Cybersecurity

Legal information for not-for-profit community organisations

This fact sheet covers:

- key cybersecurity terminology
- common cyber risks to look out for
- the life cycle of a data breach
- how to create a cyber incident response plan

Cybersecurity is fast becoming one of the most important concerns for organisations.

Regardless of the industry your organisation operates in, your organisation probably collects and stores a huge amount of information and uses many different kinds of technology in its daily operations.

Cyber security is the practice of protecting this information, your organisation's electronic systems and digital information and reducing the likelihood of a breach. While it is not possible to prevent data breaches from occurring in 100% of cases, there are steps you can take, (some of which are discussed in this factsheet) to minimise the likelihood of a breach occurring, and the extent of harm caused.

Note

This fact sheet provides information on cybersecurity. This information is intended as a guide only, and is not legal advice. If you or your organisation has a specific legal issue, you should seek legal advice before making a decision about what to do.

Please refer to the full disclaimer that applies to this fact sheet.

Terminology

Some of the cybersecurity terminology used in this fact sheet is set out below:

brute force attack	where a hacker automates millions of passwords to guess as many passwords as possible in a short space of time
DDoS	where a hacker sends huge amounts of data to a network at once to effectively paralyse it
firewall	software that automatically blocks certain traffic to a network (for example, pop-up blockers)

intrusion detection system	software that monitors a network and sends alerts when it discovers suspicious activity
logs/logging	an audit record of activity on an organisation's software or system
malware	malicious software designed to gain access to or damage a computer system
phishing	fraudulent emails designed to trick users into revealing information (such as bank details)
ransomware	malware which blocks access to your systems and then demands money in return
spear phishing	a phishing attack targeting a specific person
social engineering	a fraudster impersonates someone known to you, deceiving you into providing information, which can be used for fraud or access to systems
spyware	software installed on a computer to secretly monitor the user's activities
two factor authentication	after their password, a user must pass a second layer of security, such as entering a one-time code which is sent to their mobile phone

Common cyber risks

There are many cyber risks which organisations face.

These can be broken down into:

- **internal risks**, which originate from within your organisation, and
- **external risks**, which are the more commonly known risks are posed by third party hackers

These risks can also lead to very different consequences for your organisation, from damage to reputation to business interruption costs.

Note – insurance

While having insurance is not a solution in itself to cyber risk, you may wish to consider obtaining cyber liability insurance to protect your organisation and assist with managing the impact of a data breach. For more information about cyber liability insurance, refer to our fact sheet on insurance.

Internal risks

Note

The Office of the Australian Information Commissioner (**OAIC**) latest report (June 2021) shows that human error accounted for 30% of the total cyber breaches notified for the period 1 January to 30 June 2021. (We've set out some of the report's findings below).

Internal risks can best be addressed through training staff members. This training should be regular and customised according to your systems and internal structures.

Cyber safety is the responsibility of every individual in an organisation.

It's important to ask whether all staff members in your organisation (such as your board, employees, independent contractors and volunteers) know how to answer questions (or where to find the answers to questions), such as:

- Who can suspicious activity or emails be reported to?
- What does a suspicious email look like?
- What are the implications of the organisation's information being shared accidentally?

Who are staff members?

It is not just an organisation's employees that use or engage with the organisation's technology systems such as email. Board members, independent contractors and volunteers are at risk of a cybersecurity breach as well. In this fact sheet we collectively refer to these people as 'staff members.'

Example

Danielle works for a not-for-profit community organisation. When the Finance Manager is on leave, Danielle receives an email from the Finance Manager's email address asking Danielle to urgently pay an invoice. Danielle thinks nothing of it and transfers the money. When the Finance Manager returns from leave a few days later, she reveals she did not send any invoices. It soon becomes apparent that a hacker had gained access to her email account and used it to send a phishing email. The money has now been lost.

If Danielle knew the risk of phishing emails and to treat emails requesting money with care, she may have noticed the email was suspicious. Danielle realised her mistake within a few days, but what if she didn't realise until after the Finance Manager had sent several of these emails asking for more and more money?

Summary of some of the risks and potential effects of an internal cyber breach

Risk	Potential effects on organisation
• A disgruntled staff member takes internal data or publishes it when they leave an organisation	• Damage to reputation • Spread of commercially sensitive information
• A staff member accidentally clicks or responds to a phishing or fraudulent email impersonating an executive or third-party supplier	• Malware shutting down your systems for a day or longer, disrupting your business • Money being transferred to scammers
• A staff member forgets to BCC (blind copy) recipients of an email list, and instead makes the emails visible	• Possible breach of privacy law implications
• A staff member provides personal information and credit card details in response to a phishing email	• The information may be used to imitate a staff member or for identity theft • The information may be used to deceive the organisation into making a fraudulent payment (social engineering)

- A staff member provides its organisation login credentials in response to a fraudulent event request to update log in details

- Access to your mailbox at work and potentially the entire organisation network
- Access could be used to 'pull out' sensitive staff member or client information or for social engineering fraud

OAIC's Notifiable Data Breaches Report: January to June 2021

This report shows:

- 446 breaches were notified under the scheme for the period 1 January to 30 June 2021, (a decrease of 16% compared to 530 notifications from July to December 2020).
- The health sector remains the highest reporting industry sector, notifying 19% of all breaches. The second largest sector was finance (including superannuation), notifying 13% of all breaches, followed by legal, accounting and management services, Australian Government and insurance.
- Malicious or criminal attacks remain the leading source of data breaches, accounting for 65% of the total.
- 66% of malicious or criminal attacks involved intrusive cyber incidents with the remaining 34% caused by social engineering or impersonation, actions taken by a rogue employee or insider threat, and theft of paperwork or storage devices.
- The remaining sources of total data breaches reported were human error, accounting for 30% of the total, while 5% of the total were due to system fault.
- 43% of all data breaches resulted from cyber security incidents with the top cyber incidents from the reporting period being phishing (30%), compromised or stolen credentials (27%), ransomware (24%), hacking (9%), brute-force attack (5%) and malware (5%).
- 93% of data breaches affected 5,000 individuals or fewer, while 65% affected 100 people or fewer.
- Contact information (91%), identify information (55%) and financial details (43%) remain the most common type of personal information involved in data breaches. The remaining categories of personal information include health information and tax file numbers.
- 72% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach.

External risks

External risks can best be addressed using protection and detection software, as well as security techniques like two factor authentication. However, having software and systems in place doesn't mean your organisation will be immune from a cyber-attack. Staying vigilant is key.

Example

Tom is a volunteer for his local neighbourhood centre. Whist undertaking research, Tom downloaded a file from a website – however, when he opened the downloaded file, it was not what he expected. Tom knew he had to report the incident to the IT manager, and did so. The IT manager discovered that the downloaded file actually installed ransomware to Tom's computer, which had begun to encrypt the files on their main server. Luckily, the neighbourhood centre maintains regular backups of their system and was quickly able to restore it to a very recent version.

Depending on the extent of the data breach, how quickly you can recover, and what kinds of information were compromised, any data breach can cause significant costs, whether because of interruptions to your business, reputational damage, financial loss to clients and the public, or loss of data.

Summary of some of the risks and potential effects of an external cyber breach

Risk	Potential purposes and effects on the organisation
• A website link, spam email or similar introduces ransomware to your system	• Disruption to your systems, potentially to encourage you to pay a ransom in return for access to your files • Damage to your systems, to both disrupt your system initially and make recovery more difficult • Stealing data, e.g. credit card information or other personal information • Tricking staff members into sending money to third parties • Possible breach of privacy law implications
• A DDoS attack overloads and crashes your servers	
• A staff member accidentally clicks or responds to a phishing email (this risk has both internal and external aspects)	
• A brute-force attack on staff member credentials	

There can be various motives behind external cyber-attacks, depending on whether the hacker merely wants to disrupt your business, or wants access to specific information. This will be especially important to consider if you hold personal information, especially sensitive information about individuals, like health information.

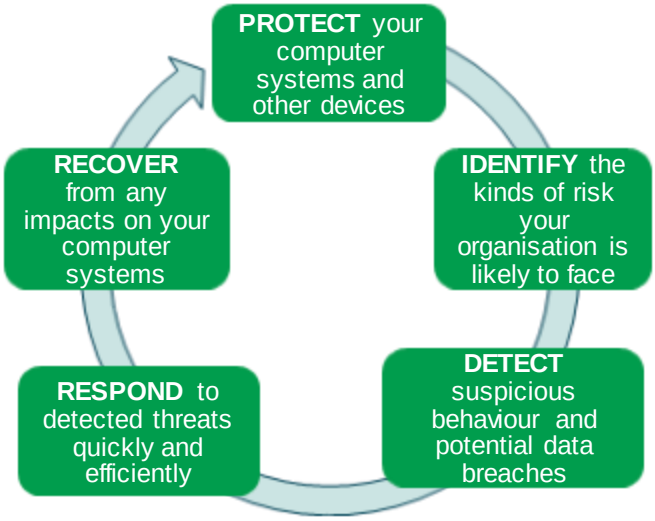
Caution

Depending on your annual revenue or other criteria, you may be subject to obligations under the Australian Privacy Principles. This includes an obligation to notify data breaches to the Office of the Australian Information Commissioner and individuals affected in some cases.

Refer to our fact sheet on the Notifiable Data Breaches Scheme and our privacy guide for further information.

Life cycle of a data breach

Each step in the life cycle of a data breach is an opportunity for you to protect your organisation's information.



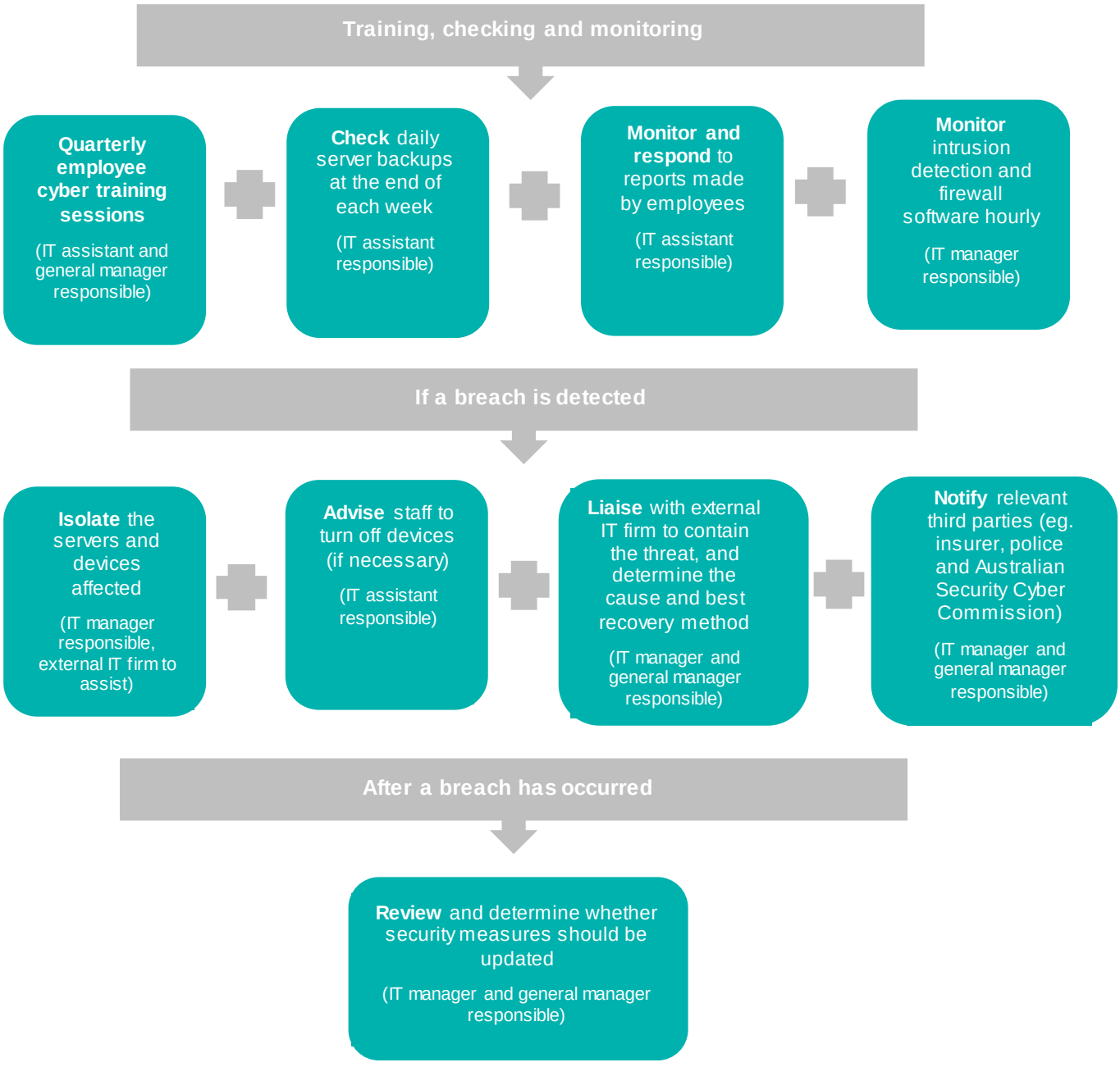
Step	What you can do
Identify risks	• Consider what types of data your organisation holds, and how you store that data (for example, financial or health information) • Consider what your 'crown jewels' are, what would particularly make you a target • Consider internal risks, like a staff member clicking a phishing email
Protect your systems	• Install and maintain up-to-date firewall and anti-malware software • Use two factor authentication, regularly update passwords, mandate different passwords for different systems and ensure complexity requirements for passwords are high • Provide regular staff member training on cyber risks including suspicious links and downloads • Delete login credentials for users that no longer require access to your systems (ie. former employees or contractors) • Ensure that login pages for administrative systems are not linked to on publicly facing webpages or discernible for malicious actors
Detect suspicious behaviour	• Install and maintain an up-to-date intrusion detection system • Appoint a staff member or team to regularly monitor notifications from this system and check for false positives • Ensure all audit and logging safeguards in key software (for example, Microsoft Outlook) are turned on
Respond to threats	• Create a simple, easy to follow data breach response plan (see below) • Organise a flowchart of staff or external IT consultants who are responsible for each step of the process • Conduct an audit into recent transfers made or requested to identify any potential instances where a cyber breach may have attempted, or would attempt, to issue fraudulent transfer instructions. Inform employees about the natures of transfers and requests that are safe, related to their employment and how to identify these. Direct employees to report requests for information from sources with which they are not familiar and to seek guidance before approving or interacting with any requests that seem unclear.
Recover from impacts	• Save regular backups of your key servers so previous versions can be restored if there is a data breach • Ensure the recovery process is part of your incident response plan, including regular reviews and testing of systems

A cyber incident response plan

A cyber incident response plan is a document which sets out exactly what you need to do in the event of a data breach.

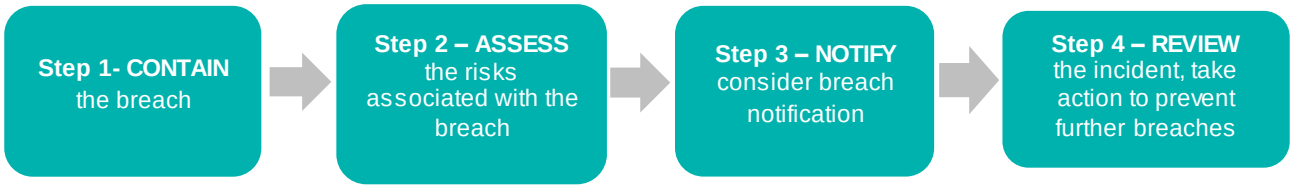
This includes **who** is responsible for what tasks and **what** steps you will take to contain the breach. Your plan should be catered to what technologies your organisation uses, the level and type of information you hold, your financial resources, and the IT resources and staff you have access to. You may create particular incident response plans for different kinds of security breaches, for example malware or tampering with payment terminals.

Your response plan should set out the contact details and responsibilities of all key personnel, including internal staff members, IT consultants, legal advisors and server hosting providers, as applicable.



Privacy law and Notifiable Data Breach Scheme

A breach in your cyber security can easily involve a breach in privacy law. If your organisation is required to comply with privacy law and/or has a privacy policy, make sure your cyber incident response plan speaks to your privacy policy and your organisation's plan to deal with privacy breaches. The steps above (contain, liaise and review) are similar to those needed to respond to a data breach.



General incident response plan check list

Incident response plan check list

- ☐ What systems and technologies do you rely on most heavily?
- ☐ Who is responsible for checking whether detected threats are legitimate, or false positives?
- ☐ How often are servers going to be backed up? Who will monitor that these backups are being completed and stored successfully?
- ☐ How often are you going to check detection software notifications?
- ☐ Who is responsible for reviewing incidents reported by employees?

Privacy law and data breach response check list

If your organisation is required to comply with privacy law and/or has a privacy policy, your organisation may benefit from the Office of the Australian Information Commissioner (**OAIC**) publications which include simple guides to privacy obligations and dealing with data breaches and a simple checklist for responding to a data breach covers of matters including:

- What is a data breach is and how can staff identify one
- Escalation procedures and reporting lines for suspected data breaches
- Members of the data breach response team, including roles, reporting lines and responsibilities
- An approach for conducting assessments
- A record-keeping policy to ensure that breaches are documented

You can access the checklist in the document entitled 'Data Breach Preparation and response plan' on the OIAC website.

Related Not-for-profit resources

We recommend you read this fact sheet in conjunction with our:

- privacy guide, which outlines what is covered by privacy law, sources of privacy laws and exemptions obligations under privacy law including consent, notification and storing personal information and compliance, and privacy policies
- fact sheet on the Notifiable Data Breach Scheme which covers what the scheme is, whether it applies to your organisation, how to identify when breaches should be notified, how to notify and penalties for non-compliance

Resources

Not-for-profit Law resources

- Privacy guide

  This guide looks at privacy laws more generally and includes detailed information about the Privacy Act and state privacy laws in Australia and explains the obligations an organisation has under these laws.

- Notifiable Data Breaches Scheme fact sheet

  This fact sheet is a supplement to our privacy guide. It is for not-for-profit organisations in Australia who want to understand more about their obligations under the notifiable data breaches scheme

- The people involved

  This webpage gives guidance to not-for-profits deciding whether to formally incorporate or remain as an unincorporated group.

Other related resources

- The Australian Government's 'Cybersecurity: Small Business Best Practice Guide'
- The Office of the Australian Information Commissioner website