



Insurance Council
of Australia

7 September 2026

Ms Sally Sitou MP
Chair
House Select Committee on Cyber Security for Small to Medium Sized Businesses

Via upload

Dear Chair

Cyber Security for Small to Medium Sized Businesses and Organisations

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to provide a submission on behalf of our members on this important topic. We appreciate the Committee's interest in the role of cyber insurance within the broader cyber security ecosystem for small and medium sized organisations.

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.

The volume of cyber threats small businesses face will not dissipate, and as the Australian economy increasingly digitises, we should expect that volume to grow. The Australian Cyber Security Centre's (ACSC) *Annual Cyber Threat Report 2024-2025* confirms this, noting that the ACSC's Cyber Security Hotline received a 16 per cent increase in calls on the previous year, with cyber incidents the ACSC responded to also growing year on year, this time by 11 per cent.¹ The need to improve small businesses' cyber security posture is clear, particularly if the Australian economy is to benefit from next generation digital technologies.

What is cyber insurance

Cyber insurance, a relatively novel product, provides coverage to businesses for liability relating to cyber threats. Cyber insurance generally includes two distinct types of cover known as first-party cover and third-party cover.

First-party cover meets the immediate expenses a business incurs in responding to a cyber incident, including immediate incident response and hardening defences 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, which covers the cost of navigating regulatory investigations, and in some instances, associated fines and penalties.

¹ Australian Signals Directorate. 2026. [Annual Cyber Threat Report 2024-25](#). Page 1.

The Australian cyber insurance industry is highly innovative and has responded to the emerging needs of businesses. Many cyber insurers actively assist their policyholders by incentivising proactive resilience that help customers build stronger defences and improve their own understanding of the cyber risks. In other words, “prevention is now built into the policy, not sold as an add-on.”² Beyond prevention, active management also helps clients navigate cyber incidents in real time by providing access to third party professionals to help limit losses and get businesses back online quicker. Additionally, innovative products such as cyber insurance “embedded” in managed service providers’ offerings (allowing businesses to obtain cover through their existing IT provider rather than sourcing it separately) are emerging, making accessing cyber insurance easier.

Small business cyber insurance market

Around the world, cyber insurance take-up among small businesses is understood to be low.³ This is particularly concerning given the vulnerabilities facing small business, which are “hit much harder by cyber incidents... with severity of claims increasing and more and more small businesses targeted.”⁴ Small organisations do not have the resources of their larger counterparts, meaning responding to and recovery from cyber-attacks is harder and more costly than for larger organisations.

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 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, alongside all levels of government and the not-for-profit sector, 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, remains a key driver of cyber insurance losses. 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.

Corporate supply chains

A small business’ cyber maturity is likely to have a material impact on its capacity to participate in the supply chains of large corporates. Increasingly, governments are requiring stricter cyber protocols of large corporates in certain industries with these protocols extending to businesses participating in those large businesses’ supply chains. These requirements (for example, the *Security of Critical Infrastructure Act 2018* and the Australian Prudential Regulation Authority’s *CPS 230 Operational Risk Management*) exist to ensure the resilience of vitally important elements of the Australian economy. These requirements often reduce the accessibility of corporate supply chains for small businesses in favour of other large entities who can more readily meet the necessary obligations. Where larger suppliers are ordinarily foreign based, trade-offs between building Australia’s sovereign capabilities and real-time cyber security must be made. How these trade-offs are balanced is ultimately a decision for government in determining appropriate regulatory settings. In any case, given the importance of

² Insurance Business Australia. 2026. [Best Cyber Insurance Providers in Australia](#).

³ Swiss Re. [Shifting cyber insurance growth into the next gear](#).

⁴ Emergence. 2025. Cyber claims data report 2025. Page 3. Available [here](#).

cyber security requirements, it is incumbent on government and larger entities to be transparent about the impact these regulations will have on smaller organisations' capacity to meet the relevant requirements and participate in some supply chains.

We thank the Committee for the opportunity to comment. Should you have any questions in the meantime, please contact Eamon Sloane, Senior Adviser Strategic Policy, at esloane@insurancecouncil.com.au.

Kind regards



Andrew Hall
Executive Director and CEO