CyberStance Assessment Report

Take a stronger stance on cyber security.

Prepared for

Acme Services Incorporated

Manufacturing | 6–10 staff | Microsoft 365 + Xero + Slack

Report Date: 8 April 2026

Report ID: CS-2026-CD4B7B46

OVERALL RISK RATING

HIGH RISK

49% risk identified

This report is tailored for business owners who manage their own technology. It includes step-by-step guides you can follow yourself, and clearly marks any items that need professional help.

Contents

How to use this report: This report is designed for business owners who manage their own technology. For each finding, you'll see a step-by-step guide written in plain English — no jargon, no assumptions. Some items are things you can do yourself in a few minutes. Others are more technical and we'll tell you clearly when it's worth getting professional help. Start with the items marked as your top priorities — they'll make the biggest difference.

1. Executive Summary

Prepared for a 6–10-person Manufacturing business using Microsoft 365 + Xero + Slack.

There are significant gaps in your cyber security that need attention. We've prioritised the most urgent items so you can start making progress today. We recommend addressing the critical and high-priority items within 30 days.

24 confirmed security gaps were identified across **7** of 8 security categories. An additional **3** item(s) could not be confirmed and should be verified. Your overall risk score is **49%** (High Risk).

2. Overall Risk Rating

Identity & Access — 100% (Critical Risk)

Email Security — 70% (Critical Risk)

Data & Sharing — 100% (Critical Risk)

Device Security — 56% (High Risk)

Backup & Recovery — 72% (Critical Risk)

People & Awareness — 15% (Low Risk)

Financial Integrity — 38% (High Risk)

Incident Readiness — 78% (Critical Risk)

3. Top 5 Priority Actions

These are your highest-priority security improvements, ranked by severity, then by the time required to implement.

1 CRITICAL Verify all bank detail change requests before processing

Effort: Low – 1 hour to create process | **You can do this yourself**

Why this matters

Invoice fraud — where a scammer impersonates a supplier or employee and requests a bank detail change — is the most common way Australian businesses lose money to cyber crime. The ACCC reported over $91 million lost to payment redirection scams in 2023 alone.

What to do

This is about creating a simple process, not changing any settings:

STEP-BY-STEP GUIDE — Follow these steps yourself

Step 1. Write a one-line rule: 'We never change bank details without a phone call to confirm.'

Step 2. Tell everyone who processes invoices or payroll.

Step 3. When a request comes in to change bank details:

Step 4. Keep a log of verifications — even a simple spreadsheet: date, who requested, who verified, confirmed Y/N.

a. Don't click any links in the email. b. Look up the supplier's or employee's phone number from your own records (not from the email). c. Call them and ask: 'Did you send a request to change your bank details?' d. Only update your accounting software if they confirm. This takes 2 minutes per verification and can prevent losses of tens of thousands of dollars.

Essential Eight: User Application Hardening (Maturity Level 1) | ISM: ISM-0269 | Privacy Act: APP 11 – financial data protection

---

2 CRITICAL Enable automatic OS updates

Effort: Low – 1-2 hours | **You can do this yourself**

Why this matters

Unpatched systems are the second most common attack vector after phishing. Patches must be applied promptly.

What to do

On each company computer:

Windows: Go to Settings > Windows Update > tick 'Get the latest updates as soon as they're available' and turn on automatic updates.

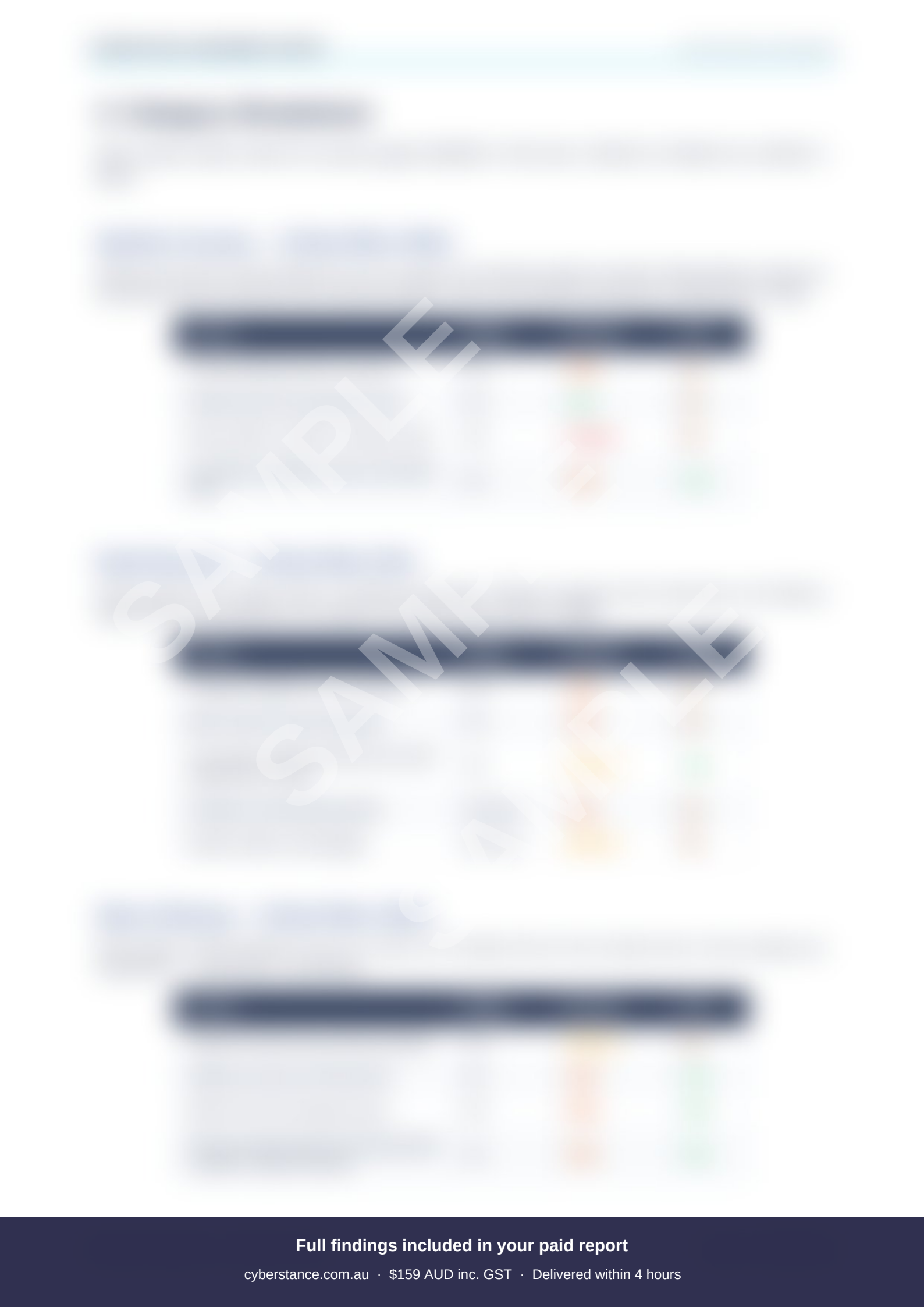
Mac: Go to System Settings > General > Software Update > turn on 'Automatic updates'.

Do this on every laptop and desktop in the business. It takes about 2 minutes per device.

TECHNICAL REFERENCE — Share this section with your IT provider

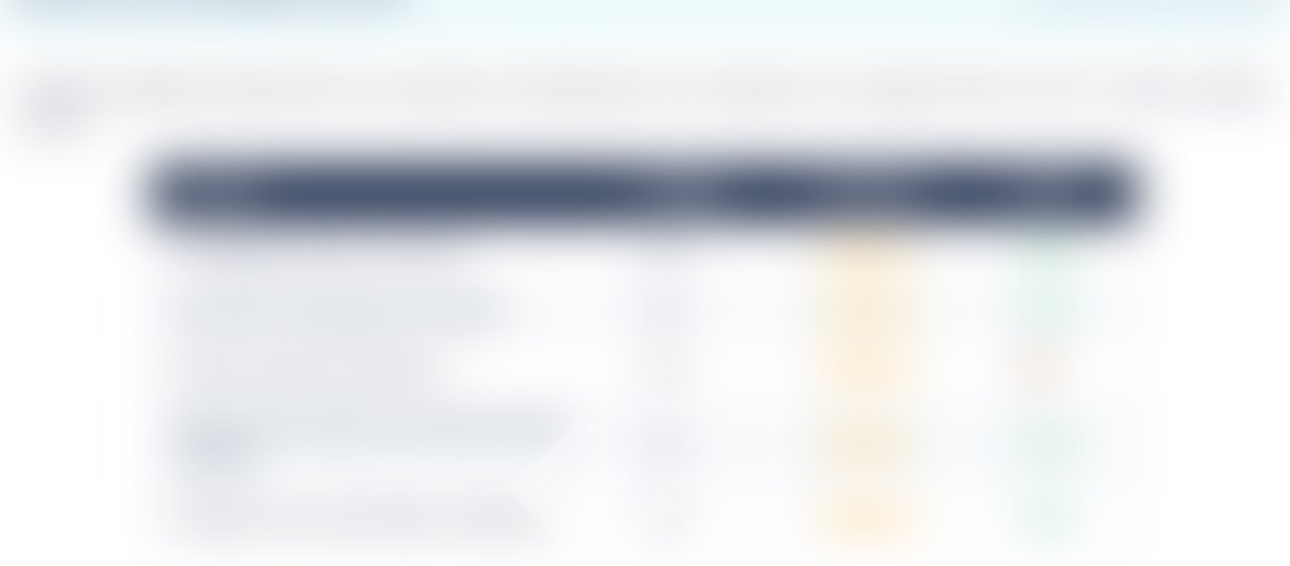
- `Windows: Settings > Update > Enable automatic updates.`
- `Mac: System Settings > Software Update > Automatic.`

Essential Eight: Patch Operating Systems (Maturity Level 1) | ISM: ISM-1407, ISM-1408 | Privacy Act: APP 11



Full findings included in your paid report

cyberstance.com.au · $159 AUD inc. GST · Delivered within 4 hours



Full findings included in your paid report

cyberstance.com.au · $159 AUD inc. GST · Delivered within 4 hours

Full findings included in your paid report

cyberstance.com.au · $159 AUD inc. GST · Delivered within 4 hours

Full findings included in your paid report

cyberstance.com.au · $159 AUD inc. GST · Delivered within 4 hours

Full findings included in your paid report

cyberstance.com.au · $159 AUD inc. GST · Delivered within 4 hours

7. Framework Alignment

Your findings have been mapped to the following Australian Government cyber security frameworks. This alignment helps demonstrate your security posture to insurers, partners, and regulators.

Essential Eight (ACSC)

The Essential Eight is the Australian Cyber Security Centre's prioritised list of mitigation strategies to protect against the most common cyber threats.

Essential Eight Strategy	Your Status	Key Gaps
Application Control	Not Met	Implement application control
Patch Applications	Not Assessed	Not included in this assessment scope
Patch Operating Systems	Not Met	Enable automatic OS updates
Restrict Administrative Privileges	Not Met	Create dedicated admin accounts; Implement mobile device management (+2 more)
Multi-factor Authentication	Not Met	Enforce MFA or SSO for all Slack users
Regular Backups	Not Met	Test backup restores quarterly; Create a basic business continuity plan (+4 more)
User Application Hardening	Not Met	Enable self-service password reset; Configure DMARC for your domain (+7 more)
MS Office Macro Settings	Gaps Found	Unverified: Configure anti-phishing policies

Privacy Act 1988 & Notifiable Data Breaches

Under the Notifiable Data Breaches (NDB) scheme, Australian businesses with annual turnover of $3 million or more must notify the OAIC and affected individuals when a data breach is likely to result in serious harm. Even if your business is below this threshold, breach notification is considered best practice.

The Australian Cyber Security Centre (ACSC) provides free resources and guidance for Australian businesses. Report cyber incidents to the ACSC at cyber.gov.au/report or call 1300 CYBER1 (1300 292 371).

8. What to Do Next

Start with your top priorities — the items at the top of your action plan. For items you can do yourself, follow the step-by-step guides in this report. For items that need technical help, use the 'Finding an IT Provider' section above to get the right support. Even tackling just the top 2–3 items will significantly reduce your risk.

This week — do these yourself

- **Disable anonymous sharing links** — Low – 30 mins
- **Enable automatic OS updates** — Low – 1-2 hours
- **Create a basic business continuity plan** — Low – 2-4 hours

Within 30 days — get some professional help

- **Create dedicated admin accounts** — Low – 1-2 hours
- **Enable self-service password reset** — Low – 1 hour
- **Configure DMARC for your domain** — Medium – needs DNS access

Ongoing

Keep devices updated, test backups quarterly, remove access promptly when staff leave, and re-assess your cyber posture annually.

9. Finding an IT Provider

If some of the recommendations in this report are beyond what you're comfortable doing yourself, that's completely normal. Here's how to find the right help:

What to look for: A local IT provider or managed service provider (MSP) who works with small businesses and is familiar with Microsoft 365 or Google Workspace (whichever you use). Ask if they've heard of the Essential Eight — it's a good sign if they have.

What to expect to pay: For a small business, expect $100–$200/hour for ad-hoc support, or $50–$150/user/month for ongoing managed services. Many of the items in this report are one-off fixes, not ongoing costs.

How to use this report: Hand the full report to any IT provider you're considering. It gives them a clear picture of where you stand and what needs fixing — which means less time (and cost) spent on discovery. You can even use it to compare quotes: ask each provider how they'd address your top 5 priorities and what they'd charge.

Tip: Get quotes from 2–3 providers. Send them this report and ask: “How much to implement the items marked ‘needs professional help’?” A good provider will give you a fixed price based on the technical steps listed here.

10. Disclaimer & Legal

This report provides general cyber security guidance based on the information you provided. It is not a professional audit, penetration test, or certification. CyberStance does not independently verify the accuracy of responses. No guarantee of security is made or implied. You should consult with a qualified IT security professional before making significant changes to your systems. This report should be used alongside professional advice appropriate to your business.

General Guidance Only. This report provides general cyber security guidance based on the information provided. It is not a certification, audit, penetration test, or guarantee of security. Findings are based on self-reported information and have not been independently verified through technical testing.

No Professional Advice. This report does not constitute professional IT, legal, or compliance advice. Consult a qualified IT security professional before making significant changes to your systems. Consult a legal professional regarding your obligations under the Privacy Act 1988 and the Notifiable Data Breaches scheme.

Self-Service Guidance. Step-by-step guides are provided as general guidance only. If you are unsure about any step, stop and seek professional advice. Incorrect configuration of security settings could result in data loss or service disruption.

Limitation of Liability. CyberStance accepts no liability for any loss, damage, or consequence arising from reliance on this report. Cyber security is an ongoing process and no assessment can guarantee protection against all threats.

Technical Guidance Currency. Technical steps are based on vendor platforms current at the time of writing. Navigation paths may change as vendors update their products.

Framework References. References to the Essential Eight, the ISM, and other frameworks are for guidance and context only. This report does not certify compliance with any framework or standard.

Confidentiality. This report is intended solely for the use of Acme Services Incorporated and should be treated as confidential.

Currency of Assessment. Cyber security threats and best practices evolve rapidly. We recommend reviewing your security posture at least annually.

CyberStance Assessment
cyberstance.com.au

Report generated: 8 April 2026

Report ID: CS-2026-CD4B7B46