ACSC ESSENTIAL 8 — TRADIE DIRECTOR'S GUIDE

Don't Get Played: The Tradie Director's No-BS Guide to Cyber Security

You built your business with your hands.
Here is how to protect it with your head.

By Kevin Whitmore, Centrase

CENTRASE.COM · 2026

centrase
TRUSTED SINCE 2007

WHY THIS MATTERS

The Numbers Your IT Person Is Not Telling You

The ASD's 2024–25 Annual Cyber Threat Report dropped some numbers that should make every tradie director put down the coffee and pay attention. These are not from corporate press releases. They are from the Australian government's own cyber security agency — the people who track every reported incident across the country.

$56,600
Average cost of a cyber incident for an Australian small business — 2024–25

1 in 5
SME owners hit by cybercrime in 2024 — ASD survey

+14%
Year-on-year cost increase for small business incidents

That $56,600 is the *average* — and SME owners lose more per incident than any other victim category. When ransomware locks your whole operation and you are sitting on site with crews waiting, the bill climbs fast. The ASD reports a cybercrime report every six minutes across Australia. **You are not too small to be a target. You are exactly the right size.**

What Is the Essential 8?

The Australian Signals Directorate identified eight controls that stop the majority of cyber attacks. Not all attacks — but most. Eight things. If you have them all in place at a basic level, you are significantly harder to hit than the average Australian business. Each control chapter covers one of the eight, with a plain-language explanation, a real-world analogy, and the exact question to ask your IT person.

Each control has three maturity levels — **ML1** (basics, stops most attacks), **ML2** (systematic, for businesses with client data or remote access), **ML3** (hardened). Most trade businesses should target ML1 across all eight to start.

Sources: ASD Annual Cyber Threat Report 2024–25 · ASD Annual Cyber Threat Report 2023–24 · ACSC Small Business Survey 2023

CONTROL ONE

1 Application Control

What Is It?

Application control means only approved software can run on your computers. If a program is not on your approved list, it cannot execute — full stop. Your staff cannot accidentally install something that has not been vetted, and malware that lands on your machine stays cold.

The Site Analogy

Think of a site induction list. Every person who comes onto your site gets inducted — checked, briefed, and added to the register. Random walk-ons do not get through the gate, no matter how convincing they sound. Application control is the same thing for software. Only inducted, approved programs get to run.

What Happens If You Ignore It?

One click on the wrong email attachment and ransomware runs on your system. It encrypts your quotes, client list, and job management software — then demands payment to unlock it. **Average ransom demand for an Australian small business: $150,000–$200,000.** Even when businesses pay, about 40% do not get all their data back.

REAL COST — AUSTRALIAN SME

A Queensland trade business was hit with ransomware in 2024. No application controls, no proper backups. Down for 11 days. Paid $95,000 in Bitcoin and got partial recovery. Total cost including downtime and recovery: over $200,000. The invoice that did it? Looked exactly like one from a regular supplier.

ML 1	ML 2	ML 3
Hash-based rules block unapproved programs from running. IT team maintains the approved list.	Publisher certificate rules added. Extended coverage across more folders and scripts. Harder to bypass.	Full allowlisting across all systems. Only what is explicitly approved can run. Anything else is blocked automatically.

THE BOTTOM LINE

You run a tight site. Randoms do not get through the gate without being inducted. Your computers should work the same way. Only software your IT person has approved gets to run — everything else stays out, no matter how official it looks.

Ask your IT person: "Do we have application control in place? Can you show me the approved software list and tell me what happens when something tries to run that is not on it?"

CONTROL TWO

2 Patch Applications

What Is It?

Software has bugs. Manufacturers fix them and release updates. Patching means applying those updates promptly — for your web browser, Office suite, accounting software, everything that runs on your computers. The window between "vulnerability discovered" and "attackers exploiting it" has shrunk to days.

The Site Analogy

Ignoring software updates is like ignoring a recall notice on your tools. The manufacturer found a problem and fixed it. If you do not apply the fix, you are running with a known fault — and everyone in the industry knows about it except you.

What Happens If You Ignore It?

Attackers scan the internet within hours of a vulnerability being made public, specifically looking for businesses still running the old version. Unpatched software is consistently one of the top three entry points for breaches in Australian small business. They do not need to find a new weakness — they just look for businesses that have not applied the known fix.

CONSTRUCTION IS A TOP-3 TARGET

Rapid7's 2025 analysis ranks construction among the three most attacked sectors globally. The reason: tight deadlines, subcontractor networks, and outdated software. Attackers know downtime halts a multi-million dollar project — so a business under pressure pays fast. The entry point is almost always an unpatched application with a publicly known fix that was never applied. The ASD confirms it: "Exploitation of public-facing applications" is the most common pathway in serious Australian incidents.

ML 1	ML 2	ML 3
Critical patches applied within 30 days. Unsupported software with known vulnerabilities removed from service.	Critical patches applied within 14 days. Regular scanning identifies unpatched software across all systems.	Critical patches applied within 48 hours. Automated scanning and patching. Unsupported software removed immediately.

THE BOTTOM LINE

A recall notice on equipment means the manufacturer found a problem and fixed it. You act on it — because running faulty kit is not how you operate. Same principle. Someone found a problem in your software and fixed it. Apply the fix.

Ask your IT person: "When were all our applications last patched? What is our process when a critical update comes out — how quickly does it get applied?"

CONTROL THREE

3 Configure Microsoft Office Macro Settings

What Is It?

Macros are small programs embedded in Word documents and Excel spreadsheets. Attackers hide malicious code inside documents that look completely normal. You open an email attachment, a pop-up asks you to "Enable Content" — if you click yes, malicious code runs immediately.

The Site Analogy

It is a delivery that looks legitimate on the outside but has something extra packed inside. You would not accept a pallet from an unknown supplier without checking the manifest. A macro-enabled document from an untrusted source is the same — a delivery with an uninvited extra hidden in the packaging.

What Happens If You Ignore It?

Macro-based attacks are among the most common ways Australian businesses get compromised. They do not require any technical weakness — they just need someone to click yes. One staff member on a Friday afternoon is all it takes.

THE RED FLAG — SHARE THIS WITH YOUR TEAM

If anyone opens a Word or Excel file and it asks to "Enable Content" or "Enable Macros" — treat that like someone asking you to sign a blank contract. Stop. Do not click. Call the office first. Legitimate documents from legitimate sources almost never need you to enable anything. Train your whole team on this one rule and it will save you.

ML 1	ML 2	ML 3
Macros disabled by default. Exceptions only for macros in trusted locations or digitally signed by a known publisher.	Only digitally signed macros from trusted, verified publishers allowed to run. Users cannot override this setting.	Signed macros only. Execution is logged. Users have no ability to change macro settings.

THE BOTTOM LINE

The cost of pausing when a document asks you to enable something is nothing. The cost of clicking yes on the wrong document can be everything. Forward this page to your staff today. One-rule training: if a file asks you to enable macros, stop and call.

Ask your IT person: "Are macro settings locked down across all our computers? Can my staff override those settings themselves?"

CONTROL FOUR

4 User Application Hardening

What Is It?

Your web browser and Office applications touch the outside world constantly — websites, emails, documents from clients and suppliers. Hardening means disabling features most people never use but attackers love to exploit: old browser plugins like Flash and Java, web-based ads that can carry malicious code, PowerShell access for regular staff.

The Site Analogy

When you set up a work vehicle, you put in what the driver needs for their job — and you lock up everything else. If the apprentice does not need the angle grinder today, it stays in the locked cabinet. Hardening strips the software back to what the person needs to do their job. Everything else is a liability.

What Happens If You Ignore It?

Advertising networks on legitimate websites have been used to deliver malware to business computers — without the user doing anything wrong at all. Just visiting a normal website that happened to show a compromised ad. Blocking web ads closes that entire attack path. It takes five minutes to configure and costs nothing.

ML 1	ML 2	ML 3
Flash, Java, and unnecessary browser plugins disabled. Web advertisements blocked across all browsers.	Office applications hardened with vendor-recommended settings. PowerShell restricted for standard users.	PowerShell use logged. Attack surface reduction rules enforced. Credential Guard enabled.

THE BOTTOM LINE

Your accounts person does not need PowerShell. Your estimator does not need Java running in the background. Strip the work vehicle back to what is needed for the job today and lock up the rest. That is hardening — and blocking web ads alone eliminates an entire category of attack for free.

Ask your IT person: "Have our browsers been hardened? Are we blocking web advertisements? Do standard user accounts have access to tools they do not need?"

QUICK WIN

Blocking web advertisements is free, takes about five minutes to configure, and eliminates malware delivery via compromised ad networks — attacks where the user did absolutely nothing wrong. Ask your IT person to action this today.

CONTROL FIVE

5 Restrict Administrative Privileges

What Is It?

Admin accounts have full control — they can install software, change settings, access all files, and override security controls. Restricting privileges means keeping admin access to the smallest possible number of people, and using admin accounts only when specifically needed — not for everyday tasks like email.

The Site Analogy

You would not give every apprentice a set of master keys. Most people need access to the specific area where they are working — nothing more. When everyone has the keys to everything, one bad hire or one moment of carelessness can cost you the whole operation. Count how many people have admin rights on your systems right now. If the number surprises you, fix it this week.

What Happens If You Ignore It?

Ransomware damage is proportional to what account the attacker gets into. A standard user account? They might encrypt that person's files. An admin account? They encrypt everything, disable backups, and lock you out completely. Most Australian small business ransomware attacks that cause total data loss happened on accounts that had more access than they needed.

WHEN STAFF LEAVE

The most common internal security incident in Australian small business involves a departing employee using admin access they should never have had in the first place. Every staff change is a reminder: audit your access list. Remove what is not needed. Check that ex-staff accounts are disabled the day they leave — not when you remember.

ML 1	ML 2	ML 3
Admin accounts kept separate from regular accounts. Admin accounts not used for everyday tasks like email or web browsing.	Just-in-time admin access — elevated permissions granted for a specific task and expire automatically. Logged and reviewed.	Dedicated Privileged Access Workstations for admin tasks. Admin accounts have no internet access. All activity is logged.

THE BOTTOM LINE

Ask your IT person for a report on who has admin rights. If it is more than two or three people, have the conversation. Admin is the master key — most people do not need it. **Action this week:** get the list, remove what is not needed, confirm all ex-staff accounts are disabled.

CONTROL SIX

6 Patch Operating Systems

What Is It?

Your operating system — Windows, macOS, the software running your phones and tablets — is the foundation everything else sits on. Patching it means keeping it current and retiring any version the manufacturer no longer supports. Same principle as Control 2, but deeper. An end-of-life OS has known holes that will never be patched.

The Site Analogy

Running an end-of-life OS is like using equipment the manufacturer stopped fixing. The fault is known — it just has not caused a problem yet. **Windows 10 reached end-of-life in October 2025.** Any business still running it is on unpatched infrastructure. Ask your IT person today.

What Happens If You Ignore It?

The moment an OS goes end-of-life, every private vulnerability becomes public knowledge. Attackers maintain lists of businesses running end-of-life systems. Staying on that list is a choice.

THE INSURANCE PROBLEM

Cyber insurance policies typically require that you maintain supported, patched software. If something goes wrong on a system you knew was end-of-life, your claim gets complicated. "We knew it was end-of-life but had not got around to upgrading it" is not a position you want to be defending. Get the upgrade on the schedule now — before you need to make a claim.

ML 1	ML 2	ML 3
Critical patches applied within 30 days. Any OS no longer receiving security updates removed from service.	Critical patches applied within 14 days. Regular scanning confirms patch status across all devices.	Critical patches applied within 48 hours. End-of-life systems retired immediately. Automated scanning and reporting.

THE BOTTOM LINE

An end-of-life OS is a liability on your balance sheet — not just a tech problem. Get the upgrade planned and scheduled. Yes, it costs money. It costs less than a breach and less than a declined insurance claim.

Ask your IT person: "What operating systems are we running? Are all of them still receiving security updates? When does each one hit end-of-life, and what is the plan?"

CONTROL SEVEN

7 Multi-Factor Authentication (MFA)

What Is It?

MFA means logging in requires two things: your password, plus a second factor — usually a code from your phone. Even if someone has your password, they cannot get in without the second factor. MFA is the single highest-impact control on this list relative to the effort required to set it up.

The Site Analogy

Your password is a regular lock — it can be copied, guessed, or bought if it appeared in someone else's data breach. MFA is the deadbolt. Even if an attacker has your key, they are not getting through the deadbolt without the second one. Takes 10 seconds to use. Stops the majority of account-compromise attacks cold.

What Happens If You Ignore It?

Business email compromise is the most profitable cyber crime targeting Australian SMEs. The ASD reports it as a top-reported crime category for businesses. An attacker gets into your email, watches how you communicate, then sends a fraudulent invoice or payment redirection to your accounts team. **Average BEC loss in Australia: around $50,000 per incident.** MFA on email stops this attack before it starts — because the stolen password alone is useless.

THE MEDIBANK LESSON

The October 2022 Medibank breach — 9.7 million Australians' records stolen — started with credentials purchased on a criminal forum. A ransomware group used those credentials to log in. MFA would have stopped that login. The credentials were useless without the second factor. The remediation cost Medibank over $250 million. MFA is free to configure and takes minutes.

ML 1	ML 2	ML 3
MFA enabled on all internet-facing services: email, cloud file storage, accounting software, VPN, remote access.	MFA required for all admin accounts. Authenticator app preferred over SMS codes.	Phishing-resistant MFA only — hardware security keys or passkeys. SMS codes not accepted for high-risk accounts.

DO THIS RIGHT NOW

If your email does not have MFA on it, stop reading and go turn it on. Everything else in this guide can wait. Your email is the master key to your business — password resets, supplier communications, client files, staff information. A deadbolt costs nothing and takes five minutes.

How: Log in to your email → Account Settings → Security or Two-Factor Authentication → Turn it on. Use Microsoft Authenticator or Google Authenticator rather than SMS where you have the option.

CONTROL EIGHT

8 Regular Backups

What Is It?

Backups are clean copies of your business data — client records, job history, financial data, documents, everything your operation runs on. Taken frequently. Stored separately from your main systems. And tested to confirm they actually work. Backups are your recovery option when everything else fails.

The Site Analogy

On site you keep a spare — fittings, cable, timber. Backups are your spare: a clean copy of everything your business runs on. The question is not whether you have them. It is whether you have *tested* them. An untested backup is like a spare tyre you have never checked.

What Happens If You Ignore It?

Ransomware without backups is a business-ending event. The ransom demand is calibrated to be just less painful than rebuilding from nothing. Businesses with clean, tested, offline backups do not pay — they restore and move on.

THE TEST QUESTION

Ask your IT person when they last did a full restore test from your backups. A restore test means actually recovering files to a clean system and confirming they work — not just checking that the backup job ran. Watch their face. That is your answer.

ML 1	ML 2	ML 3
Backups exist and run regularly. At least one copy stored offsite or in cloud. Restore tested at least once a year to confirm it works.	Offsite or cloud backup with restricted access. Restore tested quarterly. Backup accounts separate from regular admin accounts.	Offline (air-gapped) copy that ransomware cannot reach. Monthly restore testing. Strict privileged access controls on backup systems.

THE BOTTOM LINE

Backups stored on the same system they are backing up are not backups — they are copies that get encrypted alongside the original when ransomware hits. Offsite or offline storage is non-negotiable. Test the restore. Know your recovery time. Have a plan before you need it.

This week: Ask for a backup status report — what is backed up, where it goes, and when the last restore test was run. If the answer is "more than 90 days ago," schedule one.

WHERE DO YOU START?

The Priority Job List

Eight controls sounds like a lot. On a complex job site, the first question is always: what do I do first? Same applies here. Three controls stop the majority of attacks and can be implemented this week with minimal cost.

PRIORITY ONE — DO THESE THIS WEEK

1. MFA on email and cloud services. Free, takes minutes per account, stops most account-compromise attacks immediately.

2. Tested backups. Confirm offsite or cloud backups are running. Schedule a restore test. If you cannot restore from backup, you do not have backups.

3. Patch status report. Get a report of what software and operating systems you are running and when they were last patched. Retire anything end-of-life.

THE SEQUENCING

Week 1–2: MFA on all internet-facing accounts. Backup restore test. Patch status report.

Month 1: Admin access audit. Macro settings configured. Browser hardening applied.

Month 2–3: End-of-life operating systems retired. Application control scoped and designed.

Ongoing: Patching schedule maintained. Restore test quarterly. Access reviews when staff join or leave.

SELF-ASSESSMENT

Where Are You Today?

Score where you *actually* are — not where you think you should be. This is a site audit. The point is to find the gaps.

CONTROL	NOT STARTED (ML0)	BASIC (ML1)	SOLID (ML2)	LOCKED DOWN (ML3)
1. Application Control	☐ 0	☐ 1	☐ 2	☐ 3
2. Patch Applications	☐	☐	☐	☐
3. Office Macro Settings	☐	☐	☐	☐
4. App Hardening	☐	☐	☐	☐
5. Admin Privileges	☐	☐	☐	☐
6. Patch Operating Systems	☐	☐	☐	☐
7. Multi-Factor Auth (MFA)	☐	☐	☐	☐
8. Regular Backups	☐	☐	☐	☐

0–8
START HERE, THIS WEEK
Real exposure. MFA and backups today. Get help if you need it.

9–16
DECENT FOUNDATION
Better than most. Find the gaps and work through them.

17–24
STRONG POSTURE
You are doing this right. Maintain it, review every six months.

WHAT TO DO NEXT

Three Options from Here

Option 1 — Handle It Yourself

- Start with MFA on all internet-facing accounts — one hour, costs nothing
- Run the self-assessment with your IT person or office manager and prioritise the ML0 controls
- Run a backup restore test — if it fails, fix the backup before anything else
- Get a software and OS inventory, identify anything unpatched or end-of-life
- Detailed guidance is free at acsc.gov.au — the ASD has written step-by-step guides for each control

Option 2 — Work With Your Existing IT Person or MSP

- Print this guide and hand it to them — ask where you sit against each of the eight controls
- Ask for a written assessment with honest ML scores — not a sales pitch for new hardware
- Ask specifically: "When did you last run a restore test on our backups?"
- Ask: "Which of our systems are end-of-life or unpatched right now?"
- Ask: "How many accounts have admin rights and why do they all need it?"
- If they cannot answer those questions clearly, that is worth knowing too

Option 3 — Bring in a Fresh Set of Eyes

- Look for an IT firm with SME and trade business experience — not enterprise specialists who will overbuild it
- Ask them to do an Essential 8 gap assessment *before* they propose any work
- Expect a written report with an honest current-state score for each control
- A good IT adviser asks questions before they recommend anything — the same way a good tradie does a site inspection before quoting

ONE THING RIGHT NOW — BEFORE YOU PUT THIS DOWN

Go to your email account. Turn on two-factor authentication. It takes five minutes and stops the most common attack against Australian small business. Average BEC loss: around $50,000. MFA cost: zero. Do not wait until you have a plan. Do it now.

ABOUT

About Centrase

This guide was written by Centrase — a Gold Coast IT firm looking after Australian trade and SME businesses since 2007. Not a giant MSP, not a one-person operation. We work with business owners who want straight answers and a team that treats their business like it matters.

CENTRASE ESSENTIAL 8 ASSESSMENT

centrase.com/essential-8

A straightforward gap assessment against all eight controls. Written report. Honest ML score for each control. Prioritised action list. No lock-in. No surprises.

centrase.com · Gold Coast, Queensland · ABN 13 619 048 458

centrase

TRUSTED SINCE 2007