Cybersecurity

Legal information for community organisations

This fact sheet covers:

- key cybersecurity terms
- common cyber risks
- creating response plans
- data breaches
- ransomware attacks

Disclaimer

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 deciding what to do.

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

Note

This fact sheet aims to help your organisation handle personal information in a way which is consistent with both your legal obligations and community expectations.

The Office of the Australian Information Commissioner's (**OAIC**) Australian Community Attitudes to Privacy Survey 2023 demonstrates a major shift in how Australians expect their personal information to be handled – Australians value organisations who take proactive and quick reactive actions to protect customers and only collect information that is necessary.

If your organisation doesn't handle personal information in a way that is consistent with community and regulatory expectations, this can cause significant damage to the organisation from a legal, financial and reputational perspective.

Cybersecurity is one of the most important concerns for Australian organisations.

Australia is regarded as a soft target when it comes to cybersecurity, and cyber-attacks on Australian organisations are widespread.

Regardless of the industry your organisation operates in, your organisation probably collects and stores a significant amount of information and uses many kinds of technology in its daily operations. **It is extremely**

important to ensure that your organisation is taking steps to protect and secure that personal information.

Cyber security and privacy are two sides of the same coin – both work to protect your organisation's information, electronic systems and digital information and reduce the likelihood of a breach.

While it's not possible to prevent data breaches from occurring in 100% of cases, there are steps you can take, (some are discussed in this fact sheet) to minimise the likelihood of a breach occurring, and the extent of harm caused.

Depending on your organisation, some data breaches require you to assess the likelihood of harm with the data breach and notify the OAIC and affected individuals under the Privacy Act's Mandatory Notifiable Data Breach Scheme.

For more information, see 'Privacy Law and Notifiable Data Breach Scheme' below and our fact sheet on the Notifiable Data Breach scheme.

Terminology

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

ACSC	Australian Cyber Security Centre, the Australian Government's lead agency for cyber security
brute force attack (compromised credentials)	automated software is used to generate a large number of consecutive guesses as to the value of the desired data (for example, passwords)
cyber incident	a cyber incident targets computer information systems, infrastructures, computer networks, or personal computer devices
DDoS	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	software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system
OAIC	Office of the Australian Information Commissioner, the Australian Government regulator for privacy and freedom of information
phishing	an attack in which the target is contacted by email or text message by someone posing as a legitimate institution to lure individuals into providing personal information, sensitive information or passwords

ransomware	a type of malicious software designed to block access to data or a computer system until a sum of money is paid or other conditions are met
spear phishing	when a phishing attack (for example, emails and text messages) are highly targeted to the recipient
social engineering	an attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations
spyware	software installed on a computer to secretly monitor the user's activities
multi-factor authentication (MFA)	a security measure that requires two or more proofs of identity to grant you access, typically a combination of something the user knows (PIN, secret question), something you have (card, token) or something you are (fingerprint or other biometric)

Common cyber risks

There are many cyber risks which organisations face.

Cyber risks 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 unauthorised third parties (such as hackers)

These risks can also lead to very different consequences for your organisation, from harm to your customers to financial loss to reputational damage to business interruption costs.

Note – ransomware

Ransomware is an increasingly prevalent external risk in Australia, with the ACSC in its most recent Cyber Threat report assessing that:

- ransomware remains the most destructive cybercrime threat, and
- all sectors of the Australian economy have been directly impacted by ransomware in 2021-22

The OAIC has also stated that ransomware remains the **top source** of cyber incidents.

Note – insurance

While having insurance is not a solution to cyber risk, you may consider obtaining cyber liability insurance to protect your organisation and assist with managing the impact of a data breach. Insurance companies are increasingly looking at an organisation's cybersecurity framework and practices including security controls, training and education.

For more information about cyber liability insurance, see to our webpage on managing insurance and risk.

Internal risks

Note

The OAIC's latest report (June 2023) shows that human error accounted for 26% of the total notifiable data breaches notified for the period 1 January to 30 June 2023. (We've set out some of the report's findings below).

Internal risks are best addressed through training staff members. This training should be regular and fit-for-purpose in that it is customised according to the staff member's role, your business, systems and internal structures.

Cyber safety is the responsibility of every individual in an organisation and requires ongoing management.

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 does a notifiable data breach look like and who do I report or escalate it to?
- 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. One Friday afternoon, she mistakenly sends a large spreadsheet containing personal information and health information to the incorrect distribution list containing a significant number of unintended recipients (over 100 unintended recipients).

When Danielle realises she has sent this accidental email, she decides to wait until Tuesday to tell her manager as they are on leave. On Tuesday, after discussing this with her manager, Danielle sends a further email to the incorrect distribution list advising them that the email had been sent in error and requesting that the email be deleted. While some of the recipients advised they had deleted and not shared the email, she does not hear from everyone. Other recipients were angry and asked why it took so long.

While Danielle realised her mistake quickly, the response was delayed. In addition, not everyone confirmed they deleted the unintended email and spreadsheet.

In a similar example, the OAIC found the incident to be a notifiable data breach as the mitigation steps taken were not effective (as not everyone confirmed they deleted the email and spreadsheet).

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 rogue employee or insider threat takes internal data and information and discloses this to other entities	• Damage to reputation • Spread of commercially sensitive information
A human resources staff member copies employee records onto a USB stick to do further work at home. On their way home from work they accidentally misplace and lose the USB stick	• Damage to reputation • Spread of commercially sensitive information • Possible breach of privacy law implications
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
An IT staff member becomes aware that its member database has been publicly available on the internet due to a technical error	• Damage to reputation • Possible breach of privacy law implications
A third party service provider which manages customer billing information has been hacked. The third party did not tell the non-for-profit organisation who found out through the news. The organisation learns that the third party also did not have any security controls in place.	• Damage to reputation • Very likely risk of serious harm to the organisation's customers • Possible breach of privacy law implications

Responsibility for your third party providers

It's also important that boards of not-for-profit organisations take steps to manage the cybersecurity risks with third-party providers. As organisations typically rely on third parties for software and other business critical services, it is important that this risk is managed.

Australia's corporate regulator, ASIC has indicated that:

- it will target boards and executives for failures to protect its customers from cybersecurity risks, and
- third party providers are a key business weakness which it expects to be managed by organisations

The risk of third party providers can be managed by:

- assessing the privacy and cybersecurity risks before engaging the third party provider and making necessary adjustments – this can be done through a security assessment and a Privacy Impact Assessment, and
- ensuring your contractual arrangements also require that they manage cybersecurity risks

External risks

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

Cybersecurity and privacy risks are best tackled with a combination of security measures and other measures such as having adequate internal practices, procedures and systems, appropriate and regular training, and fostering a privacy and security aware culture.

Example

Tom is a volunteer for his local neighbourhood centre. While researching, 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 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 able to quickly restore the system 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 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, for example, 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 staff member scans a QR code on an email which impersonates a supplier requiring payment and bypasses the organisation's security tools	
A brute-force attack on staff member credentials	

Note

The nature of cyberattacks are constantly evolving and cybercriminals are consistently adapting to defences – it's important that staff members are trained constantly on how to recognise these changing external risks.

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.

Depending on the nature of the data breach, you may also be required to notify other regulators including:

- the Australian Digital Health Agency – if the data breach relates to the My Health Record System, and
- a NSW public sector agency if you are providing services to them as they will need to assess their obligations under the *Privacy and Personal Information Protection Act 1998* (NSW).

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 cyber incident or data breach.

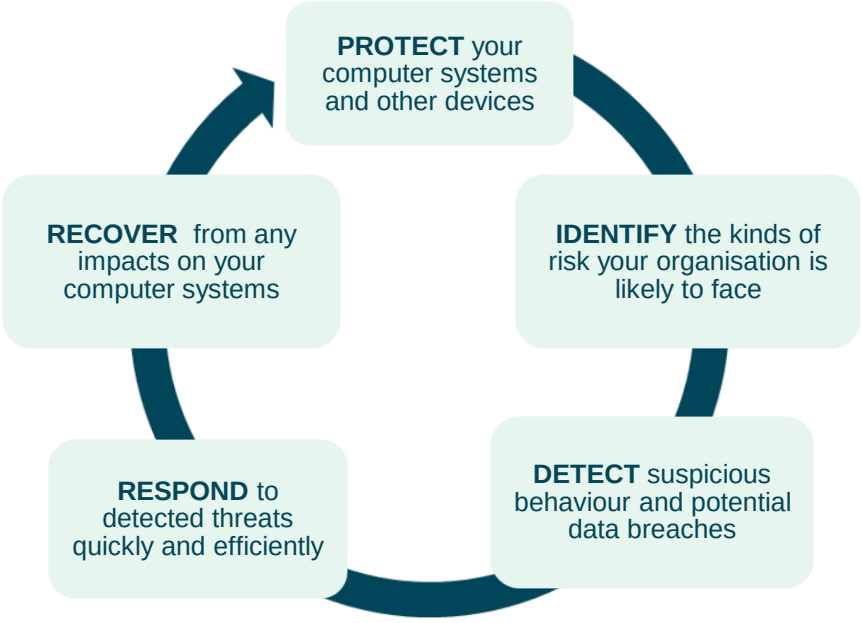
This includes **who** is responsible for what tasks and **what** steps you will take to contain the breach. Your plan should be catered to what technologies your organisation uses, the level and type of information you hold, your financial resources, and the IT resources and staff you have access to. 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.

For more information about preparing a cyber response plan, see the ACSC's webpage 'Cyber incident response plan' which include guidance, a template and a checklist.

Data breaches

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
Consider the ACSC's Essential Eight Risk Maturity Framework	• The Essential Eight are a series of mitigations the ACSC recommends as one of the most effective approaches to protect against cyber threats • Consider implementing the Essential Eight maturity model and implement measures appropriate to the type and size of your organisation

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.

step 1	• **CONTAIN** the breach
step 2	• **ASSESS** the risks associated with the breach
step 3	• **NOTIFY** Consider breach notification
step 4	• **REVIEW** the incident, take action to prevent further breaches

Every data breach is different and the four steps may not necessarily happen in order

For example, in some data breaches, it may be more important to notify affected individuals while the assessment is ongoing.

The Notifiable Data Breach Scheme is a mature regime

Your obligations under the Privacy Act's Notifiable Data Breach Scheme are important. The OAIC has said that the Notifiable Data Breach Scheme is a mature regime and that it expects entities to have not only strong practices to protect personal information but to have processes which ensure a timely response if a data breach occurs.

OAIC's Notifiable Data Breaches Report: January to June 2023

This report shows:

- 409 breaches were notified under the scheme for the period 1 January to 30 June 2023, (a decrease of 16% compared to 486 notifications from July to December 2022).
- The health and finance sector remains the highest reporting industry sector. Health reported 63 breaches (15% of all notifications) and finance 54 breaches (13% of all notifications).
- Malicious or criminal attacks remain the leading source of data breaches, accounting for 70% of the total.
- The remaining sources of total data breaches reported were human error, accounting for 26% of the total, while 3% of the total were due to system fault.
- Human error breaches were the fastest to be identified with 81% identified in 30 days or fewer. Only 57% of system faults were identified in the same timeframe.
- 42% of all data breaches resulted from cyber security incidents.
- Social engineering remains prevalent with one in five data breaches in the first half of 2023 caused by social engineering or impersonation.
- Ransomware remained the top source of cyber incidents with 31% of cyber incidents being a result of ransomware. Compromised or stolen credentials followed as the second most common source of cyber incidents at 29%, then phishing (19%), hacking (9%), malware (8%) and brute-force attacks compromising of 4% of all cyber incidents.
- 91% of data breaches affected 5,000 individuals or fewer, while 63% affected 100 people or fewer.
- Contact information (87%), identify information (65%) and financial details (40%) 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.
- 78% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach.

If your organisation is required to comply with privacy law, has a privacy policy or both these things apply, refer to the Office of the Australian Information Commissioner (**OAIC**) website which has published guides to privacy obligations and dealing with data breaches.

The ACSC website also contains resources to help your organisation manage cybersecurity.

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

Ransomware attacks

Ransomware attacks are increasingly prevalent and you should be aware of the risks.

Ransomware attacks generally aim to disrupt critical services to your organisation by preventing access to key files and systems in return for a ransom (usually in the form of cryptocurrency).

Carefully consider how a ransomware attack would affect your organisation and prepare accordingly.

The ACSC recommends considering:

- What can you replace, for example, files you downloaded from the internet?
- What can't you replace, for example, photos that aren't backed up?
- What would you spend to recover your information or device after a ransomware attack?

Also consider creating and implementing a ransomware policy which set out steps involved in responding to a ransomware attack as well as specifying individual responsibility in your organisation for taking these steps.

The ACSC webpage 'What is ransomware?' contains resources on protecting your organisation from ransomware attacks.

Also see the ACSC webpage 'Report and recover from ransomware'.

The below government agencies may also need to be notified in the event of a ransomware attack:	
Australian Cyber Security Centre (**ACSC**)	• Federal agency for cybersecurity. May provide a position on whether payment should be made, especially if a foreign government is a potential threat agent. • Make a Cyber Report to the ACSC to request their involvement. The ACSC will then forward the report to the CISC or Australian Federal Police for involvement as needed.
Cyber and Infrastructure Security Centre (**CISC**)	• If critical infrastructure is affected by the ransomware attack, CISC is the deferral agency for critical infrastructure and may provide a position on ransom payment.
Australian Federal Police	• Australian Federal Police combat cybercrime and seek to disrupt cybercriminals.
Department of Health	• May provide advice if public health is at risk resulting from the ransomware attack.