11 September 2026

Committee Secretariat
Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations
PO Box 6021
Parliament House
Canberra ACT 2600

via email: cssmbo.reps@aph.gov.au

Dear Committee Secretariat

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

The Australian Small Business and Family Enterprise Ombudsman (ASBFEO) welcomes the opportunity to make a submission to the Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations' inquiry into cyber security for small to medium sized businesses and Organisations.

Cyber security is a critical issue for Australia's small businesses. The 2026 Small Business Cyber Security Pulse Check Report found that 4 in 5 small businesses surveyed had experienced a cyber incident, up 3% since 2023.[1] The average cost of cybercrime to an impacted small business was $56,600 per report in 2024-25, 14% higher than in 2023-24.[2]

The key concerns of small business owners following a cyber attack are damage to their business reputation, revenue and sale loss, costliness of recovering from an incident, loss of customer confidence, customer attrition and potential legal ramifications and lawsuits.[3]

There are a range of factors which impact small business' implementation of cyber security measures. These include:

- the increasing prevalence and sophistication of cyber attacks,
- their ability to identify cyber security risks and weaknesses in their systems,
- being overwhelmed by, or not understanding, information on cyber security,
- underestimating the risk and consequences of a cyber attacks, and a gap in planning for, and responding to, cyber attacks,[4] and
- issues with accessing affordable cyber insurance and understanding their insurance needs.[5]

[1] Cyber Wardens, *Small Business Cyber Security Pulse Check Report*, Cyber Wards, 2026, accessed 28 August 2026.
[2] Australian Signals Directorate (ASD), *Annual Cyber Threat Report 2024-25*, ASD, Australian Government, 2025, accessed 27 August 2026.
[3] Chubb Insurance Australia Limited, *Too Small to Fail?,* Chubb Insurance Australia Limited, 2019, accessed 14 August 2026.
[4] Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), *Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey*, 2020, ASD's ACSC, Australian Government, accessed 19 August 2026. Please note the points above this footnote are from the *Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey*, unless otherwise indicated.
[5] Australian Chamber of Commerce and Industry (ACCI), Addressing the Small Business Insurance Challenge, ACCI, 2025, accessed 25 February 2026.

Small business owners hold differing views on the importance of cyber security. The Australian Cyber Security Centre's (ACSC) 2020 survey of small and medium businesses regarding their understanding of cyber security practices and knowledge, found that respondents know that cyber security is important regardless of how they rate their understanding of cyber security. However, this view may not be representative of the broader small business sector as those who responded tended to have encountered a cyber incident.[6]

In contrast to the findings of the ACSC survey, the ASBFEO has heard that many small businesses have limited or no awareness that their business requires cyber security protection or do not consider they would be a target. These differences reflect the fact that small business owners differ in their cyber security awareness and understanding, and highlight that:

1. small businesses operate in an increasingly complex and evolving cyber threat environment and would benefit from greater awareness of the impacts (if they are not already aware), and
2. small businesses should be supported to implement practical, proportionate measures to reduce cyber risks, such as the Essential Eight.[7]

Recognising the resource, time and capability constraints faced by many small businesses, business owners need access to information, tools and support to strengthen their cyber security awareness and resilience.

Publicise relatable small business cyber attacks

Small businesses who have never experienced a cyber attack consider they are less likely to face an attack compared to a small business who has experienced one. Also, the ACSC 2020 survey found that almost half of small and medium businesses rated their cyber security understanding as 'average' or 'below average' and had poor cyber security practices.[8] This suggests that the cyber awareness of many small businesses is low, despite the wealth of free cyber security resources that are available.

To improve small business cyber maturity and encourage the uptake of cyber safety practices, we suggest an awareness campaign with small business case studies that highlights the costly consequences of a cyber incident.

We note that the Government's Horizon 2 Action Plan includes extending the reach and accessibility of cyber awareness messaging from the "Act Now. Stay Secure." campaign.[9] The ACSC survey highlights how case studies can provide small businesses with both tangible and relatable examples on the specific consequences of cyber attacks, how a business can recover, and the preventative steps that can be taken to prevent future cyber attacks.[10] The campaign should include a specific focus on small business with a series of de-identified, relatable case studies of cyber attacks affecting small businesses.

---

[6] ASD's ACSC, *Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey*, 2020, ASD's ACSC, Australian Government, accessed 19 August 2026.
[7] ASD's ACSC, *Essential Eight,* cyber.gov.au website, n.d., accessed 2 September 2026.
[8] ASD's ACSC, *Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey*, 2020, ASD's ACSC, Australian Government, accessed 19 August 2026.
[9] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy, Horizon 2 Action Plan,* Department of Home Affairs, Australian Government, 2026, accessed 28 August 2026.
[10] ASD's ACSC*, Cyber Security and Australian Small Businesses Results from the Australian Cyber Security Centre Small Business Survey*, 2020, ASD's ACSC, Australian Government, accessed 19 August 2026, accessed 19 August 2026.

These case studies should focus on the key cyber threats businesses face, which in 2024-25 were email compromise resulting in no financial loss, business email compromise fraud resulting in financial loss and identity fraud, and clearly communicate:[11]

- how the cyber attack occurred,
- impact to the business, including the financial cost, reputation impact, operational downtime, business disruption, legal and regulatory consequences,
- impacts on customers and suppliers, and
- the practical steps that could have prevented the incident, and how to implement them.

An example of a case study, provided by the NSW Small Business Commission, is at Attachment A.

Alongside case studies, the campaign should include practical mitigation measures that small businesses can take to strengthen their cyber security practices. These measures could include encouraging business owners to independently verify the legitimacy of communications and payment requests, while government agencies and large organisations should clearly communicate how recipients can confirm the authenticity of their messages. Other recommended actions include implementing anti-malware protections, enabling multi-factor authentication, and conducting cyber security training for employees.

The ASBFEO is willing to assist with the development of case studies and additional information.

To maximise the effectiveness of any awareness-raising campaign, information and guidance from the campaign should be delivered through channels small businesses know and trust. In the ASBFEO's experience, small businesses are more likely to engage with information delivered through trusted industry and professional networks than through regulatory publications alone.

The government department leading the campaign should partner with a wide range of trusted bodies like state, territory and federal government agencies, business groups, and organisations that regularly engage with small businesses, for example:

- Australian Tax Office
- Australian Banking Association
- industry associations
- local chambers of commerce
- council-run business networks
- multicultural chambers of commerce
- trusted advisers such as financial advisers, accountants and business mentors.

A coordinated education and awareness campaign delivered through these channels could help improve small business understanding of cyber risks and how they can build their cyber maturity.

Consolidate access to cyber security resources and support

Feedback received by the ASBFEO from small business owners suggests experiences with available support services are mixed, with some business owners reporting difficulty accessing advice that meets their needs. For example, some small businesses face challenges identifying the

[11] ASD, *Annual Cyber Threat Report 2024–2025*, ASD, Australian Government, 2025, Canberra, accessed 27 August 2026.

appropriate source of support following cyber attacks, particularly where responsibilities span multiple organisations.

Business owners report being referred between agencies and service providers, creating additional complexity and delays, particularly for business email compromise and payment redirection scams. These challenges can be heightened for business owners requiring translation services or other accessibility supports. Also, small business owners with limited English may rely on word of mouth or require assistance to read and interpret the guidance.

Existing and previous government initiatives, including cyber.gov.au, business.gov.au, ai.gov.au, Cyber Wardens, the Small Business Cyber Resilience Service, and the Digital Solutions Program, provide valuable information, guidance and support to help small businesses strengthen their cyber resilience. The new CyberSmart Program will include a CyberSmart Hub, another government website with cyber security resources.

With the range of cyber resources delivered across multiple agencies, platforms and websites, it can be difficult for small businesses to navigate the information and support they need. This fragmentation is particularly challenging for small businesses as cyber security issues often need to be considered alongside artificial intelligence, data protection and privacy as part of a broader digital risk management approach.

To strengthen small businesses' access to government cyber security assistance, the ASBFEO recommends the following initiatives:

- Develop a single online hub specifically designed for small business that has links to the various cyber security support services, programs and information that are available. Websites like cyber.gov.au and business.gov.au already have cyber security pages for small businesses but there is no single entry-point that links to all relevant services and resources.
  - In addition, a concierge-style advisory service could be developed to help small businesses identify which services and resources suit their needs. Such a service would be particularly valuable during or immediately following a cyber incident, when business owners are often required to make urgent decisions while managing significant operational and financial pressures.
- Have language translations for all cyber resources to assist CALD small business owners. Good examples are the language translations that accompany the 'small business cyber security guide' on cyber.gov.au.[12]
- Increase awareness of the "Report" page on cyber.gov.au. This page serves as a practical decision-making tool for small businesses by directing them to the appropriate reporting channels for different types of cyber attacks, and for identifying attacks that are subject to mandatory reporting obligations.[13]

Prioritise awareness, education and support services over standards and certifications

The ASBFEO notes that the 2023-2030 Australian Cyber Security Strategy includes the proposed CyberSmart Program, a voluntary cyber security standards and certification regime for small and

[12] Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), *Small business,* cyber.gov.au website, n.d., accessed 19 August 2026.
[13] Australian Cyber Security Centre, *Report,* cyber.gov.au website, n.d., accessed 19 August 2026.

medium businesses. Small and medium businesses who are CyberSmart compliant will receive a CyberSmart trust mark.[14]

The ASBFEO notes there may be potential benefits to the CyberSmart Program. Alongside these benefits, there may be unintended consequences that warrant careful consideration. The trust mark may provide value by enabling clients to identify businesses that have implemented a cyber security standard. However, there is a risk that the trust mark could create market disadvantages for small businesses that do not hold the certification, notwithstanding that they may have effective cyber security measures in place. This could occur where businesses are either unaware of the program or choose not to participate because they are already actively managing their cyber risks.

For small businesses, obtaining and maintaining certifications can impose administrative, financial and time costs. It is therefore important that the value proposition of any certification scheme is clear and of net benefit for participants.

The ASBFEO remains of the view that well-targeted awareness, education and support measures are generally more effective than standards or certification-based approaches in lifting small business capability. However, if work towards a CyberSmart trust mark proceeds, consideration should be given to extending its applicability across all businesses, not just small and medium businesses.

Under the CyberSmart Program as currently proposed, large businesses are not within scope and would therefore be ineligible to obtain the trust mark. The ASBFEO considers that where government-endorsed standards and certifications are available to small and medium businesses, equivalent opportunities should also be available to large businesses. This would help ensure a more level playing field and avoid creating a system in which certification requirements or expectations are disproportionately placed on smaller businesses.

Develop practical AI security guidance for small business

According to the Australian Bureau of Statistics, business adoption of AI increased in 2024-25 compared to very low rates in 2021-22 when generative AI tools were not available.[15] At the same time, use of AI tools is creating cyber security risks including: data leaks and privacy breaches; unreliable or manipulated outputs due to AI systems having biases or being compromised by malicious cyber actors; supply chain vulnerabilities due to third party AI software applications being compromised, and increasingly sophisticated scams and phishing campaigns. [16]

Small businesses require practical guidance on using AI safely, particularly where AI systems interact with customer information, business systems and financial transactions. While cyber.gov.au and ai.gov.au already provides guidance on AI security, there should be an emphasis on good AI governance and guardrails tailored to small businesses explaining:

- cyber risks associated with AI-enabled systems, including what information should *not* be entered into AI systems, risks involved with AI coding, and using AI tools in ways that are consistent with laws and regulations (e.g. Australian Consumer Law),

[14] Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy, Horizon 2 Action Plan,* Department of Home Affairs, Australian Government, 2026, accessed 28 August 2026.
[15] Australian Bureau of Statistics, *Business adoption of Artificial Intelligence accelerates in 2024–25* [media release], 2026, accessed 8 September 2026.
[16] ACSC, *Artificial intelligence for small business,* cyber.gov.au website, 2026, accessed 19 August 2026; ASIC, *ASIC warns scammers are using AI to spin vast webs of deception* [media release], ASIC, 17 August 2026, accessed 19 August 2026.

- the importance of human oversight to verify AI-generated information, and
- ways to identify and avoid AI-generated scams through fake websites, social media ads, phishing scams and cryptocurrency investment scams.

This guidance should be integrated with existing small business cyber security programs and delivered in plain English.

Raise awareness on the role of cyber insurance

Cyber insurance can form an important part of a small business's cyber strategy, particularly in the role it plays in responding to, and recovering from, a cyber incident. However, similar to the relatively low uptake of cyber security measures by many small businesses, cyber insurance is typically not well understood or is seen as a lower priority compared to other forms of insurance, such as public liability, professional indemnity or property insurance.

Improved small business awareness of the role of cyber insurance and an understanding of business-specific insurance needs is therefore critical. In this regard, there is an opportunity for the insurance sector to be more active in raising small business awareness and understanding of cyber insurance, and to adopt measures that ensure that products which provide appropriate insurance coverage are both accessible, affordable and provide meaningful protections which warrant the expenditure.

Digital platforms need to provide accessible internal dispute resolution processes

Small businesses rely heavily on digital platforms to trade, advertise and communicate with customers. However, a large and growing number of small businesses have reported having their account suspended, restricted or hacked. Small businesses have sought help from the ASBFEO and state Small Business Commissioners given the platforms' lack of internal dispute resolution (IDR) processes to resolve loss of access to their accounts.

Currently, digital platform disputes comprise the largest source of small business complaints to the ASBFEO. Loss of access to accounts following cyber security issues accounts for a smaller number of complaints than the increasing number of account deactivations where the digital platforms have chosen to deactivate small business accounts for allegedly transgressing community standards. Digital platforms need to urgently implement accessible, transparent and effective IDR processes.

An IDR process should include minimum service standards, including dedicated support channels for small businesses affected by cyber attacks, timely investigation of account compromises, human review of cases, and clear escalation pathways to promptly rectify issues. Ensuring that digital platforms create effective IDR processes could enhance protections for small businesses, helping to reduce financial harm and business disruption, and improve recovery outcomes after cyber attacks.

Establish an external dispute resolution process for digital platforms through an independent external ombuds scheme

Where a digital platform complaint or dispute cannot be resolved through an IDR process there needs to be an accessible external dispute resolution (EDR) process. We note that the Australian Competition and Consumer Commission's (ACCC) Digital Platform Services Inquiry found that consumers and small businesses need an independent EDR body for digital platform services, such as an independent external ombuds scheme.[17] The ASBFEO supports this finding.

[17] ACCC, *Digital Platform Services inquiry final report – March 2025*, ACCC, Australian Government, 2025, accessed 28 August 2026.

Improving the cyber maturity of small business requires a holistic approach involving both government and the private sector. It needs to involve a range of complementary and coordinated strategies, including raising awareness on the importance of cybersecurity, increasing understanding of how to respond to cyber attacks, and educating small businesses about emerging risks associated with the use of AI.

If you require any further information, please do not hesitate to contact the Policy and Advocacy team via email at advocacy@asbfeo.gov.au.

Yours sincerely

Lynda McAlary-Smith

Australian Small Business and Family Enterprise Ombudsman

Attachment A

Case Study example: Invoice redirection scam

A regional small business owner was subject to an invoice redirection scam. They received what appeared to be a legitimate invoice relating to an existing Australian Taxation Office (ATO) payment arrangement. The correspondence appeared to have come from the business owner's accountant and included payment instructions consistent with an anticipated payment plan.

Trusting the information provided, the business owner paid approximately $34,000 to the bank details in the correspondence.

It was later discovered that the invoice was fraudulent. The banking details contained in the payment instructions had been altered, resulting in the funds being transferred to a scammer rather than the ATO. The scam was particularly convincing because the business owner was expecting correspondence regarding the payment plan. The fraudulent email closely resembled genuine communication from the accountant and appeared to exploit knowledge of an ongoing financial arrangement between the parties. It was presumed that the small business' system was compromised with the scammer monitoring their email traffic to identify an opportunity to impersonate their accountant.

A review of the accountant's email systems by their IT provider reportedly found no evidence of compromise or unauthorised access.

The accountant noted that the business owner had previously reported instances where customer payments had gone missing, raising concerns that the business owner's systems or email account may have been compromised over a longer period.

Further examination of the suspected scam email identified several warning signs, including:
- the use of a fraudulent email address impersonating the accountant.
- incorrect business identification details contained within the attached document.
- unusual document formatting and timestamps.
- banking details that did not match legitimate ATO payment instructions.

The matter was referred to relevant authorities, and the business owner was encouraged to undertake a comprehensive review of their cyber security arrangements.