

Cyber security for small to medium sized businesses and organisations

**Submission to the House Select
Committee**

August 2026





Contents

Contents.....	2
Introduction.....	3
Who is auDA?	3
auDA's role	3
Scope of this submission.....	3
About Digital Lives of Australians 2026	4
Digital Lives findings.....	4
Key small business findings	4
Business size shapes perceptions of cyber risk	4
Perceived powerlessness is linked to weaker protections	5
Additional support is required to help trusted guidance reach small businesses	5
Recommendations and conclusion	6
Conclusion.....	7



Introduction

Who is auDA?

.au Domain Administration Ltd (“auDA”) is the administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD includes the following namespaces: .au, com.au, net.au, org.au, asn.au, id.au, vic.au, nsw.au, qld.au, sa.au, tas.au, wa.au, nt.au, act.au, edu.au, gov.au.

auDA’s role

As a critical part of the digital economy, auDA’s role is to ensure the .au ccTLD remains stable, reliable and secure. Additionally, auDA performs the following functions:

- Administers a licensing regime for .au domain names based in multi-stakeholder processes, including managing enquiries and maintaining an appropriate compliance and dispute resolution processes associated with the licensing rules
- Licenses the .au registry operator and accredits and licenses registrars
- Advocates for, and actively participates in, multi-stakeholder internet governance processes both domestically and internationally.

Scope of this submission

auDA welcomes the *Inquiry into cyber security for small to medium sized businesses and organisations* being conducted by the Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations. This submission focuses on **the cyber maturity of small to medium sized businesses and organisations; the adequacy, appropriateness and accessibility of government guidance; and the importance of employee training** (terms of reference 1, 2 and 5).

Our submission primarily shares key findings on small business cyber maturity from auDA’s [Digital Lives of Australians 2026](#) research report. The Digital Lives research was not designed to evaluate specific cyber security standards, procurement markets or supply-chain participation. auDA therefore does not make detailed recommendations on those matters. The submission instead draws out the research findings most directly relevant to small business perceptions, preparedness and capability.



About Digital Lives of Australians 2026

Digital Lives of Australians is auDA's annual study of Australians' online experiences. The 2026 research included an online survey of 2,080 consumers and 408 small business owners or managers; eight online focus groups with 55 participants, including four small business groups; and ten in-depth interviews, including five small business owners. Survey samples were weighted to reflect the relevant Australian population profiles. The research was undertaken for auDA by SEC Newgate Research.

The full report can be found at <https://www.auda.org.au/DL>

Digital Lives findings

Small business size is fuelling a false sense of security for some businesses and a sense of helplessness for others.

Key small business findings

38%	believe their business would not be a target for cyber criminals because it is too small
47%	believe that if larger, well-resourced companies cannot protect themselves, they cannot protect their small business
92%	hold some form of personal or sensitive data relating to staff, customers, suppliers or the business
26%	are very confident they can keep business data secure online

Business size shapes perceptions of cyber risk

auDA's [Digital Lives of Australians 2026 research](#) finds that 38 per cent of small businesses believe their business would not be targeted by cyber criminals because it is too small. At the same time, 47 per cent believe that if larger, well-resourced companies cannot protect themselves from cyber attacks, they have little chance of protecting their own business.



Qualitative participants were often unaware that attacks against small businesses can be automated and conducted at scale, scanning the internet for vulnerabilities rather than selecting targets by business size.

This does not mean small businesses are indifferent. More than half of small businesses are quite or very concerned about online security and 86 per cent believe cyber criminals are becoming more sophisticated. However, there is a gap between concern and action, which is shaped by limited confidence, time and cost.

Concern does not always translate into action

The report also finds that cyber maturity is uneven among Australian small businesses.

- Ninety-two per cent hold personal or sensitive data, but only 26 per cent are very confident they can keep business data secure online
- Fifty-four per cent maintain up-to-date antivirus software and 50 per cent use multifactor authentication where available
- Only 18 per cent reported providing staff training, 15 per cent had an incident response plan, 14 per cent had a documented cyber security policy and 13 per cent employed someone with responsibility for cyber security.

Among businesses that were interested in staff training but did not provide it, 51 per cent cited cost and 39 per cent cited the time required to organise it.

Perceived powerlessness is linked to weaker protections

Among small businesses that believe they are too small to be targeted, 52 per cent feel powerless to stop cyber attacks. The 'too small' view increases risk by encouraging complacency. For example, small businesses that believe they are too small to attract the attention of cyber criminals are far less likely to use multifactor authentication where it is available (38 per cent compared with 57 per cent of businesses that do not hold this view).

The report identified that 13 per cent of small businesses reported having experienced a cyber attack and 12 per cent reported data being compromised in a breach.

Additional support is required to help trusted guidance reach small businesses

Only 26 per cent of small businesses are very confident finding reputable information on how to be secure online, and only 26 per cent are very confident they know where to report a data security breach. Just 36 per cent say they would go to a government website such as cyber.gov.au for online security information, despite small businesses emphasising the value of low-cost or free, trusted guidance.



Seventy-six per cent of small businesses regard cyber security skills as important to their business, but only 24 per cent report high capability. The report's broader digital-skills findings identify workplace training, online courses or webinars, and online videos or self-guided tutorials as accessible formats for building capability.

Recommendations and conclusion

1. Challenge the 'too small to be a target' myth

Government communications should directly explain that many cyber attacks are automated and exploit vulnerabilities rather than select businesses by size. Communications should present a short set of baseline protections as a normal part of operating a business online, and frame action around resilience, continuity and customer trust rather than fault or fear.

2. Build understanding that simple practices can significantly reduce cyber risk

Government should continue investing in clear, free and practical resources, while improving their reach and usability. Existing resources such as [cyber.gov.au](https://www.cyber.gov.au) and [auDA's Five Ps of website security](#) – passphrases, patching, processes, providers and people – provide useful starting points. Resources should use plain language, a clear order of priority, small business scenarios and short online formats, and be promoted through trusted business and digital networks.

3. Normalise incident planning, reporting and recovery

Small businesses should be supported to prepare a simple incident plan before something goes wrong. A practical 'before, during and after' guide should identify who to contact, where to report an incident, how to protect and restore important data, and how to maintain essential operations. Reporting pathways should be consistent, prominent and easy to follow under pressure.

4. Support practical digital skills and training

Government should support low-cost, practical training suited to the way small businesses operate, including short workplace sessions, online courses and webinars, and self-guided videos and tutorials. Training should build a small set of repeatable habits: using strong passphrases and multifactor authentication, keeping software up to date, checking suspicious emails and payment requests, limiting access to sensitive data, backing up securely, and knowing what to do and where to report an incident.



Conclusion

Australia's small businesses are innovative and resilient, but they should not be expected to become cyber security experts. The Digital Lives findings point to a role for practical support in narrowing the gap between concern and action. By challenging the 'too small to target' misconception, reducing the friction involved in taking basic steps and making incident response pathways clear, the inquiry can help small businesses protect what they have built and participate in the digital economy with confidence.

auDA would welcome the opportunity to discuss these findings and provide further information. Please contact Michael Lewis at michael.lewis@auda.org.au.

.au Domain Administration Ltd
www.auda.org.au

PO Box 18315
Melbourne VIC 3001
general@auda.org.au

August 2026

