90 DAYS TO A SECURE BUSINESS

The Daily Action Guide for
Small to Medium Business Cybersecurity

Steven Connery
Static Computers

90 Days to a Secure Business
The Daily Action Guide for Small to Medium Business Cybersecurity

© 2025 Static Computers Pty Ltd
All rights reserved.

ISBN: 978-1-7646336-0-4

www.staticcomputers.com
steven@staticcomputers.com
1300 366 638
Sydney, Australia

HOW TO USE THIS BOOK

This book is designed to meet you where you are. Whether you're starting from scratch or tightening up existing practices, here's how to get the most from it.

Small steps, big results

Each day has one focused action. The power of this guide is in building habits - small, consistent steps that compound into real security over 90 days.

Start with the foundations

Weeks 1-4 cover the essentials: mindset, passwords, email, and devices. If you only get through these four weeks, you'll already be ahead of most small to medium businesses.

Work at your own pace

Some days you'll breeze through in five minutes. Others might need 20. Every action you complete strengthens your business, and progress beats perfection every time.

Involve your team early

Security is a team sport. Share what you're learning from Week 1. The earlier your people are part of the conversation, the stronger your defences become.

Get support sooner rather than later

Whether it's internal or external, having dedicated IT support shouldn't wait until something goes wrong. If you don't have an IT partner, start that conversation now - many of the actions in this guide are easier and more effective with professional help.

Use the weekly reviews to check your progress, and the security calendar on Day 86 to keep the momentum going long after Day 90.

WELCOME

G'day!

I'm Steven, and I'm genuinely excited that you've picked up this book.

Here's the thing: cybersecurity doesn't have to be scary, overwhelming, or complicated. For most small to medium businesses, it's really about building a few smart habits - habits that protect everything you've worked so hard to build.

Over the next 90 days, I'll walk you through one small action each day. Nothing crazy. Nothing that requires a computer science degree. Just practical, proven steps that actually work for real businesses like yours.

Why 90 days? Because that's how long it takes to build lasting habits. By the end of this journey, security won't be something you have to think about - it'll just be how you operate.

So grab a coffee (or tea - I don't judge), and let's get started.

Here's to your secure future,

Steven Connery
Founder, Static Computers

CONTENTS

Week 1: SECURITY FOUNDATIONS
Building your security mindset
Days 1-7

Week 2: PASSWORD POWER-UP
Mastering authentication
Days 8-14

Week 3: EMAIL DEFENCE
Defeating phishing attacks
Days 15-21

Week 4: DEVICE SECURITY
Protecting your hardware
Days 22-28

Week 5: DATA PROTECTION
Safeguarding your information
Days 29-35

Week 6: NETWORK BASICS
Securing your connections
Days 36-42

Week 7: CLOUD SAFETY
Managing online services
Days 43-49

Week 8: HUMAN FIREWALL
Empowering your team
Days 50-56

Week 9: BACKUP MASTERY
Building your safety net
Days 57-63

Week 10: VENDOR MANAGEMENT
Third-party security
Days 64-70

Week 11: INCIDENT READINESS
Preparing for the worst
Days 71-77

Week 12: COMPLIANCE BASICS
Meeting your obligations
Days 78-84

Week 13: CONTINUOUS IMPROVEMENT
Making security stick
Days 85-90

Back of Book
- What's Next - Your Security Benefits
- About the Author
- Workshops & Events
- Glossary of Terms
- Quick Reference Index

WEEK 1: SECURITY FOUNDATIONS

Building your security mindset



DAY 1

Why Cybersecurity Matters to You

Welcome to Day 1! Let's start with a reality check that might surprise you.

43% of all cyberattacks target small to medium businesses. Not because hackers have anything personal against you - but because automated tools scan the internet looking for easy targets. Small to medium businesses often have weak defences and valuable data.

The good news? You don't need to be a tech wizard. Most attacks exploit simple mistakes - weak passwords, clicking bad links, missing updates. These are all fixable, and that's exactly what we'll do together.

What attackers want from you:

- Your customer data - credit cards, emails, personal details
- Your business accounts - banking, email, cloud services
- Your access - to your clients, suppliers, and partners
- Your money - through direct theft or ransom demands

TODAY'S ACTION: Write down THREE specific consequences if all your data disappeared tomorrow. Think beyond dollars: lost clients? Damaged reputation? Weeks of rebuilding? Missed deadlines that cost you a contract?

TIP: 80-90% of breaches come from preventable mistakes. That means most of your risk is within YOUR control.

DAY 2

The Three Pillars of Security

Every cybersecurity decision fits into one of three categories. Master these, and you'll never feel lost.

IDENTITY - Who has the keys?

DATA - What are you protecting?

OPERATIONS - How do you stay safe?

Think of these like a three-legged stool. Remove any leg and the whole thing

collapses.

- Staff accounts and login credentials
- Password management practices
- Access permissions and controls
- Verification of who people claim to be
- Customer information and records
- Financial data and bank details
- Intellectual property and trade secrets
- Emails and business communications
- Software updates and patches
- Backup and recovery procedures
- Monitoring for problems
- Incident response planning

TODAY'S ACTION: Draw three columns: IDENTITY, DATA, OPERATIONS. Under each, list one thing you do well and one thing you're worried about.

TIP: You're probably doing better than you think. Most businesses already have pieces in place.

DAY 3

Meet Your Adversary

Let's bust the biggest myth in cybersecurity: the hoodie-wearing genius in a dark basement.

Reality: Most cybercriminals run a business. A boring, numbers-driven operation focused on volume.

You don't need to be Fort Knox. You just need to be harder to crack than the business next door.

How modern attacks actually work:

- Step 1: Automated tools scan millions of targets
- Step 2: They flag easy victims - weak passwords, old software
- Step 3: Criminals buy lists of vulnerable businesses
- Step 4: They attack the easiest targets first

What makes you an 'easy target':

- Passwords like 'Company123' or 'Welcome1'
- Software that hasn't been updated in months
- Staff who click links without thinking
- No multi-factor authentication
- The belief that 'it won't happen to us'

TODAY'S ACTION: Go to haveibeenpwned.com and search your email address. See if your credentials have appeared in any data breaches. If

TIP: If your email shows up in a breach, change that password immediately - especially if you've reused it.

DAY 4

Your Security Baseline

Before we improve anything, let’s honestly assess where you stand. No judgment – just clarity.

Passwords & Access

Updates & Software

Data & Backups

Awareness

Scoring: 8+ yes = ahead of most! 5-7 = good foundation. Under 5 = lots of quick wins ahead!

Take this quick security pulse check:

- Does everyone use unique passwords for work accounts?
- Is multi-factor authentication enabled?
- Do ex-employees still have access?
- Are computers set to auto-update?
- Is any software more than 2 years old?
- Do you know where all important files are stored?
- When was your last backup tested?
- Could your staff spot a phishing email?
- Do you know who to call if something goes wrong?

TODAY'S ACTION: Count your 'yes' answers and write down your score. We'll revisit this on Day 90.

TIP: Wherever you scored, you're in the right place. Awareness is the first step.

DAY 5

The Essential Eight Framework

Australia has a brilliant framework called the Essential Eight, developed by the Australian Cyber Security Centre. It's eight practical strategies that stop the vast majority of attacks.

Sounds like a lot? We'll tackle each one over the coming weeks. Most are simple changes you can make today.

The Essential Eight:

- Application Control - only approved software runs
- Patch Applications - keep software updated
- Configure Office Macros - block dangerous macros
- User Application Hardening - disable risky features
- Restrict Admin Privileges - limit who has the keys
- Patch Operating Systems - update Windows/Mac
- Multi-Factor Authentication - extra login protection
- Regular Backups - your ultimate safety net

TODAY'S ACTION: Visit cyber.gov.au/essential-eight and bookmark it. Skim through the eight strategies.

TIP: When clients ask about your security, say: 'We follow the Essential Eight framework.'

DAY 6

The Real Cost of a Breach

Let's talk about what a breach really costs - because it's not just about money.

industries

away

If even Australia's biggest brands are susceptible to cyberattacks, small to medium businesses without dedicated security are particularly vulnerable. The flip side? Most Essential Eight controls cost little or nothing to implement.

The numbers tell part of the story:

- Average data breach cost for Australian SMBs: $46,000
- Average downtime after ransomware: 21 days
- SMBs that close within 6 months of a major breach: 60%

But the real damage goes deeper:

- Lost time - Three weeks of rebuilding instead of growing your business
- Damaged reputation - Clients lose confidence; word travels fast in tight-knit
- Broken momentum - Projects stall, proposals miss deadlines, opportunities slip
- Team morale - Staff feel exposed and frustrated; rebuilding trust takes time

TODAY'S ACTION: Calculate your daily revenue × 21 days downtime + $15K recovery costs. Write your total somewhere visible. Then think: what would three weeks of silence do to your reputation?

TIP: Share this with your team. Security becomes everyone's priority when they understand what's at stake.

DAY 7

Week 1 Review: Your First Win

Congratulations! You've completed your first week. Let's recap what you've learned: You're already ahead of 80% of business owners who never take time to understand their cyber risk. Next week: passwords - the single easiest win.

- Why 43% of attacks target small to medium businesses
- The three pillars: Identity, Data, Operations
- How attackers actually think and operate
- Your current security baseline score
- The Essential Eight framework
- The real cost of doing nothing - in time, money, and reputation

TODAY'S ACTION: Complete ONE action from this week you haven't done yet. Then reward yourself - you've earned it!

TIP: Showing up every day matters more than being perfect.

WEEK 2: PASSWORD POWER-UP

Mastering authentication



DAY 8

Why Passwords Still Matter

Welcome to Password Week! Despite all the talk about new technologies, passwords remain the front door to your business.

Here's the uncomfortable truth about how most breaches happen:

The password problem:

- 81% of data breaches involve weak or stolen passwords
- The average person reuses passwords across 5+ accounts
- '123456' and 'password' are still in the top 10 most used
- Attackers buy stolen password lists for just a few dollars

Why this matters for your business:

- One compromised password can unlock your email, banking, and client data
- Staff often use the same password for work and personal accounts
- When LinkedIn gets breached, your business might too

TODAY'S ACTION: List all the business accounts you access daily. Count how many use the same or similar passwords. If

TIP: A password manager is one of the Essential Eight controls. You're building real security.

DAY 9

The Password Manager Revolution

Here's a secret that security professionals know: you shouldn't try to remember your passwords.

A password manager is a secure vault that remembers all your passwords for you.

You only need to remember one master password.

Why password managers work:

- Generate unique, complex passwords for every account
- Auto-fill passwords so you never type them
- Sync across all your devices securely
- Alert you if a password has been compromised

Recommended password managers:

- 1Password - excellent for business teams
- Bitwarden - great free option, open source
- LastPass - popular and user-friendly
- Keeper - strong security features

TODAY'S ACTION: Choose a password manager and install it on your main device. Start with just 3 accounts.

TIP: Your master password should be a passphrase - we'll cover that tomorrow.

DAY 10

Creating Uncrackable Passphrases

Forget everything you know about passwords. The key to an uncrackable password isn't complexity - it's length.

A passphrase is a sequence of random words that's easy to remember but nearly impossible to crack.

Why passphrases beat passwords:

- 'correcthorsebatterystaple' takes centuries to crack
- 'P@ssw0rd!' takes hours to crack
- Length beats complexity every time
- Random words are easier to remember than random characters

Creating strong passphrases:

- Use 4-6 random, unrelated words
- Add a number or symbol between words if required
- Make it at least 16 characters total
- Never use phrases from books, songs, or movies

TODAY'S ACTION: Create a new passphrase using 4 random words. Use it as your password manager master password.

TIP: Use a passphrase generator like useapassphrase.com for truly random combinations.

DAY 11

Multi-Factor Authentication

If passwords are the lock on your door, MFA is the deadbolt, security camera, and guard dog combined.

Multi-Factor Authentication (MFA) requires something you know (password) AND something you have (phone) to log in.

Why MFA is non-negotiable:

- Blocks 99.9% of automated account attacks
- Even if your password is stolen, attackers can't get in
- Required by most cyber insurance policies
- Takes just seconds to use once set up

MFA methods ranked by security:

- Hardware keys (YubiKey) - most secure
- Authenticator apps (Microsoft, Google) - very secure
- SMS text codes - better than nothing
- No MFA - unacceptable for business

TODAY'S ACTION: Enable MFA on your primary email account today. Use an authenticator app, not SMS.

TIP: Microsoft Authenticator and Google Authenticator are free and work with most services.

DAY 12

Rolling Out MFA to Your Team

Now that you understand MFA, it's time to protect your whole team. One unprotected account can compromise your entire business.

Rolling out MFA doesn't have to be painful. Here's your game plan:

Priority accounts for MFA:

- Email - the master key to everything else
- Microsoft 365 / Google Workspace
- Banking and financial accounts
- Cloud storage (Dropbox, OneDrive, Google Drive)
- Accounting software (Xero, MYOB, QuickBooks)

Making the rollout smooth:

- Give staff 1 week notice before enabling
- Schedule a 15-minute setup session for each person
- Have backup codes printed and stored securely
- Start with one system, then expand weekly

TODAY'S ACTION: Create a list of your top 5 business accounts. Check which ones have MFA available but not enabled.

TIP: Microsoft 365 and Google Workspace both have admin settings to enforce MFA for all users.

DAY 13

Cleaning Up Old Accounts

Here's a security risk nobody talks about: forgotten accounts. That old Dropbox trial, the LinkedIn you never use, the random SaaS tools from 2019.

These zombie accounts are goldmines for attackers because they often have weak passwords and no MFA.

Why old accounts are dangerous:

- Often use passwords you've reused elsewhere
- No MFA protection
- You won't notice if they're compromised
- May still have access to sensitive data
- Can be used to reset other accounts

The cleanup process:

- Check your email for 'Welcome to...' messages
- Review your password manager for unused accounts
- Search your inbox for 'verify your email'
- Delete accounts you don't need
- Update passwords on accounts you're keeping

TODAY'S ACTION: Spend 15 minutes searching your email for old account signups. Delete or secure at least 3 accounts.

TIP: justdelete.me has direct links to delete accounts from hundreds of services.

DAY 14

Week 2 Review: Password Champion

You've just completed the most impactful week in this entire guide. Seriously.

Password security stops more attacks than any other single measure.

This week you learned:

- Why 81% of breaches involve passwords
- How password managers change the game
- The power of passphrases over complex passwords
- Why MFA blocks 99.9% of attacks
- How to roll out MFA to your team
- The danger of forgotten accounts

Your password wins:

- Password manager installed and running
- MFA enabled on critical accounts
- Old accounts cleaned up
- Team aware of password best practices

TODAY'S ACTION: Verify MFA is enabled on your email and at least two other critical accounts. Screenshot the confirmation.

TIP: You've now implemented two of the Essential Eight: MFA and restricting admin privileges. You're building real security!

WEEK 3: EMAIL DEFENCE

Defeating phishing attacks



DAY 15

Email: The #1 Attack Vector

Welcome to Email Week. Here's a stat that should get your attention: 91% of all cyberattacks begin with an email.

Your inbox is the front door attackers use most often. Understanding why helps you defend it.

Why attackers love email:

- It reaches everyone in your organisation directly
- People are conditioned to respond to emails quickly
- One click can bypass all your technical defences
- It's free and anonymous to send millions of attacks

Common attack types:

- Phishing – fake emails pretending to be trusted sources
- Spear phishing – targeted attacks using personal details
- Business Email Compromise – impersonating executives
- Malware attachments – infected files that install viruses
- SMS phishing (smishing) – text messages with malicious links

Don't forget SMS phishing:

- Text message attacks are just as dangerous as email. People trust texts more and respond faster. In Australia, fake delivery notifications and bank alerts are common lures. Treat unexpected texts with the same suspicion as unexpected emails.

TODAY'S ACTION: Check your spam folder. Look at 5 spam emails and identify what makes them suspicious. Then review your recent text messages for anything that looks off.

TIP: Never tap a link in an unexpected text – search for the company directly instead.

DAY 16

Spotting Phishing Emails

Phishing emails are getting sophisticated, but they almost always contain telltale signs. Learn these red flags and you'll catch 95% of attacks.

The 5 red flags of phishing:

- Urgency - 'Act now!' 'Your account will be closed!'
- Sender mismatch - display name vs actual email address
- Generic greetings - 'Dear Customer' instead of your name
- Suspicious links - hover to see the real destination
- Unexpected attachments - especially .exe, .zip, or Office files with macros

Before you click, ask:

- Was I expecting this email?
- Does the sender's email address match who they claim to be?
- Would this company really contact me this way?
- Why is this so urgent?

TODAY'S ACTION: Find a recent email asking you to click a link. Hover over the link (don't click!) and check if the URL matches what you'd expect.

TIP: Legitimate companies will never threaten to close your account if you don't click a link immediately.

DAY 17

Business Email Compromise

Business Email Compromise (BEC) is the most financially devastating email attack.

Australian businesses lost over $98 million to BEC in 2023.

Unlike spam, BEC attacks are carefully researched and highly targeted.

How BEC attacks work:

- Attackers research your company and staff on LinkedIn
- They impersonate executives, suppliers, or clients
- They request urgent wire transfers or sensitive data
- Emails often come from lookalike domains (yourcompany.co instead of .com)

Common BEC scenarios:

- CEO requests urgent wire transfer while 'travelling'
- Supplier sends 'updated' bank details for payment
- HR receives request for employee tax file numbers
- Finance asked to pay 'overdue' invoice immediately

TODAY'S ACTION: Establish a rule: any request to change bank details or make unexpected payments must be verified by phone using a known number.

TIP: Never use the phone number in the suspicious email. Look up the contact's number independently.

DAY 18

The Phone Verification Rule

Today's lesson is simple but powerful: when in doubt, pick up the phone.

A 30-second phone call can prevent a $50,000 mistake. Make it a non-negotiable habit.

Always verify by phone when:

- Bank details change for any supplier or client
- Requests come from executives for urgent transfers
- Someone asks for sensitive employee information
- Any financial request seems unusual or urgent
- Email comes from a new or slightly different address

Phone verification rules:

- Call a number you already have on file - never from the email
- Speak to someone you know, not whoever answers
- Document the verification in writing
- If you can't verify, don't proceed

TODAY'S ACTION: Write a one-paragraph policy: 'All requests to change payment details must be verified by phone using pre-existing contact numbers.'

TIP: Post this policy near your finance team's desks. Make it visible and non-negotiable.

DAY 19

Securing Your Email Account

Your email account is the master key to your digital life. If attackers get your email, they can reset passwords to everything else.

Let's lock it down properly.

Email security checklist:

- Strong unique password (or passphrase)
- MFA enabled with authenticator app
- Recovery options up to date
- Connected apps reviewed and cleaned up
- Forwarding rules checked (attackers add sneaky forwards)

Check for compromise signs:

- Emails in 'Sent' you didn't send
- Password reset emails you didn't request
- Forwarding rules you didn't create
- Login alerts from unfamiliar locations
- Missing emails (attackers delete evidence)

TODAY'S ACTION: Log into your email security settings. Check forwarding rules, connected apps, and recent login activity.

TIP: In Outlook: Settings > Mail > Forwarding. In Gmail: Settings > Forwarding.

DAY 20

Training Your Team on Email

You can't be the only one who spots phishing. Your whole team needs to be suspicious of unexpected emails.

The good news: email awareness training works.

Simple team training:

- Share this week's red flags list with everyone
- Forward real phishing examples (sanitised) for discussion
- Create a 'report suspicious email' process
- Celebrate when someone catches a phishing attempt
- Never shame someone who clicks - they'll hide it next time

Quick training wins:

- 15-minute team meeting on phishing red flags
- Post the '5 red flags' somewhere visible
- Set up a shared channel for reporting suspicious emails
- Monthly 'phish of the month' discussion

TODAY'S ACTION: Schedule a 15-minute team meeting this week to share the phishing red flags from Day 16.

TIP: Consider using a free phishing simulation tool to test and train your team regularly.

DAY 21

Week 3 Review: Email Warrior

You've completed Email Week! This is arguably the most important week for preventing real-world attacks.

This week you learned:

- Why 91% of attacks start with email
- The 5 red flags of phishing emails
- How Business Email Compromise works
- The phone verification rule
- How to secure your email account
- How to train your team

Your email security wins:

- Email account hardened with MFA
- Forwarding rules and connected apps checked
- Phone verification policy established
- Team aware of phishing red flags

TODAY'S ACTION: Send the 5 phishing red flags to your team today. One email could prevent a major incident.

TIP: You've now built strong defences around Identity (passwords, MFA) and the #1 attack vector (email). Excellent progress!

WEEK 4: DEVICE SECURITY

Protecting your hardware



DAY 22

Every Device is a Doorway

Welcome to Device Security Week. Every laptop, phone, and tablet connected to your business is a potential entry point for attackers.

One unsecured device can compromise your entire network. Let's lock them down.

Your device inventory:

- Company laptops and desktops
- Staff mobile phones (even personal ones used for work)
- Tablets and iPads
- USB drives and external hard drives
- Printers and scanners (yes, really)
- IoT devices (smart speakers, cameras, thermostats)

TODAY'S ACTION: List every device that connects to your business network or accesses business data. Include personal phones used for work email.

TIP: Don't forget the printer in the corner - it's a computer too, often with default passwords.

DAY 23

Encryption Essentials

If someone steals your laptop, can they read your files? Without encryption, the answer is yes - even with a login password.

Encryption scrambles your data so only authorised users can read it. It's your last line of defence against physical theft.

Encryption you need:

- Full disk encryption on all laptops (BitLocker for Windows, FileVault for Mac)
- Phone encryption (enabled by default on modern iPhones and Androids)
- Encrypted backups
- Encrypted USB drives for sensitive data

Enabling encryption:

- Windows: Settings > Privacy & Security > Device Encryption (or BitLocker)
- Mac: System Preferences > Security & Privacy > FileVault
- iPhone: Enabled automatically with passcode
- Android: Settings > Security > Encryption

TODAY'S ACTION: Check if full disk encryption is enabled on your primary work computer. Enable it if not.

TIP: Store your BitLocker/FileVault recovery key somewhere safe - you'll need it if you forget your password.

DAY 24

The Update Habit

Software updates aren't just annoying popups - they're critical security patches that fix known vulnerabilities.

When you click 'Remind me later,' you're leaving the door open for attackers who already know how to exploit that weakness.

What needs updating:

- Operating systems (Windows, macOS, iOS, Android)
- Web browsers (Chrome, Firefox, Safari, Edge)
- Microsoft Office / Google Workspace apps
- Adobe products (Reader, Creative Suite)
- Antivirus software
- Router and modem firmware

Update best practices:

- Enable automatic updates wherever possible
- Set a weekly 'update day' for manual checks
- Restart devices regularly to complete updates
- Don't ignore update notifications for more than 48 hours

TODAY'S ACTION: Check for updates on your computer and phone right now. Install any pending updates.

TIP: Schedule updates for end of day so restarts don't interrupt your work.

DAY 25

Admin Rights: Less is More

Here's a simple rule that prevents a huge amount of damage: don't give admin rights to everyone.

When users have admin privileges, malware they accidentally download can install itself and spread. Standard user accounts contain the damage.

The principle of least privilege:

- Users get only the access they need for their job
- Admin accounts are separate from daily-use accounts
- Admin access requires a specific reason and approval
- Admin credentials are never used for email or browsing

Implementing least privilege:

- Audit who currently has admin rights
- Remove admin rights that aren't essential
- Create a process for requesting temporary admin access
- Use separate admin accounts for IT staff

TODAY'S ACTION: Check who has admin rights on your business computers. Remove any that aren't absolutely necessary.

TIP: Even business owners should use a standard account for daily work and only elevate when absolutely necessary.

DAY 26

Endpoint Protection

Antivirus alone isn't enough anymore. Modern threats need Endpoint Detection and Response (EDR) - software that monitors for suspicious behaviour, not just known viruses.

What modern endpoint protection does:

- Blocks known malware and viruses in real-time
- Detects suspicious behaviour patterns before damage occurs
- Prevents ransomware encryption attempts
- Monitors for data exfiltration
- Provides detailed alerts and reporting

Solutions to consider:

- GravityZone Business Security - core protection for small teams
- GravityZone EDR - advanced threat detection and response
- Managed Detection and Response (MDR) - 24/7 expert monitoring
- MDR means security experts watch your systems around the clock

TODAY'S ACTION: Review your current endpoint protection. Is it basic antivirus or proper EDR? Talk to your IT provider about upgrading.

TIP: MDR is like having a security operations centre without hiring a security team. Perfect for small businesses.

DAY 27

Lost Device Protocol

Laptops get stolen. Phones get left in taxis. What happens in the first hour after a device goes missing determines how much damage occurs.

You need a plan before it happens.

Your lost device checklist:

- Report immediately (who do staff call?)
- Remote wipe if possible (MDM or Find My Device)
- Change passwords for accounts on that device
- Revoke access tokens and sessions
- Check for suspicious activity
- Report to police if theft suspected

Preparation required:

- Enable Find My Device on all phones and laptops
- Set up Mobile Device Management (MDM) for remote wipe
- Ensure encryption is enabled (limits data exposure)
- Document who to contact and what steps to take
- Test the remote wipe capability before you need it

TODAY'S ACTION: Enable Find My Device on your phone and laptop. Test that you can locate them from another device.

TIP: Microsoft 365 and Google Workspace both have built-in remote wipe for managed devices.

DAY 28

Week 4 Review: Device Defender

Device Security Week complete! You've now locked down the physical tools your team uses every day.

This week you learned:

- Every device is a potential entry point
- Encryption protects data even if devices are stolen
- Updates patch known vulnerabilities
- Admin rights should be minimised
- Modern endpoint protection beats basic antivirus
- Lost device protocols limit damage

Your device security wins:

- Device inventory complete
- Encryption enabled on computers and phones
- Auto-updates configured
- Admin rights audited
- Lost device protocol documented

TODAY'S ACTION: Review your device inventory. Confirm encryption and Find My Device are enabled on all of them.

TIP: You've now covered three Essential Eight controls: patching, restricting admin rights, and application control. Outstanding progress!

WEEK 5: DATA PROTECTION

Safeguarding your information



DAY 29

Know Your Crown Jewels

Welcome to Data Protection Week. Before you can protect your data, you need to know what data actually matters.

Not all data is equal. Some information, if lost or stolen, would be a minor inconvenience. Other data could mean reputational damage, compliance risk, legal liability, or even business closure.

Your crown jewels likely include:

- Customer personal information (names, addresses, contact details)
- Financial records and banking details
- Employee records and payroll data
- Intellectual property and trade secrets
- Client contracts and confidential agreements
- System credentials and passwords

TODAY'S ACTION: List your top 5 most sensitive data types. Where is each one stored right now?

TIP: Customer personal information is almost always crown jewel data - it's protected by the Privacy Act.

DAY 30

Approved Storage Locations

Where does your business data actually live? If you can't answer that question confidently, you have a data sprawl problem.

Data scattered across personal drives, random cloud services, and email attachments is data you can't protect or control.

Business)

Common data sprawl locations:

- Personal Dropbox or Google Drive accounts
- Email attachments (sent and received)
- Desktop folders on individual computers
- USB drives in desk drawers
- WhatsApp and SMS messages

Creating approved storage:

- Choose ONE primary cloud storage (OneDrive, Google Drive, Dropbox
- Ensure it has business-grade security controls
- Set clear rules: business data goes HERE, nowhere else
- Audit regularly for data in unapproved locations

TODAY'S ACTION: Define your approved storage location. Communicate it clearly to your team: 'All business files go in [location].'

TIP: Microsoft 365 and Google Workspace both include business cloud storage with security controls built in.

DAY 31

Access Control Basics

Here's a question: can everyone in your business access everything? If yes, you have an access control problem.

The principle is simple: people should only access the data they need for their job. Nothing more.

Why access control matters:

- Limits damage if one account is compromised
- Reduces risk of accidental data exposure
- Meets compliance requirements (Privacy Act)
- Makes it easier to track who accessed what
- Protects sensitive data from curious eyes

Implementing access control:

- Create folders/spaces for different teams or functions
- Set permissions so people only see what they need
- Review access when people change roles
- Remove access immediately when people leave
- Use 'view only' where editing isn't needed

TODAY'S ACTION: Review sharing settings on your most sensitive folder. Who has access? Does everyone listed actually need it?

TIP: Google Drive and OneDrive/SharePoint make it easy to set folder-level permissions.

DAY 32

Sharing Settings Deep Dive

Cloud storage makes sharing easy - sometimes too easy. One wrong click can expose files to anyone with the link, or even the entire internet.

Let's audit your sharing settings before they cause a breach.

Dangerous sharing settings:

- 'Anyone with the link can view' - no authentication required
- 'Anyone with the link can edit' - even worse
- Sharing to personal email addresses instead of work accounts
- Old shares that were never revoked
- Entire folders shared when only one file was needed

Safe sharing practices:

- Share with specific people, not 'anyone with link'
- Use 'view only' unless editing is genuinely needed
- Set expiry dates on shares where possible
- Regularly audit who has access to what
- Use your company domain for sharing where possible

TODAY'S ACTION: Check your cloud storage for files shared as 'Anyone with link.' Change them to specific people or remove the share.

TIP: Create a simple sharing request form. It takes 30 seconds and creates accountability.

DAY 33

Data Classification

Not every document needs the same protection. A public brochure and a client's tax return are very different things.

Data classification means labelling data by sensitivity so everyone knows how to handle it.

matters)

Simple classification system:

- PUBLIC - Can be shared with anyone (marketing materials, website content)
- INTERNAL - For staff only, not sensitive (meeting notes, general policies)
- CONFIDENTIAL - Sensitive business data (financials, strategies, contracts)
- RESTRICTED - Highly sensitive (personal information, credentials, legal

TODAY'S ACTION: Create a one-page data classification guide with 3-4 levels. Share it with your team.

TIP: Data classification doesn't need to be complicated. Three levels is enough for most businesses.

DAY 34

Secure Deletion

When you delete a file, is it really gone? Usually, no. Deleted files can often be recovered - by you, or by someone who shouldn't have them.

When secure deletion matters:

- Disposing of old computers or hard drives
- Returning leased equipment
- Deleting client data after retention period
- Removing data from lost/stolen device remotely
- Clearing USB drives before reuse

Secure deletion methods:

- Use built-in secure delete (Shift+Delete doesn't count)
- Factory reset phones before disposal
- Use disk wiping software for hard drives
- Physically destroy drives containing highly sensitive data
- Don't forget about cloud backups and synced copies

TODAY'S ACTION: Identify any old devices or drives that need secure wiping. Schedule time to properly dispose of them.

TIP: For old hard drives with sensitive data, physical destruction (drilling holes or shredding) is safest.

DAY 35

Week 5 Review: Data Guardian

Data Protection Week complete! You now understand where your valuable data lives and how to protect it.

This week you learned:

- How to identify your crown jewel data
- Why approved storage locations matter
- Access control principles and implementation
- How to audit and fix sharing settings
- Simple data classification systems
- When and how to securely delete data

Your data protection wins:

- Crown jewel data identified and located
- Approved storage location defined
- Access permissions reviewed
- Dangerous shares fixed
- Classification system drafted

TODAY'S ACTION: Confirm your top 5 sensitive data types are stored in approved locations with appropriate access controls.

TIP: You've now protecting Identity, Communications, Devices, Data, and have appropriate access controls.

WEEK 6: NETWORK BASICS

Securing your connections



DAY 36

Your Digital Nervous System

Welcome to Network Security Week. Your network is the invisible infrastructure connecting everything - computers, phones, printers, cloud services.

If your network is compromised, attackers can see and intercept everything.

Your network includes:

- Your internet connection and modem
- Your router (the box with the WiFi)
- All devices connected via cable or WiFi
- Any smart devices (cameras, thermostats, speakers)
- Your connection to cloud services

TODAY'S ACTION: Log into your router's admin page. Don't know how? Check the sticker on your router or search '[router brand] admin login'.

TIP: If you've never changed the default Your password, do is Your router

DAY 37

The Guest WiFi Imperative

Here's a simple rule: visitors should never connect to your main business WiFi.

When someone connects to your network, their device can potentially see and access other devices. A guest's infected laptop could spread malware to your systems.

Why guest WiFi matters:

- Isolates visitor devices from your business network
- Limits damage if a guest device is infected
- Keeps your internal resources invisible to outsiders
- Provides internet access without business access

Setting up guest WiFi:

- Most modern routers have a 'Guest Network' option
- Create a separate network name (SSID) for guests
- Use a different password than your main network
- Enable 'client isolation' if available
- Consider bandwidth limits for guest network

TODAY'S ACTION: Log into your router and enable the guest network. Set a simple password you can share with visitors.

TIP: Business-grade WiFi systems like Ubiquiti or Aruba make guest networks easy to set up.

DAY 38

Router Security Basics

Your router is probably the most neglected security device in your business. It’s also one of the most important.

A compromised router means attackers control your entire network traffic.

Router security checklist:

- Change the default admin password
- Update the firmware (routers need patching too)
- Use WPA3 or WPA2 encryption (never WEP)
- Disable WPS (WiFi Protected Setup) – it’s hackable
- Change the default network name (SSID)
- Disable remote management unless needed

TODAY'S ACTION: Check your router's firmware version. Search '[router model] latest firmware' to see if you're up to date.

TIP: Consider a business-grade router with built-in security features like content filtering and intrusion detection.

DAY 39

Network Segmentation

Network segmentation means dividing your network into separate zones. If attackers breach one zone, they can't easily move to others.

Think of it like compartments on a ship - a leak in one doesn't sink the whole vessel.

Simple segmentation for your business:

- Main business network (computers, servers)
- Guest network (visitors, personal devices)
- IoT network (cameras, smart devices, printers)
- Keep sensitive systems isolated where possible

Why segment IoT devices:

- Smart devices often have poor security
- They're rarely updated by manufacturers
- A hacked camera shouldn't access your files
- Many IoT devices 'phone home' constantly

TODAY'S ACTION: Identify all IoT devices on your network. Consider moving them to a separate network or VLAN.

TIP: Many business routers support VLANs (Virtual LANs) which make segmentation easy without extra hardware.

DAY 40

VPN: When You Need It

VPN stands for Virtual Private Network. It encrypts your internet traffic so nobody between you and your destination can see it.

VPNs are essential in some situations, unnecessary in others. Let's clarify when you actually need one.

When you need a VPN:

- Working from public WiFi (cafes, airports, hotels)
- Accessing your office network remotely
- Staff working from home accessing internal systems
- Connecting branch offices securely

When you don't need a VPN:

- Browsing HTTPS websites (already encrypted)
- On your secured office network
- For general privacy (VPNs don't make you anonymous)

TODAY'S ACTION: Identify which staff work remotely or use public WiFi. These people need VPN access to your business systems.

TIP: A VPN isn't just for remote workers - it protects anyone using public WiFi.

DAY 41

Network Monitoring

Would you know if someone unauthorised was on your network right now? Most businesses wouldn't.

Network monitoring means knowing what's connected and spotting anomalies.

Basic network awareness:

- Know how many devices should be on your network
- Recognise unfamiliar device names
- Notice unusual traffic patterns
- Check router logs periodically

Simple monitoring options:

- Router admin page shows connected devices
- Fing app scans your network from your phone
- Business routers often include monitoring dashboards
- Consider managed network services for ongoing monitoring

TODAY'S ACTION: Open your router's admin page and review the list of connected devices. Do you recognise all of them?

TIP: Free tools like Wireshark can reveal surprising traffic on your network.

DAY 42

Week 6 Review: Network Protector

Network Security Week complete! You've secured the invisible infrastructure connecting your business.

This week you learned:

- Your network is your digital nervous system
- Guest WiFi protects your main network
- Router security basics and firmware updates
- Network segmentation limits attack spread
- When VPNs are necessary
- Basic network monitoring techniques

Your network security wins:

- Router admin password changed
- Guest WiFi enabled and configured
- Router firmware updated
- Connected devices reviewed
- IoT segmentation considered

TODAY'S ACTION: Confirm guest WiFi is active and your router firmware is current. These two changes alone significantly improve security.

TIP: You've now secured the paths data travels. Networks are the highways of your business.

WEEK 7: CLOUD SAFETY

Managing online services



DAY 43

Your Cloud Footprint

Welcome to Cloud Security Week. 'The cloud' isn't magic - it's just someone else's computers. And you're responsible for securing your data on them.

Common cloud services:

- Email (Microsoft 365, Google Workspace)
- File storage (OneDrive, Google Drive, Dropbox)
- Accounting (Xero, MYOB, QuickBooks Online)
- Communication (Slack, Teams, Zoom)

TODAY'S ACTION: List every cloud service your business uses. Include the free ones and trials people signed up for.

TIP: Check your bank statements for subscription payments - you'll find services you forgot about.

DAY 44

Cloud Account Security

Every cloud service is an account. Every account is a potential entry point. Securing your cloud starts with securing every login.

Strong unique password for each service

MFA enabled on every service that offers it

Recovery options up to date

Admin accounts minimised

Unused accounts closed

SSO (Single Sign-On) where available

Priority accounts to secure first:

- Email (master key to everything)
- Cloud storage (your business files)
- Accounting software (financial data)
- CRM (customer information)
- Admin consoles (Microsoft 365, Google Workspace)

TODAY'S ACTION: Review your top 5 cloud services. Confirm MFA is enabled and admin access is limited to those who need it.

TIP: Microsoft 365 and Google Workspace both have security dashboards showing which users have MFA enabled.

DAY 45

Shadow IT Risks

Shadow IT is when employees use unapproved apps and services for work. It's not malicious - people are just trying to get things done.

But every unapproved service is a potential data leak you don't know about.

Common shadow IT examples:

- Personal Dropbox for sharing large files
- WhatsApp for client communication
- Free PDF converters that upload your documents
- Personal email for work files
- Random apps that 'just sync' with work accounts

Managing shadow IT:

- Understand why people use workarounds
- Provide approved alternatives that actually work
- Create a simple process for requesting new tools
- Educate, don't punish - people mean well
- Regularly audit connected apps in your main platforms

TODAY'S ACTION: Ask your team: 'What apps or services do you use for work that we haven't officially set up?' No judgment, just discovery.

TIP: In Google Workspace: Admin > Security > API controls. In Microsoft 365: Azure AD > Enterprise applications.

DAY 46

Cloud Backup Reality

Here's a dangerous assumption: 'It's in the cloud, so it's backed up.' Not necessarily true.

Cloud providers protect against their failures, not yours. If you delete a file or get hit by ransomware, that deletion syncs everywhere.

What cloud providers protect:

- Their data centre failures
- Their hardware problems
- Their software bugs
- Service availability (mostly)

What YOU must protect:

- Accidental deletions by users
- Malicious deletions by attackers
- Ransomware that encrypts synced files
- Account compromise and data theft
- Compliance requirements for data retention

TODAY'S ACTION: Check your cloud provider's data retention policy. How long can you recover a deleted file? (Often just 30 days.)

TIP: Veeam, Acronis, and Wasabi all offer affordable cloud backup for small businesses.

DAY 47

Cloud Service Agreements

When you sign up for a cloud service, you agree to their terms. Understanding your cloud agreements affects your security and liability.

Key questions for any cloud service:

- Where is your data physically stored? (Country matters for privacy laws)
- Who can access your data? (Employees, contractors, law enforcement?)
- What happens to your data if you leave?
- What's their breach notification commitment?
- What security certifications do they have?

Red flags in cloud agreements:

- No clear data deletion policy
- Unlimited rights to use your data
- No breach notification requirements
- Data stored in countries with weak privacy laws
- No option to export your data

TODAY'S ACTION: For your top 3 cloud services, find answers to: Where is data stored? What's the breach notification policy?

TIP: Look for SOC 2 Type II certification - it means the provider has been audited for security practices.

DAY 48

Microsoft 365 / Google Security

If you use Microsoft 365 or Google Workspace, you have powerful security tools built in. Most businesses never configure them. Let's fix that today.

Microsoft 365 security quick wins:

- Enable Security Defaults (forces MFA for all users)
- Turn on audit logging
- Review external sharing settings in SharePoint/OneDrive
- Enable anti-phishing policies in Exchange
- Check Secure Score in the admin centre

Google Workspace security quick wins:

- Enforce 2-Step Verification for all users
- Review third-party app access
- Configure Drive sharing settings
- Enable enhanced safe browsing
- Check Security Investigation Tool alerts

TODAY'S ACTION: Log into your admin console and check if MFA is enforced for all users.

TIP: Microsoft 365 Security Center and Google Workspace Security Center provide unified dashboards.

DAY 49

Week 7 Review: Cloud Commander

Cloud Security Week complete! You now understand how to secure the online services your business depends on.

This week you learned:

- How to map your cloud footprint
- Cloud account security essentials
- The risks of shadow IT
- Why cloud doesn't mean backed up
- Key questions for cloud agreements
- Microsoft 365 / Google Workspace security settings

Your cloud security wins:

- Cloud services inventoried
- MFA enabled on all cloud accounts
- Shadow IT identified and addressed
- Admin console security settings reviewed
- Backup strategy for cloud data considered

TODAY'S ACTION: Confirm MFA is enforced on Microsoft 365 or Google Workspace for all users.

TIP: You've now covered six security domains: Identity, Communications, Devices, Data, Networks, and Cloud.

WEEK 8: HUMAN FIREWALL

Empowering your team



DAY 50

Your People Are Your Best Defence

Welcome to Human Firewall Week. Here's the truth: technology alone cannot protect your business.

Your team members make hundreds of security decisions every day - clicking links, opening attachments, sharing files. Their choices matter more than any software.

The human firewall approach:

- Train people to recognise threats
- Make secure behaviour easy and natural
- Create a culture where reporting is encouraged
- Empower people, don't just restrict them

TODAY'S ACTION: Think about your team's current security awareness. Could they spot a phishing email? Would they report something suspicious?

TIP: Studies show security awareness training reduces successful phishing attacks by up to 70%.

DAY 51

The Security Conversation

How do you talk about security with your team? If it's all doom and gloom, people tune out.

Effective security communication is positive, practical, and ongoing.

How to talk about security:

- Focus on protecting the business, not creating fear
- Use real examples relevant to your industry
- Explain the 'why' behind security rules
- Keep it short and frequent, not long and annual
- Celebrate wins and catches, not just failures

Security messaging that works:

- 'Here's how we protect our clients' instead of 'Don't click links'
- 'Report anything suspicious - you won't get in trouble'
- 'Security is everyone's job, and here's how you help'
- Share (sanitised) real threats you've blocked or caught

TODAY'S ACTION: Plan a 5-minute security topic for your next team meeting. Keep it practical and positive. A

TIP: The most secure businesses have someone who takes personal ownership of security.

DAY 52

Making Security Someone's Job

In many businesses, security often falls through the cracks because it's nobody's specific responsibility.

You don't need a full-time security person. But someone needs to own it.

Security responsibilities to assign:

- Monitoring for security alerts and news
- Ensuring updates are applied
- Managing user access (onboarding/offboarding)
- Running backup checks
- Coordinating security training
- Being the point of contact for security questions

Who should own security:

- Could be you (the business owner)
- Could be your most tech-savvy team member
- Could be your IT provider
- Whoever it is, make it explicit and documented

TODAY'S ACTION: Decide who owns security in your business. If it's you, consider what you can delegate or outsource.

TIP: Even if you outsource IT, someone internal should be the security liaison who understands your needs.

DAY 53

Secure Onboarding

When a new person joins, how do they get access to systems? If it's ad-hoc and rushed, security gaps appear.

Secure onboarding checklist:

- Create accounts with appropriate access (not admin by default)
- Set up MFA before giving system access
- Provide security training in week one
- Issue equipment with encryption enabled
- Explain password requirements and manager setup
- Document what access they've been given

First-week security topics:

- How to spot phishing emails
- Password and MFA requirements
- Approved tools and shadow IT policy
- How to report security concerns
- Physical security (keys, access cards, screen locking)

TODAY'S ACTION: Create a one-page security onboarding checklist for new team members.

TIP: Include security in the first-day welcome, not as an afterthought weeks later.

DAY 54

Secure Offboarding

When someone leaves, how quickly is their access removed? This is where many businesses fail badly.

Former employees with active accounts are a real and common security risk.

Offboarding security checklist:

- Disable all accounts immediately (same day)
- Change shared passwords they knew
- Revoke access to cloud services
- Collect devices and access cards
- Remove from group chats and email lists
- Review what data they had access to

Common offboarding failures:

- Waiting days or weeks to disable accounts
- Forgetting about cloud services (Slack, Xero, etc.)
- Not changing shared credentials
- Letting them keep personal devices with work data
- No documentation of what access existed

TODAY'S ACTION: Create an offboarding checklist. Test it by reviewing: if someone left today, how quickly could you revoke all their access?

TIP: A good offboarding process is your last line of defence against insider threats.

DAY 55

Building Security Culture

Security culture isn't about rules and restrictions. It's about making security the normal way your business operates.

Signs of good security culture:

- People report suspicious emails without being asked
- Security is discussed in normal meetings
- No one shares passwords 'just this once'
- People ask before installing new software
- Mistakes are reported, not hidden

Building security culture:

- Leaders model good security behaviour
- Make reporting easy and blame-free
- Recognise and reward security-conscious actions
- Include security in business decisions
- Keep security visible and normal, not hidden and scary

TODAY'S ACTION: Identify one way you can visibly demonstrate security leadership this week. Model the behaviour you want to see.

TIP: Recognition works better than punishment. Celebrate security wins publicly.

DAY 56

Week 8 Review: Culture Champion

Human Firewall Week complete! You've learned how to turn your team from a vulnerability into a strength.

This week you learned:

- Why people are your best defence
- How to communicate about security effectively
- The importance of assigned security responsibility
- Secure onboarding practices
- Critical offboarding procedures
- How to build lasting security culture

Your human firewall wins:

- Team understands their security role
- Onboarding checklist created
- Offboarding checklist created
- Security responsibility assigned
- Positive security conversation started

TODAY'S ACTION: Complete your onboarding and offboarding security checklists. These are living documents - refine them over time.

TIP: You've now addressed the human element - often the strongest or weakest link in security.

WEEK 9: BACKUP MASTERY

Building your safety net



DAY 57

Backup: Your Ultimate Safety Net

Welcome to Backup Week. If ransomware encrypts all your files tomorrow, could you recover?

Backups are your insurance policy against data loss, ransomware, hardware failure,

and human error.

Why backups matter more than ever:

- Ransomware attacks encrypt your data and demand payment
- Hardware fails eventually - it's when, not if
- Humans make mistakes and delete things
- Cloud sync is not backup (deletions sync too)
- Natural disasters, theft, and fires happen

TODAY'S ACTION: Ask yourself: if everything was gone tomorrow, what would you need to recover? Make a list.

TIP: Veeam, Wasabi, and other modern backup solutions offer affordable options for small businesses.

DAY 58

The 3-2-1 Backup Rule

The 3-2-1 rule is the gold standard for backup strategy. It's simple, proven, and protects against virtually any disaster.

The 3-2-1 rule:

- 3 copies of your data (original + 2 backups)
- 2 different storage types (e.g., hard drive + cloud)
- 1 copy offsite (physically separate location)

Modern 3-2-1 examples:

- Original files + external drive backup + cloud backup
- Server + local NAS backup + offsite cloud (Wasabi)
- Workstations + NAS + Veeam to cloud storage

TODAY'S ACTION: Map your current backup situation against 3-2-1. Where are the gaps?

TIP: Many businesses only back up documents but forget emails, databases, and cloud data. That's not enough.

DAY 59

What Needs Backing Up?

Not all data is equal. Some files are critical, some are replaceable. Prioritise your backups by business impact.

Critical (backup daily, test monthly):

- Financial records and accounting data
- Customer information and CRM data
- Contracts and legal documents
- Intellectual property and proprietary files
- Email (if not already in cloud with retention)

Often forgotten:

- Browser bookmarks and saved passwords
- Application settings and preferences
- Email signatures and templates
- Desktop and Downloads folders

TODAY'S ACTION: Create a backup priority list. What's critical? What's important? What have you forgotten?

TIP: A 3-2-1 backup strategy is recommended by the Australian Cyber Security Centre.

DAY 60

The Offline Backup Imperative

Here's what ransomware attackers know: connected backups can be encrypted too.

If your backup drive is always plugged in, ransomware will find it. You need an offline copy.

Why offline matters:

- Ransomware can't encrypt what it can't reach
- Protects against malicious insiders
- Survives account compromises
- True air gap = true protection

Offline backup options:

- External drive that's disconnected after backup
- Rotating drives kept in different locations
- Cloud backup with immutable storage (can't be modified)
- Tape backup for large organisations

TODAY'S ACTION: Identify your offline backup. If you don't have one, get an external drive and set up a weekly routine.

TIP: Air-gapped backups (offline, disconnected) are your insurance against ransomware.

DAY 61

Testing Your Backups

A backup you've never tested is a hope, not a backup. Until you've restored from it, you don't know if it works.

Backup testing checklist:

- Can you actually access the backup files?
- Are the files complete and uncorrupted?
- Can you restore a single file quickly?
- Can you restore an entire system if needed?
- How long does restoration actually take?

Testing schedule:

- Monthly: Restore a random file from backup
- Quarterly: Restore a full folder or project
- Annually: Full disaster recovery test
- After changes: Test whenever backup system changes

TODAY'S ACTION: Right now: pick a file from last week. Restore it from backup. Did it work?

TIP: Schedule a quarterly backup restoration test in your calendar right now.

DAY 62

Backup Automation

Manual backups don't happen. Life gets busy, you forget, and suddenly it's been three months.

Automated backups happen whether you remember or not.

NAS-based 3-2-1 backup strategy:

- Local NAS (Synology, QNAP) for fast daily backups
- NAS replicates automatically to cloud storage
- Wasabi or similar S3-compatible cloud for offsite copy
- Veeam for orchestrating backup across all locations

Automation best practices:

- Set it and verify it's running (check logs monthly)
- Get notifications on backup failures
- Ensure backup window doesn't impact work hours
- Monitor backup storage space

TODAY'S ACTION: Check that your backup automation is actually running. When was the last successful backup? A

TIP: Automated backups are the eighth Essential Eight control. You've now covered them all!

DAY 63

Week 9 Review: Backup Master

Backup Week complete! You now have the knowledge to build a bulletproof backup strategy.

This week you learned:

- Why backups are your ultimate safety net
- The 3-2-1 backup rule
- How to prioritise what needs backing up
- Why offline backups defeat ransomware
- The critical importance of testing
- How to automate and forget

Your backup wins:

- Backup priority list created
- 3-2-1 gaps identified
- Offline backup solution in place
- Test restore completed
- Automation verified

TODAY'S ACTION: Verify your 3-2-1 backup is complete: 3 copies, 2 types, 1 offsite. Fill any gaps this week.

TIP: You've now implemented regular backups - one of the most important defences against ransomware.

WEEK 10: VENDOR MANAGEMENT

Third-party security



DAY 64

Your Security Supply Chain

Welcome to Vendor Security Week. Your security is only as strong as your weakest supplier.

When a vendor gets breached, their access to your systems becomes the attacker's access.

Vendors who might have access to your data:

- IT support provider
- Accounting software (Xero, MYOB)
- Cloud storage providers
- Email hosting providers
- Payment processors
- HR and payroll systems

TODAY'S ACTION: List all vendors who have access to your data or systems. You might be surprised how many there are.

TIP: The ASD ACSC has guidelines on supply chain security at cyber.gov.au.

DAY 65

Sorting Vendors by Risk

Not all vendors pose equal risk. Your payment processor is more critical than your office supplies company.

High-risk vendors (prioritise these):

- Access to sensitive customer data
- Access to financial systems or payments
- Remote access to your network
- Store credentials or passwords
- Would cause major disruption if unavailable

Medium-risk vendors:

- Access to internal business data
- Provide critical but replaceable services
- Limited data access but important for operations

TODAY'S ACTION: Sort your vendor list into high, medium, and low risk categories.

TIP: Your vendors' security directly affects your security. That's why choosing the right one matters.

DAY 66

Vendor Access Controls

Vendors should have exactly the access they need - no more, no less. Excessive vendor access is excessive risk.

Vendor access principles:

- Grant minimum necessary access
- Use separate vendor accounts (not shared logins)
- Enable MFA for vendor access
- Review access regularly
- Revoke access when contracts end

Access control checklist:

- What systems does each vendor access?
- Is their access time-limited when possible?
- Do they have their own credentials?
- Is their access logged and monitored?
- When did you last review their access?

TODAY'S ACTION: For your top 3 high-risk vendors, document what access they have. Is it all necessary?

TIP: Some vendors ask for admin access 'to make things easier.' Push back - they rarely need it.

DAY 67

Security Questions for Vendors

You have every right to ask vendors about their security practices. Good vendors expect these questions.

Essential questions for high-risk vendors:

- Do you have security certifications? (SOC 2, ISO 27001)
- How do you protect our data?
- What's your breach notification policy?
- Do you have cyber insurance?
- Who at your company can access our data?

Red flag responses:

- 'We've never been breached' (everyone has incidents)
- 'Trust us' without specifics
- Can't explain their security measures
- No incident response plan
- Resistance to signing security terms

TODAY'S ACTION: Prepare a short vendor security questionnaire. Use it when evaluating new vendors.

TIP: A vendor security questionnaire shows you're serious about protecting your data.

DAY 68

Vendor Contracts

Security requirements belong in your vendor contracts. Verbal promises aren't enforceable.

Contract clauses to include:

- Data protection requirements
- Breach notification timeframes (24-72 hours)
- Right to audit or request security information
- Data return/deletion when contract ends
- Subcontractor security requirements

Data handling specifics:

- Where will data be stored?
- Will data be encrypted?
- Who can access the data?
- How long will data be retained?
- How will data be securely deleted?

TODAY'S ACTION: Review your agreements with high-risk vendors. Are security expectations documented?

TIP: Ask for their incident response plan. Many don't have one.

DAY 69

Vendor Review Rhythm

Vendor security isn't a one-time check. Things change - vendors get breached, change ownership, update practices.

Regular vendor reviews:

- Annual: Review all high-risk vendors
- When renewing: Re-evaluate security before signing
- After incidents: Review any vendor involved in a breach
- Industry news: Watch for vendor breach announcements

Review checklist:

- Is their access still necessary and appropriate?
- Have they had any security incidents?
- Are their certifications still current?
- Has their ownership or management changed?
- Are we still getting value from this relationship?

TODAY'S ACTION: Schedule your first annual vendor security review. Pick a date and put it in the calendar.

TIP: Sign up for breach notification services to hear when your vendors are compromised.

DAY 70

Week 10 Review: Vendor Guardian

Vendor Security Week complete! You now know how to manage third-party risk effectively.

This week you learned:

- Why vendor security is your security
- How to categorise vendors by risk
- Vendor access control principles
- What security questions to ask
- Contract clauses that protect you
- The vendor review rhythm

Your vendor security wins:

- Vendor inventory complete
- Vendors categorised by risk
- High-risk vendor access reviewed
- Security questionnaire prepared
- Annual review scheduled

TODAY'S ACTION: Complete your vendor risk categorisation. Ensure your highest-risk vendors have appropriate controls.

TIP: You've now secured your supply chain - a critical area many businesses overlook.

WEEK 11: INCIDENT READINESS

Preparing for the worst



DAY 71

Something Will Go Wrong

Welcome to Incident Response Week. Security incidents happen to everyone. The question isn't whether you'll face one - it's whether you'll be prepared.

Common incidents you might face:

- Phishing email that someone clicked
- Malware infection or ransomware attack
- Lost or stolen laptop/phone
- Suspicious account activity or data breach

TODAY'S ACTION: Think about the last 'security scare' you had. How did you handle it? What could have gone better?

TIP: The ACSC has incident response templates at cyber.gov.au that you can adapt.

DAY 72

Your One-Page Response Plan

You don't need a 50-page incident response manual. You need one page you'll actually use under pressure.

Your one-page plan should include:

- Step 1: STOP - Don't panic, don't make it worse
- Step 2: ASSESS - What happened? What's affected?
- Step 3: CONTAIN - Isolate the problem
- Step 4: CALL - Contact your response team/IT support
- Step 5: DOCUMENT - Write down what you know
- Step 6: COMMUNICATE - Notify who needs to know

TODAY'S ACTION: Draft your one-page incident response plan using the six steps above.

TIP: Keep this plan short - ideally one page. Long plans don't get followed in a crisis.

DAY 73

Your Incident Response Team

Who does what when something goes wrong? Decide now, not during the crisis.

Key roles to assign:

- Incident Commander - Makes decisions, coordinates response
- Technical Lead - Investigates and contains (often IT provider)
- Communications Lead - Handles internal/external messaging
- Business Lead - Assesses business impact, makes operational decisions

TODAY'S ACTION: Assign the four key roles for your business. Document names and contact details.

TIP: Include backups for key people. What if your IT person is on holiday during an incident?

DAY 74

Critical Contacts List

When an incident happens, you'll need to contact people quickly. Don't waste time searching for numbers.

Essential contacts to include:

- IT support provider - after-hours number
- Cyber insurance provider - claims hotline
- Legal advisor - for breach notification guidance
- Key staff members - personal mobile numbers
- Bank - fraud hotline
- Australian Cyber Security Centre - 1300 CYBER1 (1300 292 371)

TODAY'S ACTION: Create your critical contacts list. Include after-hours numbers where available.

TIP: Keep this list in multiple places: printed, in your phone, in the cloud, with a trusted contact.

DAY 75

Containment Actions

When you discover an incident, your first job is to stop it spreading. Containment buys you time to investigate and respond properly.

Critical: Don't destroy evidence!

Common containment actions:

- Disconnect affected device from network
- Disable compromised user account
- Block suspicious IP addresses at firewall
- Change passwords for affected accounts
- Isolate affected systems from others
- Preserve evidence (don't wipe yet!)
- Don't reinstall or wipe without capturing logs
- Don't turn off devices (may lose memory evidence)
- Document everything you do
- Isolate, don't destroy

TODAY'S ACTION: Create a containment checklist for your most likely incident types (phishing click, malware, lost device).

TIP: The first hour matters most. Quick containment can be the difference between a minor incident and a major breach.

DAY 76

Tabletop Exercises

The best way to test your incident response? Practice before it's real.

A tabletop exercise is a discussion-based walkthrough of a scenario. No technology required - just conversation.

Simple scenarios to try:

- Staff member clicks phishing link and enters credentials
- Ransomware message appears on a computer
- Laptop stolen from car
- Suspicious login from overseas location
- Client reports receiving strange emails 'from' you

TODAY'S ACTION: Schedule a 30-minute tabletop exercise with your key people. Pick one scenario to walk through.

TIP: Tabletop exercises are recommended by the Australian Cyber Security Centre for all businesses.

DAY 77

Week 11 Review: Crisis Ready

Incident Response Week complete! You're now prepared to handle security incidents calmly and effectively.

This week you learned:

- Why incidents are inevitable and preparation is essential
- How to create a simple one-page response plan
- Incident response team roles
- Building your critical contacts list
- Containment actions that limit damage
- How to test with tabletop exercises

Your incident response wins:

- One-page response plan created
- Response team roles assigned
- Critical contacts list built
- Containment checklists drafted
- First tabletop exercise scheduled

TODAY'S ACTION: Review your one-page response plan. Is it clear enough to follow under stress? Refine if needed.

TIP: You've now built your incident response capability. You're ready for whatever comes.

WEEK 12: COMPLIANCE BASICS

Meeting your obligations



DAY 78

Understanding Compliance

Welcome to Compliance Week. 'Compliance' sounds intimidating, but it's simply meeting your legal obligations.

Good news: if you've followed this guide, you're already doing most of what compliance requires.

Common compliance requirements:

- Privacy Act - protecting personal information
- Notifiable Data Breaches scheme - reporting obligations
- Industry-specific regulations (health, finance, etc.)
- Contractual requirements from clients
- Cyber insurance policy conditions

TODAY'S ACTION: List the compliance requirements that apply to your business. Ask your accountant or lawyer if unsure.

TIP: The Privacy Act currently exempts businesses under $3 million turnover, but this exemption is being removed. From July 2026, accountants, lawyers, real estate agents and others lose their exemption. All small businesses should prepare now.

DAY 79

The Australian Privacy Act

If you collect personal information, you likely have obligations under the Australian Privacy Act.

Key Privacy Act requirements:

- Only collect information you actually need
- Tell people why you're collecting their data
- Keep personal information secure
- Allow people to access and correct their data
- Only use data for the purpose it was collected
- Don't keep data longer than necessary

What counts as personal information:

- Names, addresses, phone numbers
- Email addresses
- Financial information
- Health information (extra protections apply)
- Photos that identify someone
- Opinions about an identified person

TODAY'S ACTION: Review what personal information your business collects. Is all of it necessary?

TIP: The OAIC has templates and guidance at oaic.gov.au for privacy compliance.

DAY 80

Notifiable Data Breaches

Since 2018, Australian businesses must report eligible data breaches to the OAIC and affected individuals.

When you must notify:

- Unauthorised access to personal information AND
- A reasonable person would conclude serious harm is likely AND
- You haven't been able to prevent the harm with remedial action

Examples of notifiable breaches:

- Customer database stolen by hackers
- Email with personal data sent to wrong recipient
- Laptop with unencrypted client data stolen
- Ransomware attack accessing personal information

TODAY'S ACTION: Review your incident response plan. Does it include steps for assessing notification requirements?

TIP: You have 30 days to notify affected individuals after becoming aware of an eligible breach.

DAY 81

Documentation Essentials

Good documentation proves you take security seriously. If it's not written down, it didn't happen.

Essential documents to have:

- Privacy policy (required if you have a website)
- Incident response plan (you have this now!)
- Acceptable use policy for staff
- Password and access policy
- Backup and recovery procedures
- Vendor management records

TODAY'S ACTION: Create a folder for your security documentation. Start collecting what you've created during this guide.

TIP: Store all security documentation in one accessible folder. You'll thank yourself later.

DAY 82

Simple Security Policies

A security policy doesn't need legal jargon. It needs to be clear enough that everyone follows it.

Core policies every business needs:

- Password policy - how to create and manage passwords
- Acceptable use - what's OK and not OK on work systems
- Remote work - security requirements for working from home
- Incident reporting - how to report security concerns
- Data handling - how to handle sensitive information

TODAY'S ACTION: Write a one-page password policy for your business. Include requirements and the 'why'.

TIP: Have a non-technical person read your policies. If they don't understand it, rewrite it.

DAY 83

Working with Auditors

At some point, someone will want to audit your security - a client, insurer, or regulator.

Audits don't have to be scary if you're prepared.

Audit preparation:

- Gather your documentation in one place
- Be honest - auditors respect honesty over perfection
- Explain compensating controls if you don't meet a requirement
- Document improvements you're working on
- Ask questions if requirements are unclear

TODAY'S ACTION: Collect all your security documentation into one accessible folder. This is your 'audit ready' pack. If

TIP: An audit-ready pack shows clients and insurers you take security seriously.

DAY 84

Week 12 Review: Compliance Confident

Compliance Week complete! You now understand your obligations and how to meet them.

This week you learned:

- Why compliance matters and what it involves
- Australian Privacy Act basics
- Notifiable Data Breaches scheme
- Essential documentation requirements
- How to write simple, effective policies
- How to prepare for audits

Your compliance wins:

- Compliance requirements identified
- Privacy obligations understood
- Documentation folder created
- Core policies drafted
- Audit-ready pack assembled

TODAY'S ACTION: Review your documentation folder. Is everything there? What's missing?

TIP: You're almost at the finish line! One more week to cement your security foundation.

WEEK 13: CONTINUOUS IMPROVEMENT

Making security stick



DAY 85

Security is a Journey

Welcome to your final week. Congratulations on making it this far!

But here's the truth: security isn't a destination. It's an ongoing journey of improvement.

Why security never 'finishes':

- Threats evolve constantly
- Your business changes over time
- New vulnerabilities are discovered
- Staff come and go
- Technology updates continuously

TODAY'S ACTION: Reflect on your journey. What's the biggest security improvement you've made in 90 days?

TIP: Write down your top 3 security wins. Celebrate your progress!

DAY 86

Your Security Calendar

Security maintenance works best when it's scheduled. Put it in the calendar and it gets done.

Monthly tasks:

- Review backup success logs
- Check for software updates
- Review any security alerts
- Quick team security reminder

Quarterly tasks:

- Test restore from backup
- Review user access (anyone left? changed roles?)
- Check MFA is still enabled everywhere
- Review connected apps and integrations

Annual tasks:

- Full security review
- Vendor security assessment
- Policy updates
- Team security training refresh
- Insurance policy review

TODAY'S ACTION: Add quarterly backup test and annual security review to your calendar right now.

TIP: Schedule these reviews in your calendar now - don't leave it to memory.

DAY 87

Measuring Progress

How do you know if your security is improving? Measure what matters.

Simple metrics to track:

- Days since last security incident
- Percentage of staff with MFA enabled
- Days since last backup test
- Number of unpatched devices
- Time to respond to security alerts

Qualitative measures:

- Are staff reporting suspicious emails?
- How confident do you feel about security?
- Could you recover from ransomware today?
- Do you know where your sensitive data is?

TODAY'S ACTION: Choose 3 security metrics you'll track. Note today's baseline.

TIP: Security metrics help you demonstrate progress to leadership and clients.

DAY 88

Staying Current

The threat landscape changes constantly. Stay informed without being overwhelmed.

Reliable Australian sources:

- Australian Cyber Security Centre (cyber.gov.au) - sign up for alerts
- ACSC Small Business guide updates
- Your IT provider's security updates
- Stay Smart Online newsletter

What to watch for:

- Major vulnerability announcements affecting software you use
- New scam campaigns targeting Australian businesses
- Changes to compliance requirements
- Emerging threats relevant to your industry

TODAY'S ACTION: Sign up for ACSC alerts at cyber.gov.au. They're free and relevant.

TIP: The ACSC's Stay Smart Online newsletter is excellent and Australian-focused.

DAY 89

Helping Others

You've learned a lot in 90 days. Share what you've learned.

Helping others improves your own understanding and builds a more secure business community.

Ways to help others:

- Share this guide with a fellow business owner
- Mentor someone starting their security journey
- Talk about security at industry events
- Report scams to Scamwatch (helps everyone)
- Share successful security practices with peers

TODAY'S ACTION: Identify one person you could share this guide with. Send them a message today.

TIP: Security is a community effort. Share what you've learned.

DAY 90

Your New Foundation

Congratulations! You've completed the 90-Day Cybersecurity Action Guide.

This isn't the end - it's the beginning. You now have a security foundation that most most businesses never achieve.

What you've accomplished:

- 13 weeks of structured security improvement
- Essential Eight controls implemented
- Identity, communications, devices, and data protected
- Network and cloud security established
- Human firewall built
- Backup strategy in place
- Vendor risk managed
- Incident response plan ready
- Compliance requirements understood

TODAY'S ACTION: Retake the Day 4 security pulse check. Compare your score. Then celebrate - you've earned it!

TIP: This isn't the end - it's the beginning of your security journey. You've built something real.

WHAT'S NEXT

The Benefits of a Secure, Up-to-Date Business

You've invested 90 days in building a security foundation. Here's what that gives you:

Win more contracts - Clients increasingly require evidence of security practices before doing business.

Reduce insurance premiums - Demonstrable controls can lower cyber insurance premiums and strengthen claims.

Protect your reputation - Responsible data handling builds trust, loyalty, and revenue.

Recover faster - Tested backups, a response plan, and a trained team mean days, not weeks.

Meet compliance obligations - Privacy Act, NDB scheme, and industry requirements - you're across them.

Sleep better - Knowing your business is protected means less stress and more focus on growth.

Stay competitive - While competitors scramble after a breach, your business keeps running.

Empower your team - Security-aware staff make better decisions and protect your clients' data.

A note on IT support

Whether it's an internal team member or an external partner, dedicated IT support is essential - not optional. The actions in this guide are a strong start, but ongoing management, monitoring, and expert guidance keep your defences strong as threats evolve. Don't delay getting the right support in place.

ABOUT THE AUTHOR

Steven Connery

Founder & Director, Static Computers Pty Ltd

With 25 years in the IT industry, Steven has worked across enterprise environments including international healthcare technology, global assistance companies, and managed services. His career spans infrastructure management, program delivery, and technical consulting for organisations of all sizes.

Steven founded Static Computers in 2006 to give small and medium businesses access to the same calibre of IT support and security guidance that larger organisations take for granted. Based in Sydney, Static Computers partners with businesses of 10-120 users who need practical, hands-on IT management without the jargon.

He holds an Advanced Diploma in Program Management and has led complex projects including Microsoft 365 migrations, cybersecurity implementations, and IT service management advisory - helping businesses achieve frameworks like ISO 27001 and the Essential Eight.

Why this guide?

After 25 years of seeing the same preventable mistakes lead to real damage for small businesses, Steven created this guide to put practical cybersecurity knowledge directly into the hands of business owners - the people who need it most but are often the last to receive it.

WORKSHOPS & EVENTS

Want to go deeper? Static Computers runs interactive workshops designed to bring this guide to life for you and your team.

Monthly Business Security Workshop

A 60-minute interactive session covering the key topics from this guide, with live demonstrations, Q&A;, and practical takeaways. Perfect for business owners and office managers who want hands-on guidance.

Team Security Awareness Training

A tailored session for your whole team covering phishing awareness, password best practices, and incident reporting. Delivered on-site or virtually. Includes phishing simulation testing.

Lunch & Learn Presentations

Invite Steven to present at your networking group, industry event, or team lunch. Topics include: 'The 5 Cyber Threats Every Business Faces,' 'Passwords Are Dead (Almost),' and 'What to Do When You've Been Hacked.'

Security Health Check

A one-on-one assessment of your current security posture against the Essential Eight framework. Walk away with a prioritised action plan and clear next steps.

To book a workshop or enquire about a presentation for your group:

steven@staticcomputers.com | 1300 366 638 | www.staticcomputers.com

GLOSSARY OF TERMS

ACSC
Australian Cyber Security Centre - the federal government's lead agency for cybersecurity.

BEC
Business Email Compromise - targeted email attacks impersonating executives or suppliers to steal money or data.

BitLocker
Microsoft's built-in full disk encryption for Windows.

EDR
Endpoint Detection and Response - advanced security software that monitors devices for suspicious behaviour.

Essential Eight
Eight cybersecurity mitigation strategies recommended by the ACSC for Australian businesses.

FileVault
Apple's built-in full disk encryption for macOS.

IoT
Internet of Things - smart devices like cameras, thermostats, and speakers connected to the internet.

MDM
Mobile Device Management - software to manage, secure, and remotely wipe mobile devices.

MDR
Managed Detection and Response - 24/7 expert security monitoring and incident response.

MFA
Multi-Factor Authentication - requiring two or more verification methods to log in.

NAS
Network Attached Storage - a dedicated file storage device connected to your network.

NDB
Notifiable Data Breaches - the Australian scheme requiring businesses to report eligible data breaches.

OAIC
Office of the Australian Information Commissioner - the regulator for privacy and data protection.

Phishing
Fraudulent emails or messages designed to trick you into revealing passwords or clicking malicious links.

Ransomware

Malware that encrypts your files and demands payment for the decryption key.

SOC 2

Service Organisation Control 2 - an auditing standard for service providers covering security, availability, and privacy.

SSO

Single Sign-On - one set of credentials to access multiple applications.

VLAN

Virtual Local Area Network - a way to segment your network without separate physical hardware.

VPN

Virtual Private Network - encrypts your internet connection to protect data in transit.

WPA2/WPA3

WiFi Protected Access - security protocols for wireless networks. WPA3 is the current standard.

QUICK REFERENCE INDEX

Use this index to quickly find the topics you need. Days are organised by theme.

Security Foundations (Days 1-7)

Why cybersecurity matters - Day 1
Three pillars: Identity, Data, Operations - Day 2
How attackers operate - Day 3
Security baseline assessment - Day 4
Essential Eight framework - Day 5
Real cost of a breach - Day 6

Passwords & Authentication (Days 8-14)

Password managers - Day 9
Passphrases - Day 10
MFA setup - Day 11
MFA team rollout - Day 12
Old account cleanup - Day 13

Email Security (Days 15-21)

Phishing red flags - Day 16
Business Email Compromise - Day 17
Phone verification rule - Day 18
Email account hardening - Day 19

Device Security (Days 22-28)

Device inventory - Day 22
Encryption (BitLocker/FileVault) - Day 23
Updates and patching - Day 24
Admin rights - Day 25
Endpoint protection (EDR/MDR) - Day 26
Lost device protocol - Day 27

Data Protection (Days 29-35)

Crown jewel identification - Day 29
Approved storage - Day 30
Access control - Day 31
Sharing settings - Day 32
Data classification - Day 33

Network Security (Days 36-42)

Router security - Day 38
Guest WiFi - Day 37
Network segmentation - Day 39

VPN usage - Day 40

Cloud Security (Days 43-49)

Cloud footprint mapping - Day 43
Shadow IT - Day 45
Cloud backup - Day 46
M365/Google security settings - Day 48

Backup & Recovery (Days 57-63)

3-2-1 backup rule - Day 58
Offline backups - Day 60
Testing backups - Day 61
Backup automation - Day 62

Incident Response (Days 71-77)

One-page response plan - Day 72
Response team roles - Day 73
Critical contacts list - Day 74
Containment actions - Day 75
Tabletop exercises - Day 76

READY TO TAKE THE NEXT STEP?

You've built a strong foundation. Now let's make sure it stays strong.

□ Book a Free Security Health Check

A no-obligation assessment of your current security posture against the Essential Eight. Walk away with a clear, prioritised action plan.

□ Secure Your Business Today

From managed IT support to cybersecurity implementation, we'll take the complexity off your plate so you can focus on what you do best.

□ Join Our Monthly Security Workshop

Interactive, practical sessions that bring this guide to life. Perfect for business owners and their teams.

Steven Connery
Founder & Director, Static Computers

steven@staticcomputers.com
1300 366 638
www.staticcomputers.com

Your IT Team - We make your IT simple and secure

THANK YOU

for taking your cybersecurity seriously

ISBN: 978-1-7646336-0-4