Dialogue Paper

Cyber Protection Gap Widens for SMEs

November 2024



Actuaries Institute.



Win-Li Toh

Win-Li is an experienced actuarial advisor and commentator on critical issues affecting insurance in Australia and abroad. Focusing on themes that transcend borders and industries, she brings an international mindset to problem solving, backed by more than 25 years partnering with insurers, self-insurers and government across the globe.

As lead author on the Actuaries Institute report, *Cyber Risk and the Role of Insurance*, she provided crucial evidence for the industry to enhance its cyber resilience efforts. In 2023, she was awarded Insurance Leader of the Year by the Australian and New Zealand Institute of Insurance and Finance.

Today, through her proactive industry presence and several Appointed Actuary roles, she continues to bring solutions-focused insight and facilitate open dialogue between the private and public sectors amid an ever-evolving threat landscape.

Win-Li is a principal at actuarial and analytics consultancy Taylor Fry, where she leads the general insurance practice. She is 2024 Senior Vice President of the Actuaries Institute and a member of its board.



Dr Michael Neary

Michael is the Managing Director, Insurance Asia Pacific, Middle East & Africa at DXC Technology. With a deep passion for the insurance industry, Michael is committed to driving impactful solutions that benefit DXC's clients and the people they serve.

Bringing over 30 years of experience in financial services, Michael has held multiple leadership and board positions across marketing, operations, strategy, and sales. He has spearheaded strategic initiatives and implementation programs, successfully launching innovative products across insurance, banking and technology.

Michael is passionate about innovation in financial services. In addition to his professional roles, he completed a Doctor of Business Administration with a thesis on "Innovation and Corporate Entrepreneurship in Australian Financial Services". He holds a Master of Commerce in Marketing and a Bachelor of Science.

Michael is also a co-author of the Actuaries Institute report, *Cyber Risk and the Role of Insurance*.



Sarah Wood

With a background in economics and policy in Australia and New Zealand, Sarah has worked across the public and private sectors for more than 13 years. She focuses on Environmental, Social and Governance (ESG) risk, specialising in two of the most significant ESG risks for all organisations – cyber, and climate and sustainability.

Previously client manager for a multi-national law firm's cyber incident response team, Sarah is ESG advisor at Taylor Fry. In this role, she works closely with actuaries to undertake business-relevant modelling of key ESG risks, ensuring results are meaningful. Alongside Win-Li, she uses scenario modelling to assess cyber risk exposure for organisations.

Sarah presents regularly to business and government, as cyber increasingly emerges as a major ESG factor in financial and investment risk, regulatory scrutiny and real-world impact. She is a member of the Actuaries Institute Climate and Sustainability Practice Committee, and co-chairs the Committee's public policy sub-committee.

About the Actuaries Institute

The Actuaries Institute is the peak professional body for actuaries in Australia. The Institute provides expert comment on public policy issues where there is uncertainty of future financial outcomes.

Actuaries have a reputation for a high level of technical financial expertise and integrity. They apply their analytical and risk management expertise to allocate resources efficiently, identify and mitigate emerging risks and to help maintain system integrity across multiple segments of the financial and other sectors. This unrivalled expertise enables the profession to comment on a wide range of issues including life, general and health insurance, climate change and sustainability, superannuation and retirement income policy, enterprise risk management and prudential regulation, the digital economy and AI, finance and investment, and wider health issues.

Actuaries use data for good by harnessing the evidence to navigate into the future and make a positive impact. They think deeply about the issues at hand, whether it is advising on commercial strategy, influencing policy, or designing new products. Actuaries are adept at balancing interests of stakeholders, clients and communities. They are called upon to give insight on complex problems, they will look at the full picture. Actuaries analyse the data and model scenarios to form robust and outcome-centred advice.

Acknowledgement of Country

The Actuaries Institute acknowledges the traditional custodians of the lands and waters where we live and work, travel and trade. We pay our respect to the members of those communities, Elders past and present, and recognise and celebrate their continuing custodianship and culture.

About this Paper

Dialogue Papers are a series of papers written by actuaries and published by the Actuaries Institute as part of its Public Policy Thought Leadership program. Enquiries should be directed to the Institute's Public Policy Team at public_policy@actuaries.asn.au. The papers aim to stimulate discussion on important, emerging issues. Opinions expressed in this publication are the opinions of the Paper's authors and do not necessarily represent those of either the Institute of Actuaries of Australia (the "Institute"), its members, directors, officers, employees, agents, or of the employers of the authors.

Disclaimer: This paper is provided for discussion purposes only and does not constitute consulting advice on which to base decisions. To the extent permitted by law, all users of the Paper hereby release and indemnify the Institute of Actuaries of Australia and associated parties from all present and future liabilities, that may arise in connection with this paper, its publication or any communication, discussion or work relating to or derived from the contents of this paper. The authors declare that they have provided professional advice to some of the insurers, governments or other entities discussed in this paper.

© Institute of Actuaries of Australia 2024
All rights reserved
ISBN: 9781763754218
Suggested citation: Toh, W., Neary, M., & Wood, S. (2024). *Cyber Protection Gap Widens for SMEs*. Actuaries Institute.

Table of Contents

1 Executive Summary 4

2 Introduction 6

3 Corporate Australia Has Received a Cyber Wake-up Call 9

4 What Is Preventing SMEs From Uplifting Their Cyber Capabilities? 11

5 Why Cyber Insurance Remains Uncommon for SMEs 14

6 Reducing the Cyber Protection Gap for SMEs 16



1. Executive Summary

- Corporate Australia has received a cyber wake-up call in the past couple of years, with major incidents and the government response to these dominating the headlines.
- This has prompted significant investment in improving the security posture and preparedness of Australia's largest businesses, and a rapid upskilling on behalf of company directors. While improvements have been made, the changing threat landscape means no businesses can rest on their cyber laurels.
- However, over the same period, it is clear Australia's small and medium enterprises (SMEs), who are facing a challenging economic climate, have not had similar bandwidth or resources to devote to their cybersecurity. With an increasing level of threat, the cyber protection gap for SMEs is widening.
- While many of the stakeholders we talked to believe the SME segment has the most to lose from a cyber incident, and therefore the most to gain by purchasing cyber insurance, only 10-25% of SMEs hold a standalone cyber insurance policy. The cost and complexity of cyber insurance are significant barriers for many SMEs.
- Bridging the cyber protection gap for SMEs will require continued (and relentless) collaboration and effort across government and the insurance industry, as well as within the small business community and the providers of technology solutions that support them.



2. Introduction

In October 2022, the Actuaries Institute released the report *Cyber Risk and the Role of Insurance*[1] that analysed the cyber vulnerability of organisations from SMEs to large corporates. The Report noted that, while the first lines of defence against cyberattacks were good cyber hygiene and security, a vibrant cyber insurance market could provide more than financial recompense for risks that break through – it can strengthen those first lines by offering clear signals and incentives to business (in the form of eligibility, pricing and sharing of insights) on best-practice standards. The Report urged government, businesses and insurers to collaboratively address significant insurance gaps in protection against cyberattacks that had already cost the Australian economy billions of dollars.

Following the release of that report, Australia experienced several large, high-profile cyber incidents…

Table 1 highlights the high-profile cyber incidents in Australia over the past couple of years.

Table 1: Major Australian data breaches over the past two years

Organisation	When breach occurred	Summary
Optus	September 2022	Data breach affecting up to 10 million current and former customers, including names, dates of birth, home addresses, telephone numbers, email contacts, and numbers of passports and drivers licences.
Medibank	November 2022	Data breach affecting 9.7 million people, including names, dates of birth, Medicare numbers and sensitive medical information. Some records were published on the dark web.
Latitude	March 2023	Data breach which exposed the personal data of up to 14 million customers, including drivers' licence numbers, and some passport numbers and Medicare numbers.
HWL Ebsworth Lawyers	April 2023	This data breach was notable for impacting 65 government agencies' client data, including participants of the National Disability Insurance Scheme.
Medisure	May 2024	This incident impacted the personal and health information of 12.9 million people relating to prescriptions, as well as healthcare provider information.

In addition to the high-profile breaches, there was also an increase in reported cybercrime in general. In FY2022/23, almost 94,000 reports were made to the Australian Signals Directorate (the intelligence and security agency responsible for preventing and disrupting offshore cyber-enabled crime, and providing cybersecurity advice), an increase of 23% in the number of cybercrime reports on the previous year.[2]

… which resulted in a series of policy and legislative responses from government.

Over the past couple of years, government has responded in several ways, including:

- Additional funding allocated to cybersecurity by the Australian Government – For example, the 2023 Budget announced $102 million over five years (and $11.8 million per year ongoing) to support and uplift cybersecurity in Australia, including enhancing small business cyber awareness.[3]
- Establishing a National Office of Cyber Security and appointing a National Cyber Security Coordinator, to support the Minister for Cyber Security to lead the coordination of:
  - National cyber security policy
  - Responses to major cyber incidents
  - Whole of government cyber incident preparedness efforts
  - Strengthening Commonwealth cyber security capability.[4]

- The release of a new national cybersecurity strategy – In November 2023, the Australian Government released its new cybersecurity strategy, with the vision of Australia being a world leader in cybersecurity by 2030. The strategy outlines six cyber shields, which provide layers of defence against cyber threats:
  1. Strong businesses and citizens
  2. Safe technology
  3. World-class threat sharing and blocking
  4. Protected critical infrastructure
  5. Sovereign capabilities
  6. Resilient region and global leadership.[5]
- Stronger action taken by financial and privacy regulators, including:
  - In December 2022, the maximum penalties for breaching the Privacy Act were increased from $2.22 million to the greater of: $50 million, three times the value of any benefit obtained through the misuse of the information, or 30 per cent of a company's adjusted turnover in the relevant period.
  - The Australian Prudential Regulation Authority (APRA) took action against regulated entities for breaches in cyber controls. In June 2023, APRA imposed an extra $250 million of regulatory capital on Medibank[6] – a 50% increase – and, in December 2023, it imposed additional licence conditions on NGS Super following deficiencies in its cyber controls.[7]
  - The Australian Securities & Investments Commission (ASIC) Chair Joe Longo warned ASIC will commence proceedings against company directors and boards that fail to take reasonable steps, or make reasonable investments proportionate to the risks that their businesses pose.[8]
  - The Office of the Australian Information Commissioner (OAIC) filed civil penalty proceedings in the Federal Court against Medibank in relation to its data breach, alleging Medibank failed to take reasonable steps to protect customers' personal information from misuse and unauthorised access or disclosure in breach of the *Privacy Act 1988*.[9] The theoretical maximum penalty, although highly unlikely, totals $21.5 trillion (which is $2.2 million per contravention of the Privacy Act times by the 9.7 million impacted customers) – signalling the gravity of the case.[10]
- Tightening of privacy regulation – The Attorney-General's Department released the *Privacy Act Review Report* in February 2023 which included 116 proposals for how to make the Privacy Act "fit for purpose" and able to "adequately protect Australians' privacy in the digital age".[11] The Australian Government released its response to the *Privacy Act Review Report* in December 2023,[12] agreeing with 38 of the 116 proposals, with commentators calling the response "concise, cautious and (certainly) consultative".[13] In September 2024, the first wave of amendments (23 in total) was introduced to Parliament, with the remainder of reforms due to be introduced in 2025.[14]

It is timely to reassess the cyber risk landscape two years after the report.

Given the activity that has occurred in this space since the publication of the cyber risk report, it is timely to return to the issue of cyber risk. We have conducted a series of conversations with more than 20 stakeholders, including insurers and brokers, members of the legal profession, financial institutions, cybersecurity professionals and industry bodies.

The remainder of this paper presents findings from those conversations[I] and further research.



[I] Additional information is available in the authors' presentation to the 2024 All Actuaries Summit and available at https://content.actuaries.asn.au/resources/resource-ce6yyqn64sx3-786882053-7244

3. Corporate Australia Has Received a Cyber Wake-up Call

From our conversations and research, the major events in the past two years and government response to these have provided a stark cyber wake-up call to corporate Australia.

Australia's corporate board members have upskilled on cyber.

The cyber wake-up call has sharpened boards' attention on all things cyber. In addition to the potential for regulatory actions and fines at the company level, there is also increased awareness of director-level responsibility for cyber preparedness. The ASIC Chair commented in late 2023 that, "if boards do not give cyber security and cyber resilience sufficient priority, this creates a foreseeable risk of harm to the company and thereby exposes the directors to potential enforcement action by ASIC, based on the directors not acting with reasonable care and diligence".[15]

According to the Australian Institute of Company Directors (AICD), cybercrime and data security has consistently been the top issue "keeping directors awake at night" since H2 2021.[16,17] In H1 2024, 43% of directors selected cybercrime and data security as a top issue, a level significantly higher than any other issue.[18]

It appears the elevated concern about cyber has been met by action. Additional AICD research suggests there has been an uplift in boards' perceived ability to oversee cybersecurity. In H2 2022, 60% of surveyed company directors agreed that "our board has effective oversight of cybersecurity threats to our organisation". By H1 2024, that had risen to 69%.[19] Our conversations with industry suggest the materials and focus of the AICD itself has been valuable in helping board members upskill.

Corporate Australia has increased its spend on cyber technology…

Our conversations revealed the prevailing mindset is no longer "if we're attacked" but "when we're attacked", and that approach is reflected in greater expenditure on IT security. Gartner, for example, estimates that Australian organisations are expected to spend more than A$7.3 billion on security and risk management products and services in 2024, an increase of 11.5% from 2023.[20]

… and increased its cyber workforce.

In 2024, "cybersecurity analyst" was the fastest growing job in Australia,[21] but shortages of skilled professionals remain. The World Economic Forum, for instance, estimates:

- There is a shortage of nearly four million cybersecurity professionals globally[22]
- The percentage of business leaders reporting they were missing the skills and people they needed to respond to a cyberattack had risen from 6% in 2022 to 20% in 2024.[23]

Cybersecurity salaries have also increased, with recruitment firm JS Careers citing a 35% increase in salaries in the cybersecurity field since the start of 2023.[24]

In response, the Australian Government has committed to:

1. Grow and expand Australia's skills pipeline
2. Improve the diversity of the cyber workforce
3. Professionalise the domestic cyber workforce.[25]

These changes will take time to achieve their goals, and some organisations we spoke to were thinking creatively about how to fill more immediate skills gaps – including looking at candidates from non-IT backgrounds and training them in-house.

With the ever-evolving threat landscape, however, corporate Australia must remain vigilant.

On the whole, most people we spoke to believe there has been a significant step up in understanding and focus on cyber issues by corporate Australia. With the fast-moving threat landscape – for example, ChatGPT was not publicly available when we released our original report – they also universally believe there is no time for "patting themselves on the back". A consistent theme emerged: organisations should be focused squarely on data governance, ensuring data is appropriately classified, stored and disposed of when it is no longer required.

4. What Is Preventing SMEs From Uplifting Their Cyber Capabilities?

In contrast, Australia's SMEs on average have not experienced the same amount of cyber awareness and capability uplift. ASIC's 2023 survey of the cyber maturity of regulated organisations found that smaller organisations consistently reported less cyber maturity than medium and large organisations.[26]

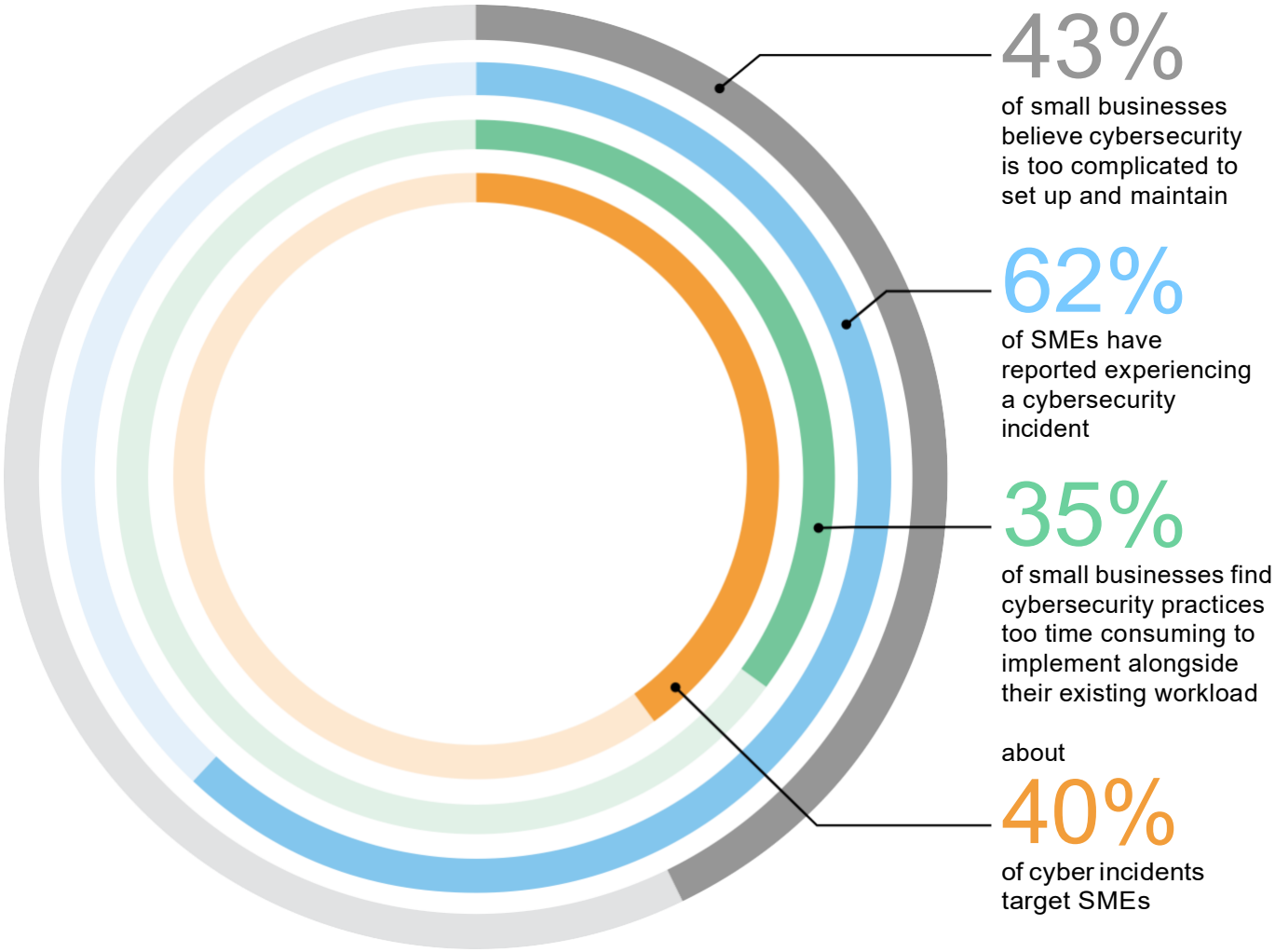
A survey of Australian small businesses (i.e., businesses with fewer than 19 FTEs) revealed that 44% are classed as "unaware and inactive" in their cyber maturity, meaning they are:

- highly unconcerned about cyber threats and not thinking about or talking about cybersecurity at all;
- have minimal cyber-safe practices in place;
- are not providing cybersecurity training; and
- do not have a culture of cyber safety.[27]

From our conversations and research, we understand there are several reasons for this.

The technical nature of cyber and IT means it can be easy to "put your head in the sand"…

Many small businesses put cyber in the "too hard basket", feeling it is full of technical jargon and they do not know where to start. More than 4 in 10 (43%) small businesses believe cybersecurity is too complicated to set up and maintain.[28] A survey of global small businesses suggests that Australian small businesses report, at a higher rate than their international peers, that their biggest barrier to online protection is understanding how to implement cybersecurity measures.[29]



… and the challenging economic climate means no funds or headspace to devote to cyber.

Small businesses are facing challenging economic circumstances. Australian Small Business and Family Enterprise Ombudsman research in 2023 indicated around 43% of small businesses failed to make a profit.[30] While the risk of larger businesses failing has recently improved, younger and smaller businesses are continuing to struggle.[31]

More than one-third of small businesses (35%) find cybersecurity practices too time consuming to implement alongside their existing workload.[32]

Another significant barrier is cost.[33, 34] A 2023 survey of small business leaders revealed 31% had reduced their cybersecurity budgets, and that cost is the primary barrier to small businesses exploring their cybersecurity options.[35]

Many SMEs think they are "too small to target" by cybercriminals...

A survey of small Australian businesses revealed only 35% feel vulnerable to attack due to being a small business.[36] The qualitative results from the same survey indicated that the high-profile attacks of the past couple of years may be further reinforcing the view among SMEs that big businesses are the more likely targets of cyberattacks.

SMEs are very much targets, and the consequences can be existential.

Small businesses are sadly not immune to cyber incidents. The data reveals about 40% of cyber incidents target SMEs,[37] and 62% of SMEs have reported experiencing a cybersecurity incident.[38]

The costs can be significant, and they are rising. In the 2022-23 financial year, the average cost of cybercrime for small businesses increased to $46,000 from $40,000 in 2021-22, and for medium businesses it increased to $97,000 from $88,000 in 2021-22.[39]

For many SMEs, a serious cyber incident would result in business collapse. Anecdotal evidence – not based on Australian data – suggests that 50 to 75% of SMEs would not recover financially from a significant cyber incident.[40]

In recognition of the challenges facing SMEs, there have been several initiatives aimed at lifting their capabilities.

Recent initiatives targeting SMEs' cyber capabilities include:

- In Budget 2023, $23 million was allocated to a small business Cyber Wardens program delivered by the Council of Small Business Organisations Australia.[41] The Cyber Wardens program helps small businesses train their staff to identify cyber safety practices they can implement to better protect their business, employees and clients. The Cyber Wardens program aims to train up to 50,000 Cyber Wardens across 15,000 small businesses.
- In November 2023, the Australian Signals Directorate published its *Small Business Cyber Security Guide* in more than 25 languages.[42]
- In May 2024, the AICD and Australian Information Security Association (AISA) jointly released the *Cyber Security Handbook for Small Business and Not-for-Profit Directors.*[43]

5. Why Cyber Insurance Remains Uncommon for SMEs

Cyber insurance for SMEs at a glance

- Cost of a cyber insurance policy for an SME: Starts at around $700 per annum for a sole trader and can exceed $50,000 for medium-sized businesses.
- Number of cyber insurers offering cyber policies to SMEs: More than 10 insurers and underwriting agencies (several of which are backed by Lloyd's) offer cyber insurance to Australian SMEs.
- Distribution channels: Cyber insurance is typically purchased through a broker, although it is possible for some SMEs to purchase online.
- Percentage of SMEs with cyber insurance: Estimates range from 10% to 25%

Despite the threat landscape, cyber insurance is still relatively uncommon in the cyber toolkit for Australian SMEs, with estimates for cyber insurance coverage of Australia's SMEs ranging from about 10% to 25%.

Our research suggests this is due to several factors.

Cyber insurance is still a relatively new product…

The cyber market is growing but still only comprises a very small proportion of the Australian insurance industry by Gross Written Premium (GWP) – that is, the amount of premiums collected – estimated at around $600 million, compared to around $16 billion GWP for home insurance. As a sign of its growing importance, earlier this year for the first time, APRA started reporting cyber insurance as a separate line of business in its quarterly statistics release.

One industry stakeholder we spoke with believes cyber insurance is today where management liability was 15 to 20 years ago – difficult to sell but common practice. They thought cyber insurance must similarly "earn its stripes" to gain credibility in the market.

… and SMEs are not necessarily aware of what it covers…

Given cyber for SMEs is a relatively new product, insurers are still innovating to discover the right solution to resonate with SMEs. Cyber coverage is not standard, and there can be confusion about what is or is not covered under a cyber insurance policy.[44] The CrowdStrike outage of July 2024 was a timely reminder, requiring policyholders to check whether the outage constituted a "cyber incident" under the relevant insuring clause.[45]

… and what value it can provide.

Many stakeholders we spoke to said SMEs were exactly the types of organisations that would benefit the most from taking out a cyber insurance policy, for factors including:

- A major cyber incident, which was more likely to be an existential threat for an SME compared to a large corporate;
- SMEs being less likely to have access to and resources for the incident response services typically offered as part of a cyber insurance policy – such as access to public relations firms to shoulder discussing data breaches with customers, specialist legal representatives, IT services for investigation and remediation, and even ransom negotiations; and
- Access to free or discounted services available as add-ons to many policies, e.g., access to cybersecurity expertise and threat intelligence services, IT vulnerability assessments and cybersecurity training – all of which can pre-emptively decrease the vulnerability and consequences of the SME to a cyberattack.

Many SMEs are unaware of the benefits available to them. While SMEs can buy cyber insurance online with a handful of underwriting questions, most organisations typically go through their broker to purchase coverage. Through our research, we understand brokers have upskilled rapidly over the past couple of years, but they are limited by the number of one-on-one client conversations they can have in a day to explain how a cyber insurance policy works.

While SMEs can get policies easier than a couple of years ago, for many, price is still a significant barrier.

When we published our report in 2022, cyber insurance was a hard market (i.e., capital available to underwrite cyber risk insurance was relatively tight and therefore policies were relatively expensive with limited coverage). Things have certainly changed since that time:

- There is now more capacity in the market – especially provided by the numerous new entrants to the market arriving over 2023 and 2024. Many of these are targeting the SME sector.
- Insurers are demonstrating greater flexibility and willingness to offer tailored coverages to businesses.[46,47]
- Premiums are flat or falling.

That said, SMEs are particularly resource constrained due to the economic climate, resulting in pressures on expenses, including overall insurance budgets. Our conversations with the insurance industry and SME representatives were clear: affordability of cyber insurance remains a significant barrier. Many SMEs are not yet seeing the value in cyber insurance – it is viewed as a relatively expensive insurance product, especially compared to more traditional insurance products like property and liability insurance.

6. Reducing the Cyber Protection Gap for SMEs

Small business is vitally important to the Australian economy – the small businesses of Australia provide jobs for 5.1 million people and contribute to skills development by employing 42% of all apprentices and trainees.[48]

With the threat of cyberattacks increasing, and little capacity for small businesses to deal with this, a continual and concerted effort is needed to ensure small businesses are not left behind.

Continue to strengthen national cyber defences

Reducing the overall cyber threat level will benefit Australians and Australian businesses, including SMEs. The 2023-2030 Australian Cyber Security Strategy (which the Actuaries Institute supports[49]) recognises that the responsibility for cyber deterrence should sit with those most capable of taking defensive action. The strategy includes an intention to disrupt and deter cyber threat actors from attacking Australia by building law enforcement and offensive capabilities, and shaping international legal frameworks, cooperation and cybercrime.

Evaluate and scale up education and upskilling initiatives

As highlighted in Section 4, there are several actions underway to improve cyber awareness and resilience of Australia's SMEs – including the Cyber Wardens program and guidance in multiple languages published by the Australian Signals Directorate.

While it is too early to assess the effectiveness of recent efforts, we recommend thorough evaluation of these initiatives targeted at SMEs – especially in considering their power to address some of the common challenges also outlined in Section 4. If successful, the various projects could be rolled out more broadly.

Make it easy for SMEs to show they take cyber seriously

Efforts are underway to develop consistent, achievable and affordable cybersecurity certifications for SMEs. For example, Cyber Security Certification Australia is a joint industry/government initiative specifically set up to address SME cyber resilience through an annually updated certifiable standard, led by prominent experts in public and private cybersecurity sectors.

Adopting these standards as industry norms (e.g., it becomes mandatory to hold cyber insurance or sign contracts with government) could help SMEs by simplifying the process of demonstrating their cyber-safe attitudes and cyber preparedness. This would be analogous to the objective external rating systems present in other industries, such as Green Star Buildings rating program undertaken by the Green Building Council of Australia.

Consider SMEs unique cyber challenges in the upcoming round of Privacy Act changes

The Australian Government has announced further amendments will be made to the Privacy Act (in addition to the amendments announced in September 2024). One of the potential changes under consideration is removing the small business exemption (Australia's privacy law does not apply to businesses with annual revenue less than $3 million).

Should the exemption be removed, the Government has indicated that support will need to be provided to assist small businesses to make the change (e.g., tailored guidance and a transition period). This support should be designed with consideration of the capacity concerns outlined earlier in Section 4.

Keep the dialogue open between government, the insurance industry and small business

We understand conversations are already underway between the Australian Government, the Insurance Council of Australia and the Council of Small Business Organisations Australia, including on how to make cyber insurance more accessible and affordable for SMEs. Continued and enduring dialogue and partnership will be required to uplift cyber resilience as the threat landscape continues to evolve.

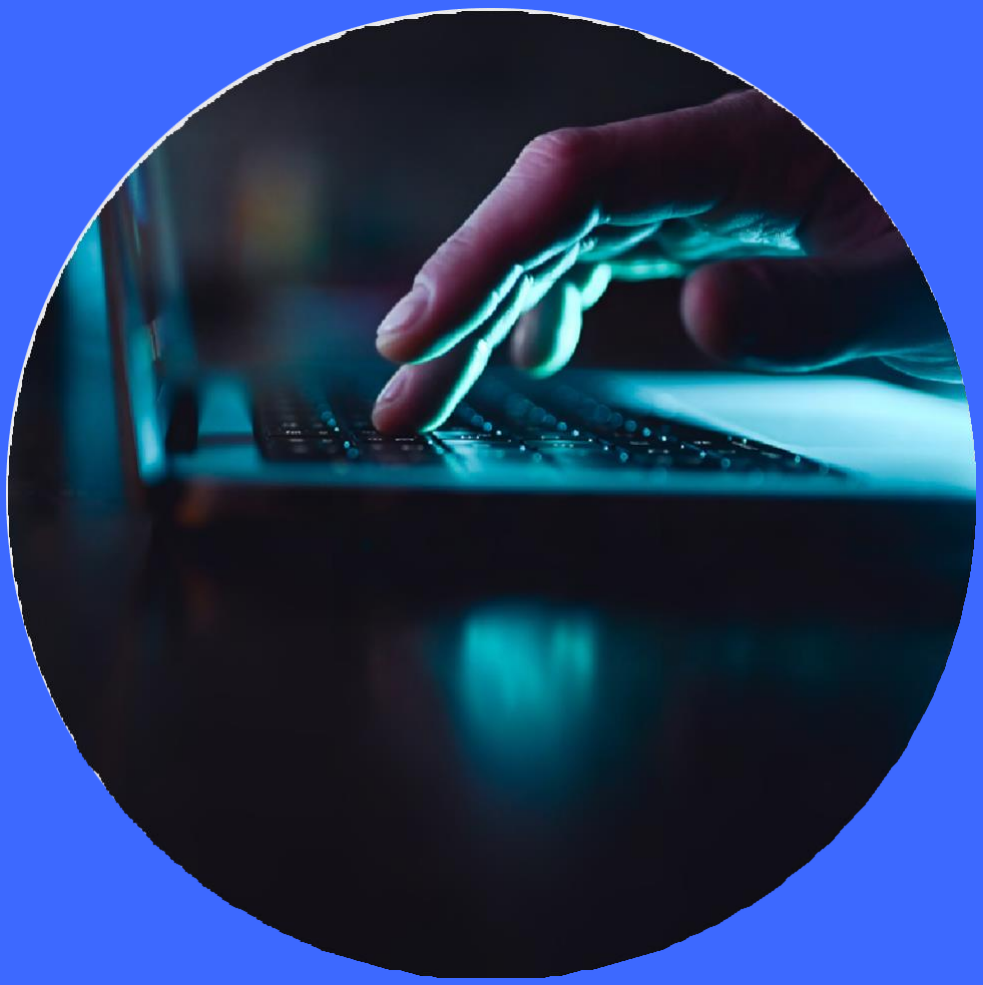


References

1. Toh, W., Simmonds, R., & Neary, M. (2022). *Cyber Risk and the Role of Insurance*. Actuaries Institute. https://content.actuaries.asn.au/resources/resource-ce6yyqn64sx3-2093352434-54014
2. Australian Signals Directorate (ASD). (2023). *2022-23 ASD Cyber Threat Report*. https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf
3. Commonwealth of Australia. (2023). *Budget Measures Budget Paper No. 2*. https://archive.budget.gov.au/2023-24/bp2/download/bp2_2023-24.pdf
4. Department of Home Affairs. (2024). *Cyber Coordinator*. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator
5. Australian Government. (2023). *2023 – 2030 Australian Cyber Security Strategy*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
6. Australian Prudential and Regulation Authority (APRA). (2023). *APRA takes action against Medibank Private in relation to cyber incident*. https://www.apra.gov.au/news-and-publications/apra-takes-action-against-medibank-private-relation-to-cyber-incident
7. Australian Prudential and Regulation Authority (APRA). (2023). *APRA imposes additional licence conditions on NGS Super.* https://www.apra.gov.au/news-and-publications/apra-imposes-additional-licence-conditions-on-ngs-super
8. Smith, P., & Mizen, R. (2023. September 19). ASIC to target boards, execs for cyber failures. *Australian Financial Review*. https://www.afr.com/technology/asic-to-target-boards-execs-for-cyber-failures-20230913-p5e4bf
9. Office of the Australian Information Commissioner (OAIC). (2024). *OAIC takes civil penalty action against Medibank.* https://www.oaic.gov.au/newsroom/oaic-takes-civil-penalty-action-against-medibank
10. Dentons. (2024). *Are we heading for a $21.5 trillion penalty order for a data breach in Australia?* https://www.dentons.com/en/insights/articles/2024/june/14/are-we-heading-for-a-21-5-trillion-penalty-order-for-a-data-breach-in-australia
11. Attorney-General's Department. (2022). *Privacy Act Review Report 2022*. https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf
12. Australian Government. (2023). *Government Response Privacy Act Review Report*. https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF
13. Gilbert & Tobin. (2023). *Federal Government offers modest response to Privacy Act Review*. https://www.gtlaw.com.au/knowledge/federal-government-offers-modest-response-privacy-act-review
14. Clyde & Co. (2024). *Setting the Foundation for Significant Privacy Law Reform in Australia*. https://www.clydeco.com/en/insights/2024/09/setting-the-foundations-for-significant-privacy-la
15. Australian Securities & Investments Commission (ASIC). (2023a). *Marconi's illusion: What a 120-year-old magician's trick can teach us about cyber preparedness*. https://asic.gov.au/about-asic/news-centre/speeches/marconi-s-illusion-what-a-120-year-old-magician-s-trick-can-teach-us-about-cyber-preparedness/
16. Australian Institute of Company Directors (AICD). (2022). *Director Sentiment Index. Second Half 2021. Insights Report.* https://www.aicd.com.au/content/dam/aicd/pdf/news-media/research/2021/roy-morgan-aicd-dsi-2021-2-insights-report.pdf
17. Australian Institute of Company Directors (AICD). (2024). *Director Sentiment Index Survey. 1st Half 2024. Insights Report.* https://www.aicd.com.au/content/dam/aicd/pdf/news-media/research/2024/dsi-1h-24-web.pdf
18. Ibid.
19. Ibid.
20. Gartner. (2024, March 19). *Gartner Forecasts Enterprise Security and Risk Management Spending in Australia to Grow 11.5% in 2024*. https://www.gartner.com/en/newsroom/press-releases/2024-03-19-gartner-forecasts-security-and-risk-management-spending-in-australia-to-grow-more-than-11-percent-in-2024
21. LinkedIn. (2024). *LinkedIn Jobs on the Rise 2024: 25 Australian in-demand roles*. https://www.linkedin.com/pulse/linkedin-jobs-rise-2024-25-australian-in-demand-aka5c/?trackingId=EvsGEZ%2F4kUUBd%2FBaMwlCMA%3D%3D
22. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
23. World Economic Forum. (2024). *Strategic Cybersecurity Talent Framework*. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf
24. JS Careers. (2024). *Cyber Security Market Update*. https://jscareers.com.au/cyber-security-market-update/

25. Australian Government. (2023). *2023 – 2030 Australian Cyber Security Strategy*. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf
26. ASIC. (2023). *Spotlight on cyber: Findings and insights from the cyber pulse survey 2023*. https://download.asic.gov.au/media/yiqjhv0p/rep776-published-13-november-2023.pdf
27. Cyber Wardens. (2024). *Building a culture of cyber safety in Australian small business: Cyber Wardens Research Report*. https://cyberwardens.com.au/wp-content/uploads/2024/03/Research-Report-Building-a-culture-of-cyber-safety-in-Australian-small-businesses.pdf
28. Ibid.
29. McAfee. (2024). *Cybersecurity for Small Businesses*. https://media.mcafeeassets.com/content/dam/npcld/ecommerce/en-us/docs/guides/gd-small-business-resource-guide.pdf
30. Australian Small Business and Family Enterprise Ombudsman (ASBFEO). (2023). *Small Business Matters*. https://www.asbfeo.gov.au/sites/default/files/2024-02/Small%20Business%20Matters_February%202024.pdf
31. Illion. (2024). *Commercial Risk Barometer. Australia. August 2024*. https://www.illion.com.au/wp-content/uploads/2024/08/Australian-Commercial-Risk-Barometer-August-2024.pdf
32. Cyber Wardens, *Building a culture of cyber safety in Australian small business: Cyber Wardens Research Report*.
33. Chidukwani, A., Zander, S. and Koutsakis, P. (2024). Cybersecurity preparedness of small-to-medium businesses: A Western Australia study with broader implications. *Computers & Security*. 145. https://www.sciencedirect.com/science/article/pii/S0167404824003316
34. McAfee, *Cybersecurity for Small Businesses*.
35. Mastercard. (2024). *New data reveals up to 309,000 Australian small businesses say they've been targeted by cyberattacks, yet many are forced to cut cybersecurity costs*. https://www.mastercard.com/news/ap/en/newsroom/press-releases/en/2023/new-data-reveals-up-to-309-000-australian-small-businesses-say-they-ve-been-targeted-by-cyberattacks-yet-many-are-forced-to-cut-cybersecurity-costs/
36. Cyber Wardens, *Building a culture of cyber safety in Australian small business: Cyber Wardens Research Report*.
37. AAG. (2024). *The Latest 2024 Cyber Crime Statistics (updated July 2024)*. https://aag-it.com/the-latest-cyber-crime-statistics/
38. Australian Cyber Security Centre (ACSC). (2020). *Cyber Security and Australian Small Business Survey Results*. https://www.cyber.gov.au/sites/default/files/2023-03/Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results%20-%2020201130.pdf
39. ASD, *2022-23 ASD Cyber Threat Report*.
40. ASBFEO, *Small Business Matters*.
41. Commonwealth of Australia. (2023). *Budget Measures Budget Paper No. 2*. https://archive.budget.gov.au/2023-24/bp2/download/bp2_2023-24.pdf
42. Australian Signals Directorate & Australia Cyber Security Centre. (2023). *Small business cyber security guide*. https://www.cyber.gov.au/sites/default/files/2023-07/acsc_small_business_cyber_security_guide.pdf
43. Australian Institute of Company Directors (AICD) and Australian Information Security Association (AISA). (2024). *Cyber Security Handbook for Small Business and Not-for-Profit Directors*. https://www.aicd.com.au/content/dam/aicd/pdf/tools-resources/director-tools/board/cyber-security-handbook-web.pdf
44. Falk, R., & Brown, A. (2024). *Underwritten or Oversold? How cyber insurance can hinder (or help) cybersecurity in Australia*. Cyber Security Cooperative Research Centre. https://cybersecuritycrc.org.au/sites/default/files/2021-10/Underwritten%20or%20oversold%20%20-%20DV.pdf
45. Clayton Utz. (2024). *Crowdstrike Outage: will cyber insurance respond?* https://www.claytonutz.com/insights/2024/july/crowdstrike-outage-will-cyber-insurance-respond
46. Aon. (2024). *Q2 2024: Global Insurance Market Overview*. https://www.aon.com/en/insights/articles/global-insurance-market-overview-q2-2024
47. Marsh. (2024). *Mid-Year Insurance Market Update 2024*. https://www.marsh.com/au/services/international-placement-services/insights/australian-mid-year-insurance-market-update.html
48. ASBFEO, *Small Business Matters*.
49. Actuaries Institute. (2023). *Response to Discussion Paper: 2023 – 2030 Australian Cyber Security Strategy*. https://content.actuaries.asn.au/resources/resource-ce6yyqn64sx3-2093352434-56949

Actuaries Institute.



Actuaries Institute
Level 2, 50 Carrington St
Sydney NSW 2000 Australia

T +61 (0) 2 9239 6100
E public_policy@actuaries.asn.au
W www.actuaries.asn.au