Cyber Security Action

As technology evolves, so does the risk of becoming a victim of cybercrime. Cyber criminals will exploit loopholes and vulnerabilities in your business's technology systems with the aim of disrupting operations or accessing sensitive data.

It is vital that SMEs and NFPs take action to reduce cyber risk.

There are a range of tools and resources available to help boost your cyber security practices.

✓ As a starting point, we suggest businesses review the following Cyber Security Checklist[1], adapted from best practice guidance.

The Australian Cyber Security Centre (ACSC) Cyber Security Assessment Tools will also help you identify strengths and potential gaps. This includes:

✓ Benchmark your current practices against the Essential Eight 'baseline' mitigation strategies
✓ Develop and test your business's cyber threat response using the Exercise in a Box tool

We recommend you undertake a **Cyber Resilience Health Check** or **Cyber Security Internal Audit** to fully assess your business's security environment against best practice frameworks. The resources provided here are not intended to be exhaustive. A Synectic adviser can help you consider your business's unique needs – contact us to get started.

Contact Synectic

Cyber Security Checklist

1. Most important measures, which you should aim to have in place at minimum

Are your systems up to date?	Yes / No	This includes software, operating systems, and hardware (including network equipment)**.** Ensuring systems and up-to-date and patched improves and enhances security. It is important not to overlook hardware as well as software. As there are multiple layers and levels to updating hardware, this may be best carried out by an IT professional.
Do you have anti-virus software installed and up to date?	Yes / No	Viruses and other malicious software (known as malware) present a constant threat to the cyber security of systems, so it is important to have reputable anti-virus software installed and set to automatically updated.
Do you use a password manager?	Yes / No	Using a password manager to store passwords and help you create unique passwords with non-traditional characters, and ensure they are stored in an encrypted location, increases your chances of surviving a dictionary attack[2].
Have you enabled multi-factor authentication (MFA) where available?	Yes / No	Multi-factor authentication is when you are required to use more than one means of verification to access data or systems. In addition to a password, being asked for an additional authentication factor increases security and makes it harder for an attacker to gain access.
Is everyone in your organisation aware of and educated in cyber security?	Yes / No	All staff should have a satisfactory level of knowledge of cyber security and undergo training on a regular basis, so they are alert to potential threats. Training should start during the onboarding process and remain an ongoing area of education for staff.
Do you conduct ongoing training on your cyber policies for staff?	Yes / No	Having policies and providing staff training are two key parts of a cyber security strategy. Additionally, you should have a cyber security incident response plan to assist your business and staff in the event of an attack or breach.
Do your suppliers and third parties in your supply chain have cyber security measures in place?	Yes / No	A third-party in your supply chain with poor cyber security practices presents a risk to your business and includes both outsourcing and offshoring arrangements.
Do you regularly make backups of your data and test if they can be restored?	Yes / No	It's important to know what data you have collected, where it is stored (jurisdiction), and what laws and regulations apply to this data. It is also important to have the data backed up and restorable in case of loss.
Do you have cyber insurance?	Yes / No	In the event of a cyber-attack, an insurer could help you mitigate the impact to your business. Cyber liability insurance can offer coverage for third-party cyber liability, first party hacker damage, cyber extortion, public relations expenses, business interruption and data breach notification.

2. Measures you should focus on once you have addressed category 1 measures

Can you identify a phishing attack[3]?	Yes / No	If you can identify a malicious email, text message or voice message you greatly reduce your chances of inadvertently actioning malware.
Do you limit administrative privileges and access to sensitive information?	Yes / No	Have you considered who in your business has access to sensitive information and systems and if it is required for their job? A key step to minimising the damage from a potential cyber-attack is to ensure access to your administrator accounts is limited in case they become compromised.
Do you use a Virtual Private Network (VPN)?	Yes / No	VPNs encrypt internet traffic in real time and disguise online identify making it harder for threat actors to track your activities online and steal your data. VPNs are a vital privacy tool, especially when working remotely, such as in places that offer access to free public Wi-Fi.
Do you disable Microsoft Office Macros?	Yes / No	Macros are programming code that you can add to Microsoft Office applications, such as Excel, to automate repetitive tasks. Macros can contain malicious code, which may result in unauthorised access to sensitive information as part of a targeted cyber-attack.
Could any software application run on your computer?	Yes / No	'Application control' is designed to protect against malicious software by ensuring only approved applications and software can be executed on your computers. It includes controlling who can access, install and modify programs, how controls are implemented, maintained and modified, as well as the controls themselves and their implementation.

3. Measures which demonstrate best practice and ensure the strongest defence

Have you tried to conduct a penetration test?	Yes / No	'Penetration testing' can help you understand your vulnerabilities and provide actionable steps to improve your security standpoint. Any identified weaknesses or issues during the penetration test should be rectified as a matter of urgency. Note: Make sure you conduct your own research to identify your own goals and end results from the conducted test and ensure the engagement is clearly detailed, with a reputable vendor.
Are you able to identify all the hardware devices in your workplace?	Yes / No	Bring Your Own Devices (BYOD) practices can increase the risk of a cyber-attack. Remote working also increases the likelihood, especially if the risk is not managed appropriately. Personal devices are more vulnerable to an attack or being misplaced.
Do you limit Wi-Fi access?	Yes / No	Could anyone access your network and devices? Wi-Fi networks and passwords should be considered sensitive business information, only provided to those who absolutely require it. To further enhance this security measure, rotate your network password to ensure any redundant devices or associates no longer have unnecessary access. Additionally, set-up guest networks to limit the ability of users to access devices they should not.
Do you encrypt your data?	Yes / No	Encryption scrambles data into a code which requires a secret key or password to crack, and ensures data is not readable by those who do not have the key. This is an additional measure to protect the security of data your business holds. If encrypted data were to fall into the wrong hands, the hacker would not be able to read it.
Do you enable user application hardening?	Yes / No	'User application hardening' refers to turning off unnecessary features in applications to secure against malicious code. Flash, advertisements and Java, for example, are popular ways to deliver and execute malicious code on systems.

[1] Adapted from CPA Australia's Cyber Security Checklist and other best practice guidance published by the Australian Cyber Security Centre (www.cyber.gov.au) including the Essential Eight Maturity Model.

[2] 'Password dictionaries' are long lists of commonly-used passwords and character combinations used by attackers to guess passwords and break into systems.

[3] A 'phishing attack' is a malicious email designed to look like a legitimate email to obtain user engagement to steal information or infect a device with malware. Business email compromise (BEC) is a significant cyber threat. It is critical that all email users can identify a phishing attempt or know when to seek guidance.