

# 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.

## An overview of cyber crime in Australia.



**There's a cyber attack every six minutes** compared to every seven minutes last financial year.



### Average loss per cyber crime reported

- Small business: \$49,000
- Medium business: \$62,800
- Large business: \$63,600.



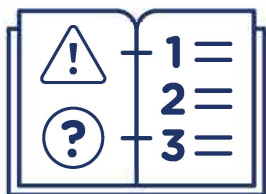
**Over 87,400 cyber crime reports** over the past financial year.



**Over 100 calls a day** to the Australian Cyber Security Hotline. Up 12% on last financial year.

# Step 1.

## A smart playbook answers big questions in advance.



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

# Step 2.

## Who needs to know?



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

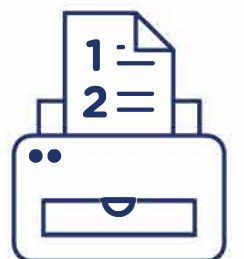
A Cyber Response Playbook is a series of actions that will help your business prepare for and reduce the impact of a cyber attack.

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.

## 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.



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

Who should be on your list?

### Australian Cyber Security Centre

Online: [cyber.gov.au/report](https://cyber.gov.au/report)

Phone: 1300 CYBER1 (1300 292 371)

### 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' cyber response plan.

### Insurer

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

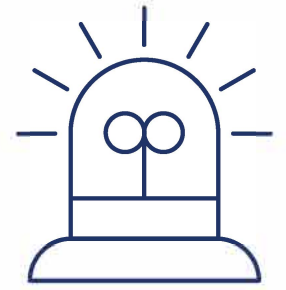
# Step 3.

## You've been hacked...

### Now what?

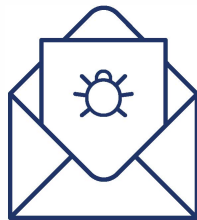
## 1. Sound the alert.

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.

**Tip**



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

## 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.



## Step 4. Reset and restore.



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

## Step 5. Stop future attacks.



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

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



### Check backups.

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



### Clean in place, if you must.

If you can't completely wipe, work with an IT provider to clean all affected devices.



### Wipe clean.

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

---

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.

### 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.

### Tighten security.

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

### Update and 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).

# Useful Links.

## Start here.

The ACSC’s [The Essential Eight](#) outlines a series of cyber safe strategies for all organisations.

## Be proactive.

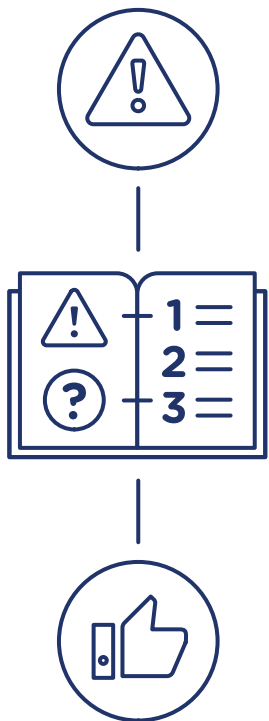
Follow the ACSC’s [cyber incident response plan](#) template to plan for action in a cyber attack.

## Be collaborative

Learn more on the latest cyber threats and protections and share your insights via [Joint Cyber Security Centres](#).

See BankSA’s Security Centre [banksa.com.au/security](#) for more information on how to keep you and your business safe.

You can also discuss cyber security strategies with your Customer Relationship Manager.



**“A plan or Cyber Response Playbook is crucial for hitting the ground running if there is a cyber incident”**

Matt Smith, Assistant Director-General,  
Incident Management, Australian Cyber Security Centre