TECHNOVATE
IT SOLUTIONS

CYBERSECURITY ESSENTIALS FOR SMES

Protect Your Data in 2025

WWW.TECHNOVATEIT.COM.AU

INTRODUCTION

TECHNOVATE
IT SOLUTIONS

Cyber threats in 2025 are more advanced, targeted, and automated than ever before. While large enterprises often have mature security programs and full-time security teams, small and medium businesses remain the most vulnerable — and the most targeted.

We seen how a single phishing attack, misconfigured cloud bucket, or insider error can bring operations to a halt — or worse, permanently damage a business's reputation.

This guide is your practical, business-friendly cybersecurity roadmap, designed for SMEs with limited resources but high digital exposure.

UNDERSTAND THE THREAT *LANDSCAPE*

What’s Changed:

- AI-Powered Attacks: Cybercriminals use generative AI to launch highly convincing phishing, deepfake videos, and synthetic voice scams.
- Ransomware-as-a-Service (RaaS): No coding skills needed — criminals can buy ransomware kits to target businesses like yours.
- Supply Chain Vulnerabilities: Attacks often originate from third-party providers, integrations, or plugins you trust.

Why SMEs are Targeted:

- Less likely to have 24/7 security monitoring
- Undertrained employees and weak access controls
- Use of outdated or unsupported software

Key Insight: Attackers don’t care about your size. They care that you're exposed.

PERFORM A CYBER RISK *ASSESSMENT*

Step-by-Step Risk Discovery:

Identify Digital Assets

Servers, laptops, phones, cloud apps (e.g. Microsoft 365, Xero), customer databases.

Classify Data by Sensitivity

- Public (e.g. marketing brochures)
- Internal (e.g. staff memos)
- Confidential (e.g. payroll, customer data)

Assess Threats & Vulnerabilities

1. **Use free tools like:**
   - **Qualys FreeScan**
   - **Microsoft Secure Score**

Evaluate Business Impact

What happens if systems go down for 24 hrs? What if client data is breached?

Document Risks

Use a Risk Register to track threats, likelihood, impact, and mitigation.

Tool Provided: Cyber Risk Register Template in Toolkit

STRENGTHEN YOUR CORE *DEFENSES*

Control	Action	Free/Low-Cost Tools
🔑 Password Security	Use password managers, enforce complexity	Bitwarden, 1Password Teams
🔒 Multi-Factor Authentication	Enable MFA for all users and apps	Microsoft Authenticator, Google Auth
🔍 Endpoint Protection	Use advanced antivirus + threat detection	Sophos, SentinelOne, CrowdStrike
☁️ Secure the Cloud	Disable public file sharing, configure access logs	Microsoft 365 Secure Score
🔄 Patch Management	Automate OS and software updates	WSUS, PDQ Deploy
🔥 Firewalls	Use both network and local firewalls	FortiGate, pfSense

TRAIN YOUR PEOPLE

YOUR FIRST LINE OF DEFENSE

Why It Matters

Over 85% of breaches involve human error. Staff must recognize:

- Phishing emails
- Social engineering attempts
- Suspicious links or attachments
- Secure ways to share files and data

Build a Culture of Cyber Awareness

- Monthly phishing simulations
- Quarterly security awareness training
- (use platforms like KnowBe4, Infosec IQ, or Microsoft Defender for Business)
- Cybersecurity policy onboarding for new hires
- Create a no-blame reporting culture — encourage employees to report suspicious activity

BACKUPS & BUSINESS *CONTINUITY*

Backup Best Practices (3–2–1 Rule)

- 3 copies of your data
- 2 stored on different media
- 1 stored off-site or in the cloud

✓ Automate daily backups
✓ Test restores quarterly
✓ Encrypt backup data
✓ Don’t store backups on the same network as live systems

Pro Tip: Ensure backup systems are isolated from ransomware threats (air-gapped or immutable backups).

BUILD A BASIC INCIDENT *RESPONSE PLAN*

Even if you're not a security expert, having a simple, tested response plan can limit damage.

Incident Response Template

1. Identify – How was the issue detected?
2. Contain – Isolate affected devices or accounts
3. Notify – Inform management, affected users, and external providers
4. Eradicate – Remove malware, block attackers, patch vulnerabilities
5. Recover – Restore from backup
6. Review – Conduct post-mortem and update policies

Bonus: Include who to call (e.g. your IT provider, MSP, legal advisor, insurer)

VENDOR & SUPPLY CHAIN *RISK*

Why It's Critical
Your security is only as strong as your weakest third-party link.

Checklist:

- Maintain a vendor register with contact, services, access levels
- Ensure vendors sign a Data Processing Agreement (DPA)
- Ask vendors about their own security posture (SOC 2, ISO 27001, etc.)
- Limit vendor access to only what's necessary
- Disable vendor access when contracts end

COMPLY WITH CYBER *REGULATION*

In Australia, SMEs are subject to the following cybersecurity and privacy regulations:

- Privacy Act 1988 (incl. Notifiable Data Breaches scheme)
- Australian Cyber Security Centre (ACSC) Essential Eight (Baseline)
- ISO 27001 (if dealing with sensitive or international clients)
- PCI DSS (for handling card payments)

Stay Compliant By:

- Maintaining privacy policies
- Enabling MFA and logging
- Reporting notifiable data breaches within 72 hours

MEASURE AND *IMPROVE*

Key Cybersecurity KPIs:

- % of users who fail phishing tests
- % of systems with unpatched software
- % of staff completing training
- RPO (Recovery Point Objective) / RTO (Recovery Time Objective)
- Number of detected threats per month

Quarterly Review Questions:

- Have we had any incidents or near misses?
- Are our backups working?
- Are employees following security protocols?
- Do we need to update our policies or tools?

In 2025, cybersecurity is not optional — it’s foundational to business resilience. SMEs don’t need million-dollar security budgets to stay safe. With the right plan, the right culture, and a trusted IT advisor, you can significantly reduce your risk of attack.

At Technovate IT Solutions, we help SMEs implement tailored, scalable cybersecurity programs that align with your budget, your goals, and your regulatory requirements.

TECHNOVATE
IT SOLUTIONS