

Small Business Cyber Security Pulse Check Report

2025 Cyber Wardens Research

Executive Summary

Over the past 12-18 months, the rise in cyber threats—such as scam calls, texts, and emails—has put cyber security at the forefront of Australians' minds.

We are now hearing about the importance of cyber-safe habits from various sources, including banks, insurers, governments, and through media coverage of cyber attacks. These efforts have highlighted the profound impact of such threats and the importance of securing business and personal data.

COSBOA's Cyber Wardens program, backed by the Australian Government and an industry alliance, is also actively reaching out to and supporting thousands of small business owners and employees to help protect themselves from cyber threats with simple and free online education, resources and workshops.

The Cyber Wardens program is built on extensive research with Australian small businesses. This 2025 *Small Business Cyber Security Pulse Check Report* summarises the findings of the second year of a multi-year research project to measure and map small business cyber security behaviours and attitudes.

Small business attitudes, concerns, awareness and behaviours relating to cyber security have seen a positive shift in the past 12 months. Our research shows that fewer small businesses would be categorised in the least aware and active segment of cyber security maturity, down 12% since last year. These segments help us tailor our support and track progress (full segment breakdown on page 7).

This is encouraging, yet Australian small businesses continue to be prime targets and face challenges from emerging technologies.

- **4 in 5 (82%)** small businesses have been exposed to or experienced a cyber incident, up 3% from the previous year.
- **Only 2 in 5 (41%)** feel confident their business is protected from emerging threats, such as AI-driven attacks and ransomware.

This research summary report highlights 12 key findings across three themes:

Growing exposure and concern about cyber threats

1. There has been an increase in cyber attacks on small businesses.
2. Higher reporting of personal exposure to cyber incidents.
3. Small businesses are more concerned about cyber attacks.
4. Cyber security is seen as a growing threat and ranked third highest among all threats.

Risks and opportunities from AI and operating online

5. Small businesses need support to keep pace with AI.
6. Develop tailored resources for small businesses operating 100% online.
7. Support small businesses in managing online payments securely and safely.

Encouraging cyber safety improvements

8. Fantastic progress in the use of strong passwords and passphrases.
9. Fewer small businesses are unconcerned, unaware and unprepared.
10. Increased perception of the difference individuals can make.
11. Encouraging cultural shifts within the small business community.
12. More confidence in how to prepare.

Cyber attacks on small businesses can cause devastating financial loss and personal distress for owners, employees and customers.

It is encouraging to see from these research findings that cyber security awareness and cyber-safe habits are steadily improving.

This demonstrates that Cyber Wardens and other initiatives are making a difference, but we know cyber attacks will become more sophisticated.

We urge all Australian small businesses and suppliers to prioritise cyber security and take advantage of the free courses, resources and support [Cyber Wardens](#) offers.



Luke Achterstraat

COSBOA Chief Executive Officer

About this research

The 2025 Pulse Check Report reflects findings from a national survey of 1,559 Australian small business owners (n=536) and employees (n=1023).

89 Degrees East conducted this research at the end of October 2024.

The 2024 results (Year 2) have been compared and contrasted with the survey results from the benchmark study in 2023 (Year 1).

To accurately track, compare and contrast year-on-year shifts in attitudes and behaviours across representative samples, a weighting framework (reflective of the market structure of Australian small businesses in terms of the number of employees) was applied to the Year 2 sample and to the Year 1 data retroactively.

This weighted data is reflected in this report.



Key findings and emerging trends

Growing exposure and concern about cyber threats

1.

There has been an increase in cyber attacks on small businesses

4 in 5 (82%) small businesses have been exposed to or experienced a cyber incident, up 3% from Year 1. The greatest increase is in the number of owners/employees who have received a suspicious SMS, email or phone call (76% in Year 2, +5%). Data leaked due to an attack on another organisation is up 3%, and password or accounts hacked is up 3%.

2.

Increased personal exposure to cyber incidents puts businesses at risk

Compared to Year 1, small business owners and employees were more likely to have had their personal data leaked due to an attack on another organisation (76%, +11%), their personal passwords or accounts hacked (69%, +13%) and/or been exposed to an online marketplace scam when using their personal account (59%, +11%).

The rise in personal attacks is concerning as many employees use their personal devices for work and use the same passwords at home and work.

3.

Small businesses are more concerned about cyber attacks

4 in 5 small business owners/employees (82%) are concerned about a cyber attack, scam or hack impacting their work or business. This is up +5% from Year 1 (77%).

4.

Cyber security is seen as a growing threat and ranked third highest among all threats

More than 1 in 2 small business owners/employees (54%) see cyber security threats as a medium or high risk to their business in the next five years, up 5% from Year 1 (49%).

Cyber security threats were seen as the third highest 'threat' behind economic instability (67%) and cost of staff (56%), with energy prices less of a concern in fourth (52%). In Year 1, it was also ranked third, behind energy prices and cost of staff.

Risks and opportunities from AI and operating online

5. Small businesses need support to keep pace with AI

Only 2 in 5 (41%) 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. 8 in 10 (78%) believe cyber criminals are becoming more sophisticated due to advancements in AI (therefore increasing cyber security risk).

6. Develop tailored resources to protect small businesses operating 100% online

1 in 5 small businesses (21%) are not communicating with their customers or clients in person at all.

Conducting business purely online presents a unique set of cyber security challenges which small businesses need support to navigate.

7. Increased perception of the difference individuals can make

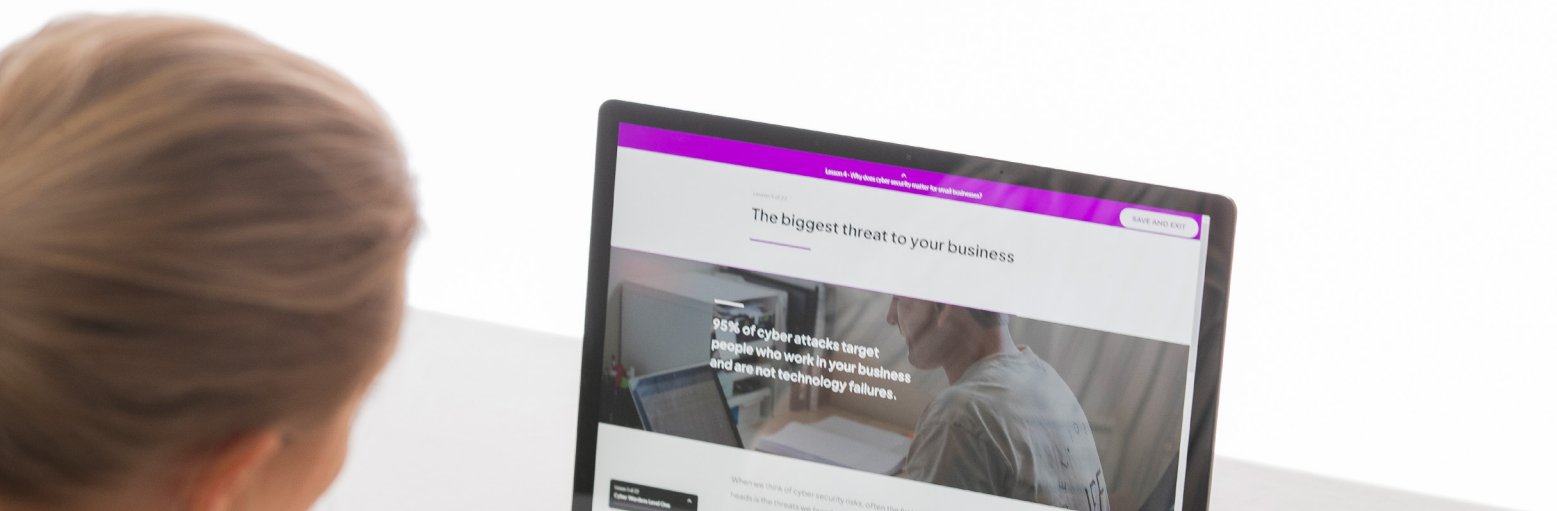
4 in 5 small businesses (83%) process client/customer payments using online banking or EFTPOS (60%) and third-party apps such as Google Pay, Apple Pay and PayPal (23%), exposing them to various risks in processing online payments.



Key findings and emerging trends

Encouraging cyber safety improvements

- | | | |
|-----|--|---|
| 8. | Fantastic progress in the use of strong passwords and passphrases | The number of small businesses using unique passwords and strong passphrases has more than doubled, from just 30% in Year 1 to 64% in Year 2 (+34%). The growing volume of messaging and discussion around this important habit is likely influencing this encouraging behaviour shift. |
| 9. | Fewer small businesses are less aware and less prepared | In Year 1, 45% of small businesses surveyed were considered 'Unaware and Inactive' regarding cyber maturity. This decreased to 33% in Year 2 (-12%), demonstrating increased cyber awareness and a more intentional cyber-safe mindset. |
| 10. | Increased perception of the difference individuals can make | There has been a growth in the proportion of people working in small businesses who report that <i>it makes a difference in my small business if I practice cyber-safe habits</i> (71% agree/strongly agree, +5%). |
| 11. | Encouraging cultural shifts | Small business owners and employees are more likely to <i>recognise team members who demonstrate cyber-safe habits and can spot and prevent common cyber threats</i> (52%, +6%) and that <i>team members are more motivated to act in a cyber-safe manner</i> (53%, +5%). |
| 12. | More confidence in how to prepare | Small business owners/employees are slightly more likely to have medium or high confidence in how to prepare for a cyber incident (60%, +5%). |



Tracking cultural shifts through cyber maturity segments

The Year 1 Cyber Wardens Research *Building a culture of cyber safety in Australian small businesses* established benchmarks for understanding cyber maturity segments. Cyber security behaviours/practices and beliefs/levels of concern were identified.

Small business attitudes, concerns, awareness and behaviours relating to cyber security have seen a positive shift in the past 12 months.

Fewer small businesses (-12% in Year 2) are categorised as Unaware and Inactive.

This segment is the least concerned about their cyber security and least likely to practice cyber-safe behaviours. This result reflects a heightened cyber awareness and a more intentional cyber-safe mindset, which the Cyber Wardens program is designed to encourage.

	Unaware and Inactive	Passive and Foundational	Aware and Emergent	Attentive and Maturing	Ready and Resilient
YEAR 1 2023	45%	17%	13%	12%	14%
YEAR 2 2024	33%	19%	16%	15%	17%
% DIFFERENCE	-12%	+2%	+3%	+3%	+3%

Year 1 and Year 2 figures reflect weighted samples

Research sample



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

Business Types



1,559
Small business



264
Sole traders



340
Micro businesses
1-4 employees



955
Small businesses
5-19 employees

Role



536
Owners



1,023
Employees

Gender



58%
Female



41%
Male



1%
Non-binary

Geography



71%
Metro



29%
Regional

NSW 30% • VIC 28% • QLD 19% • SA 9% • WA 9% • Other 4%

Age

18-24 years 4%
25-34 years 23%
35-44 years 23%

45-54 years 20%
55-64 years 18%
65+ years 12%

Prioritise small business cyber security with Cyber Wardens

Cyber security doesn't stop with just one person—it's a team effort!

Make sure your entire team has 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 expanding course offering:

1.

CYBER WARDENS FOUNDATIONS

A 10-minute module helping you identify the cyber security red flags that pose a threat to your business.

3.

CYBER WARDENS LEVEL ONE

A short course introducing you to basic cyber security measures and actions to improve your cyber awareness.

2.

CYBER WARDENS FOUNDATIONS WEBINAR

An interactive session delivered live or on demand where participants can learn through live engagement with a Cyber Wardens educator.

4.

CYBER WARDENS REFRESH

A module where Level One graduates can refresh their skills and knowledge while being introduced to new and emerging threats.

Visit cyberwardens.com.au to enrol in **FREE** training and access resources to share with your team.

