Tertiary Education Commission
Te Amorangi Mātauranga Matua

Cyber Security Controls

Overview

Cyber security controls: a guide for where to start

Getting started with cyber security

Cyber threats are real and evolving. Most organisations are aware of cyber security but may not be sure where to start to become more cyber secure. Information on this topic is often complex, and cyber security is seen as complicated, time-consuming and expensive.

This guide aims to make things easier by providing clear guidance and simple actions that result in a big increase in security.

Who this guide is for

This guidance is aimed at smaller organisations with limited capacity and capability that are reasonably new to cyber security. It targets organisations that run Windows on their devices and use either Microsoft 365 or Google Workspace.

Tip: See our guide about accessing Microsoft Academic Licensing, which is often much cheaper than retail pricing and offers a lot more functionality
>R01 Access to Microsoft Academic Licensing

How to use this guide

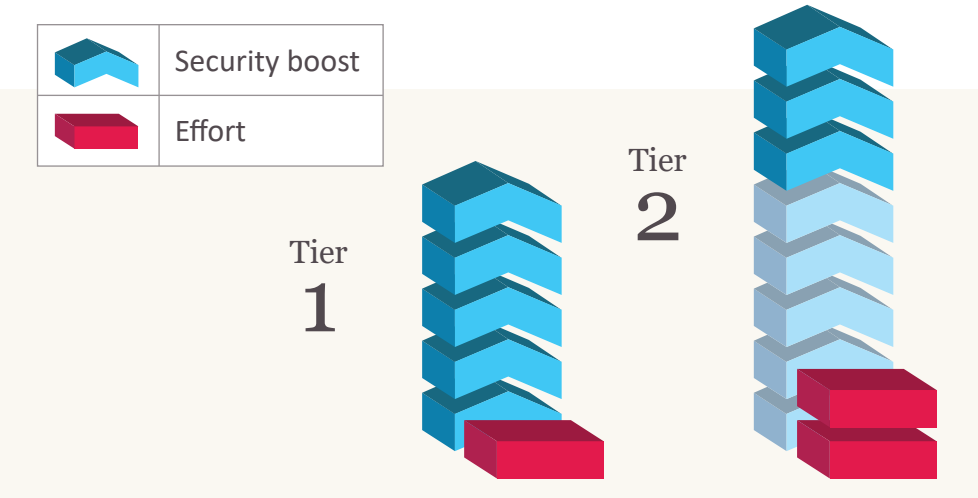
The guidance is organised into 2 tiers and 10 controls covering people, process and technology. The initial focus is on “best bang for your buck”: simple actions with the biggest effect on security. We suggest you work your way through the different controls in order. Focus on completing Tier 1 first.

- Tier 1 consists of 5 controls that will provide the most impact with the least amount of investment. Each control is an action that a small organisation with limited IT capability should be able to do in less than eight hours.
- Tier 2 requires more investment and generates smaller returns but is still strongly recommended to continue increasing your security maturity.

Each control includes:

- WHAT: what is the control about?
- WHY: why is it important?
- HOW: what should an organisation do (step by step)?
- RESOURCES: further support, like examples or manuals.

We have ranked all controls by priority (best bang for buck first).



Tier 1

Cyber security controls

Effort: 1

Security boost: 5

1. Cyber security training and awareness

What & why

Your staff are the first line of defence against a cyber attack, and unfortunately also the weakest link. It's crucial to make sure they are aware of cyber threats and know how to recognise an attack.

How

1. Inform your staff re the importance of cyber security.
Promote practical resources staff can use (for home and work) like ownyouronline.govt.nz. See the example email below as a starting point.

2. Provide staff with e-learning.
Ideally use specialist tools (like Phriendly Phishing, Knowbe4 or Proofpoint) which offer a wealth of focused and automated training. If this is too difficult, ask your staff to have a look at publicly available e-learning material. See some examples below.

Resources

>R02 Example communication to staff about cultivating a strong security culture

>R03 Examples of publicly available e-learning modules

Tips

- Make training mandatory.
- Train staff at least annually. Try to provide topics for training regularly during the year.
- Review your content regularly to make sure training is up to date.

2. Use strong passwords & MFA

What & why

Passwords are used for everything. Like a key to the front door, they're the most common way of gaining access to accounts. We rely on them to protect sensitive information about ourselves and others. Unfortunately, attackers can get hold of easy-to-guess or reused passwords.

Even the most "unbreakable" password can be cracked by a determined hacker or exposed in a privacy breach. If an attacker successfully accesses an employee or administrator account, they could compromise your organisation's entire network. You can add a strong layer of security by using multi-factor authentication (MFA), which requires users to have more than one form of identification to access IT systems.

How

1. Inform your staff about the importance of strong passwords.
Explain the importance of strong passwords and provide tips on how to keep passwords safe. See the communication example in the resources below.

2. Turn on MFA.
Turning on MFA by default helps protect your organisation's user accounts from the outset. Existing users will receive a request to set up MFA and new users can do this as part of onboarding. See the instructions below.

Resources

>R04 This article describes how quickly a password can be hacked: How Long Does It Take a Hacker to Brute Force a Password in 2023 – NetSec.News

>R05 Example communication to staff about the importance of passwords

>R06 CERT NZ tips on: How to create a strong password – Own Your Online

>R07 Using multi-factor authentication (MFA) - Microsoft

>R08 Using multi-factor authentication (MFA) – Google

>R09 Move Microsoft Authenticator to a new phone

>R10 Move Google Authenticator to a new phone

>R11 Recovering a standard or administrator account in Microsoft 365

>R12 Recovering a standard or administrator account in Google Workspace

Tips

Avoid using SMS-based MFA, as this is outdated and less secure. Use an application-based MFA (such as Microsoft or Google Authenticator) instead. However, SMS-based MFA is better than no MFA.

3. Keep software and systems up-to-date

What & why

Attackers use networks of computers (bots) that scan the internet to identify and hack vulnerable software and systems. Patching is the process of "patching up" or fixing bugs or issues with software and systems to improve their security and performance. You should apply fixes as soon as they are available.

Modern operating systems like Windows 11 include the latest security enhancements and features by default (like anti-virus/malware, firewalls and more). So, by staying up to date and using the latest operating system, you can significantly improve your cyber security posture.

Also, online services like M365 are updated automatically for you and provide the latest in security enhancements, including protecting your data with encryption. They also offer secure features that let you communicate and collaborate safely through email and secure file sharing.

How

1. Upgrade to the latest version of your operating system.
Windows comes with an automatic software update mechanism (Windows Update) that keeps your operating system updated with the latest patches and security updates. It will also recommend upgrading to the latest version of Windows when this becomes available.

2. Turn on auto updates for applications.
In Windows, turn on 'receive updates for other Microsoft products' within the Windows Update service. You should also turn on auto updates for all other applications that offer update functionality, including browsers. See the guide on how to update your Chrome browser.

3. Don't forget to patch your on-premise infrastructure.
On-premise infrastructure is the physical hardware, software, and networking components located within an organisation's premises or facilities rather than in the cloud, eg, firewalls and file servers. On-premise infrastructure should be patched by either your internal IT expert/team or your service provider (eg, Spark or OneNZ).

Resources

>R13 Update Google Chrome

Tips

- Let your staff know they should allow updates or upgrades to be installed when prompted.
- Check if maintenance contracts with IT suppliers cover patching of on-premise infrastructure.

4. Use a password manager

What & why

A password manager helps you to create, store and manage all your passwords securely in an encrypted vault or database.

When using a password manager, you only need to remember one strong master password. The manager takes care of generating, storing and auto-filling strong, complex passwords for all your other accounts, enhancing your overall security.

How

1. Use a password manager for organisational passwords.
Organisational passwords (ie, for break glass accounts and other accounts that are not linked to any one individual) should be stored in a password manager. This password manager must not be linked to an individual or there is a risk of losing access when that person leaves. The password manager could also be used to store other sensitive login information, such as entry codes.

Choose a reputable password manager. Some popular options include LastPass, 1Password, Dashlane and KeePass. Do not use the free password managers built into web browsers like Chrome and Edge, because these are always linked to an individual.

2. Recommend staff use a password manager.
If your staff need to remember several passwords for work, recommend that they use a password manager to securely store their passwords. Again, choose a reputable password manager. If all their passwords are for websites, they could also choose the free password manager built into web browsers like Chrome and Edge. See the guides for using these.

Resources

>R14 Using Edge password manager

>R15 Using Chrome password manager

Tips

Your master password to access your password manager should be long, complex, and something you can remember but others can't easily guess.

5. Limit administrative privileges

What & why

By using different account types and assigning the minimum necessary privileges to each account, you limit the potential damage caused by a compromised account or user error.

Standard accounts (also known as user accounts or non-privileged accounts) are used for day-to-day access that does not require administrative permissions.

Administrator accounts are used for the highest level of privileges and unrestricted access to the system. These accounts can perform system-wide changes, install software, modify system configurations, and access all files and resources. You should only use these accounts when necessary and for administrative tasks.

Note: The person in your organisation who has set up M365 or Google Workspace is automatically granted the administrator role.

An organisation should have following administrator accounts:

1. A dedicated administrator account for each of your administrators (not their day-to-day account)
2. An emergency account used only if you have lost access to your other administrator accounts (called a break glass account)

This helps reduce the risk of a hacker gaining privileged access to your organisation if your day-to-day account is compromised.

Best practice: Manage users and devices centrally. This means you can manage all your devices without granting all staff administrator privileges. This greatly reduces the risks of accounts being compromised.

How

1. Create a dedicated administrator account for each of your administrators.
These should not be shared but linked to an individual. However, they must not be used as their day-to-day account.

2. Create an emergency account.
This is called a break glass account and must only be used if you have lost access to your other administrator accounts.

3. Check that no other accounts have administrator functions.
In your admin portal, check that no administrator roles are assigned to a standard account.

4. Connect your devices to M365 or Google Workspace.
Enable administrators and users to sign in to Windows using their M365 or Google Workspace credentials.

5. Ensure each staff member has an individual standard account. Where needed, create new user accounts for your staff to log into their M365 or Google accounts. See the quick guide on how to set up a new user below. Don't use shared accounts.

6. Create separate admin accounts for all applications. If you use applications that are not part of either M365 or Google Workspace, you should create a separate administrator account for each application, which is only used if you need to configure this application.

Resources

>R16 Setting up an administrator account in Microsoft 365

>R17 Setting up an administrator account in Google Workspace

>R18 Connecting devices to Microsoft 365

>R19 Connecting devices to Google Workspace

>R20 Setting up a new user account in Microsoft 365

>R21 Setting up a new user account in Google Workspace

Tips

› Before giving a new device to a staff member, make sure an administrator logs in and completes the first time set-up (Because Microsoft automatically makes the first person that logs into a new device the device administrator).

› Make sure that the password for your break glass account is changed every time it is used.

Tier 2

Cyber security controls

Effort: 2

Security boost: 3

6. Have backups

What & why

Backing up your systems involves making an up-to-date copy of your data. With a backup copy stored safely, you can quickly restore your information if it's lost or damaged by a cyber attack or another issue.

How

1. Back up your data regularly.
A number of online products are available that make it much easier to back up your data. This will ensure your data is protected, independent of where it's stored. See examples of products and pricing in the resources.

Resources

>R22 Backup as a Service overview

>R23 Compromised! A "lesson learnt" story of a TEO

Tips

- Run tests to make sure you can restore systems and information in the expected timeframe.
- Know where your data is, how it is protected, and how to recover it. Don't wait until you have a problem to figure out how to solve it. See the example of a tertiary education organisation (TEO) that was compromised and what they could have done differently.

7. Secure your email

What & why

Email protection is an important safeguard against email-based threats. It includes a combination of techniques, such as spam and phishing filters, anti-virus scanning and data loss prevention capabilities. By implementing effective email protection, organisations can significantly reduce their cyber risk exposure and ensure the secure and reliable exchange of email communication.

A positive by-product of email protection is that when you reduce the influx of spam and malicious emails, employee productivity improves because IT staff spend less time manually addressing these threats.

How

1. Use a reputable secure email provider.
Microsoft 365 and Google Workspace offer an advanced email service that offers the latest security features, advanced protection, and the ability to use your organisation email domain. Because this service is included in the M365 and Google Workspace, it's recommended to use this service.

2. Use your organisation domain.
Using your organisation domain provides many security benefits. See the overview in the resources.

2. Secure your email domain.
Secure your email service by configuring the appropriate Domain Name System (DNS) records.

Resources

>R24 Benefits of using your organisation email domain

>R25 Secure your email domain

8. Include cyber security in staff onboarding and offboarding

What & why

Include cyber security in onboarding and offboarding processes. Ensure staff understand their security responsibilities from the start. This helps to reduce the risk of insider threats, data breaches and unauthorised access. In turn, an organisation can better protect its sensitive information and systems because there is limited access to them.

How

1. Include cyber security in onboarding and ensure new staff:

- receive cyber security training (see control 01)
- have access to only the systems and information they need to do their job (see control 05)
- read, understand and agree to comply with the organisation's information security policies and acceptable use guidelines
- understand their responsibilities regarding cyber security.

2. Include cyber security in offboarding and ensure:

- access to all systems and information is revoked
- any company-owned devices, access cards or other company assets are returned.

See the employee exit checklist for the full overview.

Resources

>R26 Information security policy (example)

>R27 Acceptable use of technology policy (example)

>R28 Employee exit checklist

Tips

- Include a cyber security training module in your induction process.
- Use an exit interview to remind the employee about ongoing obligations regarding confidentiality and data (this maintains protection even after they've left the organisation).

9. Use endpoint protection

What & why

Endpoint protection is the process of securing the various endpoints or devices (such as computers, laptops, mobile devices and servers) connected to a network.

How

1. Ensure Defender Anti-Virus, SmartScreen and Windows Firewall are turned on by default.
Tell your staff not to ignore warnings or turn them off.

2. Ensure the on-premise servers have anti-virus software running.
On-premise servers should be configured by either your internal IT expert or your service provider (eg, Spark or OneNZ).

3. Deploy Defender for Endpoint.
See the prerequisites in the resources below, and the technical guide on implementing Defender for Endpoint.

Resources

>R29 Turning on Defender Antivirus, SmartScreen and Windows Firewall

>R30 Setting up Microsoft Defender for Endpoint

10. Have a response plan and a person assigned

What & why

Every organisation should be ready for a cyber security incident (it's a matter of "when", not "if").

It's vital to have a plan in place and someone in charge that people can go to.

How

1. Confirm who is accountable for cyber security within the organisation.
For example, this could be the owner of the organisation.

2. Nominate a person to go to if something bad happens.
Ideally make this part of someone's job description and communicate this to staff.

3. Have a plan ready.
Ensure the nominated person knows what to do or who to go to if there is an incident. See the example phishing response guidance.

4. If you don't have internal security capability, engage a security partner.
This could be a "phone a friend" set-up – a security partner you call to help you deal with a cyber security incident.

Resources

>R31 Phishing response guidance

Tips

- Protective Security Requirements (PSR) outlines the New Zealand government's expectations for managing personnel, physical and information security. All organisations in New Zealand are encouraged to follow the 20 best practice recommendations. Best Practice – Protective Security Requirements
- CERT NZ offers valuable advice on cyber security responsibilities. Useful information can also be found on websites like About Cyber Security.
- Test the response plan regularly (at least annually).
- Ensure you can access response documents and let staff know what they need to do if infrastructure, such as Microsoft Teams, is compromised.
- Document roles and responsibilities (eg, in job or role descriptions).

What's next

Cyber security controls

What's next

After completing the previous 10 controls you have significantly improved your cyber security.

Among other things:

› You lowered the chance of a successful cyber-attack by training your staff and having a response ready.

› You made it much harder for hackers to find vulnerabilities by keeping your software and systems up to date.

› You made it much harder for hackers to gain access by enforcing strong passwords and MFA.

› You limited risk exposure through email by adding email protection.

› You limited potential damage by using different account types, enforcing admin privileges and using backups.

However, cyber security is ever evolving which means continuous improvement is going to be needed to stay ahead. In short: the work is not (and will never be) done.

Some of the areas you could consider next are:

› Positive security culture

› Device management

› Risk management

› Asset management

Positive security culture

Cyber security is everyone's responsibility. By cultivating a security-conscious mindset across your organisation, you can enhance your overall security. Fostering a positive security culture requires a combination of leadership commitment, employee training and awareness programmes, clear policies and procedures, and continuous reinforcement and improvement. It is also supported by a "no blame" culture. You want your staff to report issues and be safe doing this. Security events will happen, and people do make mistakes. Focus on addressing the issue at hand rather than pointing the finger.

Resources

>R02 Example communication to staff about cultivating a strong security culture

>R32 Tips and ideas to foster a positive security culture

Device Management

Set up centralised device management using Microsoft 365 or Google Workspace device management capabilities to benefit from centralised security management, enhanced data protection, and a comprehensive set of security controls and features designed to safeguard devices, data and overall organisational infrastructure against cyber threats.

Risk Management

Setting up a security risk management process will help your organisation protect digital assets and identify potential security risks. It also allows an organisation to take proactive measures to address identified risks and reduce the risk of security incidents. Setting up risk management starts with capturing risks in a risk register and then regularly discuss and report on these risks.

Resources

>R33 Risk register template (Excel)

>R34 Risk Management Group Terms of Reference

Tips

› Agree your risk tolerance and priorities with your executive leadership/board/owners.

› Be transparent.

Asset Management

Applying effective security measures in your organisation requires you to understand your assets. It is much easier to protect things if you know about them. The right visibility gives you the best chance of taking corrective action even before an incident occurs.

From a cyber security perspective, an asset is any valuable part of an organisation's IT infrastructure that requires protection from potential threats or vulnerabilities. This can include:

› hardware (servers, workstations, network devices)

› software (operating systems, applications, databases)

› data (customer records, financial data, intellectual property)

› networks (LANs, WANs, and their components)

› cloud resources

› and even human assets (employees with access to sensitive information).

Resources

>R35 Information asset register template (Excel)