CYBER RESILIENCE CHECKLIST

Who's checking the checker?

Cyber resilience isn't just IT—it's business survival. **60% of SMEs never recover from a cyber breach.** Your IT provider plays a role, but the ultimate risk is **yours**. If they miss something critical, you won't know until it's too late. This checklist helps you stay in control and outlines who's responsible for what.

SECURITY CONTROL	WHO IS RESPONSIBLE	CHECKED
1. ACCESS & AUTHENTICATION SECURITY		
Use **Multi-Factor Authentication (MFA)** on all critical accounts - email, remote access, admin accounts.	Business Owner	□
Ensure employees use **strong, unique passwords** - consider a **password manager**.	Business Owner	□
Remove or disable **unused user accounts** immediately e.g. after an employee leaves.	MSP/IT Provider	□
Limit **administrator privileges** - employees should only have access to what they need.	MSP/IT Provider	□
2. EMAIL & PHISHING PROTECTION		
Train staff to **identify phishing emails** and social engineering attacks.	Business Owner	□
Enable **email filtering** to block spam, malicious links, and attachments.	MSP/IT Provider	□
Set up **DMARC, SPF, and DKIM** records to prevent email spoofing.	MSP/IT Provider	□
3. DEVICE & SOFTWARE SECURITY		
Keep **all software and operating systems updated** (patch regularly).	MSP/IT Provider	□
Uninstall **unnecessary or outdated applications**.	MSP/IT Provider	□
Use **endpoint protection (antivirus/EDR)** on all devices.	MSP/IT Provider	□
Restrict **USB usage** and external storage devices to prevent malware infections.	Business Owner	□
4. DATA PROTECTION & BACKUPS		
Back up critical data regularly and store backups offline.	MSP/IT Provider	□
Encrypt sensitive data to prevent unauthorised access.	MSP/IT Provider	□
Restrict access to critical files using **role-based permissions**.	MSP/IT Provider	□
5. NETWORK SECURITY		
Ensure **firewalls** are enabled and configured correctly.	MSP/IT Provider	□
If using **remote access (VPN, RDP)**, ensure it's secured with MFA.	MSP/IT Provider	□
Separate guest Wi-Fi from business **Wi-Fi networks**.	MSP/IT Provider	□
6. INCIDENT RESPONSE & CYBER INSURANCE		
Have a **cyber incident response plan** (know what to do if an attack occurs).	Business Owner	□
Subscribe to **ACSC alerts** to stay updated on threats (cyber.gov.au).	Business Owner	□
Consider **cyber insurance** to mitigate financial risk from cyber attacks.	Business Owner	□

Your provider may be responsible for managing your IT, but that doesn't mean they're perfect or that every vulnerability is caught. *Who's checking the checker?* Blind trust is a risk but an independent review ensures nothing is overlooked.

Contact us for an objective cybersecurity review—because If **they** miss something, it could cost **you** everything.
cyber@focusnet.com.au