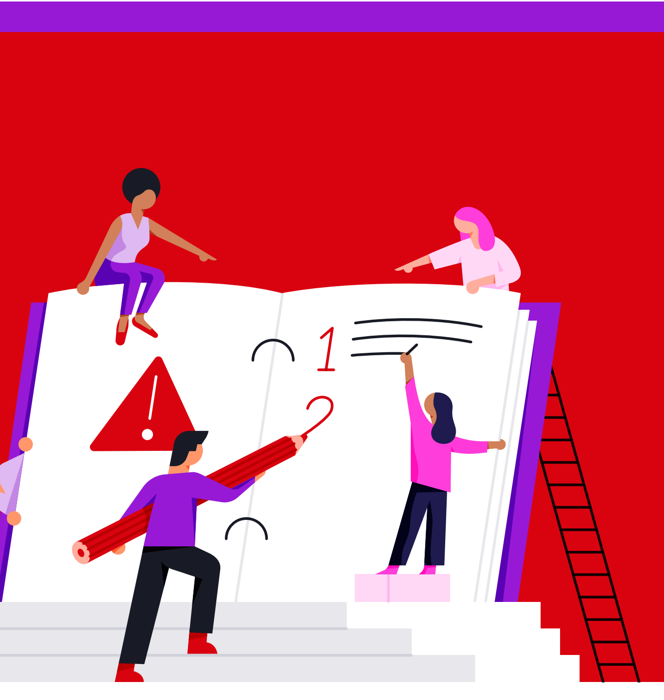
CREATE YOUR CYBER RESPONSE PLAYBOOK

5 STEPS TO MANAGE A CYBER ATTACK



BUSINESSES NEED TO BE READY FOR WHEN A CYBER ATTACK OCCURS, NOT IF

The impact of cyber crime in New Zealand in 2021.

8,831 INCIDENTS WERE REPORTED

a 13% increase on 2020

$16.8 MILLION in direct financial loss reported to CERT NZ

Scams and fraud accounted for almost **71%** of the total financial loss

3,709 phishing and credential harvesting reports

1,930 malware reports

1,897 scams and fraud reports

Source: CERT NZ 2021 Report Summary, cert.govt.nz/about/quarterly-report/2021-report-summary

STEP 1 A SMART PLAYBOOK ANSWERS BIG QUESTIONS IN ADVANCE

A Cyber Response Playbook is a series of actions that will help your business prepare for and reduce the impact of a cyber attack.

It's important to know the answers to the following before a cyber attack occurs.

1. Who is the lead for capturing information, managing meetings and providing updates?
2. Who will communicate with key stakeholders, including suppliers, customers, business leaders, employees, consultants, regulators, media and the public?
3. What are your key systems, data and accounts, and where are they backed up to?
4. Do you have a disaster recovery plan? How will you ensure business continuity? E.g., for goods coming in and out?
5. Do you have a backup of your most recent payroll, to ensure you can continue to pay staff?
6. Do you have third party incident response/IT/legal teams you deal with?
7. Do you have cyber insurance? Make sure you know how to activate it, and what it will cover.

TIP Rehearsing your Cyber Response Playbook can identify security gaps and improve recovery times.

PRINT OUT A COPY

In some ransomware attacks, you might lose access to your systems, including the place where you've stored your playbook. Once you've prepared your playbook print a copy to ensure you can still access it in the event of a cyber incident.

STEP 2 WHO NEEDS TO KNOW?

A well-planned playbook will include a list of people and institutions to be notified.

Who should be on your list?

CERT NZ

Email: info@cert.govt.nz
Phone: 0800 CERT NZ (0800 2378 69)
Online: CERT.govt.nz

YOUR BANK
Protect your digital banking services and cash flow.

IT VENDORS/CONSULTANTS
Ensure phone numbers are easily accessible in a crisis.

SUPPLIERS
Advise on data breaches that may impact their operations.

POLICE
Report the incident as part of cyber crime shutdown efforts.

MEDIA
Release a statement, if relevant, noting you have executed your business's cyber response plan.

INSURER
Check coverage for a ransom payment or forensic investigations, for example.

TIP You may have legal obligations to notify regulators, and the NZX if you're publicly listed.

STEP 3 YOU'VE BEEN HACKED... NOW WHAT?

1. SOUND THE ALERT

Engage IT advisers or employees so they can limit any damage. Time for cyber response team members to activate response checklists.

2. DETECT THE THREAT

Identify the nature of the cyber attack. The most common cyber threats are:

PHISHING
Fake emails or messages trick people into clicking links or attachments, downloading malware, or providing personal or financial information.

RANSOMWARE
Cyber criminals lock up computer files and data and demand payment for release.

BUSINESS EMAIL COMPROMISE
Attackers infiltrate networks and initiate emails to trick people into sending payments or sensitive information.

DENIAL OF SERVICE
Servers are flooded with traffic to shut down systems.

3. CONTAIN THE DAMAGE

Take initial steps to mitigate business fallout.

- Disconnect all devices from your network to stop infections spreading.
- You will need your IT support to provide a detailed forensic analysis of your systems to highlight breaches.
- Scan backups for malware on a safe computer.

TIP Take a picture of the cyber attack message or ransom note. It may contain key information for your IT team.

STEP 4 RESET AND RESTORE

Once the attack is contained, get up and running again.

CHECK BACKUPS
And ensure that the attacker hasn't accessed or modified your data.

WIPE CLEAN
If you can, do a complete wipe and restore from a verified backup.

CLEAN IN PLACE, IF YOU MUST
If you can't completely wipe, work with an IT provider to clean all affected devices.

TIP These kinds of incidents can be very stressful. Keep an eye on your employees' stress levels.

STEP 5 STOP FUTURE ATTACKS

Continuously review and update your playbook. Prevention is the best protection.

UPDATE SOFTWARE
Keep all applications, software and point-of-sale systems up-to-date.

TIGHTEN SECURITY
Use multi-factor authentication (MFA) as proof of identity to stop unauthorised access to systems.

BACK UP DATA
Back up your systems and critical data regularly, and store that data in a secure external location. This includes using a cloud-based solution or removing hard drives/USBs from your network once a backup is complete.

UPDATE & EVOLVE
Make sure your playbook includes strategies to counter evolving cyber threats (e.g., have a remote access protocol for employees working from home, and set up firewall rules).

TIP Treat cyber crime as a business risk – not just an IT problem.

USEFUL LINKS

FRAUD & SCAMS
netsafe.org.nz

CYBER SECURITY ISSUES
cert.govt.nz

INVESTMENT SCAMS
fma.govt.nz

See Westpac's Security Hub **westpac.co.nz/cybersecurity** for more information on how to keep you and your business safe. You can also discuss cyber security strategies with your Relationship Manager.

TOGETHER GREATER

CERT SAW A 65% INCREASE IN THE NUMBER OF CYBER SECURITY REPORTS MADE BY INDIVIDUALS, SMALL BUSINESSES AND LARGE ORGANISATIONS IN 2020, COMPARED TO 2019.

Source: cert.govt.nz/about/quarterly-report/2020-report-summary

GTS10336-1222