CyberAssure

Redgum Property Group
Cyber Security Health Check

Assessment Date: 16 February 2026

EXAMPLE ONLY

How to Read This Report

Understanding Your Score

Your overall score (0-100%) shows how well your current practices align with good security. Higher is better, but don't worry if you're not at 100% — most businesses have room to improve.

- 75%+ = Strong foundation — you're doing well
- 50-74% = Good progress — some gaps to address
- Below 50% = Getting started — focus on the essentials first

How Your Score Is Calculated

Each question is worth points based on your answer: Yes = full points, Mostly = 75%, Partially = 50%, Rarely = 25%, No = 0%. Topic scores are the weighted average of all questions in that topic, and your overall score is the weighted average of all topic scores. This approach aligns with common security assessment methodologies and gives appropriate weight to fundamental controls.

Essential vs Recommended

Essential items are the security basics every business should have. Start here. Recommended items build on the basics and provide stronger protection. Advanced items are for businesses wanting comprehensive security.

What Priority Means

Gaps are ranked by priority to help you focus. High priority items pose the greatest risk and should be addressed first. Medium priority items are important but less urgent. Low priority items are good to fix when you have time.

Using the Improvement Plan

The Improvement Plan lists everything that needs attention with clear actions. Work through it at your own pace — you don't need to fix everything at once. Start with high priority items and tick them off as you go.

Important Note

This is a self-assessment tool to help you understand and improve your security — it is not a formal audit or certification. Results are based on your own answers. For important decisions, consider getting advice from an IT professional.

Executive Summary

This assessment evaluates Redgum Property Group's current cyber security practices. It shows where you are now and what to focus on next.

Redgum Property Group Score: 63% — Good Progress — Some Gaps to Address

There are 17 essential items to work on — these are your priority.

Top 5 Quick Wins

These five actions give you the best security improvement for the least effort:

1. Turn on two-factor authentication (2FA) on email and critical accounts.
2. Remove access for staff who have left.
3. Secure remote access with VPN or 2FA.
4. Enable automatic updates on all devices.
5. Test that your backups actually work.

Gap Summary

High Priority: 17 items need urgent attention

Medium Priority: 12 items to address soon

Lower Priority: 0 items for ongoing improvement

What You're Doing Well

Security is a journey, and Redgum Property Group has already made good progress in several areas. Here are the strongest topics:

Secure Setup — 84% — Strong

Your devices are configured securely with appropriate settings. Default passwords have been changed and unnecessary features disabled, reducing your attack surface.

Security Software — 73% — Good

Some devices have protection but coverage is incomplete. Ensure every computer, laptop, and mobile device has reputable security software installed, enabled, and set to update automatically.

Backups & Recovery — 71% — Good

Backups exist but may not be complete or tested. Verify your backups actually work by doing a test restore, and ensure you're backing up everything critical including cloud data.

Your Data — 71% — Good

Some data protection measures exist but gaps remain. Identify where all sensitive data is stored, who can access it, and implement appropriate protections including encryption for the most critical information.

Suppliers & Services — 71% — Good

You know your key suppliers but haven't fully assessed their security practices. Check what data they access, how they protect it, and whether they've had any security incidents.

Keep maintaining these practices — consistency is key to long-term security.

How You Scored By Topic

Topic	Score	Status	What This Means
Secure Setup Configuring systems with security in mind from the start.	**84%**	Strong	Your devices are configured securely with appropriate settings. Default passwords have been changed and unnecessary features disabled, reducing your attack surface.
Security Software Antivirus and protection tools that defend against malware and threats.	**73%**	Developing	Some devices have protection but coverage is incomplete. Ensure every computer, laptop, and mobile device has reputable security software installed, enabled, and set to update automatically.
Backups & Recovery Protecting your business data with regular backups you can restore when needed.	**71%**	Developing	Backups exist but may not be complete or tested. Verify your backups actually work by doing a test restore, and ensure you're backing up everything critical including cloud data.
Your Data Safeguarding sensitive information and meeting privacy obligations.	**71%**	Developing	Some data protection measures exist but gaps remain. Identify where all sensitive data is stored, who can access it, and implement appropriate protections including encryption for the most critical information.
Suppliers & Services Managing security risks from third parties and cloud services.	**71%**	Developing	You know your key suppliers but haven't fully assessed their security practices. Check what data they access, how they protect it, and whether they've had any security incidents.
Firewalls & Networks Protecting your internet connection and internal network.	**70%**	Developing	Basic network protection exists but could be stronger. Review your firewall rules, ensure WiFi uses WPA3 or WPA2 with a strong password, and consider separating guest and business networks.
Passwords & Access Controlling who can access your systems and how they prove identity.	**68%**	Developing	Basic password controls exist but there's room to improve. Focus on implementing multi-factor authentication for critical systems and ensuring staff use unique, strong passwords for each account.
When Things Go Wrong Preparing for and responding to security incidents effectively.	**65%**	Developing	Some incident preparation exists but plans may be incomplete. Document who does what during an incident, how to contact key people, and basic steps for common scenarios like ransomware.
Updates & Patching Keeping software current to fix known security vulnerabilities.	**60%**	Developing	Some updates are happening but gaps remain. Enable automatic updates on all devices and software where possible, and create a regular schedule to check for updates that need manual installation.
Leadership & Planning Management commitment, policies and security planning.	**59%**	Developing	Some security oversight exists but ownership could be clearer. Ensure someone specific is responsible for security, even part-time, and that security gets discussed regularly at leadership level.
Staff Awareness Training your team to recognise and avoid common threats.	**53%**	Developing	Some security training has happened but knowledge needs reinforcing. Regular reminders about phishing, password security, and reporting suspicious activity help keep security front of mind for everyone.
Your Devices & Software Managing computers, phones and applications securely across your business.	**22%**	Gaps	Unknown devices and software on your network are hidden risks. You need a complete inventory—unauthorised or forgotten devices are often the weak point attackers exploit to gain access.

Redgum Property Group Improvement Plan

Redgum Property Group has 29 items that need attention. Work through at your own pace — start with high priority items.

Understanding Effort & Cost Estimates

Effort: Low = 1-4 hours (quick wins) • Medium = 1-2 days (may need help) • High = 1+ weeks (significant project)
Cost: Low = Free-$500 • Medium = $500-$2,000 • High = $2,000+

#	Gap	Priority	Effort	Cost	What To Do
1	No clear access rules	**High**	Low	Low	Write down basic rules about who should have access to what — who can see financial data, who has admin rights, who can access customer information. Clear rules help everyone understand expectations and make it easier to spot when something's wrong. Without documented rules, people make their own judgments, which often leads to over-sharing access or confusion about responsibilities. Start simple and refine over time.
2	Remote access not protected with 2FA	**High**	Low	Low	If staff access work systems from home or on the road, ensure they use 2FA (two-factor authentication - a second verification step via your phone). Remote access is a common target for attackers because it's exposed to the internet. Criminals actively scan for remote access points and try stolen passwords. 2FA adds vital protection that stops most of these attacks, even when passwords have been compromised through phishing (fake emails designed to trick you into revealing passwords or clicking dangerous links) or data breaches.
3	Update status not checked	**High**	Low	Low	Sometimes automatic updates fail, get postponed, or require a restart that never happens. Check every few months that all devices are actually up to date. Look for any that have fallen behind and fix them promptly. Many ransomware (malicious software that locks your files and demands payment) attacks succeed because a single machine missed critical updates. A quick monthly check of your devices' update status can prevent this common weakness from being exploited.
4	Backups not done	**High**	Low	Low	Set up automatic backups of your important data — customer information, financial records, business documents, and anything else you couldn't recreate. Backups are your safety net against ransomware (malicious software that locks your files and demands payment), hardware failure, accidental deletion, and theft. Without backups, a single ransomware attack could destroy years of work. Choose backup software that runs automatically so you don't have to remember, and verify it's actually working quarterly.
5	No firewall	**High**	Low	Low	A firewall (security software or hardware that blocks unauthorised network access) is your first line of defence, blocking unauthorised access attempts from the internet. Your router likely has a firewall built in — make sure it's enabled and configured properly. Check that only necessary ports are open and that remote management is disabled or secured. Without a firewall, your network is directly exposed to constant scanning and attack attempts from the internet.

#	Gap	Priority	Effort	Cost	What To Do
6	Insecure remote access	**High**	Low	Low	Remote access should use VPN (virtual private network - creates a secure, encrypted connection) or secure tools with 2FA (two-factor authentication - a second verification step via your phone), not just open ports on your router. Criminals actively scan for exposed remote desktop and other remote access services. Limit who can access remotely and to what systems. Log all remote sessions so you can detect suspicious activity. If suppliers need remote access, provide it only when needed and revoke it afterward.
7	No device inventory	**High**	Low	Low	Create a simple list of all business devices — computers, laptops, tablets, phones, and any other connected equipment. Include who uses each one, its location, and basic specifications. This helps ensure every device gets updated, protected with security software, and properly configured. Unknown devices on your network represent unmanaged risk. Update the list when devices are added, replaced, or retired.
8	Software not tracked	**High**	Low	Low	Keep a list of your software and cloud services — accounting, email, file storage, project management, industry-specific applications, and anything else your business relies on. Include login details stored securely in a password manager. This helps ensure everything stays updated, that accounts are disabled when staff leave, and that you know what's at risk if a service is compromised.
9	Critical systems not identified	**High**	Low	Low	Mark which systems are essential to your business. If your accounting system, customer database, or email was down, how would that affect you? Could you operate for a day? A week? Critical systems need extra protection: better backups, stronger access controls, and priority for updates. Understanding criticality helps you allocate limited security resources where they matter most.
10	No regular training	**High**	Low	Low	Regular training helps staff recognise scams, phishing (fake emails designed to trick you into revealing passwords or clicking dangerous links), and other threats that evolve constantly. Annual training keeps knowledge fresh and introduces new threats. There are many free resources available online, or consider a short workshop covering real examples relevant to your business. Make it engaging rather than a checkbox exercise — people remember stories and examples better than policies.
11	Reporting process unclear	**High**	Low	Low	Staff often spot problems first — a suspicious email, unusual system behaviour, or something that doesn't seem right. Make it easy to report concerns: who to tell, how to reach them, and that reporting is encouraged without blame even if it turns out to be nothing. Quick reporting helps contain incidents before they spread. Praise people for reporting, even false alarms.

#	Gap	Priority	Effort	Cost	What To Do
12	Staff can't recognise incidents	**High**	Low	Low	Staff need to recognise warning signs so they can report problems quickly. Cover common indicators: unexpected password reset emails, strange pop-ups or warnings, computers running unusually slowly, files they can't open or with strange extensions, unfamiliar programs running, or colleagues receiving suspicious emails from their account. Quick recognition means faster response and less damage. Share real examples of what incidents look like.
13	No incident plan	**High**	Low	Low	Know what to do before an incident happens — in the moment, you'll be stressed and rushed. Write down: Who to call first, immediate steps to contain damage, how to communicate with staff and customers, and when to engage external help. Even a simple checklist helps you respond faster and more effectively. Review it every few months so it's fresh in your mind.
14	Supplier access unknown	**High**	Low	Low	List all suppliers with access to your systems or data: IT support, accountant, cloud service providers, marketing agencies, payment processors, and anyone else who touches your information. Note what access each has and what data they can see. You can't manage supplier risk if you don't know who has access. This list is also essential for incident response.
15	Leadership commitment not shown	**High**	Low	Low	When leadership takes security seriously, everyone else does too. Make it clear to your team that security matters — mention it in meetings, ask about it in reviews, lead by example with your own practices. If the boss ignores security rules, why would anyone else follow them? Visible leadership commitment sets the tone for your whole organisation's security culture.
16	Responsibility unclear	**High**	Low	Low	Someone needs to be the go-to person for security questions and decisions, even if it's just part of their role alongside other responsibilities. Make it clear who this is so everyone knows who to ask, who to report issues to, and who has authority to make security decisions. Without clear ownership, security improvements tend to fall through the cracks.
17	Privacy compliance gaps	**High**	Medium	Low	Most countries have laws about handling personal information, including Australia's Privacy Act. Know the basics for your location: what you can collect and why, how to store it securely, when to delete it, and people's rights over their data. Have a privacy policy that explains your practices. Non-compliance can result in fines, reputational damage, and loss of customer trust. Consider getting professional advice for complex situations.
18	Email/downloads not scanned	**Medium**	Low	Low	Many threats arrive via email attachments or downloads from websites. Ensure your security software scans these automatically before they can cause harm. Most modern security software includes this feature — check that it's enabled. Some email providers also scan attachments in the cloud before delivery, adding another layer of protection. Be especially careful with unexpected attachments, even if they appear to come from known contacts.

#	Gap	Priority	Effort	Cost	What To Do
19	Software versions not tracked	**Medium**	Low	Low	Keep a simple record of what software versions you're running on important systems. This helps when security issues are announced for specific versions — you can quickly check if you're affected. Without this information, you may waste time investigating vulnerabilities that don't apply to you, or worse, miss ones that do. A spreadsheet listing key applications and their versions is often sufficient.
20	Recovery needs unknown	**Medium**	Low	Low	How long can you operate without your key systems? A few hours? A few days? Knowing this helps you choose appropriate backup and recovery approaches. If you need to be back online within hours, you'll need different solutions than if you can tolerate several days of downtime. Consider the financial impact of downtime, customer expectations, and regulatory requirements when setting your recovery objectives.
21	Settings may have drifted	**Medium**	Low	Low	Settings can drift over time — updates might change defaults, users might disable security features that annoyed them, or misconfigurations might creep in. Check security settings every few months, quarterly is a good rhythm. Look for anything that's been turned off, weakened, or changed from your standard configuration. Comparing current settings against your documented baseline makes this review straightforward and repeatable.
22	No change approval process	**Medium**	Low	Low	Have a simple process where significant changes to important systems get a quick check before they happen. Even just asking 'have you backed up first?' and 'who knows you're doing this?' helps prevent problems. For critical systems, ensure changes are planned, tested where possible, and that someone knows how to roll back if something goes wrong. This prevents well-intentioned changes from causing unexpected outages.
23	Changes not tested first	**Medium**	Low	Low	Before applying changes to systems you depend on, test them where possible. Try updates on one device first before rolling out widely. Make changes during quiet times when disruption would be less impactful. Have a plan ready if something breaks — know how to roll back. This approach balances making necessary improvements with avoiding self-inflicted outages that disrupt your business.
24	No rollback capability	**Medium**	Low	Low	Before making changes, know how you'd reverse them if things go wrong. Keep notes on original settings, maintain current backups, and test that you can actually roll back. For significant changes, document the specific steps to undo them. Being stuck with a broken system because you can't reverse a change is a preventable situation with a little advance planning.
25	Severity not understood	**Medium**	Low	Low	Not all incidents are equal. ransomware (malicious software that locks your files and demands payment) actively encrypting your systems needs immediate action. A suspicious email can wait a few hours. Help your team understand what needs immediate escalation versus what can be handled in normal course. Simple categories like 'drop everything' versus 'address today' versus 'investigate when convenient' help prioritise responses appropriately.

#	Gap	Priority	Effort	Cost	What To Do
26	No security plan	**Medium**	Low	Low	You don't need a fancy strategy document — even a one-page summary helps focus your efforts. Write down: What are our main security goals this year? What are we doing to achieve them? Who's responsible? What's our budget? Review and update it annually. Having a plan ensures security gets intentional attention rather than being purely reactive to problems as they arise.
27	Vulnerabilities not checked	**Medium**	Medium	Low	Vulnerability scanning can find weaknesses before attackers do. Many security tools include basic scanning features, and there are affordable options for small businesses. Consider having a professional do a more thorough security assessment annually, especially for internet-facing systems or those handling sensitive data. Scanning reveals not just missing patches but also misconfigurations and other weaknesses you might not know about.
28	Single layer of defence	**Medium**	Medium	Low	Don't rely on just one security measure. Combine security software with a firewall (security software or hardware that blocks unauthorised network access), strong passwords, 2FA (two-factor authentication - a second verification step via your phone), regular updates, and user awareness. Multiple layers mean attackers must get past several defences, and if one layer fails, others still protect you. Think of it like physical security: you have locks, perhaps an alarm, maybe cameras — each layer adds protection. The same principle applies to cybersecurity.
29	No resources allocated	**Medium**	Low	Medium	Security doesn't have to be expensive, but it needs some dedicated attention and occasional spending. Set aside a realistic budget for tools, training, and professional help when needed. Make sure someone has time allocated for security tasks — if security is always deprioritised for 'real work', improvements won't happen. Even a small, consistent investment compounds over time.

Risk Association

Understanding the specific risks associated with each gap helps prioritise your security investments.

#	Gap	Risk Level	Risk
1	No clear access rules	**High**	Unauthorised users may access sensitive business data and systems without proper controls in place.
2	Remote access not protected with 2FA	**High**	Remote connections are constantly scanned by attackers and represent a primary entry point for network breaches.
3	Update status not checked	**High**	Automatic updates can fail silently, leaving individual devices vulnerable while you assume they are protected.
4	Backups not done	**High**	Without backups, a ransomware attack, hardware failure, or accidental deletion could permanently destroy critical business data.
5	No firewall	**High**	Without a firewall, your network is directly exposed to constant automated scanning and attack attempts from the internet.
6	Insecure remote access	**High**	Exposed remote access services are constantly scanned by attackers and are among the most common breach entry points.
7	No device inventory	**High**	Unknown devices on your network cannot be secured, updated, or monitored, creating unmanaged security gaps.
8	Software not tracked	**High**	Untracked software and services may be unpatched, misconfigured, or abandoned with active credentials still in place.
9	Critical systems not identified	**High**	Without knowing what matters most, security resources may be spread thin rather than focused on critical assets.
10	No regular training	**High**	Without regular training, staff knowledge becomes outdated and they fail to recognise evolving threats like new phishing tactics.
11	Reporting process unclear	**High**	Security incidents that staff notice but don't report can spread and cause far greater damage before discovery.
12	Staff can't recognise incidents	**High**	Unrecognised incidents spread and cause more damage because staff don't realise something is wrong until it's too late.
13	No incident plan	**High**	Without a plan, incident response becomes chaotic and slow, allowing damage to spread while you figure out what to do.
14	Supplier access unknown	**High**	Unknown third-party access creates unmanaged risk and makes incident response impossible when you don't know who has access.
15	Leadership commitment not shown	**High**	Without visible leadership commitment, staff will not prioritise security and your security culture will remain weak.
16	Responsibility unclear	**High**	Without clear ownership, security tasks fall through the cracks and nobody takes responsibility for improvements.
17	Privacy compliance gaps	**High**	Privacy law violations can result in significant fines, regulatory action, reputational damage, and loss of customer trust.
18	Email/downloads not scanned	**Medium**	Email attachments and web downloads are primary delivery methods for malware, ransomware, and phishing attacks.
19	Software versions not tracked	**Medium**	Without version tracking, you cannot quickly determine if your systems are affected by newly announced vulnerabilities.
20	Recovery needs unknown	**Medium**	Without defined recovery objectives, your backup approach may not meet business needs when disaster strikes.

#	Gap	Risk Level	Risk
21	Settings may have drifted	**Medium**	Security settings degrade over time through updates, user changes, and misconfigurations that weaken your protections.
22	No change approval process	**Medium**	Unreviewed changes to critical systems can cause outages, security gaps, or data loss without anyone aware.
23	Changes not tested first	**Medium**	Untested changes can break critical systems, causing business disruption that could have been prevented.
24	No rollback capability	**Medium**	Without rollback capability, a failed change can leave you stuck with broken systems and extended downtime.
25	Severity not understood	**Medium**	Without severity levels, critical incidents may be treated casually while minor issues cause unnecessary panic.
26	No security plan	**Medium**	Without a plan, security efforts are reactive and ad-hoc, leaving systematic gaps that only become apparent during incidents.
27	Vulnerabilities not checked	**Medium**	Unknown security weaknesses in your systems provide attackers with entry points you are not aware of or protecting.
28	Single layer of defence	**Medium**	Relying on a single security control means one failure or bypass leaves your entire business exposed to attack.
29	No resources allocated	**Medium**	Without dedicated time and budget, security is constantly deprioritised and improvements never actually happen.

What To Do Next

Month 1-2: Quick Wins & Essential Fixes

Focus on high-impact items that are quick to implement:

- Turn on 2FA for email and key accounts
- Remove access for staff who have left
- Enable automatic updates everywhere
- Test your backups work

Month 3-4: Recommended Improvements

Build on your foundation with stronger practices:

- Document your security practices
- Set up basic monitoring and alerts
- Train staff on recognising threats
- Review supplier access

Month 5-6+: Maturity Building

Maintain and continuously improve:

- Review practices quarterly
- Address remaining lower-priority items
- Stay informed about new threats
- Re-assess in 6-12 months

Cyber Security Resources

These government and not-for-profit resources can help you implement improvements and stay informed about threats.

Australian Resources

Resource	What It Offers	Website
ACSC	Government advice, alerts, and free resources for businesses	cyber.gov.au
ACSC Small Business Guide	Step-by-step guidance tailored for small business	cyber.gov.au/smallbusiness
ReportCyber	Report cybercrime incidents to authorities	cyber.gov.au/report
OAIC	Privacy guidance and data breach notification requirements	oaic.gov.au
ACSC Essential Eight	Baseline security strategies recommended by Australian Government	cyber.gov.au/essential-eight
Scamwatch	Report and learn about current scams	scamwatch.gov.au
IDCARE	Free support service for identity theft and cyber fraud victims	idcare.org

United States Resources

Resource	What It Offers	Website
CISA	Cybersecurity & Infrastructure Security Agency — federal guidance and alerts	cisa.gov
NIST Cybersecurity	Cybersecurity Framework and best practice guidelines	nist.gov/cyberframework
FTC Business Guidance	Data security guidance for businesses	ftc.gov/business-guidance
IC3	FBI Internet Crime Complaint Center — report cybercrime	ic3.gov
StopRansomware	US Government ransomware resources and guidance	stopransomware.gov

United Kingdom Resources

Resource	What It Offers	Website
NCSC	National Cyber Security Centre — guidance and incident reporting	ncsc.gov.uk
NCSC Small Business Guide	Free cyber security guidance for small businesses	ncsc.gov.uk/smallbusiness
ICO	Information Commissioner's Office — data protection guidance	ico.org.uk
Action Fraud	UK national fraud and cybercrime reporting centre	actionfraud.police.uk

Resource	What It Offers	Website
Cyber Essentials	UK government-backed certification scheme	cyberessentials.ncsc.gov.uk

European Union Resources

Resource	What It Offers	Website
ENISA	EU Agency for Cybersecurity — guidance and threat reports	enisa.europa.eu
EDPB	European Data Protection Board — GDPR guidance	edpb.europa.eu
Europol EC3	European Cybercrime Centre — cybercrime reporting	europol.europa.eu

New Zealand Resources

Resource	What It Offers	Website
CERT NZ	New Zealand's cyber security agency — alerts and guidance	cert.govt.nz
Own Your Online	NZ Government cyber security awareness resources	ownyouronline.govt.nz
Privacy Commissioner	NZ privacy guidance and breach reporting	privacy.org.nz

Incident Response Contacts

Being prepared for a cyber incident means having key contacts ready before you need them. The Excel export includes an Incident Response Contacts worksheet with fields for your key service providers.

Key Contacts to Document

- Internal Security Lead — First point of contact for all security concerns
- IT Support Provider — Include after-hours/emergency number
- Cyber Insurance Provider — Policy number and incident hotline
- Legal Advisor — For breach notification and regulatory advice
- Bank Fraud Team — Fraud reporting hotline

Australian Government Contacts

- ACSC ReportCyber: 1300 292 371 / cyber.gov.au/report — Report significant cyber incidents
- OAIC: 1300 363 992 / oaic.gov.au — Notifiable data breach reporting
- IDCARE: 1800 595 160 / idcare.org — Free victim support for identity theft
- Scamwatch: scamwatch.gov.au — Report and learn about scams
- Australian Federal Police: 131 AFP (131 237) — Serious cybercrime

United States Contacts

- CISA: cisa.gov/report — Report cyber incidents to Cybersecurity & Infrastructure Security Agency
- FBI IC3: ic3.gov — Internet Crime Complaint Center for reporting cybercrime
- FTC: reportfraud.ftc.gov — Report fraud, scams, and bad business practices
- US-CERT: us-cert.cisa.gov — Security alerts and vulnerability information
- Identity Theft: identitytheft.gov — Federal resource for identity theft victims

United Kingdom Contacts

- NCSC: ncsc.gov.uk/report — Report cyber incidents to National Cyber Security Centre
- Action Fraud: 0300 123 2040 / actionfraud.police.uk — UK national fraud and cybercrime reporting
- ICO: ico.org.uk — Data breach reporting to Information Commissioner's Office
- Cyber Essentials: cyberessentials.ncsc.gov.uk — UK government-backed certification

European Union Contacts

- ENISA: enisa.europa.eu — EU Agency for Cybersecurity guidance and alerts
- Europol EC3: europol.europa.eu — European Cybercrime Centre for serious incidents
- EDPB: edpb.europa.eu — European Data Protection Board for GDPR guidance
- National DPAs: Contact your country's Data Protection Authority for breach reporting

Important: Print a copy of your completed contact list and keep it accessible even if your systems are down.

Regulations That May Apply

Businesses may be subject to various privacy and security regulations depending on their size, industry, location of customers, and the data they handle.

Australian Regulations

Privacy Act 1988 & APPs: Applies to businesses with turnover over $3M, health services, and some others. Requires privacy policy and appropriate handling of personal information.

Notifiable Data Breaches (NDB): Organisations covered by the Privacy Act must notify affected individuals and the OAIC when breaches are likely to cause serious harm.

SOCI Act 2018: Applies to critical infrastructure across 11 sectors. Requires incident reporting and risk management programs.

Industry-Specific: Financial services (APRA CPS 234), healthcare (My Health Records Act), government contractors (PSPF/ISM).

International Regulations

If you have US or European customers, you may need to consider: CCPA/CPRA (California), HIPAA (US healthcare), GDPR (Europe), UK GDPR. Each has specific requirements for data protection and breach notification.

Disclaimer: This is general guidance only, not legal advice. Regulations change frequently. Seek legal advice if you have international customers or operations.

Cyber Insurance Considerations

Understanding how cyber insurance fits into your overall risk management strategy.

What Cyber Insurance Covers

Typical policies cover incident response costs, business interruption losses, ransomware payments (where legal), legal fees, notification costs, regulatory fines, and third-party liability. Coverage varies by policy — always read the fine print.

Is It Right for Your Business?

Consider: What data do you hold? What's your industry risk profile? What's the financial impact of a breach? Businesses holding customer personal information or financial data should strongly consider cyber insurance.

How It Complements Technical Controls

Insurance is a risk transfer mechanism, not a replacement for security. Many insurers require baseline controls like 2FA, regular backups, and timely updates as conditions of coverage. Strong security may also reduce your premiums.

What Insurers May Ask

Common underwriting questions: Do you use MFA? Do you have regular backups? Do you have an incident response plan? Completing this assessment helps you answer these questions confidently.

Finding a Policy

Speak with an insurance broker who specialises in cyber or technology risks. Policies for small businesses typically range from $1,000–$5,000 AUD per year depending on coverage levels, industry, and your security posture.

Disclaimer: This is general information only, not insurance advice. Consult a licensed insurance professional for advice specific to your situation.

Glossary

Plain English explanations of terms used in this assessment.

2FA / Two-Factor Authentication

An extra security step when logging in. After entering your password, you also need a second thing — like a code sent to your phone or generated by an app. This means even if someone steals your password, they still can't get in without your phone.

Access Controls

Rules about who can use which systems and see which information. Good access controls mean people only have access to what they need for their job — not everything.

Admin Access / Administrator

A powerful account that can change settings, install software, and access everything on a computer or system. Because admin accounts can do so much, they're a prime target for attackers and need extra protection.

Backup

A copy of your important files stored separately from your main computer. If something goes wrong — like ransomware, accidental deletion, or hardware failure — you can restore your files from the backup.

Cloud Services

Software and storage that runs on the internet rather than on your own computers. Examples include Gmail, Dropbox, Xero, and Microsoft 365. You access them through a web browser or app.

Data Breach

When someone who shouldn't have access gets hold of personal or sensitive information. This could be through hacking, a stolen laptop, or even an email sent to the wrong person. Many jurisdictions require serious breaches to be reported to affected people and regulators.

Encryption

Scrambling information so only authorised people can read it. If an encrypted laptop is stolen, the thief can't read your files without the password. Most modern phones and computers can turn on encryption in their settings.

Security Framework

A set of guidelines that help organisations manage cyber security. Frameworks like Cyber Essentials (UK), the Security Basics (Australia), and NIST (USA) provide structured approaches to security. They typically cover basics like keeping software updated, controlling access, and using multi-factor authentication.

Firewall

A security barrier between your network and the internet. It blocks unwanted incoming connections while letting legitimate traffic through. Your home router has one built in, and Windows/Mac computers have software firewalls.

Incident

A security event that has caused or could cause harm to your business — like a virus infection, a successful phishing attack, or unauthorised access to your systems. Having a plan for handling incidents helps you respond quickly.

Malware

Malicious software designed to harm your computer or steal information. This includes viruses, ransomware, spyware, and trojans. Security software (antivirus) helps detect and remove malware.

Password Manager

An app that securely stores all your passwords so you only need to remember one master password. It can also generate strong, unique passwords for each account. Examples include 1Password, Bitwarden, and LastPass.

Patch / Update

A fix released by software makers to repair security holes or bugs. Installing updates promptly is one of the most important things you can do — many attacks exploit known problems that updates would have fixed.

Phishing

Fake emails, texts, or websites designed to trick you into giving away passwords, payment details, or other sensitive information. They often pretend to be from banks, delivery companies, or services you use. Always check the sender carefully.

Privacy Laws

Laws that control how businesses collect, use, store, and share personal information. Examples include GDPR (Europe), CCPA (California), and various national privacy acts. Check what rules apply in your location — most require you to have a privacy policy and handle personal data responsibly.

Ransomware

A type of malware that locks your files and demands payment (ransom) to unlock them. Even if you pay, there's no guarantee you'll get your files back. Good backups are the best defence — you can restore your files without paying.

Remote Access

The ability to connect to your work systems from outside the office — from home, a café, or while travelling. Because it opens a door into your network, remote access needs strong protection like VPNs and two-factor authentication.

Security Software / Antivirus

Programs that protect your computer by detecting and removing malware, blocking dangerous websites, and watching for suspicious activity. Windows Defender comes free with Windows; other options include Norton, Bitdefender, and Malwarebytes.

VPN (Virtual Private Network)

Creates a secure, encrypted tunnel for your internet connection. When working remotely, a VPN protects your data from being intercepted, especially on public WiFi. It's like a private pipe between your device and your office network.

Vulnerability

A weakness in software or systems that attackers could exploit to break in. Software makers release patches to fix vulnerabilities when they're discovered. Keeping software updated closes these security holes.

— End of Report —