Submission to the Inquiry into cyber security for small to medium sized businesses and Organisations

Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations, August 2026

Lumenas

Lumenas submission to the Inquiry into cyber security for small to medium sized businesses and Organisations

Small businesses are the commercial connective tissue of Australia's economy. They often give young Australians their first job; they're how many migrant families make a new start; and they're where new products and services are often created before they scale into globally successful companies.

Small businesses can be mightier than they seem. Australian cafes famously faced down Starbucks[1], a $120bn[2] multinational with a workforce the size of the Sunshine Coast's population.[3] The Australian startup community also continues to beat the odds, producing 1.2 unicorns for every US$1 billion of venture capital invested, ahead of Israel (1.1) which is widely known as the 'Startup Nation'.[4,]

But many small businesses are being devastated by cyber security incidents. The average loss per cyber crime incident for an Australian small business is $56,600, more than double the average small business tax bill[5].[6] The less visible damage is what it does to confidence in technology itself, and in the businesses and providers that supply it. auDA's 2026 Digital Lives research found that 47% of small businesses feel helpless against cyber threats on the basis that if larger, better-resourced companies cannot prevent attacks, they stand little chance either.[7]

A business owner who cannot tell whether their existing systems are safe is unlikely to put more of the business into new ones. Australians already behave this way as consumers: auDA found that 67% actively avoid certain online activities as a precaution against online harm.[8] The cost of that caution is meaningful GDP growth. Deloitte Access Economics estimates that if just one in ten Australian SMBs moved one rung up the AI maturity ladder, annual GDP would rise by around $44 billion.[9]

Small businesses can be vibrant and economically resilient, while also vulnerable to cyber security incidents, like people can be healthy and hard-working but incapacitated from a virus. This analogy also reveals the nature of the solution we propose: fix the system, not the small businesses.

---

[1] Starbucks Corporation (2008) Starbucks Takes Significant Actions to Position the Company for 2009, media release, 30 July 2008; Australian Food Timeline, Starbucks closed Australian stores.
[2] Starbucks market capitalisation of US$118.5 billion at 20 August 2026, per companiesmarketcap.com and stockanalysis.com.
[3] Starbucks Corporation (2025) Form 10-K for the fiscal year ended 28 September 2025; Australian Bureau of Statistics (2025) Regional population.
[4] Dealroom, Side Stage Ventures and AWS (July 2025) Australia Venture & Startup Report 2025.
[5] Australian Taxation Office, Small business income tax gap.
[6] Australian Signals Directorate (2025) Annual Cyber Threat Report 2024-25.
[7] auDA (2026) Digital Lives of Australians report.
[8] auDA (2025) Digital Lives of Australians 2025.
[9] Deloitte Access Economics (2025) The AI Edge for Small Business, commissioned by Amazon.

1. Introduction

The Australian Government has undertaken a significant amount of work to uplift national cyber security over the last few years. But we know there's still a big gap in cyber security when it comes to small and medium businesses (SMBs). While SMBs contribute more than half (55%) of Australia's private sector GDP[10], they account for 88% of business cyber crime reports.[11]

Uplifting the cybersecurity of small and medium businesses is different, because unlike large businesses, they don't have the time or resources to do it largely by themselves. This is true of IT management generally for SMBs, which is why it's common to engage an external IT provider commonly known as 'managed services providers' (MSPs). They will normally handle the day-to-day IT work, setting up laptops and email accounts for new staff, keeping software updated, fixing the printer when it breaks, and providing advice on cyber security.

While there are many excellent MSPs in Australia, we find experiences of bad or outright negligent providers are far too common. These experiences are common because the MSP market suffers from three critical market failures, outlined in the next section. These make it too easy for bad providers to survive and too hard for good providers to succeed.

2. Small businesses get their cyber security actively and passively

Small businesses rarely buy "cyber security" as a discrete product. They acquire it in two ways. Actively, through advice from a managed service provider and passively, bundled into the platforms they already use.

The passive channel is doing far more of the work than is generally recognised. Software platforms focused on small businesses often provide excellent security, and companion products – like authenticators and passkeys – that help small business customers use those products in a more secure manner. Though we note that many small businesses could be better served, through ensuring core security features – like single sign on – is included in the lowest tier rather than being a premium option. This is one part of ensuring that products, for all customers, are secure-by-design.

Even if a technology product is secure, it can easily create cyber security vulnerabilities if it's not configured properly. This problem is analogous to IKEA furniture. IKEA makes good, affordable and robust furniture; but you still have to secure the bookcase to the wall for it to be safe.

---

[10] Australian Small Business and Family Enterprise Ombudsman, Contribution to Australian Gross Domestic Product, drawing on ABS Australian Industry, Table 5.
[11] Australian Signals Directorate (2025) Annual Cyber Threat Report 2024-25.

The most useful thing IKEA can do is put the bracket in the box with clear instructions. The remaining job needs to be done by the buyer or someone they hire to help them secure the bookshelf. MSPs are the IKEA bookcase-securers of technology.

MSPs ensure that the technology tools are set up safely for a small business to use; and that gaps are closed as they emerge. But this work often costs extra, on top of creating new email addresses or collecting laptops when employees leave. The extra cost for extra work is not an issue, but it can be tricky for customers to judge whether their MSP is recommending additional work because it's warranted or they're just trying to make more money. This is potential conflict faced by most professionals, but we believe it reveals the pervasive lack of trust and inability to verify the validity of MSPs advice, both of which relate to the market failures present in the MSP market.

3. The market for cyber security advice is broken

There are many excellent providers in the MSP market. But the market does not currently reward good behaviour efficiently, which makes it too easy for bad providers to survive and difficult for good providers to succeed. There are three reasons the market doesn't work as effectively as it could.

1. **High switching costs.** Once a provider holds administrative control of a small business's systems, changing provider is costly, disruptive and technically risky. This means poor MSP performance does not reliably cost the provider the customer, and bad providers can survive while good providers aren't 'rewarded' by the market with additional customers switching towards them.
2. **Information asymmetries at engagement.** The MSP market is unregulated. This means unlike engaging an accountant or lawyer, you can't check if they have completed a standard qualification nor can negligent providers be 'removed' from the market. The best signals available, certifications such as ISO standards, describe process rather than outcome. A provider with the technology equivalent of a five-star safety rating is not necessarily more secure itself, nor more likely to do right by you as a customer.
3. **Ongoing information asymmetries.** Even a well-served small business generally cannot tell whether its provider is doing the right thing. Unlike in human health, there is no pain signal: the business owner does not know their technology systems are 'hurt'.

These three market failures create a broken environment for cyber security advice. This is because bad providers aren't forced out by a well-functioning market, but trust also appears to be low which also unfairly taints small businesses' relationships with good providers whose advice they often question – even if they are happy with their IT provider's performance.

4. Fixing SMB cyber security requires a systematic shift in the MSP market

Small businesses should expect that they can rely on the advice from their MSP. This does not mean that the MSP market will be 'perfect' – some bad providers exist; nor does it mean that cyber security incidents will be eradicated – these can still be caused by human error and weather events. What we propose is changing the norm to typically doubting MSP cyber security advice, to small businesses just wanting to verify this advice is accurate because that's good governance. Much like double checking your tax return because you acknowledge your accountant is human and can make mistakes, rather than refusing to put in a tax return because they recommended doing so.

We think the solution requires multiple actions across the three market failures outlined, with contributions from the business community, industry associations and government. What it does not require is asking small businesses to carry more load themselves.

Reducing switching costs – business community & Government

Making it easier for businesses to switch IT providers means we encourage the market to solve more of this problem itself, and consistently, over time. This would be enabled by tools or services that give businesses better visibility over what data and access their MSP holds.

Business community. We believe there is a market for tools and services that empower small businesses to have a better understanding of their IT environment. Lumenas already provides one tools in this space, our IT Check. We think the business community should pay more attention to this problem, because we think it's worth solving.

Government. Government could develop a simple checklist to support small businesses to switch IT providers. This could be developed in partnership with the large small business platforms to provide tool-specific information on how to identify what data or access your MSP may have.

Reducing information asymmetries at engagement – Government

A systematic shift in the MSP market requires commensurate change in how it operates, and we believe that includes some regulation of this business critical service. This is partly already underway through the CyberPath pilot.

We propose continuing with the CyberPath pilot and examine how any professionalisation of the cyber security profession would impact the efficacy of the MSP market. Does it make it easier to spot a good provider? Does it create a mechanism to address wilfully negligent conduct? How does it support better SMB cyber security?

Reducing ongoing information asymmetries – business, industry associations & Government

IT providers will always know more about IT than their customers. But the customers need a third-party (or method) to verify the IT provider's advice or work. This can be done through undertaking a cyber security audit, engaging a fractional CTO or regularly using tools which assess aspects of your cyber security resiliency. One challenge for many small businesses to accessing these services is often cost.

Large businesses & industry associations. These organisations can use their purchasing power to negotiate better rates for small businesses in their supply chain or membership. Many industry associations already negotiate discounted airline lounge memberships as a member perk, for instance, presumably this could extend to tools and services that improve cyber security resiliency.

Government. Government can provide objective information on what 'good' looks like for SMB cyber security. The Essential Eight was a strong starting point. Further we recommend two actions:

- Continue the refresh of the Essential Eight, with guidance tailored to business size. Tailoring guidance by business size is the change that will do most to make the framework usable for businesses and non-technical leaders.
- Simplify the sources of information. Government agencies and industry bodies should stop producing slightly different versions of the same guidance and point consistently to the ACSC.

Enabling actions - Government

There is additional work that could be undertaken to better ensure that the technology products purchased by small businesses are secure-by-design. This makes it easier for the SMBS and their MSPs to improve cyber resiliency. This includes:

- Set minimum security expectations for business technology sold in Australia, ideally pursued as an OECD standard or with like-minded partners. We acknowledge that an Australian standard alone is unlikely to affect global tech businesses behaviour because we're too small, and note that this isn't uniquely an Australian problem. This standard doesn't have to be prescriptive and should be regularly updated, it could be voluntary in the form of an industry code.

- Use procurement as leverage: Rather than asking small businesses seeking to procure to Government to do more, ask large businesses them what they have done to make their small business customers safer, and whether they are charging more for it by excluding simple features like single-sign on from the lowest-priced tiers of their products. This could be more easily incorporated into procurement processes if there was an existing standard, such as industry code, to self-assess against which then requires some ongoing verification.

These actions can reshape the MSP market in Australia so that small businesses can learn to trust their MSP's advice. It could create an environment where changing provider is not an enormous risk in itself, and small business leaders feel they have agency over their own IT environments. Those outcomes are the product of market settings, not individual discipline, and they are within reach of government, large businesses and the technology industry acting together. Get the settings right, and cyber security stops being a handbrake on how small businesses use technology.

About Lumenas

Lumenas is an Australian startup that provides IT management software for accidental IT leaders. The Lumenas IT Check provides an independent assessment of an organisation's IT environment and cyber risk in business language to enable non-technical leaders to proactively manage their technology.

Appendix A: Calculations and notes

The notes below are numbered to match the footnotes in the body of this submission. Only footnotes that involve a calculation, a derivation or a definitional caveat have a corresponding note.

1. Australian cafe market and Starbucks. In 2008 Starbucks closed 61 of its 84 Australian stores, retaining 23, following accumulated losses of roughly $105 million over its first seven years in the market and citing business challenges unique to Australia.

2. Starbucks market capitalisation. US$120 billion is rounded point-in-time figure at 20 August 2026 and is volatile. It is drawn from stock market data rather than the annual report, which does not contain a market capitalisation figure, so it is dated separately from the employee count at note 3.

3. Starbucks workforce comparison. Starbucks reported approximately 381,000 employees at 28 September 2025, and headcount has been declining in recent years. The Sunshine Coast, at approximately 390,000 people, is the closest Australian population match.

4. Unicorn capital efficiency. The figure of 1.22 unicorns for every US$1 billion of venture capital invested is cumulative since 2000, not an annual rate. The report was produced by a venture capital firm together with a data provider and a cloud vendor, so it is industry research rather than official statistics. Unicorn counts vary between databases.

5. Average small business tax bill. Expected small business income tax collections of $128.8 billion in 2022-23, divided by the ATO's small business population of 5.91 million entities, gives an average of approximately $21,800 per business. Three caveats apply. It is a mean across a population heavily weighted towards the smallest businesses, so a typical small business pays considerably less. It covers income tax only, excluding GST, superannuation guarantee and payroll tax. And the two figures compared in this submission are not from the same year: the $56,600 is FY2024-25, while 2022-23 is the latest tax year published.

6. Average loss per cybercrime report. The $56,600 is the average self-reported cost per cybercrime report lodged by a small business, up 14% on the previous year. It is a cost per report rather than per business, so a business affected twice is counted twice, and it is self-reported rather than audited. It describes businesses that reported a loss, not the small business population as a whole.

8. Consumer avoidance of online activity. The 67% figure measures individual Australians avoiding certain online activities as a precaution against online harm, not businesses withholding investment in technology. We are not aware of Australian research testing the equivalent question for small businesses, and the finding is offered as a parallel rather than as direct evidence.

9. AI productivity opportunity. The $44 billion figure is Deloitte Access Economics modelling commissioned by Amazon, based on a survey of 1,000 Australian SMBs against a bespoke AI Maturity Index. It is a modelled scenario in which one in ten SMBs advances one step in maturity, not an observed outcome.

10. SMB share of GDP. ASBFEO puts small business at 32% and medium business at 23% of private sector value added, giving 55% combined. These figures cover selected industries and exclude financial and insurance services. ASD does not publish the business size thresholds used in its cybercrime reporting, so the categories behind the 88% figure and these GDP shares may not be a precise match.

11. SMB share of business cybercrime reports. ASD reports that large businesses accounted for just over 12% of cybercrime reports from all businesses in FY2024-25, so small and medium businesses account for just under 88%.