PUBLIC-FACING EDITORIAL DEMONSTRATION

Cyber risk for Australian small business

A concise 2024-25 briefing built from the Australian Signals Directorate's Annual Cyber Threat Report.

Why this matters
Cybercrime can interrupt operations, expose customer information and create significant financial loss. This briefing pulls the most useful small-business messages from a much larger national threat report and restructures them into a quick public-facing publication.

At a glance

- 84,700+ cybercrime reports were received in FY2024-25, around one every 6 minutes.
- The average self-reported cost per cybercrime report for small businesses was $56,600.
- ASD recommends strong MFA, strong and unique passwords or passphrases, software updates, phishing awareness and regular backups as basic cyber protections.

Independent demonstration prepared by Plainward from publicly available Australian Government material. Not commissioned, approved or endorsed by ASD or the Australian Cyber Security Centre.

THE 2024-25 PICTURE

Cyber threats are frequent and costly

The national data shows a high volume of reported cybercrime alongside substantial financial losses for businesses. The figures below are based on reports to ASD's ACSC and should be read as indicators of the threat environment, not a complete count of all incidents.

84,700+ **cybercrime reports**
Around one report every 6 minutes.

$56,600 **average self-reported cost**
Per cybercrime report for small businesses, up 14%.

42,500+ **hotline calls**
Up 16% from the previous year.

1,200+ **cyber security incidents**
Incidents ASD's ACSC responded to, up 11%.

What small businesses should take from this

Identity and account security matter. Cybercriminals continue to seek usernames, passwords and personal information. MFA can make a stolen password alone insufficient to access an account.

Old or unpatched technology creates openings. Keeping devices and software supported and updated reduces exposure to known vulnerabilities.

Preparation improves response. A tested incident response plan helps a business prioritise actions and get appropriate assistance when something goes wrong.

> **Data note**
> ASD's ACSC states that the vast majority of cybercrime continues to go unreported. Its ReportCyber statistics are point-in-time, self-reported data and do not reflect every cyber threat or incident in Australia.

ACTION GUIDE

Five actions to take now

These measures are drawn directly from ASD's ACSC resilience guidance in the 2024-25 report and are written here as practical actions for a small-business audience.

1. Turn on strong multi-factor authentication
Use strong MFA wherever it is available, especially on important business accounts. ASD now prefers phishing-resistant MFA, such as passkeys, where supported.

2. Use strong, unique passwords or passphrases
Do not reuse credentials across business services. ASD recommends strong and unique passwords or passphrases and suggests considering a reputable password manager.

3. Keep software and devices updated
Install software and device updates promptly and replace technology that is no longer supported by the vendor.

4. Back up important information
Regularly back up important files and device configuration settings. Make sure your business knows how it would restore important data if systems became unavailable.

5. Treat unexpected messages with caution
Be alert for phishing messages and scams, especially unexpected requests to sign in, disclose sensitive information or transfer money.

Quick business check

- ☐ Check that MFA is enabled on business email and administrator accounts.
- ☐ Confirm devices and software are receiving current security updates.
- ☐ Confirm important business information is backed up and can be restored.
- ☐ Write down who staff should contact if they suspect a cyber incident.
- ☐ Remind staff to verify unusual payment or bank-detail changes using a known, verified contact method.

IF SOMETHING GOES WRONG

Respond quickly and use official support

If you suspect a cyber incident, follow your incident response arrangements, act to limit further harm and seek appropriate support. ASD's ACSC encourages organisations to report suspicious activity and incidents so it can provide advice and assistance.

1. Contain
Follow your incident response plan and trusted IT or cyber security advice to contain the incident. Preserve relevant information and logs where practical, and avoid actions that could make investigation harder.

2. Escalate
Contact your IT provider or cyber security support and notify the relevant people in your business. If bank or payment-account details may be at risk, contact the relevant financial institution promptly using its official contact details.

3. Report
Report cybercrime or cyber security incidents through ReportCyber. For cyber security assistance, call the 24/7 Australian Cyber Security Hotline on 1300 CYBER1 (1300 292 371).

Source and editorial treatment

Primary source: Australian Signals Directorate, Annual Cyber Threat Report 2024-25, first published 14 October 2025. The briefing selects small-business-relevant findings, retains important qualifiers, removes material outside the audience need and reorganises the information around practical decisions.

Primary report: Annual Cyber Threat Report 2024-25

Official reporting and support: ReportCyber

Supplementary official guidance: Preventing business email compromise, Report and recover from business email compromise and Cyber security incident response planning

Demonstration notice
This is an independently prepared Plainward portfolio demonstration. It is not an official ASD or ACSC publication and should not replace current advice from cyber.gov.au, professional cyber security advice or legal advice where required.