CyberUP
powered by theprojectlab

Your assessment and recommendations

Starter Developing Graduate Champion

Based on your responses, your cyber security maturity and knowledge level is **Starter**.

Your business is in the early stage of its cyber security journey. You need to focus on putting into place some basic measures to have a more effective approach to cyber security.

Key actions

- Undertake the recommendations in this report
- **Redo this survey again in 12 months** – to view your maturity level after you take steps to improve your approach to cybersecurity. Cyber security is constantly evolving and needs to continually address newly emerging threats.
- **Speak to your IT support person/team** – about actioning the recommendations in this report.
- **Good** resources **to share with staff** are provided by the Australian Cyber Security Centre, who offer guides and reference information for businesses of all sizes.
- The Small Business Cyber Security Guide may be particularly helpful.

Recommendations

Each recommendation below lists everything that needs to be actioned in order to reduce your risk of a cyber security threat for this topic. Make sure you review each recommendation in detail to understand which actions you may have already applied and which actions we recommend you still need to apply.

For action now

- Use multi-factor authentication
- Test your business' backups on a regular basis
- Use strong passwords
- Control or manage software installation

For action next

- Detect cyber security issues in your internal IT systems
- Handle sensitive client, business and staff information securely
- Use secure methods to share confidential or sensitive information
- Provide staff cyber security awareness training

For action later

- Carry out regular security testing
- Understand your business' compliance obligations
- Keep your business mobile phones, laptops and tablets secure
- Recover your business systems after a cyber security incident
- Select suppliers who are diligentwith cyber security
- Create a plan to respond to cybersecurity incidents

Use multi-factor authentication

Action Now

What you need to do

Implement MFA wherever possible, and particularly for important internal and external accounts.

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides step-by-step MFA guides for many popular services:

- Turning on Two-Factor Authentication for Apple ID
- Turning on Two-Factor Authentication for Facebook
- Turning on Two-Factor Authentication for Facebook Messenger
- Turning on Two-Factor Authentication for Gmail
- Turning on Two-Factor Authentication for Instagram
- Turning on Two-Factor Authentication for LinkedIn
- Turning on Two-Factor Authentication for Microsoft accounts
- Turning on Two-Factor Authentication for Signal
- Turning on Two-Factor Authentication for Twitter
- Turning on Two-Factor Authentication for WhatsApp and WhatsApp Business
- Turning on Two-Factor Authentication for Yahoo

Why is this important?

MFA is a security measure that requires two or more proofs of identity to grant you access to a device, system or application. The multiple layers of proof of identity make it much harder for criminals to attack your business.

MFA typically requires a combination of:

- something you know – pin,
- secret question something you possess – card,
- token something that's part of you – fingerprint,
- retina

Test your business' backups on a regular basis

Action Now

What you need to do

Check if the information stored on your backups is accessible and working, every 2-3 months, or so. In particular, consider:

- Is the information you want to have backed up there?
- Are the copies of the information stored on those backups accessible and fully intact? For example, do key documents open whenyou try to access them?
- Is the information you are backing up recent enough? If it's too old, it may be time to consider increasing the frequency of your backups.

Why is this important?

If your business experiences a security incident where important information is corrupted or lost, having backups you can rely on is critical. Sometimes backups can fail:

- it may not have copied over correctly
- it becomes corrupted over time – particularly where those backups occur to physical media such as an external USB drive.

Use strong passwords

Action Now

What you need to do

- Educate staff about how they can create strong passwords – this can include passphrases (a phrase or sentence) or passwordmanagers
- Ask staff to use unique passwords for each one of their accounts
- Check you have password enforcement policies in place for cloud software usersPut technical measures in place to enforce strong passwords

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides detailed guidance and step-by-step instructions to help you understand andimplement recommended actions:

- Creating Strong Passphrases.

Why is this important?

You must ensure staff use strong passwords.

A common belief is that strong passwords are 7 or 8 characters, use a combination of upper and lower case letters, numbers and special characters. They are not strong passwords. Cyber attackers can easily crack them with modern tools and techniques and gain access to your accounts.

It's important that staff understand how to create strong passwords to prevent this from happening.

Control or manage software installation

Action Now

What you need to do

- Educate your staff about only downloading software from reliable sources, especially on tablets and mobile devices Install antivirus software and keep it up-to-date by enabling automatic updates
- Manage user accounts to limit what staff can download to a minimum

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides detailed guidance and step-by-step instructions to help you understand andimplement recommended actions:

- Managing user accounts for macOS
- Managing user accounts for Microsoft Windows 10
- Online apps - do your own research first
- Guide on Implementing Application Control

Why is this important?

The more software or applications you have installed on your devices, the more chance there is for cyber attackers to target your business. This could be through the use of malware or exploiting vulnerabilities in installed software or applications. Some software may secretly include adware or malware which could impact your systems. For these reasons it's best to limit what's installed to what is absolutely necessary for you to do business.

Detect cyber security issues in your internal IT systems

Action Next

What you need to do

For any business, the simplest thing that can be done to help identify and detect potential security issues is:

- having antivirus software installed on all systems
- making sure it is kept up to date (enable the auto-update option).

If your IT environment is large or complex, you may need to use a managed service provider (MSP) or an external IT expert. They canhelp to identify and block malicious activity.

If you already engage an MSP, discuss if they can also proactively log and monitor events in your IT environment.

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides detailed guidance and step-by-step instructions to help you select and useantivirus software:

- Choosing antivirus software
- Performing a malware scan using Microsoft Defender Antivirus for Windows 10
- Turn on real-time protection in Windows 10

Why is this important?

Cyber security threats are rapidly evolving, and sometimes despite your best efforts a security incident can still happen. Being able toquickly identify when it occurred can make the difference between a big or small impact on your business. Proactively monitoring your business' technology environment is important to detect suspicious activity.

Handle sensitive client, business and staff information securely

Action Next

What you need to do

Understand exactly what types of important information you have in your business and where it is located. Examples of storage locations include:

- USB drivesemails
- computers / mobile devices
- cloud based solutions such as Dropbox, Google Drive and OneDrive.

To determine types of important information in your business and locations, you could request this information by:

- conducting a survey with all staff
- having a face-to-face meeting with all staff
- sending an email to all staff
- all of the above, depending on what's practical for your business.

When you know where you currently have your important information, you can then collate it in central locations. Spend some time securing all your important information:

- Ensure you have secure storage methods for your information. These could include encryption and /or restricting access bymanaging user account privileges
- Limit storage locations so you can keep track of your information
- Make sure staff know where and how to securely store important informationRestrict access to only those staff who need it to do their job
- Encrypt important information on laptops, mobile devices an external hard drives
- Store hard copies of important information securely in a locked drawer or locked filing cabinetImplement a secure way of sharing confidential or sensitive information

Helpful guidance

Enabling encryption on your devices:

- Apple provides advice about how to set up encryption on Mac devices
- Microsoft provides advice about how to set up encryption on Windows devices
- Most modern Android and iPhone mobile devices have encryption enabled by default if you have a strong PIN or password. Check your device settings to make sure.

Why is this important?

Your sensitive information could be of potential value to cyber attackers. Examples of this could be:

- customer details or other personal informationemployee details
- bank account details, credit card numbers or other payment related information
- intellectual property
- contracts or sales related information.

Make sure you store sensitive information securely to limit the potential of anyone accessing or modifying it without your authorisation. A leak of important information could expose your business, customers or partners to significant harm. This may include potential financial loss, reputational damage and regulatory penalties.

Use secure methods to share confidential or sensitive information

What you need to do

Some methods of information sharing are more secure than others but none are 100% infallible:

Emails

- Limit as much as possible attaching sensitive documents or including sensitive information in emails
- You have no visibility where recipients are sharing the information and with whom
- Use the Password Protect Feature password manager

File sharing tools

Popular file-sharing tools such as Dropbox, Google Drive and OneDrive are used by many businesses to share information. It's critical to make sure you use file-sharing tools securely. Things to keep in mind include:

- Share the file only with the people who need to see it
- Password protect the shared file and share the password by phone or password manager
- Disable downloads to limit copies being downloaded without your permission
- Set an expiry date for any shared links to prevent people from accessing it after that date

Most file-sharing tools can prevent anyone else from gaining access, even if they have a link to the file. This is useful if the link gets forwarded on to other people without your permission.

External USB drives

Consider encrypting the information before you store it on the USB drive and then share it. Microsoft Office files have a Password Protect Feature. Only share the password with those you trust – by phone or password manager.

You can purchase USB drives that have encryption built in. You'll need to set a pin code and provide that to the recipient, so they access the contents.

Paper-based sharing

You may sometimes need to share sensitive information using hard copies of documents.

- Limit the number of hard copies you create,
- Ask the recipient to securely destroy the documents when they no longer need them, by shredding them. Consider using one of the electronic methods of sharing information instead of by paper.

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides detailed guidance and step-by-step instructions to help you understand and implement recommended actions:

- Guidelines for cryptography
- Using a risk management framework

Why is this important?

Data breaches can occur where a business engages in ways of sharing sensitive information that are insecure.

There's an increasing number of regulations around the way businesses handle sensitive information. It's important to be aware of and practice robust methods for sharing information securely. This can help limit the potential for that information to fall into the wrong hands, which may cause you, your customers or partners harm. It could even expose your business to financial penalties.

Provide staff cyber security awareness training

Action Next

What you need to do

Provide cyber security awareness training to new staff. Provide reminder training at least once a year to all staff.

The content of awareness training may vary depending on the specific risks your organisation will likely face. Awareness programs for all staff should cover the following topics as a minimum:

- Malicious software (malware) – unauthorised software including viruses, spyware, trojans and worms designed to cause harm to your devices
- Scam emails (phishing) – emails, SMS or social media messages that attempt to mimic individuals or organisations you may know. They trick you to click on a link or an attachment and ask you to provide personal information (passwords or credit card numbers) or pay a fake account. These emails can also include attachments designed to look genuine, but which contain malware
- Ransomware – a specific type of malware that locks down your computer and files on it until a ransom is paid
- Good practices when it comes to cyber security – using strong passwords, multi-factor authentication, backing up data and using automatic updates
- Responding to an incident – what staff should do if they detect a potential security incident and where to reported it.

There may be other topics that are relevant to specific staff, depending on the way your business operates. Advise these staff about all the cyber security risks that apply to them. Staff who are at a heightened risk will vary depending on your business, but may include:

- Travellers
- Staff working from home
- Staff with a significant public profile
- Staff who manage your business' financial accounts
- Staff with elevated access to your business' systems via administrative accounts

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides detailed guidance and step-by-step instructions to help you understand and implement recommended actions:

- Small Business Cyber Security Guide
- Guidance on COVID-19 Malicious Cyber Activity
- Travelling Overseas with Electronic Devices
- Tips on Working from Home Securely

Why is this important?

Many cyber security breaches are mostly caused by human error – clicking on a malicious link or attachment in an email. Training your staff to understand and avoid common security threats is important in reducing the risk of cyber security incidents.

Some staff may have a higher level of risk of being targeted, simply because of the nature of their role. It's important to make these staff aware and the steps they can take to help manage this risk.

Carry out regular security testing

Action Later

What you need to do

Determine which parts of your IT environment may need security testing:

- identify internal or internet-facing systems that either host important data or applications, or support critical business operations. If some of these are cloud-based, then your cloud service provider may do security testing. Check with them.
- the importance of testing your website will vary. It will be more critical to test if your website is transactional than if it is static. Transactional websites are more at risk as they have sensitive or confidential data and more avenues for a cyber attack.Transactional websites include those which sell to the public or other businesses.

Identify who will do the security testing and how it will be done:

- there are a range of security testing options – from free scanning services (many are available online) to customised services. Many free services provide a good starting point, but may not identify all potential security issues with your systems / website.
- engaging a security expert specialising in security testing services can ensure a tailored solution is developed for your business' needs. The testing may be more detailed and provide guidance on prioritising remedial work for any security issues identified.

If you're already using a managed service provider, speak to them about your business' security testing needs.

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides detailed guidance and step-by-step instructions to help you understand and implement recommended actions.

CREST International and CREST CREST ANZ provide a list of accredited companies that provide quality security testing services:

- https://www.crest-approved.org
- https://www.crestaustralia.org

Why is this important?

It's important to identify potential security issues that cyber attackers might exploit by periodically undertaking security testing of important systems. High risk and important systems can include:

- your business' public website(s)
- any internet-facing systems that provide access into your business.

There are automated tools and experts that can help you with security testing.

Understand your business' compliance obligations

Action Later

What you need to do

Speak with your legal advisers to understand your cyber security and information handling obligations. Some of these obligations may include the following:

- Privacy Act 1988 (C'th) – in particular the Australian Privacy Principles and the Notifiable Data Breaches Scheme
- The Australian Prudential Regulatory Authority's Prudential Standard CPS 234
- The Payment Card Industry Data Security Standard (PCI DSS) if your business handles payment card information.
- The European Union's General Data Protection Regulation (GDPR) – if you offers goods and services and there's a connection with the European Union.

Helpful guidance

The Office of the Australian Information Commissioner (OAIC) has provided some guidance:

- What is personal information?
- Part 4: Notifiable Data Breach (NDB) Scheme

Why is this important?

In the last few years, more and more compliance obligations have been introduced both in Australia and globally. They may impact your business' approach to cyber security and the way you handle information, either directly or indirectly.

Other regulatory and compliance requirements may apply if you conduct business globally. Non-compliance could result in heavy fines and other penalties, as well as reputational damage.

Australian businesses may be subject to a data breach scheme. It requires them to notify customers, employees or anyone else affected by a data breach. They mustalso notify the Office of the Australian Information Commissioner. It's important your business understands whether the information it holds is subject to the scheme.

Non-compliance with legal and regulatory requirements could result in heavy fines and other penalties against your business and reputational damage.

Keep your business mobile phones, laptops and tablets secure

Action Later

What you need to do

In order to effectively secure portable devices in your business, there are two steps.

Firstly, you need to understand which measures you need to action. Key measures to secure portable devices include:

- **Encryption** – enable device encryption if you're storing or accessing important business information on portable devices. This ensures the information can't be accessed by someone else without your permission, even if you lose it.
- **Updates** – use the automatic update feature to install application and operating system updates on portable devices as soon as they're available. Apps should only be installed from official device application stores.
- **Unlocking** – enforce the use of a strong password, PIN, gesture or fingerprint to unlock portable devices. Ensure devices are set to automatically lock when not in use. Information could be compromised on devices that are not locked, if those devices are lost.
- **Remote locking** – enable remote locking and/or wiping functions (if supported). If a portable device is lost these functions can help reduce the risk of information being compromised.
- **Security software** – install reputable security software that includes antivirus and anti-theft/loss protection. Your device's retailer or service provider can provide recommendations.
- **Passwords** – set the device to require a password before anyone tries to install applications. This will prevent unauthorised modifications to the device.

Secondly, it's important to consider what actions you can take to put into place security measures on all your portable devices. What will be practical from a time, efficiency and cost perspective will depend on your business. Some options are outlined below:

- **Educate staff** – educate your staff about how to securely configure their portable devices and then ask them to do it themselves. The downside of this approach is that there is no guarantee your staff will configure devices correctly.
- **Manual device security** – you may wish to set up device security before providing them to staff. You can either do this yourself or engage the services of an external IT expert. The advantage of this approach is the confidence devices are set up securely before staff start to use them.
- **Central tool** – a centralised tool may be a more practical way of enforcing secure configuration settings. It can help ensure your devices are configured securely on an ongoing basis. To help with this process you may wish to engage the services of an external IT expert.

Helpful guidance

The Australian Cyber Security Centre (ACSC) provides simple guidance to help you understand and implement recommended actions:

- Mobiles and tablets
- Secure your mobile or tablet device
- Secure your information on your mobile or tablet device
- Be mindful of where and how you use your mobile or tablet device
- Education to protect your staff and business against cyber threats

Why is this important?

Most businesses rely on some portable devices such as laptops, mobile phones and tablets for work purposes. These devices are often used to access, store and process important business information. Portable devices are not always set up with the most secure settings as a default by the manufacturer. You will need to set them up securely to minimise the risk of a cyber incident.

Recover your business systems after a cyber security incident

Action Later

What you need to do

Develop a plan for maintaining continuity of operations for the following:

- the priority of critical systems and information your business holds, whether on premises or in the cloud contact details for key stakeholders internal and external to your business and their roles and responsibilities
- strategies for maintaining systems availability. Examples include, enabling employees to access alternative systems from home or an alternative work site, using backup / alternate systems.

Develop a recovery plan to restore critical systems in your business as quickly as possible for:

- managed cloud service systems – the provider may already have processes in place to help restore them promptly. It's important to engage with them.
- on-premises systems – to detail the process to repair damage to critical business processes and systems through to the point where normal operational capabilities can be resumed.

Engage an expert to help with developing these plans if required:

- continuity and recovery plans can be complex depending on the nature of your business and how many systems you have.consider if you need external help with the services of a cyber security expert.

Some businesses may merge continuity and recovery plans into a single document. For the purposes of this recommendation they have been treated as separate concepts and plans.

Why is this important?

- While an incident response plan helps your business deal with the immediate need to limit the effects of an incident and engage with all relevant stakeholders. It's also valuable to have plans in place to identify how your business:
- maintains continuity of operations when an incident occurs (Business Continuity Plan) restores key systems back to normal after an incident occurs (Disaster Recovery Plan).

Select suppliers who are diligent with cyber security

Action Later

What you need to do

While it may not always be practical to negotiate individual contracts with cloud service providers, you can still check:

- **Security certifications** – do they have accreditations to cyber security standards such ISO 27001, Service Organization Controls (SOC) 2 or the Payment Card Industry Data Security Standard?
- **Terms of service** – which will often include cyber security measures they take and what responsibilities they expect your business to take. Make sure you are comfortable with these stipulations. If you aren't sure, speak to your legal advisers for guidance.

If you can negotiate the terms of their engagement with your business, you should ensure to cover cyber security matters. Specify and make clear the respective responsibilities of both parties.

Consider including terms to cover the following:

- Adhering to your security requirements or an industry security benchmark Security breach notification and what remedial action they will take to address it
- Right to audit and test the security measures the third party has in place
- Management of supply chain risks with the same security requirements Communication of changes.

Ultimately, the clauses that should go into a contract with a third party is a legal question so always consult with your legal advisers.

Why is this important?

All relationships you have with third party suppliers and/or vendors should have a formal legal agreement. It should include how they will apply security measures to protect your systems and/or information which they will have access. This is especially important if they have access to sensitive information. A security breach involving any of these suppliers can have significant negative consequences for your business.

Create a plan to respond to cyber security incidents

Action Later

What you need to do

A plan to respond to security incidents does not need to be extensive. You still need to have one, even if it's just a basic plan. Include the following in this plan:

1. Contact details of external people and organisations your business may need to engage if you experience a security incident. It's important to have these details on hand during an incident. Include phone numbers and email addresses where appropriate
2. Details of who is responsible for managing the response process, including making and/or signing off on decisions
3. Possible signs of an incident, which could include:
4. devices running slower than usual or restarting unexpectedly
    - unexpected pop-ups appearing continuously
    - alerts from anti-malware software
    - unexpected configuration changes to devices unfamiliar files
    - unexpected changes to your website
5. A sequence of steps to follow if there are concerns an incident has occurred:
    - Who to contact for support and advice – IT support, legal and cyber security advisers, and/or law enforcement Basic steps to take while seeking advice – isolating affected devices from use until an expert can review the issue
6. Undertaking a review process once the incident is resolved. This can help you identify lessons learned to improve your incident response process for the future.

Once you develop the plan, make sure it is easily accessible and you share it with your staff.

Use the Australian Government's ReportCyber service to report cybercrimes.

Why is this important?

It's important to take steps to protect your business as much as possible from a cyber security incident. The reality is that there will always be some risk that your business does experience one. The way you respond can be the difference between your business experiencing aminor disruption or suffering major damage.

Having a plan prepared in advance is crucial. It will help your business understand what needs to be done if there is an incident. Trying to handle an incident without a plan is not wise. You'll be under great pressure which will make decisions without clear direction, very challenging.

If your business handles security incidents effectively, it can also enhance your relationships with external stakeholders (customers and partners).

Get help to action these recommendations

The CyberUP team at The Project Lab is here to help you continue on with your cyber journey. Please contact us to discuss these recommendations.

If you need more help, you may want to engage an IT Service provider or cyber security professional.

Selecting a service provider is a challenging process that requires appropriate planning and evaluation before, during and after you sign a contract for their services. Get helpful tips about how to protect your business from cyber security threats

AuCyberscape can help connect you with Australian cyber security firms in your local area.

If you just want to talk to someone about cyber security, the Australian Cyber Security Centre operate a 24/7 Cyber Security Hotline providing over the phone support to both prepare for and respond to cyber incidents. To use this service call 1300 CYBER1.