most frequent costs that fall into this category are privacy liability, the cost of navigating regulatory investigations, and in some instances associated fines and penalties.

The Australian cyber insurance market

Through 2025 and into 2026, Australia's cyber insurance market has been softening. That is, the cyber insurance market has seen a reduction in premiums, increases in coverage and new entrants heightening competition.[1] This softening market follows years of hard market conditions influenced by major data breaches such as the 2022 attacks on Optus and Medibank. While the pool is relatively small and novel, cyber insurance will continue to increase in importance for Australian businesses. Australia has been an early adopter of digital technologies and the rapid pace of digitisation across the economy means the need for cyber resilience is increasingly prominent for Australian businesses. This risk is amplified by social trends such as increased working from home and the significant increase in

[1] Marsh. 2025. *Australian Mid-Yeat Insurance Market update 2025.* Available here; Finity. 2025. *Optima Lite – Cyber*.

Insurance Council of Australia

the collection of personal information by businesses since COVID-19, which can open new attack vectors for nefarious actors to steal additional data that can be digitally accessed or stolen.[2]

Additionally, Australia's deteriorating geostrategic environment means increased state-sponsored cyber espionage aimed at Australian businesses alongside increasing cybercriminal activities already targeting Australia. This is evidenced by the increases in calls to the Australian Cyber Security Hotline and in the number of incidents the Australia Cyber Security Centre is responding to show that cyber risk is not declining and must be navigated.[3]

It is important to acknowledge that because of cyber insurance's relative novelty in Australia, there is comparatively limited publicly available actuarial data in relation to the market. As this data builds up over the coming decades, we expect less pricing volatility.

The Australian cyber insurance industry is highly innovative. Many cyber insurers actively assist their policyholders by incentivising proactive resilience, rather than simply accepting a premium and paying a claim.[4] This active management helps clients navigate cyber incidents by providing access to third-party professionals to limit losses and get back online quicker. Additionally, innovative products such as cyber insurance "embedded" in managed service providers' offering are coming to market, making accessing cyber insurance more seamless.

Impact on small business and not-for-profits

Cyber insurance take-up among small businesses is understood to be low.[5] This is particularly concerning as industry participants have pointed out the vulnerabilities facing small business noting small businesses are "hit much harder by cyber incidents… with severity of claims increasing and more and more small businesses targeted."[6]

Government entities and sophisticated corporate entities have well-known cyber vulnerabilities. These include third-party risk (the 2024 outage of CrowdStrike systems highlighted the nature of third-party risk alongside national concentration risk where one supplier forms a critical part of many businesses' supply chains), risks associated with artificial intelligence and a lack of robust contingency planning.[7] Importantly however, these businesses have the resources, commensurate with their national significance, to manage these risks. Small businesses, however, face similar risks, albeit with far less resources than larger entities. Resource constraints can amplify impacts which for small businesses can include the livelihoods of business owners.

Increasing general awareness of cyber risk (and by extension awareness of cyber insurance) is an important first step towards bridging this cyber protection gap and small business access to cyber insurance and government should be commended on existing programs, such as *Cyber Wardens*, designed for this goal.[8] As awareness of cyber insurance grows, it should not be seen as a panacea to a small business' cyber risk. Instead, cyber insurance should be considered as part of a suite of options available to small businesses to support them in managing and mitigating their cyber risk. Small business owners and operators, alongside their trusted advisers (such as insurance brokers), remain best placed to determine how capital should be allocated against their specific risks. These

[2] McKinsey. 2020. *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever.* Available here.
[3] Australian Signals Directorate. 2025. *Annual Cyber Threat Report 2024-2025*.
[4] McGrathNicol. 2025. *Ransomware: a shift from payment dependent strategies*. Available here.
[5] Finity. 2025. *Optima Lite – Cyber*.
[6] Emergence. 2025. *Cyber claims data report 2025*. Page 3. Available here.
[7] Department of Home Affairs. 2025. *Critical Infrastructure Annual Risk Review*. Page 11.
[8] More information about Cyber Wardens can found here. further government resources for businesses are available here.

Insurance Council of Australia

decisions can be supported by educational programs that encourage cyber resilience among small businesses.

Further, cyber risk and cyber insurance should not be viewed through a set and forget mindset. Cyber risk is constantly evolving and the entire business community, supported by government, must stay vigilant. The collective attitude shift required to achieve great cyber resilience cannot be driven by regulation alone. By way of example, business email compromise where employees unwittingly expose a business' system to cyber criminals, remain key drivers of cyber insurance losses.[9] However, Australia cannot criminalise clicking the wrong link. Instead, the focus needs to be on embedding greater cyber awareness into Australians' everyday thinking and actions.

Encouragingly, attitude shifts are already evident, with a poll of 800 Australian business decision makers finding that the average amount businesses are willing to pay in cyber ransoms decreased from $1.42 million in 2024 to $906,000 in 2025.[10] This attitude shift reflects several trends, each determined by greater cyber awareness. Government and industry must continue to work together to drive attitude shifts towards a more cyber resilient Australia, which in turn will be a more insurable Australia.

Recent enhancements to national cyber security legislation will also serve to harden the entire Australian business community against cybercrime. We encourage the Government to explore how information collected on Australia's cyber risk, such as through the new *Mandatory ransomware and cyber extortion* reporting framework, can be shared with insurers and other parts of the cybersecurity ecosystem to improve Australia's collective cybersecurity.

We thank the Committee for the opportunity to comment and look forward to engaging further throughout this inquiry. Should you have any questions in the meantime, please contact Eamon Sloane, Senior Adviser Strategic Policy, at [redacted]

Regards

[redacted]

Andrew Hall
Executive Director and CEO

[9] Emergence. 2025. *Cyber claims data report 2025*. Page 5.
[10] McGrathNicol. 2025. *Ransomware: a shift from payment dependent strategies*. Available here.