CyberWardens.

Small Business Cyber Security **Pulse Check** **Report**

2026 Cyber Wardens Research

COSBOA COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

cyberwardens.com.au

Executive Summary

For Australia's small businesses, the spectre of cyber crime is no longer a distant concern, it's a daily reality.

In fact, small businesses cite cyber crime as one of the top threats to their survival, in equal third place with staff costs such as superannuation.

AI is increasingly supercharging scams, and most small businesses (79%) fear they couldn't financially recover from an attack.

But new Cyber Wardens research has found a disconnect between concern and action across Australia's 2.6 million small businesses. The adoption of multi-factor authentication remains low in critical areas such as email and bank accounts.

Only 3 in 10 owners ensure new employees receive cyber security training, while everyday risky habits continue to leave businesses open to online break-ins. But the positive news is that a culture of cyber safety has increasingly been embedded into the DNA of small businesses over the past three years.

This report reveals small business owners and employees are becoming more confident in managing digital risks, introducing stronger passwords, actioning software updates faster and understanding that cyber security is a whole-of-team responsibility.

The 2026 Small Business Cyber Security Pulse Check Report summarises the findings of the final year of a multi-year Cyber Wardens research project to measure and map small business cyber security behaviours and attitudes. More than 1570 small business owners and employees participated in the research.

The report found:

- **4 in 5 (84%)** small businesses have experienced an incident, up 3% since 2023
- **Cyber security remains a top three threat,** with 79% of small businesses expressing concern about a cyber attack (down 3% from the previous year)
- **Nearly 7 in 10 (67%)** employees are using a personal device at work
- **Less than half of respondents (46%)** are confident their business is protected from emerging threats, such as AI-driven attacks and ransomware.

Behaviour change takes time, and the findings underscore the importance of continuing to build a cyber-safe culture among small businesses.

The report contains 20 key findings and emerging threats under five themes:

1. **Unprepared for the growing threat of AI**
2. **Risky behaviours needing attention**
3. **The cyber threat landscape for small businesses**
4. **Cyber wins: areas of biggest improvement**
5. **Awareness varies between industries**

About Cyber Wardens

COSBOA's Cyber Wardens program, backed by the Australian Government and an industry alliance led by Telstra, CommBank and the Australian Cyber Security Centre, is supporting thousands of small business owners and employees to protect themselves from cyber threats with simple and free online education, resources and workshops.

The program is expanding its reach every week through key government and industry partnerships, webinars and events as it becomes a trusted national initiative.

Training has been completed across industries as diverse as retail, healthcare, construction and tourism.

Matthew Addison
Chair, COSBOA

About the research

This Pulse Check Report reflects findings from a national survey of 1,576 participants: 529 small business owners, and 1,047 employees.

The 2025 results (Year 3) have been compared with the 2023 benchmark study and 2024 survey to identify changes in cyber security culture and behaviours.

The 2023 Cyber Wardens Research *"Building a culture of cyber safety in Australian small businesses"* established benchmarks for identifying cyber security practices, and barriers facing small businesses in cyber protection.

A consistent framework and weighting were used across all three surveys to improve the reliability of year-to-year comparisons.

The participating small business owners and employees in 2025 represent a broad range of ages, business types, industries and roles across metropolitan, regional and rural locations.

The sample included men, women and non-binary people aged 18+ with varying levels of cyber security awareness and experience.

Unprepared for the **growing threat of AI**

1. AI-driven threats become harder to spot	**8 in 10 small businesses (81%)** believe cyber criminals are becoming more sophisticated due to AI advancements. From word-perfect phishing emails to convincing deepfake calls and fake chatbots, employers and employees are being targeted by increasingly realistic methods.
2. Small businesses fail to use AI tools safely	**1 in 3 (32%) are sharing sensitive business and customer information** with AI tools, such as ChatGPT. A further 40% are using AI-generated content without checking its accuracy.
3. Absence of AI policies leave small businesses exposed	**Less than 1 in 5 (18%) have set up guardrails for using AI safely** (such as governance and policy frameworks) to ensure advanced technologies help instead of harm their business.
4. More support needed to ward off AI threats	**Less than half (46%) feel confident their business is protected from emerging threats, such as AI-driven attacks and ransomware.** 7 in 10 owners/employees (74%) think rapidly advancing technology, including AI, poses a risk to their small business in the next five years.

Risky behaviours needing attention

1. **Gaps in use of multi-factor authentication (MFA)**

While more small businesses are implementing MFA, less than 6 in 10 (57%) use it to protect their financial services accounts. Even fewer (56%) use it for accounts storing bank and credit card details, and other important business information. About 1 in 2 (49%) have enacted MFA for their business emails.

2. **Personal device use on the rise at work**

Nearly 7 in 10 (67%) employees are allowed to use their personal devices for work – a rise of 1% from last year. This increases risk as data sits on devices that the business cannot fully secure. More than 3 in 10 are also downloading personal software onto a work phone or computer without approval – a practice called 'Shadow IT'.

3. **Cyber security absent from onboarding**

Only 3 in 10 (32%) owners include cyber security awareness training in staff induction procedures. But this is a simple approach that could help save businesses from a potentially devastating attack.

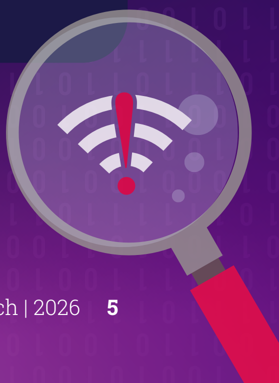
After all, human error is the most common cause of a security breach.

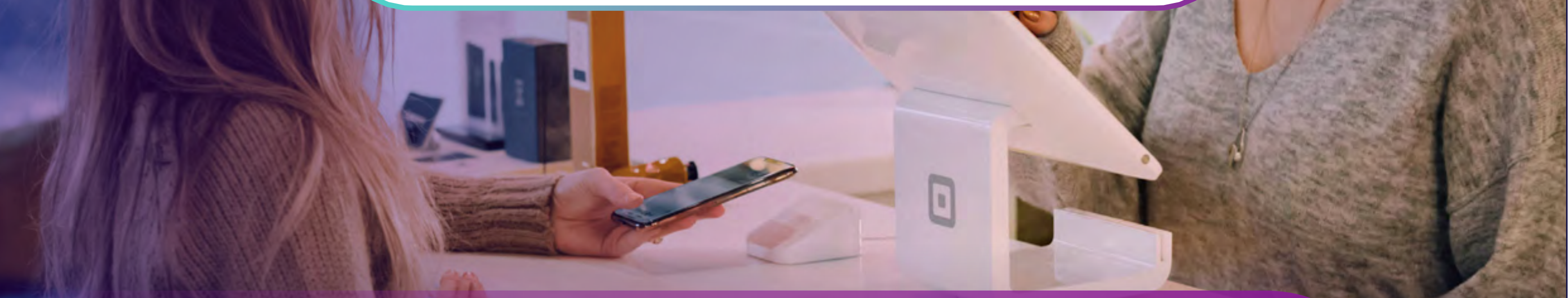
4. **Hitting snooze on software updates**

1 in 2 respondents (53%) hit 'snooze' on their software updates in 2025, instead of actioning them immediately. This makes systems much easier to attack, but fortunately, the risky habit is declining (down from 64% last year).

5. **Cyber incident response planning remains low**

Just 25% of businesses report having a cyber incident response plan in place, down from 26% in 2024.





The cyber threat landscape for small businesses

1. Cyber crime a top three threat

Cyber threats are considered the third biggest risk to small businesses in the next five years, on equal footing with staffing costs.

It is considered a higher threat than workforce shortages, rapid technological advances such as automation, and extreme weather events.

2. Growing culture of cyber security

Levels of concern about the risk of a cyber security threat have decreased in the past year from 82% in 2024 to **79% in 2025 (-3%).**

This indicates that businesses are becoming more confident in managing digital risks.

3. Financial ruin is a rising concern

Confidence in their financial capacity to recover has been dented, with 79% saying it would be hard to bounce back, compared to 72% in 2024.

The average cost of a cyber incident for small businesses rose 14% to $56,600 in 2024-25, according to the Australian Signals Directorate.

The hospitality industry flagged the highest level of financial fragility, with nearly a third believing they didn't have the resources to recover at all.

4. Cyber incidents are common

8 in 10 have experienced an incident in the past year, with scam communications, such as a suspicious SMS, email or phone call, the most common (75%), as well as invoice scams (21%) and data leaks (19%).

Cyber wins: areas of biggest improvement

Good progress in passwords, passphrases and old software

The use of unique passwords or passphrases has more than doubled in three years, from 30% in Year 1 to 67% in Year 3.

Password manager use also grew by 12% over the three years, to a high of 46% in 2025.

More businesses are regularly deleting and uninstalling old software in the two years this was measured (from 40% in 2024, to 44% in 2025).

MFA use for emails is rising

Nearly half (49%) use MFA for their company emails, up 3% from 2023.

Cyber security becomes a topic of conversation

Cyber security is being discussed more in the workplace, with 3 in 5 (60%) talking about the topic at least once every few months in Year 3, up 4% since Year 1.

The number of businesses that have never talked about cyber security has nearly halved in the same period.

Strong interest in free, expert training

Awareness is growing among small businesses of the free Cyber Wardens program, with 44% interested in signing up. Interest is strongest among start-ups, people aged 18–34, and those with a tech background.

Awareness varies between industries

Hospitality businesses slow to embrace cyber safety

Hospitality is the most at-risk sector, with bosses and staff the least likely to adopt cyber-safe practices.

Only about 1 in 2 (47%) providers in the hospitality, food services and accommodation sector use unique passwords or passphrases.

4 in 10 businesses have cloud-based back-up systems, and just 1 in 3 protect their business emails with multi-factor authentication (MFA) .

The findings are particularly concerning as hospitality is one of the top users of digital and platform-based payment options, which face higher technical risks such as account takeovers.

Professional services are Australia's small business cyber heroes

Small businesses in the professional, scientific and technical services industry are leading the way with the strongest cyber habits.

The sector reported the highest level of concern, with 59% either very or somewhat concerned about cyber threats, reflecting their heavier reliance on digital systems and sensitive client data.

About 8 in 10 (76%) use unique passwords or passphrases, and 72% have implemented MFA for important business information and banking and credit card details. Nearly a quarter (22%) have already introduced AI governance and policy frameworks.

Healthcare businesses need to strengthen defences and planning

The healthcare industry is a top target for cyber criminals. But the sector is trailing behind most other industries in foundational cyber security measures such as password managers and secure cloud-based backups.

Small businesses in healthcare and social assistance also lag behind professional services and retail in developing cyber response plans, while only 15% have set up formal guidelines for AI use.

Cyber awareness varies sharply by industry — from high risk to best practice.

Opportunities to boost **knowledge and preparedness**

Overall, small businesses are becoming more cyber savvy. But despite the fast-evolving world of online crime, most small businesses remain reactive in their responses.

The report has highlighted three top areas of focus for the future.

AI and emerging threats

- Expanding guidance, support and resources as AI becomes increasingly embedded in everyday business practices. Businesses will face more challenges in the years to come, underscoring the need for ongoing vigilance and education.

Preventative measures

- Promoting the importance of taking proactive steps to boost a culture of cyber safety, including AI policies, regular health checks and integrating training into staff onboarding. SMEs need support to establish incident response plans, with the findings indicating these are not seen as a priority.

Vulnerable industries

- Targeted outreach and support to hospitality and related businesses, as well as healthcare, including raising awareness of the specific threats they face and tailoring training through webinars.

Methodology

The research was undertaken by 89 Degrees East and conducted between Thursday 2nd October and Tuesday 21st October 2025 among 1,576 Australian small business owners and employees.

The sample included the views from 529 Australian CEO's, Founders and SME Owners and 1,047 employees of small business organisations. The results have been compared to the study undertaken in 2023 and 2024 to identify changes in cyber security culture and behaviours.

ADDITIONAL NOTES

The business and employee surveys were administered online with participants sourced from a commercial opt-in research panel (Pureprofile). The sample was recruited with quota management in place to reflect the population for gender, age and location. Weighting was applied to Year 1 (2023), Year 2 (2024) and Year 3 (2025) data to reflect the market structure of SME Australian businesses measured by employment size (www.asbfeo.gov.au) for comparability and consistency.

Research sample

Email research@89degreeseast.com for further information on the sample and detailed findings.

Business Types

- **1,576** SME business
  - **260** Sole traders
  - **363** Micro businesses
  - **953** Small businesses

Role

- **529** Owners
- **1,047** Employees

Gender

- **53%** Female
- **46%** Male
- **1%** Non-binary

Geography

- **71%** Metro
- **29%** Regional

NSW **29%** • VIC **27%** • QLD **19%** • SA **9%** • WA **9%** • Other **7%**

Age

18-24 years	5%
25-34 years	16%
35-44 years	21%
45-54 years	22%
55-64 years	20%
65+ years	17%

Small business cyber security made simple with Cyber Wardens

Keeping your business safe online is a team effort. Get started today, and equip your team with the knowledge and tools they need to keep your business safe online.

There are many ways for you and your team to complete the Cyber Wardens training. Choose from our growing course catalogue:

Cyber Wardens **Foundations** 10 mins

Learn to spot cyber security red flags and essential strategies to protect your business.

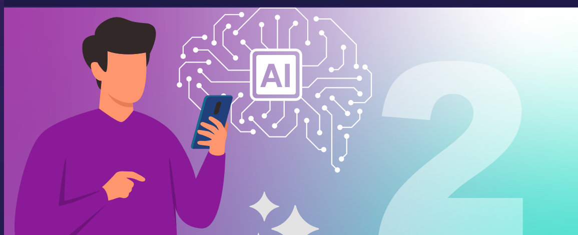
Suitable for: Busy business owners and employees

Cyber Wardens **Level One** 45 mins

Master four essential cyber security practices to protect your small business from common threats.

Suitable for: Small businesses seeking improved cyber resilience

Cyber Wardens **Level Two** Safe AI for Small Business 30 mins



Simple and effective ways to keep small businesses safe from complex AI scams.

Suitable for: Small businesses seeking a deeper understanding of AI's cyber security threats

Cyber Wardens **Level Three** Cyber Fit for the Supply Chain 30 mins

Strengthen your business's cyber security and meet the expectations of clients, partners and suppliers in your supply chain.

Suitable for: Small businesses seeking to understand their critical role in the supply chain

Cyber Wardens **Champions** 45 mins

Help others stay cyber aware, build safer habits, and protect their business.

Suitable for: Individuals seeking to help others become more cyber aware

All our courses are available as online courses or on-demand webinars.

CyberWardens.

Protect your small business from cyber crime

Make sure your entire team has the knowledge and tools they need to keep your business safe online.

Register today cyberwardens.com.au

Proudly supported by

Australian Government

COSBOA