cyber security

Guidance for Sole Traders and Small Businesses

by Mike (Mish) Davenport

techweek2025 Whanganui

whanganuitech
te tarahiti whatunga hangarau o Whanganui

About the author **Mike** (Mish)

Foreword

Mike (or 'Mish' to his friends) has many years' experience working in Information Security, originally in UK before migrating to New Zealand with his family in mid-2001. Much of his work has focused on security risk management; security governance, risk and compliance; and security consultancy. He has worked in both the government and private sectors, working for and with mostly large and medium enterprises, but also some smaller businesses.

This document is derived from a presentation given by Mike at a lunchtime Cybersecurity seminar as part of Whanganui TechWeek'25. Mike is a much valued and respected member of our organisation, and we thank him for his contributions to date.

Alan Nixon - Trustee
The Whanganui Tech Network

Intro
And guess what?

This guidance

is derived from a presentation given at a lunchtime seminar for Whanganui TechWeek on May 22, 2025. I have removed some of the original statistics and examples, instead expanding it to include tips, recommendations and notes.

In Sections 1 to 5 I outline the key areas for protecting a sole trader and small business's critical and important business data and assets; in Section 6 I touch on a couple of topics relevant to personnel security and information security documentation that could be useful; and I close with Section 7, which lists the primary sources I used to produce this guidance. Here I also include additional reference material that some readers may find useful if they wish to dig deeper into more technical aspects of cybersecurity as well as compliance.

There are no silver bullets...

I'm afraid there are no silver bullets to fix your cybersecurity woes (although you'll find plenty for sale on the Internet...) One of many reasons is that every business is unique (even those in the same line of business as other companies), having its own business objectives, needs, customers, culture, and risks (and risk tolerance), so a single security 'thing' that protects against everything cyber is an impossibility.

But, everyone can do something to help protect their business, and if you haven't started yet the purpose of this guidance is to point you in the direction to start helping yourself (even if that means engaging someone else to help you and let you get on with your job.)

What is cybersecurity?

Cybersecurity can be described as the protection of your critical and important business data and IT assets from deliberate or accidental harm. This may originate from the Internet as a network attack, virus-infected email or phishing message (for example), your own network by a disgruntled employee or someone making a mistake, or physical access to – or theft/loss of – your computing assets.

The next 5 sections contain key steps for protecting your important and critical data unauthorised access, theft, tampering, loss/destruction and misuse.

In some scenarios the harm could be accidental, but the protective measures are the same.

Section 1
Backup your data!

Backup your important business data

All businesses rely on critical and important data to operate, and without regular and effective backups you could be at serious risk of financial and reputational harm if your data is irretrievably lost (such as after a ransomware attack), tampered with leading to incorrect outputs or outcomes, or if it is unavailable when you need it (such as payroll runs).

What counts as critical and important business data?

Defining and identifying critical and important data can be difficult if you're starting from scratch. For small businesses and sole traders, it is likely to be sufficient to define it as any data or information that you rely on to achieve your business objectives, such as customer details and registers, orders, quotes, payment details, financial records, and so on.

Basically, if you cannot operate without it or prolonged unavailability will cause you operational difficulties, then it is critical or important.

Here are 5 tips/options for you to consider for backing up your important data:

Tip 1 - Identify critical and important data:

Identifying and, if necessary, classifying or labelling critical and important data, will aid in prioritising, managing and storing it, thus helping you to identify exactly what must be backed up.

Tip 2 - Use cloud service(s) for backups:

You may be storing critical and important data in the cloud already (such as Microsoft 365 and Google Workspace), which means your data is already separate from your location and benefits from robust, secure and highly-available storage without needing to invest in separate storage. If

Section 1 Backup your data!

you are not, there are other cloud storage providers to consider if you wish to move away from local USB storage (cloud backups are generally recommended over USB/local storage for general security reasons these days, but you may have your own reasons to stay with local backups – see Tip 3 next).

Recommendation:
By default cloud storage services usually offer only a limited amount of storage capacity, but additional storage is usually low cost and easy to increase.

Recommendation:
Read your cloud storage service's terms and conditions or SLA to make sure it meets your security and privacy needs. Most do, but smaller providers may not.

Tip 3 - USB storage backups:

Although generally not ideal from a security perspective, your business may have reasons to keep backups locally. If so, enable password-protected encryption to reduce the risk if the drive is stolen, and take care to test your backups regularly to ensure they are working as expected and you know how to restore data from them. Also, make sure the backup drives are protected against unauthorised access by staff and visitors and the passwords aren't shared with anyone who doesn't need them.

Recommendation:
Always disconnect USB storage after a backup is complete and secure it in a separate location. Consider buying a fire safe if you don't have one. Reconnect backup devices only for the next backup and remove when complete, because keeping storage devices permanently connected puts them at risk of being compromised with malware or encrypted with ransomware.

Recommendation:
Keep a second USB backup as a fail-safe. All storage devices fail at some point, usually when you need them most. Remember to use the same password as the original, otherwise this may lead to confusion in an emergency.

Section 1 Backup your data!

Tip 4 - Make backing up a daily business activity:

Backing up can be boring and is easy to forget about or put off to tomorrow. Most cloud storage solutions allow automatic backups (and may even backup automatically by default), but if you are backing up locally (to USB storage or cloud storage) commercial backup software (and even some free open-source backup software) can be configured to automatically backup your data. Just make sure you have defined what needs to be backed up and that you are backing up the right data (and know how to restore it!).

Recommendation:

However you are managing your backups, make sure to write down the process, what you are backing up, where it is being backed up to, and that you test the data recovery process from time-to-time to validate that the backups are working and that the process works correctly.

Tip 5 Configure antivirus software to scan USB devices automatically when connected:

This can protect you if someone inserts a malware infected device into a work computer.

Recommendation:

If feasible in your environment, restrict or block access to USB ports on company computers.

Tip 6 -Avoid using network attached storage (NAS) devices for backups:

NAS devices are primarily intended for use as file storage with a few bells and whistles for security and resilience. They are not recommended for backups, because they are normally permanently connected to the network and as such are vulnerable to malware infection (including ransomware), as well as unauthorised network access and theft.

Section 2

Malware Protection!

Malicious software, or malware for short, is defined by the Australian Signals Directorate as "… any type of code or program that is used for a malicious purpose, such as stealing your information and account details, encrypting your data for ransom and installing other software without your knowledge" .

Malware is spread in a number of ways, commonly by phishing email (see Section 5), but also by infected USB media, hacking (normally exploiting unpatched vulnerabilities on Internet-accessible computers), staff installing dodgy software, and visiting unsafe websites.

You should always enable malware protection on all your business devices and keep it up to date.

Note: Some people believe incorrectly that Apple Macs and Linux are immune from malware.

They are not, and while it is true there are fewer viruses designed to infect them, your business could suffer reputation harm if you forward an infected document to another business that uses Windows.

Here are four tips to reduce the risk of being infected with malware:

Tip 1 - Enable and configure built-in antivirus software:

Malware protection is a standard feature in recent versions of Windows and MacOS. You still need to enable it in Windows (though you are usually 'walked' through this when first configuring it), while in MacOS it is enabled by default and updates automatically .

Third-party malware protection for Windows and MacOS is optional and sometimes provides additional features that some find useful, so this is your choice. Some businesses may be

Section 2 Malware!

required to use commercial malware protection for contractual reasons (some larger customers may demand it to comply with their third party supply chain risk management programme), in which case this is unavoidable.

Recommendation:

Not all commercial anti-virus is created equal. Make sure you do your research before buying a subscription, because some commercial antivirus software has been known to be notoriously difficult to remove when the user changes to a different product.

Note: Although some free antivirus software is highly rated in established online media outlets, this is normally from a personal use perspective. If you use or plan to use free antivirus software in your business, take care to read and understand the privacy and security clauses to ensure they meet your business security and privacy needs.

Tip 2 - Prevent staff from using jailbroken mobile devices:

It is rare for malicious apps to make it through the validation process and onto Android and Apple app stores. However, staff using jailbroken mobile devices can install pretty much anything they choose, which significantly increases the likelihood of malicious software being unintentionally installed, which in turn increases the risk of business data being compromised.

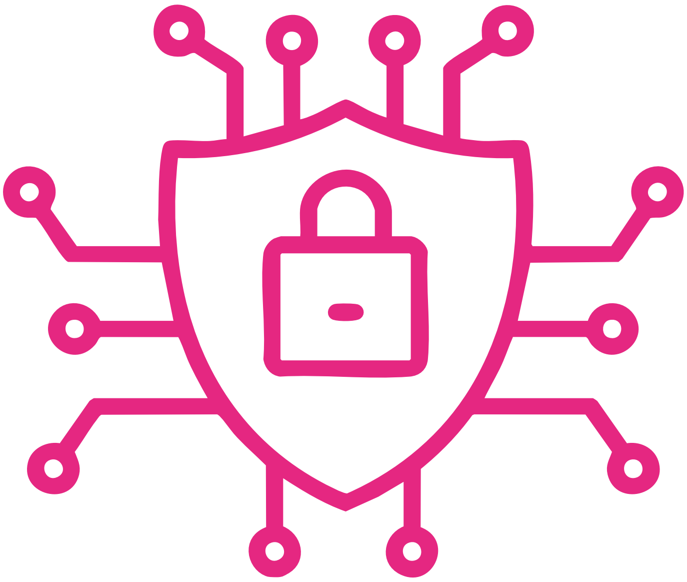
Recommendation:

If you run a business, don't use jailbroken devices yourself or allow your staff to do so. If you are unable to enforce this through technical measures, consider a prohibition clause in the acceptable use policy or equivalent.

Section 2 Malware!

Tip 3 - Keep computers and handheld devices up to date with regular, automated patching:

Most operating systems (including handhelds) receive notifications of security and application updates when they are released. Ensure that you and your staff are instructed to apply updates at the earliest convenient opportunity, and if possible force the update to apply automatically after 3 days if staff keep deferring it.



Tip 4 - Enable your computer's firewall:

Most desktop operating systems have built-in firewalls. Although initially disabled, Windows may guide the user to enable the firewall during initial setup. The MacOS firewall is disabled by default and must be enabled manually. In both cases, I recommend you either read the setup guidance for the devices on the respective websites or watch the vendor's instruction videos online.

Enabling the computer's firewall adds another layer of defence to protect against malware and unauthorised remote acesss.

Section 3 Securing handheld devices

Mobile technology is essential for businesses today, enabling work to be done on the move. It is increasingly common for sole traders (and tradies in particular) and possibly even some small businesses, to rely on handheld devices entirely for all the digital aspects of their work. Unfortunately, although convenient, handheld devices are easy to misplace, lose or have stolen, which can severely disrupt the business, especially if not stored and secured properly, online data is deleted or bank accounts are accessed and money stolen.

Here are three tips to keep mobile devices and their data secure:

Tip 1 - Enable a longer PIN/password protection and biometrics:

Configure an at least 6-digit PIN or password (if the latter is feasible), and always:

1. Enable biometric protection (fingerprint and/or facial recognition) and/or a hardware token such as a Yubikey if the latter is a business requirement (you'll know if it is.)
2. Verify that these features are set up correctly and work as expected.
3. You'll normally only have to enter the PIN/password once every 1, 2 or 3 days depending on the device's policy (the default seems to be 3 days if self-managed) or after a restart, the rest of the time using fingerprint or facial recognition to unlock the device.

Tip 2 - Enable location and device tracking:

Most devices (including laptops and modern desktop operating systems, for that matter) come with location tracking technology that enables them to be traced using web-based tools. If you discover that your device has been lost or stolen and it's location is still discoverable (thieves will often turn phones and tablets off or put them in faraday bags to shield them from

Section 3 Securing handheld devices

electronic access), follow these steps:

1. From the web console, instruct the device to ring – if it's nearby you might hear it (and can breath a sigh of relief), and if it's been left elsewhere or handed into lost property, someone else may hear it. The tracking software may permit you to post a message to call your phone number or email address for whoever finds it to respond to.
   If you don't hear it and no-one responds, then:
2. Remotely lock the device, and
3. Retrieve the data if you know there's sensitive information on it and it might not be backed up yet, and
4. Remotely erase data if necessary, then
5. Report the theft to the Police and inform them of the device's current or last known location and the steps you've taken to secure it.

Tip 3 - Apply phone and app updates as soon as possible after receiving updates.

Also see Section 2, Tip 3.

Tip 4 - Avoid using public Wi-Fi hotspots when travelling:

Unless it is essential (perhaps in an emergency?), avoid using public Wi-Fi hotspots for business use. Most mobile plans have a data component, and I recommend using this, because they are more secure and trustworthy. Smartphones are also very handy as hotspots for using laptops and tablets.

Recommendation:

This is not for everyone. Virtual private networks (VPNs) add another layer of security to your Internet connections. VPNs are normally straightforward to use and worth considering if you need additional network traffic protection while travelling, but do your homework and make sure the terms and conditions, particularly around security and privacy, meet your business needs.

Section 4 Use “strong enough” passwords

Passwords are frustrating but we’re stuck with them until something better comes along. Unfortunately, if passwords are too long and complex we forget them and write them down, but if they are too short they are easy to remember but also easy to guess. Here are four tips that may help:

Tip 1 - Avoid predictable passwords by using “strong enough” passwords:

Passwords should be relatively easy for you to remember but hard for others to guess. A rule of thumb for a ‘strong enough password’ is that, a) someone who knows you well shouldn’t be able to guess it in less than 20 attempts, and b) you will be able to remember it easily without writing it down (unless you have a genuinely secure place only you have access to store it temporarily). If you struggle to remember strong passwords, Tip 2 to follow may help.

Recommendation:
Windows and MacOS both have disk encryption built in (BitLocker and FileVault respectively.) Check that it is enabled, and if not enable it straightaway. This will protect your data if your device is lost or stolen because without your password the data cannot be decrypted.

Tip 2 - Consider using three random words for your primary password(s):

If you find strong passwords hard to remember, a method that some find helpful is to pick three (or more) random(ish) words separated with special characters (e.g. ‘-,), *, &’) and start or end each word with a capital letter and a number (or pick a variation of this). Two examples are: Cloud2*Security9*Alliance3 or C1oud-5ecuritY-4lliancE. Unfortunately, some automatic web-based password validators reject this approach (I think they ‘see’ the use of plain text dictionary words and reject them automatically),

Section 4 Use "strong enough" passwords

while some websites still reject passwords over 20 characters in length.

Tip 3 - When possible, enable 2-factor authentication:

Enabling 2-factor authentication to access important systems and cloud services (email, Microsoft 365, Google Workspace, banking, etc.) adds significant extra protection with minimal disruption once people get used to it.

Use smartphone authenticator apps or hardware tokens (such as Yubikey) for 2-factor authentication; SMS tokens are not recommended due to the risk of compromise from social engineering attacks, and there is a relatively recent form of social engineering attack called "SIM swapping" designed to gain access to SMS tokens and hijack bank accounts (for example).

Recommendation:
Do not permit any exceptions for 2-factor authentication to cloud services and important business apps. While tempting, if your business were to be targetted by a scammer, anyone exempted from using 2FA is your weakest link.

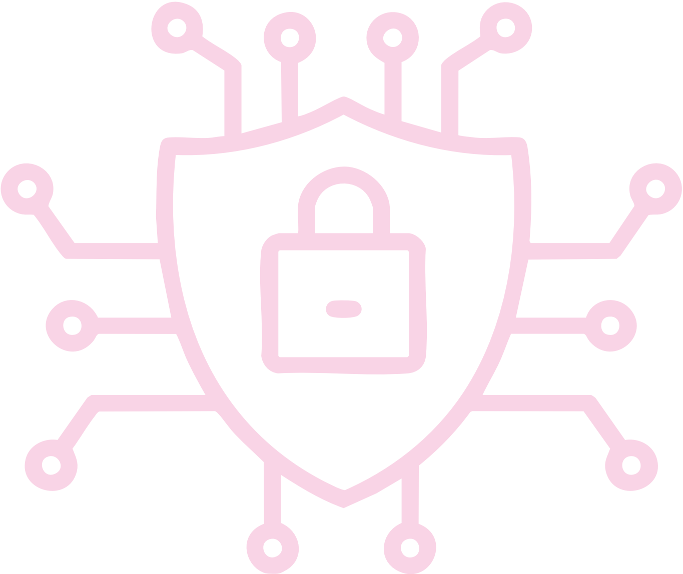
Tip 4 - Use a password manager:

Password managers can help people cope with password overload. They help manage multiple accounts across multiple systems and services, by automatically generating and storing strong passwords (some even enrol authenticator tokens), so you don't have to remember them yourself. All you have to do is create a strong enough password to unlock the password manager (NOT your logon password!) to prevent anyone else gaining access to your password manager, using 2-factor authentication if possible.

Section 4 Use “strong enough” passwords

If you don’t wish to use a password manager (not everyone gets on with them), provide secure storage for individuals to write down and store their passwords securely, but keep this separate from their devices. Recommendation 1: Don’t forget to include your password manager database in your backup plan!

Recommendation: Cloud-based password managers can be very useful, because they can be synchronised across multiple devices and are automatically backed up. However, these usually require an annual subscription, so know the first year cost (usually subsidised) and the subsequent full cost to avoid unpleasant surprises. Also read and understand the terms and conditions to make sure they meet your business needs.



Section 5 Avoiding phishing attacks

Phishing emails are sent by scammers hoping to trick you into paying fake invoices, steal your data or gain access to your network, or damage/destroy your business data (i.e. ransomware).

Phishing emails are gradually becoming harder to spot because scammers are beginning to use AI to tailor content for specific countries, but there are still plenty of 'old school' phishing emails being sent.

The three tips below should limit, but won't eliminate, some of the worst consequences of falling victim to a phishing attack:

Tip 1 - Awareness - Keep up to date with current phishing scams:

Major new phishing scams and viruses are often reported in the print and online media, as well as on banking websites and the CERT NZ website (such as https://www.ownyouronline.govt.nz/business/). Keeping up to date with the news and keeping yourself and your team informed goes a long way to keeping the risk of scams at the front of people's minds. Also, encourage staff to report actual or potential mishaps with phishing emails immediately to avoid delays, particularly with ransomware or financial fraud.

Tip 2 - Always use standard user accounts for normal business use: The principle of 'least privilege' ensures that staff have the lowest user rights necessary to do their jobs. This reduces potential damage to the business and its data if you or staff fall victim to a phishing attack.

Recommendation:

If you have any staff with system administrator privileges, ensure they use a standard user account for day-to-day business, elevating their privileges only when necessary using a separate administrator account. This reduces the exposure of the administrator accounts to compromise, which could have very serious consequences to your business.

Section 5 Avoiding phishing attacks

Tip 3 - When possible, enable 2-factor authentication:

(This is a repeat of Section 3, Tip 3, but worth reinforcing) Enabling 2-factor authentication to access important systems and cloud services (email, Microsoft 365, Google Workspace, banking, etc.) adds significant extra protection with minimal disruption once people get used to it.

Recommendation:

Ensure everyone in your business knows to NEVER enter an authenticator code into the same form that contains their username and password. No bank or cloud service will ever ask for this, so it is a strong an indication of a phishing email.

Recommendation:

Report phishing scams to https://www.cert.govt.nz/report/business-and-individuals/

Section 6

Personnel security tips

This section contains some suggestions for small business owners to consider.

Suggestion 1 - Robust pre-employment screening:

It is not unusual for smaller businesses to take people at their word and rely on 'gut instinct' when evaluating CVs and during interviews, which is undesirable, particularly for staff with access to finances and sensitive business or customer data.

Pre-employment screening is invaluable to help reduce the risk of recruiting unsuitable people, and while these steps cannot prevent risk, they can reduce the likelihood of it happening.

1. **Ministry of Justice Criminal Record Checks (MoJ CRC):** MoJ CRCs are helpful for assessing the suitability of an applicant for roles that demand trustworthiness, and the simple requirement to obtain them may deter potential fraudsters and untrustworthy people from applying. Clearly not all convictions will be relevant if the applicant has any but at least you will know and can make a judgement call. If this interests you, the MoJ Criminal Record Homepage is the place to start reading up on it.
2. **Reference checks:** Reference checks are important and even vital for some roles, particularly when technical ability, claimed knowledge and experience, organisational skills, interpersonal skills and personality 'fit' are important to your business.
3. **Education/qualifications checks:** If the role requires specific educational qualifications or industry certifications, verify that the applicant holds those they claim if these are a requisite of the role.

6 Personnel security tips

Suggestion 2 - Security policies, processes and procedures:

Your business security policy and processes and procedures should be documented, kept up to date, and available for staff to access when needed.

1. **Information security policy:** This should be one or no more than two pages that outline your expectations of what staff are required to do to keep the business, its data and its assets safe. It could be little more than outlining section 1 to 5 in this guidance.

2. **Security processes and procedural documentation:** These should be written in a format that suits your business and your staff so they will understand what is expected of them when the need arises, and know where to find the documentation (I recommend keeping digital copies online and printed copies available). Examples of procedural documentation include,
   a) Backups: making, testing and restoring data from backups;
   b) Patching and software updates: how to update your handheld device and laptop;
   c) Malware infection: what to do if you are infected with malware or ransomware;
   d) Handling phishing emails: phishing emails – how to spot them and what to do if you receive one; and
   e) Password management: password selection and management.

3. **Acceptable use policy/code of conduct (or include employment agreements):** This should be an as short as possible plain English set of rules about what staff are, and are not, permitted to do with business data and IT assets, and the consequences of failing to adhere to them. This should be accompanied by a security awareness or induction briefing and staff should individually sign and date acknowledgement and acceptance. This should be repeated annually because failure to do so can lead to legal challenges in the event of an employment dispute.

Section 7 Resources

The tables to follow list the sole trader and small business resources I used to prepare this guidance as well as other resources that may be helpful. Note that the level of detail tends to depend on the country that produced the material.

For example, the NIST cybersecurity guidance is produced for a US audience, and while extremely good and comprehensive, US small businesses are by order or magnitude larger than NZ small businesses and tend to have IT security personnel (or have outsourced security).

Primary Source ('PS'): UK National Cyber Security Centre

Resource	Outline
UK NCSC Small Business Guide: Cyber Security https://www.ncsc.gov.uk/collection/small-business-guide **NOTE:** All the information made available by the UK NCSC is published under the **UK Open Government Licence for Public Sector Information**. https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ Anyone is free to copy, adapt, use and 'exploit' the information (even commercially if combined with other information), **but the source must be acknowledged by linking or an attribution statement.**	This was the primary source of the sole trader and small business cybersecurity presentation and this guidance. I recommend the Resources section, especially: **1. Cybersecurity e-Learning** for small organisations and charities, covering five topics (backups, malware protection, strong passwords, securing devices, and phishing) as a series of lessons. And yes, anyone can access it (at the moment, anyway), https://www.ncsc.gov.uk/training/v4/Small+organisations/Web+package/content/index.html#/ ; and **2. Cybersecurity Small Business Guide** (a downloadable PDF and more detailed version of the online material I used). https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf

Section 7 Resources

PS: UK National Cyber Security Centre

Resource	Outline
UK NCSC Small Business Guide: Actions to Take https://www.ncsc.gov.uk/files/NCSC_SBG_Actions.pdf	This is a useful ‘checklist on a page’ of actions for sole traders and small business to use to plan the implementation of the general guidance in this document (saving you from creating your own or having to keep referring back to this document.)
UK NCSC home page for self-employed and small trader guidance and advice https://www.ncsc.gov.uk/section/advice-guidance/self-employed-sole-traders	This is the homepage of the NCSC self-employed and small trader guidance. It is useful and leads into the Small Business Guide, though somewhat UK-centric in places.

PS: Australian Signals Directorate Small Business Guides

Small business cyber security guide https://www.cyber.gov.au/sites/default/files/2025-03/Small business cybersecurity guide (January 2025).pdf	This is a comprehensive document, though probably more useful for technologists and IT security savvy readers, because it touches on secure software development, emergency plans, security awareness, as well as physical security and general information security measures generally beyond the scope of this guidance.
Cyber security checklist for small business https://www.cyber.gov.au/sites/default/files/2025-03/Small business cyber security checklist (June 2023).pdf	This is similar to the UK NCSC ‘Actions to Take’ list (see above). Although shorter, it refers out to other ASD resources so not everything is on one page.
Small business cloud security guides https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/small-business-cybersecurity/small-business-cloud-security-guides	This is largely technical guidance intended for cloud administrators, but technically knowledgeable and experienced staff may benefit from it.

Section 7 Resources

PS: National Institute of Science and Technology (NIST), Cybersecurity Framework 2.0 (CSF): Small Business

Resource	Outline
Small business cyber security corner https://www.nist.gov/itl/smallbusinesscyber	This is the homepage of the NIST Small Business Cybersecurity Corner. The CSF for Small Business is a slimmed down version of the full CSF, but is still a big beast that is beyond the scope of this document and the means of many New Zealand small and medium-size businesses.
CSF for Small Business Guidance by Topic https://www.nist.gov/itl/smallbusinesscyber/guidance-topic	I've included this link because some who attended the seminar were interested to understand more about cyber security risk management and compliance requirements, and some of these topics will provide good background

For more information

For more information on Cybersecurity
Contact the author of this document:
Mike (Mish) Davenport
e: mish-davenport@pm.me

Contact

whanganuitech
te tarahiti whatunga hangarau o Whanganui

For all other enquiries, contact
The Whanganui Tech Network Charitable Trust:
kiaora@whanganui.tech
https://whanganui.tech/

A BIG thanks to all our supporters

Thanks to our sponsors

CRAIGS®
INVESTMENT PARTNERS

WHANGANUI
& PARTNERS

Whanganui
Community
Foundation

also thanks to support from

Te Kaahui o Rauru

WDETT
Whanganui District
Employment Training Trust

THE
BACKHOUSE

TE MANU ATATŪ

NECTA

displaytechnology.co.nz