Department of
Employment, Small Business and Training

Mentoring for Growth

Helping small business succeed

Cyber security self-help toolkit for mentors

business.qld.gov.au/mentoring

Queensland Government

The purpose of this toolkit

The Mentoring for Growth (M4G) team are constantly looking for ways to further support both the mentors volunteering their time, as well as the businesses benefiting from the service.

Technology plays an important role in business today and can be used to improve efficiencies and productivity, yet also carries risk. To help businesses across Queensland better manage the cyber security elements of this risk, the M4G team partnered with Cynch to develop this cyber security self-help toolkit that can be used as a reference guide for M4G mentors. The goal is to make it easy for mentors to guide the businesses they mentor to the resources they need to effectively manage their cyber risk.

Supported by: cynch

Copyright

Licence

Other languages and formats

The Queensland Government is committed to providing accessible services to Queenslanders of all cultural and linguistic backgrounds. If you have difficulty understanding this publication and need a translator, please call the Translating and Interpreting Services (TIS National) on telephone 131 450 and ask them to contact DESBT on 1300 654 687.

Alternative formats (including large print) are available on request. If you would like this in another format, please contact us (calls from mobile phones are charged at applicable rates).

Persons with a hearing impairment:

TTY: 07 3896 3471

Disclaimer

This publication is to be used as a guide only. The authors have taken reasonable steps to ensure the publication is correct at the time of publication. The State of Queensland accepts no responsibility and gives no warranty, guarantee or representation about the accuracy, reliability, timeliness, suitability or otherwise of the information contained within this publication. The State of Queensland expressly excludes legal liability in all jurisdictions concerning the use or reliance of any information contained in this publication. Any direct or consequential loss or damage suffered because of reliance on this publication is the user's sole responsibility. Persons using information contained in this publication should conduct enquiries and rely on independent professional advice. This exclusion shall extend to all users and related parties who may suffer loss because of the use of information contained in this publication and applies despite any negligence on the part of the State of Queensland.

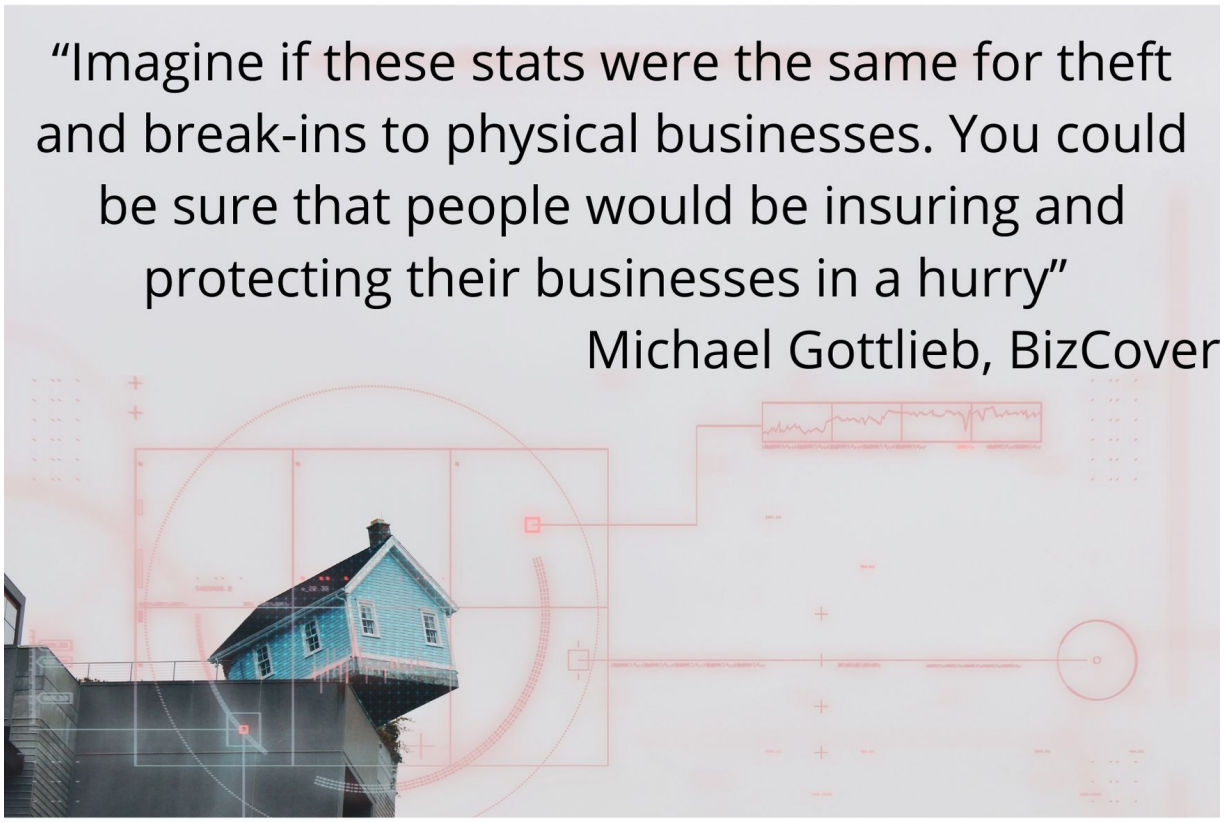
Table of Contents

**Note: Disclaimer applies, refer page 2 of toolkit.*

Part 1: Why does cyber security matter?

How often do attacks happen?

- **Two out of five** small businesses have suffered an incident in the last year (https://cynch.com.au/small-business-cyber-fitness-2021)
- According to Bizcover, the average time to recover from a cyber incident is **23 days**.



Glossary – common cyber security attack terms

- **Password attack** – access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing - they are then used to log in without you knowing.
- **Ransomware** – malicious software that locks up your files and demands a ransom payment in exchange for the decryption key. Other **Malware** may be designed to do anything from collecting and stealing sensitive information to presenting unwanted ads to causing permanent damage to an infected machine.
- **Phishing** – an attacker tricks a user (often via email) into clicking on a malicious link or opening an attachment that can achieve a variety of goals, including stealing usernames and passwords, financial fraud, and theft of sensitive data. **Smishing** (SMS-based attacks) and **Vishing** (voice-activated attacks) are also common.

- **Man-in-the-Middle (MitM) attack** – bypasses built-in encryption protections by breaking a connection into two pieces and then reading your data without you knowing.
- **Malicious apps** – malicious applications can do anything that desktop malware can, including stealing sensitive data, encrypting files with ransomware, and more, but do so on a mobile phone or device.
- **Denial of Service attack (DoS)** – are designed to deny access to critical services by causing a system to crash or flooding a system with more data than it can handle.
- **Zero-Day exploit** – all software contains weaknesses and vulnerabilities, and until these are fixed/patched the cyber attackers can exploit these 'zero day' vulnerabilities in the system and gain access to your device.
- **Drive-by attack** – attackers target insecure websites and plant a malicious script on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers.

Where can I find the latest information?

Avoid heading to Google for the latest threat information and head to these trusted sources:

- **Australian Cyber Security Centre (ACSC)** – industry-specific and general threat reports can be found here: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics
- **SCAMwatch** – regularly update the site with the latest scams that are circulating Australia: https://www.scamwatch.gov.au/
- **Ponemon Institute** – research center dedicated to privacy, data protection and information security policy: https://www.ponemon.org/
- **Verizon** – Annual Data Breach Investigation Report: https://www.verizon.com/business/resources/reports/dbir/
- **National Cyber Security Centre (NCSC)** – the UK's CSC releases weekly cyber threat reports here: https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc
- **Cybersecurity & Infrastructure Security Agency (CISA)** – this US agency releases regular threat advice: https://www.cisa.gov/

It should be noted that outside of Australia, the size of a business still considered a small business is significantly larger (up to 500-1000 staff), so some of the statistics discussed in overseas advice are inflated in comparison to Australian information, where data is limited.

Real-life case studies

USA's National Institute of Standards and Technology (NIST) have some fantastic small business case studies available on their website. Whilst these are US-based, similar attacks are prevalent in all developed countries.

Examples of recent cases are:

- Case 1: A Business Trip to South America Goes South
- Case 2: A Construction Company Gets Hammered by a Keylogger
- Case 3: Stolen Hospital Laptop Causes Heartburn
- Case 4: Hotel CEO Finds Unwanted Guests in Email Account
- Case 5: A Dark Web of Issues for a Small Government Contractor

Read the details here: https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series

Part 2: What technologies are at risk?

Take a virtual walk through your day...

The starting point of understanding risk is to identify what technologies software, hardware, data, and physical locations exist within your organisation. It's a fundamental step to get right and underpins things like ensuring that they have Anti-Virus, patching, logging and checking that they have appropriate licences for software. This can also help to identify what access needs to be removed when someone leaves.

Try visualising a typical day and list each piece of software, hardware and mobile device that is touched from the first moment their eyes open, to the last thing before their eyes close.

Technology checklist

This list is not exhaustive, but includes examples of the different technologies that should be listed:

- software (everything installed on your computer or network)
- hardware (desktop computers, laptops, printers, external hard drives etc)
- mobile devices (phones, tablets, portable scanners etc)
- network devices (modems, routers etc)
- websites
- social media accounts
- internet/WiFi-connected devices (Nespresso machines, washing machines, fridges, security alarm systems, smart TVs etc)
- API connections (this stands for Application Programming Interface, which is a software intermediary that allows two applications to talk to each other)
- automation tools and software
- servers and other legacy systems
- operating systems
- physical entry systems (doors using swipe cards etc)
- consider other applications/software on devices used for both home and work (kids usage).

Consider those technology assets that are critical to revenue, productivity and data storage.

Triggers to listen out for

In your conversations with mentee business, you may hear or discuss the following which should trigger a discussion around their cyber security maturity and if they have invested in securing their data and systems.

- “We’ve recently moved to the **cloud…**”
- “Our team are now **all working and dialing in from home**…”
- “We want to **sell more online**…”
- “We’re about to have a **new website created**…”
- “We have a team of **developers overseas** building our product for us…”

- "It's been quite a while since we **upgraded the computers** in the office…"

Just about any discussion around technology can lead to questions about security.

Create an asset register

Create an asset register that contains the following information (this can be in a spreadsheet or system where other assets are listed):

- type of software: Software/Software as a Service/Operating System/Application
- licence information (numbers, date of expiry etc)
- owner
- date when ownership was given
- a unique identification number / serial number
- support: internally managed, the End of Life and by whom
- data classification (what information is stored on it?)
- purpose of the asset (eg accounting software)

It's a good idea to make the updating of this asset register part of a procurement process, so any new software is added or deleted from the register immediately. This is much easier than trying to go back later and remembering what they have added/changed.

Cynch has a template that can be downloaded and used: https://docs.google.com/document/d/1M9SbO6OodQBfmeABpgwx4Bcn-JNxGvhzVsN10VtAnJQ/edit?usp=sharing

Asset	Version	Asset Type	Data Classification	Support	Risk Score Risk Rating	Risk Score Residual Risk Rating	Top Risk
Insert Icon and Short Description		Email and Documents					
		CRM					

How will you know if something is wrong?

It is important to ensure you are regularly checking your technology for unusual activity as it can otherwise be many months before an issue is detected.

For advice on how to set up detection for each different asset, businesses can refer to the ACSC for further advice: https://www.cyber.gov.au/acsc/view-all-content/guidance/detecting-cyber-security-incidents

Who to call if an incident occurs?

The support services available to businesses vary by industry and size, but the following advice from the ACSC on how to respond to a ransomware incident has some good advice and links to support: https://www.cyber.gov.au/ransomware/what-to-do

Part 3: Where to start and get help?

The other CIA

When thinking about the cyber risks in each different technology used, consider the following three types of risks:

- **Confidentiality** – the risk of information being made available or disclosed to unauthorised individuals, entities, or processes. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.
- **Integrity** – the risk that data is modified in an unauthorised or undetected manner. Examples include emails with bank details being intercepted and the details being changed without being detected.
- **Availability** – the risk that information or systems are not available when needed. Examples include systems or devices being subject to ransomware.

Each technology will have a risk under each category, but the likelihood and severity of each may be different depending on the use of the technology. All three should be considered for each technology.

The NIST cybersecurity framework

Source: https://www.nist.gov/cyberframework

The NIST cybersecurity framework provides a good mental model of the steps businesses should take to manage the cyber risks in each technology. While it may seem that these steps are done one after the other, practically these activities occur on an ongoing basis and therefore should be managed concurrently.

1. **Identify** – Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
   By creating an asset register, and then a risk register as described earlier in this kit, the business will be well-place to manage these activities in an ongoing manner.
2. **Protect** – Develop and implement appropriate safeguards to ensure delivery of critical services.
   This means introducing new technology (such as anti-virus software), processes (procedures such as steps to verify bank details before sending payments) and people related controls (such as regular staff cyber awareness training) to protect your technology from harm.
3. **Detect** – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
   Regularly checking audit logs or using monitoring services can help with these activities.
4. **Respond** – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
   The worst time to create a plan to respond to an incident is when you are already experiencing one. Having an Incident Response Plan in place is an example of this.
5. **Recover** – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
   Purchasing cyber insurance is a good example of managing your recovery activities.

Businesses should refer to the NIST cybersecurity framework for further guidance or seek appropriate support from a professional or firm to assist them with this.

Government and other trusted resources

The following (not exhaustive) list of tools and resources can be a great place for businesses to go for further information and support.

- **Australian Cyber Security Centre** – Australian Government resources for citizens and businesses: https://www.cyber.gov.au/
  Importantly, the following small business guide may be helpful: https://www.cyber.gov.au/acsc/view-all-content/publications/small-business-cyber-security-guide
- **SCAMwatch** – for advice on avoiding falling victim to scams: https://www.scamwatch.gov.au/
- **eSafety Commissioner** – for advice regarding online bullying and abuse: https://www.esafety.gov.au/
- **Office of the Australian Information Commissioner (OAIC)** – for privacy-related advice: https://www.oaic.gov.au/
- **Cynch Security** – the free tier of the Cynch Cyber Fitness platform can create a tailored cyber risk assessment, asset register and beginners cyber fitness program in under 10 minutes: https://cynch.com.au
- **IDCARE** – National Identity and Cyber Support: https://www.idcare.org/

- **Cyber security assessment tool** – a free tool to help you assess your general cyber risk: https://digitaltools.business.gov.au/jfe/form/SV_cRMe9MTmaq6QmrA?ref=acsc
- **HaveIBeenPwned.com** – a free service to check if your email address and associated information has been leaked in publicly known data breaches: https://haveibeenpwned.com/

Glossary of common processes and products

The following is a non-exhaustive list of the common processes and products that are recommended for businesses to implement (depending on their specific needs).

- **2FA/MFA** – Two-Factor Authentication or Multi-Factor Authentication is a security process in which users provide two different authentication factors to verify themselves. This is usually having a numerical code sent via SMS to your phone or generated in an app.
- **Adblocker** – add-on software in your internet browser which stops malicious advertising and pop ups from displaying.
- **Application whitelisting** – a set of automatic rules that places control over which programs are permitted to run on a user's machine or on a network in the hands of administrators, rather than end users.
- **AV/Anti-Virus software** – a software program designed to protect your computer or network against computer viruses
- **Encryption** – the process of making data unreadable by others for the purpose of preventing others from gaining access to its contents.
- **Firewall** – a network device that filters incoming and outgoing network data based on a series of rules.
- **Patch** – a piece of software designed to remedy security vulnerabilities or improve the usability or performance of software and ICT equipment.
- **Penetration test** – designed to exercise real-world targeted cyber intrusion scenarios in an attempt to achieve a specific goal, such as compromising critical systems or information.
- **SSL Certificate** – a type of digital certificate that provides authentication for a website and enables an encrypted connection.
- **VPN (Virtual Private Network)** – a network that maintains privacy through a tunneling protocol and security procedures. VPNs may use encryption to protect traffic.

Part 4: Common solutions for small business

There are thousands of cyber security solutions available across the world, but below are a series of quick wins and bigger investments that most businesses should consider and implement at some time in the future.

Quick and cheap (or free) cyber wins

- **Asset register** – creating a register of all technology assets used in a business is a great first step and doesn't have to take a lot of time or money. For help, check out the asset register template included in Part 2 above, or sign up to the free tier of the Cynch Cyber Fitness platform and let their system manage it for you: https://cynch.com.au/
- **Cyber risk assessment** – generate a cyber risk assessment for a business by using the Australian Government's free Cyber Security Assessment Tool: https://digitaltools.business.gov.au/jfe/form/SV_cRMe9MTmaq6QmrA?ref=acsc or Cynch's Cyber Fitness platform: https://cynch.com.au/
- **Purchase and install a password manager** – password managers are affordable and vital for ensuring unique, strong passwords are used for each account, reducing the chance of having multiple accounts compromised if one service has a data breach. For a recent review of the best password managers, head here: https://au.pcmag.com/password-managers/4524/the-best-password-managers
- **Use up-to-date anti-virus software** – installing and maintaining up-to-date anti-virus software on all computers is very important and will result in notifications of potential security issues. A review of many available can be found here: https://au.pcmag.com/antivirus/8949/the-best-antivirus-protection
- **Adopt e-signing software** – using e-signing software to manage executing contracts helps you also control access to important documents as well as version control. Here's a review: https://www.techradar.com/au/best/best-esign-software-solutions
- **Subscribe to SCAMwatch** – receive alerts to the latest scams circulating Australia: https://www.scamwatch.gov.au/
- **Install an adblocker** – adblockers are a great way to block malicious software downloading from websites, and they block annoying ads too! uBlock Origin is a free Chrome extension that is effective: https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en
- **Check HaveIBeenPwned** – check if an email or phone number has shown up in data breaches and subscribe to alerts: https://haveibeenpwned.com/
- **Check web browser version** – check web browsers are up to date regularly in the settings.
- **Turn on FindMyDevice** – FindMyDevice/FindMyiphone is a useful tool that helps you wipe your device if it is stolen or misplaced, as well as locate it.
- **Enable MFA** – enable MFA on email accounts and everywhere else it is available. Check here for accounts it can be enabled on: https://2fa.directory/
- **Install updates** – Make sure your device is using the latest version and enable auto-updates to make sure it stays up to date.

More time-consuming, expensive or complicated wins

- **Cyber insurance** – cyber insurance is a worthwhile investment but can be tricky to purchase. Work with an insurance broker or advisor to find the right cover for the business.
- **UBIKeys** – physical hardware used to restrict and manage access to critical systems.
- **Backups** – make sure the business has adequate and regular backups in place that are tested regularly.
- **MSSPs** – Working with a Managed Security Service Provider (MSSP) to take control of the administration of some technology can be expensive, but if you work with a good firm, can be very effective.
- **Penetration testing** – Arranging for an annual penetration test of your systems and technology can be costly but very effective at finding vulnerabilities you didn't know existed.

Contact details

For any queries regarding this toolkit, please email the M4G team: m4g@desbt.qld.gov.au

For information on the Mentoring for Growth program, visit: www.business.qld.gov.au/mentoring