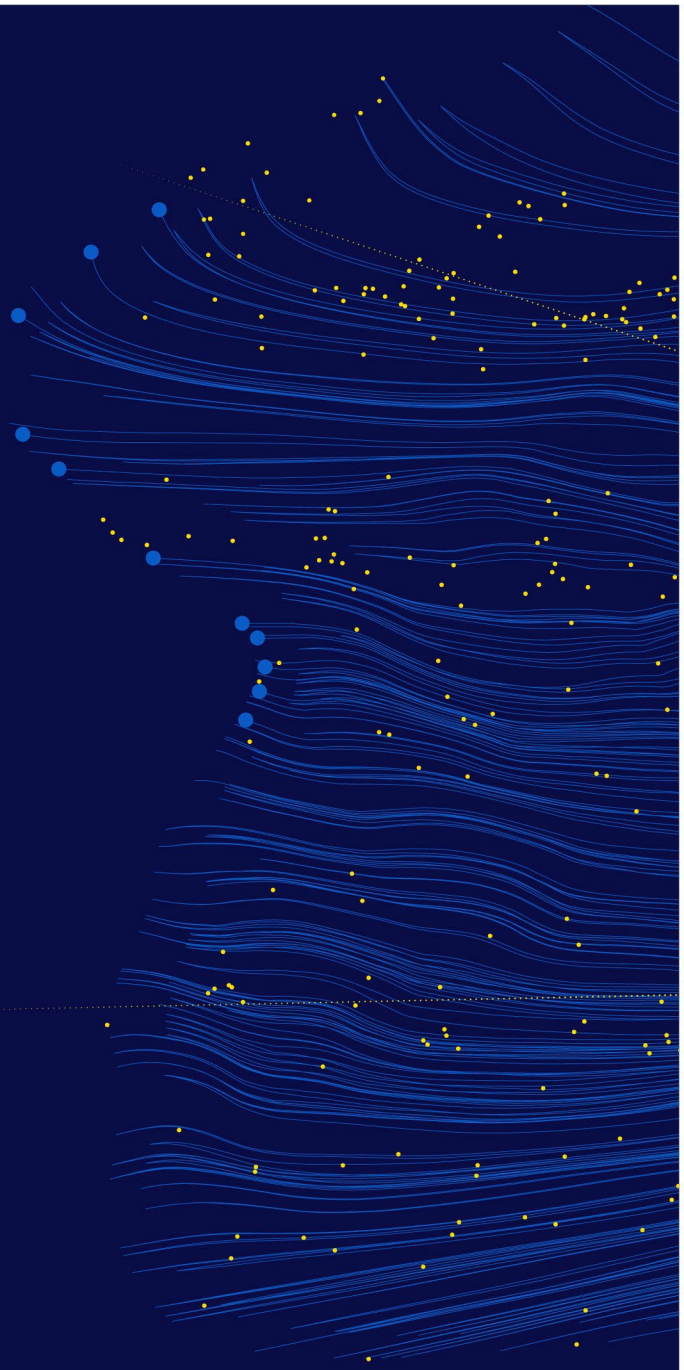

Cyber security checklist

Practical guidance for CPA Australia member

CPA AUSTRALIA

Cyber security checklist

The following version control information has been included to assist you to monitor changes to the checklist to ensure you are using the latest version.

Document Title	Cyber security checklist	Version #	4
Effective Date	September 2024		

Version #	Change Description	Introduced
1	Original document	July 2022
2	New red item ‘Do you know what data you collect?’ added. Item ‘Do you encrypt your data?’ is now classed as a red item instead of green. Item ‘Do you limit administrative privileges and access to sensitive information?’ now classed as a red item instead of orange. Item ‘Do you enable application control?’ now classed as a red item instead of orange. New information about end of support dates added to item ‘Are your systems up to date?’ New information added to item ‘Do you use a password manager?’	October 2022
3	Amended existing links. New link for ACSC Exercise in a Box added to item ‘Is everyone in your business aware of and educated in cyber security? Do you conduct ongoing training on your cyber security policies for your staff?’ New links to ACSC Small Business Cloud Security guides added to item ‘Do you back up your data?’ New link to ACSC Scams page added to item ‘Can you identify a phishing attack?’ New link to ACSC Secure Administration page added to item ‘Do you limit administrative privileges and access to sensitive information?’ New link to ACSC guidance on mitigating Java-based intrusions for item ‘Do you enable user application hardening?’	September 2023

4	Amended existing links. New link to ACSC guidance on multi-factor authentication page for item ‘Have you enabled multi-factor authentication (MFA) where available?’ New link to ACSC guidance on hardening Microsoft Windows 10 and 11 workstations for item ‘Do you enable user application hardening?’ Removed link to ACSC guidance on mitigating java based intrusions for item ‘Do you enable user application hardening?’	September 2024

Introduction

Protect yourself and your business against cyber security threats

As technology evolves, so does the risk of becoming a victim of cybercrime.

Cybercriminals seek to exploit loopholes and vulnerabilities in your technology systems to disrupt business operations and access sensitive data for profit.

This checklist is designed to help you review your systems and suggest cyber security measures you can implement to reduce the risk to yourself, your business, clients and others in your supply chain.

How this checklist works

Each cyber security measure in this checklist uses a traffic light system:

Red - these are the most important cyber security measures for you and your business, you aim should be to answer YES to all of these questions.

Orange - you should focus on these measures once you have addressed all red measures.

Green - demonstrate strong cyber security skills and ensure you have a strong defense against a potential cyber security attack.

Each measure in the checklist includes guidance and useful links to resources if you need further assistance to implement that measure, including links to the Australian Cyber Security Centre (ACSC) resources.

You can also engage a cyber security professional or external IT consultant for further support for you or your business.

TIP: Before you begin, we recommended you have the following information on hand:

- List of all the software applications you use
- List of all the hardware devices in your office and / or used by your team from home
- List of all your staff, contractors and suppliers including their level of access to your technology and systems
- When your last three back-ups were conducted, including if they were offline / online and contain all the essential information and files you need to run your business

This checklist is a brief introduction to the world of cyber security. To build your cyber security knowledge CPA Australia offers four one-hour cyber security eLearning modules that will help you understand cyber risk, how to build your cyber security strategy, respond to a cyber threat and explore your business obligations relating to your data.

These red measures are for the most important cyber security – you should aim to achieve all of these measures for your business at a minimum.

Are your systems up to date?	YES	NO
This includes your software, operating systems and hardware (including network equipment).		

An update or patch to your existing software programs and operating systems improves and enhances security. You can adjust the settings to have updates completed automatically or set to a scheduled time to minimise disruption to your business. Software that has reached its end of support (expiry) date do not receive any updates and should be replaced as soon as possible, as cyber criminals target vulnerabilities in unsupported software.

In addition to having your software up to date, it is important not to overlook your hardware. At minimum, you should regularly update all hardware you directly own to avoid any vulnerabilities that could be exploited, including network printers and routers. As there are multiple layers and levels to updating your hardware, this may be best carried out by an IT professional.

Find out more:

- Read: Australian Cyber Security Centre (ACSC) information on updates and follow links to instructions on updating for Windows, Apple, Android and other devices and software.
- Read: ACSC: Quick Wins for your End of Support

Do you have anti-virus software installed and up to date?	YES	NO
Could viruses be present on your computer without you knowing this?		

Viruses and other malicious software (known as malware) present a constant threat to the cyber security of your systems, so it is important to have anti-virus software installed and set to automatically update.

Find out more:

- See examples of anti-virus software: Cyber security: Top tips for remote workers.
- Learn about different types of malware in the MY FIRM. MY FUTURE eLearning module, **Evaluating Cyber Risk**.

Do you use a password manager?	YES	NO
Passwords should be unique, complex, long and never reused across multiple log-ins.		

Using a password manager to securely store passwords and help you create unique passwords with non-traditional characters increases your chances of surviving a dictionary attack. A reputable password manager will ensure passwords are stored in an encrypted location, be that locally or utilising their servers. Be sure to also replace any default passwords for new software and devices, such as your Wi-Fi modem and router.

Find out more:

- Read: INTHEBLACK: Password protection in the cloud accounting era.
- Read: INTHEBLACK: Everything you've been told about passwords is wrong.

Have you enabled multi-factor authentication (MFA) where available?	YES	NO
Multi-factor authentication is an additional layer of security you should apply to your accounts.		

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, which is *something you know*, being asked for an additional authentication factor increases security and makes it harder for an attacker to gain access. The extra authentication factor can be *something you have* (like a mobile phone that receives one-time codes via text message or mobile application) or *something you are* (a biometric feature such as a fingerprint, or face or voice recognition).

Find out more:

- Read: ACSC: Protect yourself: Multi-Factor Authentication (user and email accounts, financial services, online shopping, social media and communication, government services and gaming accounts),

Is everyone in your business aware of and educated in cyber security? Do you conduct ongoing training on your cyber security policies for your staff?	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 cyber threats.		

Cyber security awareness training for all staff should start during the onboarding process and remain an ongoing area of education for staff.

There are resources to help you draft your cyber security training policy, which should include education on what accesses are removed when an employee leaves your business, rules around Bring Your Own Devices (BYOD) and remote working. If you live or conduct business outside of Australia, you should also familarise yourself with the relevant guidance of that particular region.

Having policies and providing staff training are two key parts of a cyber security strategy. Additionally, you should also have a cyber security incident response plan to assist your business and staff in the event of an attack or breach.

Find out more:

- Tips on creating a cyber security-conscious culture in the workplace.
- Australian Government resource: Create a cyber security policy.
- Learn to build a cyber security strategy: MY FIRM. MY FUTURE eLearning module, **Building a cyber security strategy**.
- Learn how to create a cyber security incident response plan: MY FIRM. MY FUTURE eLearning module, **Responding to cyber threats and breaches**.
- Practice your response to different types of cyber threats using ACSC: Exercise in a Box

Do your suppliers and other 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.		

It's important to know if a third-party in your supply chain has adequate cyber security measures in place, especially if they have access to your data. This includes suppliers and parties who are part of any outsourcing or offshoring arrangements you may have.

In the event of cyber attack to the third-party, it opens up your risk of your business in turn being targeted.

Find out more:

- Learn more in the MY FIRM. MY FUTURE eLearning module, **Protecting Your Data: Your Business Obligations**.

Do you know what data you collect?	**YES**	**NO**
Are you required to retain certain information, and should a breach occur, do you know what data you've lost and the associated risks?		

A data breach can happen to anyone. As a business owner, it's important to know if you collect any personal data, why you collect it, what laws and regulations apply to it and ensure it is handled securely from the start (at point of collection) to end (when it is de-identified or securely destroyed).

Never collect personal information or data that is not needed for a business function or is no longer required to be kept.

Find out more:

- Read: Office of the Australian Information Commissioner website: Guide to securing personal information
- Learn more in the MY FIRM. MY FUTURE eLearning module, **Protecting Your Data: Your Business Obligations**.

Do you encrypt your data?	**YES**	**NO**
If your data falls into the wrong hands, would it be unreadable?		

Encryption scrambles data into a code that 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.

Ensure data is encrypted at rest, when being transmitted and in backups.

Do you back up your data?	**YES**	**NO**
Do you regularly make backups of your data and test if they can be restored?		

In addition to knowing what data you collect, you need to know where it is stored (jurisdiction) and if this means there will be any additional regulations applicable to the data. It is important to have data backed up and restorable in case of loss.

Backups can be stored offline and online (in the cloud). Aim to have at least one copy of your data accessible always - offline, and in a separate location, in case of a cyber attack to your systems.

Having automatic cloud backups of your data can avoids the risks of forgetting to do this manually. However, these files may become corrupt in the event of a cyber attack, so it is also good practice to

regularly back up your data offline. You should also regularly test your backups to ensure your data can be restored in event of a loss or breach.

If you are storing data in the cloud you need to know where this is being stored (country or state), noting this can be in different locations, and how it is managed such as will you have access to back-ups or will be notified if there is a breach.

Remember you are still responsible even if you are using a third-party provider.

Find out more:

- Have a look at some suggested questions to ask your cloud providers to manage the risk. For further reading, refer to APES 305: Terms of Engagement and a Practice Note from the Tax Practitioners Board in relation to Cloud computing and the Code of Professional Conduct. The ACSC provides information on back-ups and links to step by step guides on how to back up and restore files for Microsoft Windows 10, 11 devices, OneDrive and Apple iOS and macOS.
- The ACSC also provides considerations for backups for Microsoft 365 as part of their Small Business Cloud Security guidance.

Do you have cyber insurance?	**YES**	**NO**
Accountants are at high-risk of experiencing a cyber attack. 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.

In the event of a cyber attack, the insurance company will have consultants from legal, IT and PR firms to assist you and lessen the impact and aid your recovery. However, it is important to note that you will need to adhere to requirements set by the insurer to be eligible to make a claim.

Find out more:

- Read: INPRACTICE: Cybercriminals target accounting firms.

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. Administrator accounts have the authority to control the computer and carry out actions such as installing software, so it is important these privileges are only granted to those who absolutely require it.

A user account does not have complete control over the computer and is therefore more appropriate for everyday use and for employees who do not require full privileges.

Find out more:

- Learn: ACSC: Managing user accounts
- Read further: ACSC: Secure Administration

Do you enable application control?	YES	NO
Could any software application run on your computer?		

Application control is a security measure 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 these programs, how controls are implemented, maintained, and modified, as well as the controls themselves and how they are implemented. Start with an inventory of the applications you have and who is required to use them in your business.

Find out more:

- Read: ACSC: Implementing Application Control.

Orange items are ones that should be targeted next ideally once all red items have been completed.

Can you identify a phishing attack?	YES	NO
If you are able to identify a malicious email, text message or voice message you greatly reduce your chances of inadvertently actioning malware.		

A phishing attack is a malicious email that is designed to look like a legitimate email in order to obtain user engagement to steal information or infect a device with malware.

Business email compromise is a significant cyber threat, so it is important that all of your internal stakeholders can identify or seek guidance if there is a phishing attempt to ensure your data remains safe and secure.

Find out more:

- Learn: ACSC: Business email compromise.
- Learn: ACSC: What is phishing and what to do if you've been targeted.
- Read about other types of scams: ACSC: Scams
- Use: ACSC: Practical email security guides.

Do you use a Virtual Private Network (VPN)?	YES	NO
A VPN is essential to protect your web usage from nefarious snoopers.		

VPNs encrypt internet traffic in real time and disguise online identity. This makes 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. All devices, including mobile phones, should be protected with a VPN. Many VPNs can be purchased via a subscription.

Do you disable Microsoft Office macros?	YES	NO
Microsoft Office files can have macros that run malicious code.		

Macros are programming code that you can add to Microsoft Office applications, such as Excel, to automate repetitive tasks. However, macros can contain malicious code, which may result in unauthorised access to sensitive information as part of a targeted cyber attack.

To protect your business against malicious macros, ACSC recommends that you implement one, or a combination, of the following approaches:

- disable macros for users that do not have a demonstrated business requirement
- only enable macros from trusted locations
- only enable macros digitally signed by trusted publishers.[1]

Find out more:

- Read: ACSC: Microsoft Office Macro Security

Green items demonstrate strong cybersecurity skills and defense against a potential attack.

Have you tried to conduct a penetration test?	YES	NO
Understand your vulnerabilities by paying a professional to attempt to infiltrate your network and steal your data.		

You may wish to consider testing your overall security position by having ethical hacker from a reputable cyber security firm attempt to attack your systems and information. This is known as a penetration test. You are then provided with actionable steps to improve your security standpoint.

Conduct your own research to identify your own goals and end results from the conducted test; and ensure that the engagement is clearly detailed, with a reputable vendor. Any identified weaknesses or issues during the penetration test should then be rectified as a matter of urgency.

Are you able to identify all of the hardware devices in your workplace?	YES	NO
Bring Your Own Devices (BYOD) can increase the risk of a cyber attack occurring.		

BYOD to the workplace and remote working increases the likelihood of a cyber attack occurring, especially if the risk is not managed appropriately. In addition to the above measures, another way to mitigate risk for your employees is to have work devices that are separate from their personal devices and used for business activities only. This keeps your sensitive business data off personal devices – devices that are more vulnerable to an attack or being misplaced.

While ownership of all hardware is expensive, it could cost less than the damage caused by a cyber attack that breaches client data, leaves systems unusable or puts your business out of action for a long period of time.

Find out more:

- Read: INTHEBLACK: Safe from harm: online security when working remotely.

[1] © Commonwealth of Australia 2020. "Microsoft Office Macro Security" Australian Cyber Security Centre, last updated October 2021, https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

Do you limit Wi-Fi access?	YES	NO
Could anyone access your Wi-Fi network and devices?		
Consider your Wi-Fi network and password as sensitive business information only to be 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. Find out more: • Learn: ACSC: Secure your Wi-Fi and router.		
Do you enable user application hardening?	**YES**	**NO**
Have you stopped malicious code from running on applications?		
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. Find out more: • Read: ACSC: Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016 and ACSC: Hardening Microsoft Windows 10 and Windows 11 Workstations •		

Further notes and resources

This checklist is designed to provide you with some practical steps to help protect your business from a cyber attack.

There may be local legislative obligations that will also apply, influenced by the services you provide, location of your business or where you provide services to. You must be aware of and comply with your applicable legislative obligations.

You should also report any cybercrimes or data breaches to your relevant body as required. For further information, refer to the links below:

Australia

- Australian Cyber Security Centre
- If obligated under the Privacy Act 1988 (Cth), report data breaches to the Office of the Australian Information Commissioner (OAIC).

New Zealand

- New Zealand National Cyber Security Centre
- If obligated under the Privacy Act 2020, report data breaches to the New Zealand Privacy Commissioner.

Further resources

- MY FIRM. MY FUTURE Cyber security modules
- Cyber liability insurance
- Cyber security resources and support.