

Connect Smart for Business

SME TOOLKIT



WELCOME

To the Connect Smart for Business: SME Toolkit



The innovation of small and medium sized enterprises (SMEs) is a major factor in New Zealand's economic growth. Businesses with 20 staff or less account for 97% of all enterprises, employ around 30% of the working population and generate more than a quarter (27.8%) of our Gross Domestic Product (GDP).

The internet and mobile working environments are now embedded in the way most businesses operate. Important business data, including financial information, customer data, business plans, and intellectual property, are stored online. Very few businesses could do without the internet and mobile devices nowadays.

This brings unrivalled opportunities for New Zealanders to do business with each other and the rest of the world – regardless of geographic location. It has reduced costs and increased business efficiency. But alongside these benefits, there are some risks.

According to recent research compiled by Vodafone, small businesses are the target of 30% of online attacks. Having your business information compromised is more than an inconvenience. It can have financial consequences for you and your valued customers, as well as an impact on your business' reputation.

The scale and nature of many SMEs means that often they do not have the internal IT capability or the resources to engage specialists. But some simple security practices can make a big difference.

This SME toolkit is aimed at demystifying cyber security.

Improving the cyber security of your business is easy – it's not complicated or expensive to take basic steps to protect yourself, your business and your customers online across all devices.

Demonstrating good cyber security practices will enable your business to benefit from the greater flexibility, mobility and efficiency of working online.

Connect Smart is an initiative led by the National Cyber Policy Office (NCPO), part of the Department of the Prime Minister and Cabinet (DPMC). The aim of Connect Smart is to encourage New Zealanders to take proactive steps to protect themselves, their contacts, and their businesses online.



Executive Summary

This SME toolkit is aimed at demystifying cyber security.

Improving the cyber security of your business is easy – it's not complicated or expensive to take basic steps to protect yourself, your business and your customers online across all devices.

Important business data, including financial information, customer data, business plans, and intellectual property, are all stored online.

Unintended or unauthorised access to your computers, laptops and mobile devices could result in theft of information, access to bank accounts, disruption to trading and reputational harm.

Follow these four easy steps to improve the cyber security of your business. Connect Smart and protect your business and customers online.

ONE

Assess the cyber security of your business



Do you have security systems and processes in place?



What business and financial information could be at risk from a cyber breach?

TWO

Develop a cyber security policy for your business



Do you have a cyber security-conscious work culture?



Do you have basic IT security controls in place?

THREE

Establish an incident management plan



Can you identify unusual activity that might risk your business systems?



What action would you take to resolve an incident?

FOUR

Regularly review and update your network security systems



Do you regularly review your cyber security policy and processes?



Are you sure your cyber security is adequate?

Start talking about what you can do to enhance your business' cyber security, now.

Don't feel overwhelmed or wait until it's too late. Convene a meeting to consider the steps in this toolkit and establish how your business can protect itself online.

WHAT IS THE CYBER SECURITY RISK?

The risks come from many sources. There are criminal groups – many of them off-shore – out for financial gain; there may be business competitors looking for commercial advantage; and there may be current or former employees who deliberately or accidentally compromise information security.

Unintended or unauthorised access to your computers, laptops and mobile devices could result in theft of information, access to bank accounts, disruption to trading and reputational harm.

The damage to your IT systems may prevent you from doing business for a period or compromise your customers' information. Cleaning up the system may be expensive. The damage may affect other companies that you interact with – and lead to fines or reputational harm.



CYBER SECURITY WARRANT OF FITNESS

Four steps to better online security

Take the Cyber Security Warrant of Fitness (WOF)
– a simple checklist of basic security measures.

Just like operating a motor vehicle, it is important to give your business periodic cyber safety inspections so that you have the right foundations in place and can feel confident that you're protecting your business, staff and customers online.

Below is a simple four step Cyber Security WOF
to achieving better online security:

**1. Assess the cyber security of
your business.**



**2. Develop a cyber security policy
for your business.**



**3. Establish an incident management
plan.**



**4. Regularly review and update
your network security systems.**



STEP ONE

Assess the cyber security of your business



What does it mean?

A cyber security assessment simply means reviewing the systems and processes of your business, so you can take necessary steps to mitigate risks and improve the foundations of your business' cyber security.

Why is it important?

Undertaking a cyber security assessment is an essential first step in ensuring you are operating in a secure online and mobile working environment. You need to consider whether the business information you hold could be a target for cyber criminals or others. What are the critical financial and information assets for your business? In other words, what is your risk?

This enables you to understand any areas of vulnerability within your business that may expose you and your customers to online threats, so you can proactively put in place steps to mitigate these risks.

What does it involve and where do I start?

Start by asking yourself some basic yes and no questions:

1. Do you have an overall security policy?
2. Do you and / or your employees access business emails on mobile devices (including phones and tablets)?
3. Do you train your staff about using mobile, the internet and email securely?
4. Do you back up your critical business data regularly?
5. Do you have a firewall installed on the computer(s)/servers used for your business?
6. Do you use security software (such as anti-virus and anti spyware) and up-to-date operating software?
7. Do you connect any of the computers or mobile devices in your business to the internet using a wireless network?
8. Do you know how to prevent data theft?
9. Do you know how to reduce and manage spam?
10. Do you store business critical information on mobile devices?
11. Do you educate your staff not to give out confidential information that could compromise your company's cyber security, either over the phone or online?
12. Do you delete or disable your staff's IT accounts when they leave the company?



How did you rate?

If you answered 'Yes' to:

- **9 or more of these questions** – congratulations on taking proactive steps to protect your business online. You may however still be exposed to cyber threats. It is important that you remain vigilant and continue to review and update your business' cyber security policies. We encourage you to review the steps in this toolkit to ensure you're doing everything you can to protect your business online.
- **Between 5 and 8 questions** – well done on putting in place some basic steps to protect your business online, however, there is more that you can be doing. Make sure you look closely at those questions you answered 'no' to as this will provide a good indication of other things you can do to improve your online security. We also encourage you to closely review the steps in this toolkit and consider engaging an expert to provide advice or source further information about cyber security.
- **Fewer than 4 questions** – you need to be doing more to protect your business online to ensure that your company and customer information is safe. Failure to do so may leave your business exposed, so we encourage you to closely review the steps in this toolkit, and consider seeking expert advice, including from accredited IT security consultants or internet service providers.



Based on materials developed by Stay Smart Online, Australia.

“Undertaking a cyber security assessment is an essential first step in ensuring you are operating in a secure online and mobile working environment. You need to consider whether the business information you hold could be a target for cyber criminals or others.”

STEP TWO

Develop a cyber security policy for your business



What does it mean?

A cyber security policy establishes the rules of engagement for protecting your business online. It includes simple security controls with regard to staff use of your network, and the operation of devices and systems used by your business.

Why is it important?

Businesses that do not have a policy in place can be leaving themselves exposed, both to external threats but also to potential legal and / or regulatory sanctions. This is particularly important for businesses that have an online e-commerce platform or collect customer data online.

It also helps to provide guidance for staff around acceptable use of devices and online materials so they understand the important role they play in protecting your company's cyber security.

A cyber security policy can also help in giving your customers confidence in your business and can, if relevant, be good to include on your company's website for this reason.

Promoting a cyber security-conscious work culture

Employees play a vital role in helping to protect a business from cyber security threats. Many people within a business who use computers and mobile devices are unfortunately not aware of security risks and their personal responsibility in helping to protect a company's cyber security.



Connect Smart research from April 2014 found 48% of Kiwis don't have passwords on their work smartphones and 56% of Kiwis don't have passwords on their work iPad or tablet. Recent research from Vodafone also found that 83% of smartphones lost have compromised business data, and that 50% of mobile device users don't set passwords or make back-ups.

It is critical then that all staff of an organisation understand at least the basics:

- Organise regular updates on your business' cyber security policies and practices.
- Make sure your staff understand the incident management processes – and the importance of reporting unusual activity or events (see step 3 of this toolkit)
- Ensure that new staff receive one-on-one or induction training on cyber security policies and practices.
- Invite external experts to provide specialist support in key areas:
 - Understanding the basics: knowing your malware and securing your wi-fi
 - Security on the move: smart home and mobile working practices
 - Understanding password security on PC and mobile devices
 - Simple steps for safer emailing and browsing online
- Raise awareness of 'social engineering', the practice whereby cyber criminals target individuals within a company in an attempt to obtain confidential information that may be used to compromise a business' cyber security. This is also known as 'spear phishing'. More information about social engineering can be found at connectsmart.govt.nz

What does it involve and where do I start?

There are a number of areas that a security policy should cover, including why it is important for your business to have one in the first place. A basic security policy may include:

- **Acceptable use of email and the internet for staff** – should certain websites be blocked to staff? Should there be a restriction on the size of email attachments?
- **Protecting your mobile** – have you articulated that a work mobile device should not be shared? Or that any mobile on which you can access work emails or information must be PIN or password protected?
- **Handling sensitive data** – who and how should sensitive data be handled and stored? You may need to consider whether there should be restrictions on access to sensitive information (“user privileges”).
- **Securing and handling equipment** – is there a system in place to track who is using equipment in the organisation? Is there an inventory of all IT equipment and software?
- **Using the internet safely** – what system is in place to ensure anti-virus, anti-spyware, operating systems, web browsers and other software are kept up to date?
- **Remote access** – what is the system to ensure security is maintained while accessing work documents from the road or at home?
- **Are there policies regarding things such as use of USB drives, CDs, DVDs etc to ensure that malware is not introduced (and important data is not stolen)?**
- **Workplace surveillance and monitoring policies** – how can you ensure that your policies are being followed by staff, and are there clear disciplinary procedures in place to deal with consequences of a breach?
- **Guidelines for customers** – what’s your business policy on what will and will not be sent via email in order to minimise exposure to phishing scams?

In addition, it can be useful to also have:

- **A process for reporting security breaches** – this may be confidential if you feel there is a scenario whereby it could be difficult for employees to speak out. For example, an employee is aware that a colleague lost a device containing sensitive information but is yet to report it.
- **Develop a code of conduct** – this would outline appropriate employee behaviour in the workplace.
- **Develop an incident management plan** (see step 3 of this toolkit)



BASIC IT SECURITY CONTROLS

- Install security software that includes a firewall, anti-virus and anti-spyware. Ensure that it is updated automatically.
- Develop a backup strategy for your critical data. A good strategy includes daily backups, an additional weekly or monthly backup, and offsite storage of at least the weekly back-up media. Test that you can recover materials with back-up data.
- If you do not have a dedicated IT Manager, assign at least one person in your organisation to have responsibility for network security (password, backups, AV updates).
- Use software from reputable sources. Keep your software patches up-to-date.
- Use spam filters to reduce the amount of spam that your business receives. Know how to manage the spam that gets through and ensure your staff know how to recognise scam and hoax emails and to avoid clicking on links or opening attachments from suspicious emails.
- Keep yourself informed about the latest online safety and security risks. Subscribe to email notification services that keep you informed about the latest online safety and security risks and solutions.

STEP THREE

Establish an incident management plan



What does it mean?

An incident management plan outlines processes for your business to deal with a cyber security breach, including what constitutes a breach and who should be contacted if one occurs.

Why is it important?

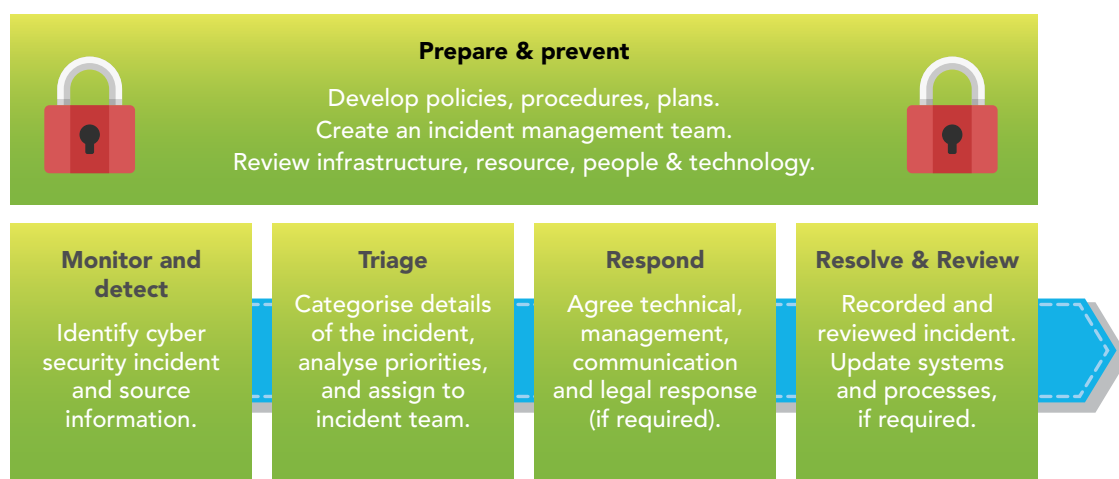
Being able to identify and address a cyber security issue quickly is critical in managing and containing the situation. This way you can minimise impacts and get back to business as soon as possible.

Unfortunately, we cannot predict when a cyber breach will occur and what exactly it might involve. The nature of online threats is constantly evolving, so even if your business already has robust cyber security systems and processes in place, a breach involving your network platforms or a member of your team could still occur.

In the worst case scenario, failure to deal with an incident quickly could lead to a major and continued disruption of your business' operations or even a breach of legal requirements.

What you can do, however, is ensure that your business is as prepared as possible so that any incident can be managed as quickly as possible and impacts minimised.

What does it involve and where do I start?



Prepare & prevent

Preparation and prevention are your most effective tools in managing a cyber security incident. See Steps 1 & 2 of this toolkit. This includes:

- Setting out the roles and responsibilities for dealing with cyber incidents, including an incident database, communication channels, and reporting forms.

Monitor & Detect

Monitor and identify any unusual activity or events that may compromise the integrity of your business' information and systems. This may involve taking steps to protect your business against topical new threats.

Unusual activity or events may include:

- Alerts and reports about potential malicious activity or vulnerabilities. This can include alerts from Intrusion Detection System software or reports from your technology or network provider.
- The theft, loss or breach of a device, including personal mobiles that staff use to access work emails. Staff may feel uncomfortable about reporting such incidents so it's important to encourage people to speak up proactively.
- External events and publicised or high-profile cyber security incidents, both overseas and in New Zealand. Read media reports and ask whether your business could be impacted – don't assume you are immune.
- General day-to-day indicators, such as unusual email activity, incident reports, or being informed by staff or customers that a breach has already occurred.

It is essential that details of any incident or potential breach in your company's cyber security are properly recorded and documented, so it can be moved on to the Triage process for further investigation and resolution.

Triage

The Triage process is a critical decision point in any incident management. It involves collecting all available information on an incident to determine the scope of the incident, its impact, and what assets are affected.

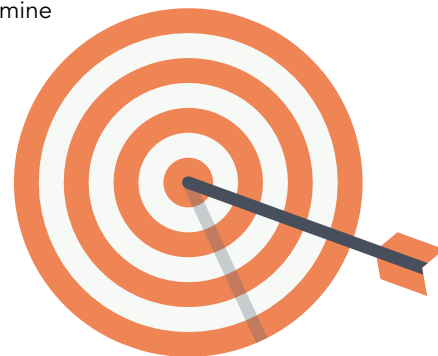
- **Categorising the incident** – how severe is it and what are the potential impacts?
- **Prioritising** – does this require an urgent escalation or can it be easily resolved?
- **Assigning** – who is responsible for managing and resolving the incident, and by when?

This information then informs the Respond process.

Respond

This involves taking actions to resolve or mitigate an incident by analysing, coordinating, and distributing information. This is likely to involve more than just a technical response; management, communications and legal responses may also be required simultaneously. Coordination and information-sharing is important.

- The technical response can include analysing the incident, advising on or planning a resolution, coordinating actions internally and externally, containing any on-going malicious activity, repairing or recovering any affected systems, generating post-mortem analysis reports, and performing incident closure. Advice from your technology / service provider or accredited IT security consultant may be required.



- Management response focuses on activities such as notifying staff and / or affected customers of a breach and advising of steps taken to resolve the situation, approving courses of action, and other communications.
- Legal response includes actions associated with an incident that could have legal or regulatory implications, such as those that involve privacy issues, non-disclosure, copyright, and other legal matters. If the incident involves fraud or cybercrime, you should report the incident to the police.

Resolve & Review

Once an incident has been resolved, make sure you understand the cause of the incident. Review your company's systems and processes to ensure that you've done all you can to minimise the risk that a similar event could occur again. Also take the time to review how the incident was managed – is there anything that your incident response team could have done better?

Emergency Incident Checklist

If an incident should occur, here's a helpful list of key questions you need to ask yourself that will help to shape your response:



- Have you called the experts? Get specialist help if needed. Do not necessarily rely on family, friends, or talented amateurs to diagnose the problem and solution – a specialist at short notice could cost you less in the long-term than getting your response wrong.
- Can you contact affected customers directly if required, and what will you tell them?
- What response is your business taking to rectify the situation? For example, resetting passwords, implementing new security procedures, remotely locking or wiping a mobile device, or temporarily suspending services and business?
- How can staff and / or customers with concerns contact you?
- Does this incident require you to contact and advise the Police, Privacy Commission or other regulatory body?
- Who is on your emergency call-tree or incident management team, and are these contact details up to date? It is critical to have cell phone numbers for outside working hours.
- Who is leading your incident response? For example, the first identifier, senior management, or someone else?
- Do you have a conference call number so all parties can share updates and progress with managing the response?
- Do you have or know media experts who can manage enquiries if required? This includes managing the situation on social media where the rules of engagement are different.

This guide is based on the model developed by the Computer Security Incident Response Teams at the CERT Division of the SEI [Alberts 2004]*. This is a high-level process that can be adapted to suit businesses of all sizes:

STEP FOUR

Regularly review and update your network security systems



What does it mean?

Congratulations! If you have followed steps 1 – 3, of this toolkit you will have taken significant steps in improving the cyber security of your business.

Once these systems are established, it is important that they become ingrained as part of a cyber security-conscious culture in the day-to-day operations of your business.

Why is it important?

Unfortunately, the type and nature of cyber threats are evolving every day.

In order to maintain high standards for your business' cyber security, it is important that you regularly review and revisit the systems, processes and policies you have in place.

What does it involve and where do I start?

Agree a timeframe for revisiting your cyber security policies, incident management plan, and training initiatives. We suggest you do this on a quarterly basis, but try and make technology updates (operating software, anti-virus software etc) as automatic as possible.

Consider whether there have been any recent security breaches – either involving your businesses or other organisations or incidents reported in the media - and determine whether or not your policies provide adequate protection from these threats. This could include general physical security breaches as well as specific cyber security breaches - often they can be linked.

Monitor and test the security policy you have in place to identify potential and actual security problems that may cost your business time and money before they become issues.

If you undertake any changes to your digital infrastructure, such as building new pages on your website, adding functionality, or changing your hardware or software, remember to check that the security of your integrated system remains robust.

Remove any software or equipment that you no longer need – but make sure you have removed any sensitive information first.

Continually review user access privileges – keep this up-to-date with your current staff and their requirements.



We hope that this toolkit provides useful guidance on the foundations to improve the cyber security of your business. That way, you can Connect Smart and protect your business and customers online.

What do I do now?

The first step is to convene a meeting to consider the steps in this toolkit and establish how your business can enhance its cyber security. Don't feel overwhelmed and decide to do nothing.

Most small businesses do not have a dedicated in-house cyber security resource, and we recommend contacting an expert in the first instance. After all, what will cost you more – a security specialist to help diagnose potential areas of exposure, or the loss of your business's valuable data, IP or reputation?

Further Information:

If you would like further information about business cyber security, the following resources may be useful:

[NetSafe New Zealand](#)

[Stay Smart Online, Australia](#)

[Cyber Security: what small businesses need to know](#)

We would also like to acknowledge the National Cyber Security Centre, Australian Government's 'Stay Smart Online' initiative and GOV.UK's '10 Steps to Cyber Security' for providing resources that have helped to inform this document.

With thanks to our SME panel of cyber security experts

In order to develop the Connect Smart for Business: SME Toolkit, a panel of experts shaped the material in this document. We would like to thank this panel of experts:

- **Colin James** – Head of Information Security, Vodafone
- **Richard Bateman** – Head of Product – Enterprise, Vodafone
- **Dr Ryan Ko** – Head of the Cyber Security Lab (CROW) and Senior Lecturer in Computer Science, Waikato University
- **Peter Plowman** – Senior Manager Fraud Risk, ANZ
- **Stephen Summers** – Economist, Business New Zealand

newzealand.govt.nz



We hope that the toolkit provides a starting point for you and your team. If you would like further information:

National Cyber Policy Office
Department of Prime Minister and Cabinet
Phone: +64 (4) 819 8200
Email: connectsmart@dpmc.govt.nz
Twitter: [@ConnectSmartNZ](https://twitter.com/ConnectSmartNZ)