Cyber security

Legal information for community organisations

This fact sheet covers:

- key cyber security terms
- common cyber risks
- protecting information from data breaches
- creating response plans
- reforms under the Cyber Security Act

Disclaimer

This fact sheet provides information on cyber security. 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.

Cyber-attacks on Australian organisations are becoming increasingly widespread and Cyber security is one of the most important concerns for Australian organisations.

Cyber security and compliance with privacy laws 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 guarantee that your organisation will never suffer a cyber incident or data breach, there are steps you can take to minimise the likelihood of an incident or breach occurring, and to limit the extent of harm caused.

Note – law reforms

In 2023, the Australian Government released the 2023-2030 Australian Cyber Security Strategy, a roadmap to manage cyber risks and support citizens and Australian businesses.

The *Cyber Security Act 2024* (Cth) (**Cyber Security Act**) implements four initiatives under this strategy and includes measures to:

- mandate minimum cyber security standards for smart devices
- introduce a mandatory ransomware and cyber extortion reporting obligation for certain businesses to report ransom payments
- introduce a Limited Use obligation for the National Cyber Security Coordinator to encourage industry engagement with the government following cyber incidents, and
- establish a Cyber Incident Review Board to conduct reviews of significant cyber incidents and share lessons learned

The Australian Government has published fact sheets on these measures. Also see below for more information about the Cyber Security Act.

Terminology

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

ASD and ACSC	Australian Cyber Security Centre, the Australian Government's lead agency for cyber security which operates within the Australian Signals Directorate Agency (**ASD**)
Brute force attack (compromised credentials)	This is when automated software is used to generate many consecutive guesses as to the value of the desired data (for example, passwords)
Business email compromise (BEC)	BEC is a targeted form of phishing. Criminals target organisations and try to scam an individual to provide money or goods, using a fraudulent email within the business. Criminals also target employees to reveal important business information.
Cyber incident	This is an unauthorised impairment or attack that targets computer information systems, infrastructure, computer networks, or personal computer devices
Cyber Incident Review Board (CIRB)	The independent statutory advisory body established to conduct post-incident reviews on a no-fault basis, after a cyber security incident has been voluntarily shared with the ASD
Distributed Denial of Service (DDoS)	This is when a threat actor (hacker) sends huge amounts of data to a network at once to effectively paralyse it
Firewall	This is software that automatically blocks certain traffic to a network (for example, pop-up blockers)

Intrusion detection system	This is software that monitors a network and sends alerts when it discovers suspicious activity
Logs/logging	This is an audit record of activity on an organisation's software or system
Malware	This is software which is specifically designed to disrupt, damage, or gain unauthorised access to a computer system
Multi-factor authentication (MFA)	This is 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)
National Cyber Security Coordinator	The National Cyber Security Coordinator leads the whole of Government in the coordination and triaging of action in its response to significant cyber security incidents.
OAIC	This is the Office of the Australian Information Commissioner, the Australian Government regulator for privacy and freedom of information
Phishing	This is 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	This is 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
Ransomware payment	Where a demand is made of the reporting a business that is subject to the law and it, provides or is aware that another business has provided on their behalf, a payment or benefit that is directly related to the demand.
Spear phishing	This is when a phishing attack (for example, emails and text messages) is highly targeted to the recipient
Smart devices	Smart devices, also called 'internet of things (**IoT**) devices' are everyday items that are capable of internet or network connectivity (for example, payment terminals, drones, security cameras and smart televisions)
Social engineering	This is 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	This is software installed on a computer to secretly monitor the user's activities
Threat actor	This is an individual or organisation that conducts malicious activity, such as cyber espionage, cyber-attacks or cyber-enabled crime

Common cyber risks

There are many cyber risks which organisations face.

Cyber risks can be:

- **internal risks** – these originate from within your organisation, and
- **external risks** – these are the more commonly known risks posed by unauthorised third parties (such as threat actors)

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

Note – cyber security incidents

The OAIC reports that compromised or stolen account credentials are the leading cause of all data breaches.

From July to December 2023, cyber incidents were the source of 44% of all data breaches, and phishing (28%) took over from ransomware (27%) as the top source of cyber incidents. Compromised credentials through phishing, a brute force attack or unknown method compromised 58% of all cyber incidents.

Ransomware remains a prevalent external risk in Australia and is one of the most destructive cybercrime threats. Ransomware attacks aim to disrupt critical services to your organisation by preventing access to key files and systems in turn for ransom (usually in the form of cryptocurrency).

The Australian Signals Directorate (**ASD**) in its most recent ASD Cyber Threat Report 2022-2023 reports the most common cyber security incidents for businesses to watch out for are business email compromise fraud. Business email compromise fraud continues to significantly impact businesses with an average financial loss of over $39,000 for each incident.

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 cyber security framework and practices including security controls, training and education.

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

Internal cyber risks

Note

The OAIC's notifiable data breaches report for July to December 2023 shows that human error accounted for 30% of the total notifiable data breaches notified during the reporting period (compared to 26% in the previous period).

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 organisation's business, systems, and internal structures.

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

To defend against email attacks, organisations should set aside time for regular cyber security training and ensure all employees are cautious of emails that contain requests for payment or notify a change of bank details.

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 cyber-related 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 cyber security breach as well. In this fact sheet we collectively refer to these people as 'staff members.'

Example

Danielle works for a 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 are angry and asked why the follow up action 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).

Potential effects of a cyber breach resulting from internal risks

Risk examples	Potential effects on the 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
A staff member forgets to BCC (blind copy) recipients of an email list, and instead makes the emails visible	• Possible breach of privacy law
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

Responsibility for third-party providers

It's also important that boards of not-for-profit organisations take steps to manage the cyber security risks associated 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.

Example

Damian works for an accounting firm (a third-party service provider) that manages customer billing information for a not-for-profit organisation. When the organisation is hacked, the accounting firm does not tell the organisation about the data breach, and the organisation finds out about the breach through the news. The organisation then learns that the third-party provider did not have any security controls in place.

In these circumstances, there is a risk of:

- serious harm to the organisation and its help-seekers
- breach of privacy law by the organisation, and
- damage to the organisation’s reputation

See below for guidance on managing this third-party risk.

Data breach report highlights supply chain risks

In a media release in February 2024, the OAIC reported:

The risk of outsourcing personal information handling to third parties is highlighted in the latest data breach statistics, released today by the Office of the Australian Information Commissioner (OAIC).

Australian Information Commissioner Angelene Falk said the OAIC continues to be notified of a high number of multi-party breaches, with most resulting from a breach of a cloud or software provider.

Multi-party data breaches

Although the OAIC's notifiable data breaches report for January to June 2024 observed a decrease in the number of secondary notifications relating to multi-party breaches, these types of breaches can still present challenges for organisations using software provided by third parties. It's, therefore, important to remain aware of and vigilant against these third-party cyber-attacks.

Multi-party breaches are breaches which relate to third parties that exist beyond that business' immediate suppliers. Most multi-party breaches involve a data breach of a cloud or software provider, which then impacts the organisations who outsourced their personal information handling to those providers. Examples of such breaches include the MediSecure and Outabox incidents.

Issues that contribute to multi-party breaches include the absence of:

- data retention or destruction clauses in contractual agreements following the end of a contract with a third party service provider, and
- clearly defined responsibilities should a data breach occur, including who should assess or notify the breach, in these agreements

Note

ASIC, Australia's corporate regulator, has indicated that:

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

Your organisation can manage the risk of being impacted by cyber security risks associated with third-party providers by:

- assessing the privacy and cyber security risks before engaging a third-party provider (this can be done through a security assessment and a privacy impact assessment) and making necessary adjustments (including to the terms of the agreement between the parties), and
- ensuring your contractual arrangements with third-party providers:
  - require that they manage cyber security risks
  - include data retention or destruction clauses to follow the end of a contract and clearly defined responsibilities should a data breach occur, including who should assess or notify the breach

What is a privacy impact assessment?

A privacy impact assessment is a systematic assessment of a project that identifies potential privacy impacts and recommendations to manage, minimise or eliminate them.

For more information, see the OAIC's guide to undertaking privacy impact assessments.

External cyber 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 security software and systems in place doesn't mean your organisation will be immune from a cyber-attack.

Cyber security 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.

Factors such as the speed of recovery and the sensitivity of the stolen data can significantly impact the consequences of a data breach. Consequences of a breach may include business disruption, reputational damage, financial loss or the loss of valuable data.

Potential effects of a cyber breach resulting from external risks

Risk examples	Potential effects on the organisation
A website link, spam email or similar introduces ransomware to your system	• Disruption to your systems, potentially to force 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
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 (known as 'quishing')	
A brute-force attack on staff member credentials	

Note – the importance of training

The nature of cyber-attacks 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 threat actor 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.

Note – privacy law obligations

Depending on your annual revenue or other criteria, you may be subject to obligations under the Australian Privacy Principles under the *Privacy Act 1988* (Cth). This includes an obligation to notify data breaches to the OAIC and individuals affected in some cases.

Refer to 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).

Protecting information from data breaches

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

What your organisation can do:	
Protect your systems	• Install and maintain up-to-date firewall and anti-malware software • Use multi 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
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 • Cyber criminals often take advantage of weak or reused credentials to access systems and networks. Cyber criminals also use social engineering to gain access to systems or data by manipulating businesses and employees. Consider internal risks, like a staff member clicking a phishing email or reusing credentials, or weak passwords
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 cyber incident response plan and/or 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

Recent reforms recommend that organisations voluntarily give the National Cyber Security Coordinator and ACSC information concerning the cyber incident experienced (discussed in more detail below).

In addition, your organisation should consider implementing the ACSC's Essential Eight Risk Maturity Framework with measures appropriate to the type and size of your organisation.

The Essential Eight are a series of mitigations the ACSC recommends as one of the most effective approaches to protect against cyber threats.

For more information, see the ACSC webpages Essential Eight Maturity Model and Essential Eight Assessment Process Guide.

Creating a cyber incident response plan

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

A cyber security incident is:

- one or more acts, events, or circumstances which involves unauthorised impairment of electronic communication to or from a computer, or
- the discovery of unintended or unexpected vulnerabilities in a computer, computer data or a computer program that, if exploited, would result in an act or circumstance that involves an impairment of electronic communication to or from a computer

A cyber incident response plan 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 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. Your plan could also include a process chart of when to report cybersecurity incidents to relevant government bodies or seek assistance from them.

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

Note

Impacts to critical infrastructure are also considered cyber security incidents under the *Security of Critical Infrastructure Act 2018* (Cth). This fact sheet does not cover compliance under this Act.

Reforms under the Cyber Security Act

The Cyber Security Act aims to help manage cyber risks and includes measures to:

- introduce a mandatory ransomware and cyber extortion reporting obligation for certain businesses to report ransom payments
- introduce a Limited Use obligation for the National Cyber Security Coordinator to encourage industry engagement with the government following cyber incidents, and
- establish a Cyber Incident Review Board to conduct reviews of significant cyber incidents and share lessons learned

Mandatory ransomware payment reporting obligation

From 30 May 2025, ransomware payment reporting rules apply to any business that, at the time the business made a payment in response to a cyber incident, is:

- carrying on a business in Australia with an annual turnover for the previous financial year that exceeds the $3 million threshold for that year, and
- not a Commonwealth body or a State body, or a business responsible for a critical infrastructure asset to whom Part 2B of the *Security of Critical Infrastructure Act 2018* applies

In these circumstances, the organisation must report within 72 hours of making the ransomware payment or becoming aware that the ransomware payment has been made (whichever is applicable) to avoid penalties.

Failure to comply may result in civil penalty of $19,800 (as at March 2025).

For more information, see the Australian Government's fact sheet on the mandatory ransomware payment reporting obligation.

The Cyber Incident Review Board

The Cyber Incident Review Board (**Board**) has been established under the Cyber Security Act and will operate from 30 May 2025.

The Board will conduct post-incident reviews of significant cyber security incidents in Australia and make recommendations to Government and industry about actions that could be taken to prevent, detect, respond to, or minimise the impact of cyber security incidents in the future.

A cyber security incident or series of incidents will be significant if it:

- has seriously prejudiced the social or economic stability of Australia or it's people, the defence of Australia or national security

- has involved novel or complex methods or technologies, or
- could reasonably be of serious concern to the Australian people

For more information about reporting a cybercrime, incident or vulnerability, see the ACSC's webpage 'Report'.

National Cyber Security Coordinator

The Cyber Security Act has formalised the role of the National Cyber Security Coordinator at the ASD (and ACSC), by establishing a voluntary information regime for organisations to submit information about significant and non-significant cyber security incidents which have occurred, are occurring or may potentially occur.

Under the Cyber Security Act, a 'limited use obligation' restricts how the National Cyber Security Coordinator (**Coordinator**) and the ASD can record, use or disclose information that is voluntarily provided under Part 4 of the Act in specified circumstances.

This obligation ensures that the ASD can't use information shared against the business that disclosed it. However, this protection does not prevent separate law enforcement and regulatory bodies from conducting their own investigations.

Limited use will apply to your organisation's information if it's likely that your organisation will be impacted by the cyber security incident, or potential cyber security incident – you don't need to wait to be impacted, if you think it is reasonably foreseeable that your organisation will be impacted.

For more information, see the Australian Government's fact sheet on Limited Use for the National Cyber Security Coordinator.

Privacy law and the Notifiable Data Breach Scheme

If your organisation is subject to privacy laws or has a privacy policy, ensure that your cyber incident response plan aligns with these. The plan should specifically address how your organisation will handle privacy breaches and comply with the Notifiable Data Breach (**NDB**) Scheme.

Your organisation should typically follow these steps if it has 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

The NDB Scheme is a mature regime

Your obligations under the Privacy Act's NDB Scheme are important. The OAIC takes the view that the NDB Scheme is a mature regime and expects entities to have both:

- strong practices to protect personal information, and
- processes which ensure a timely response if a data breach occurs

OAIC's Notifiable Data Breaches Report: July to December 2023

This report shows:

- 483 breaches were notified under the scheme for the period 1 July to 31 December 2023, (a decrease of 19% compared to 407 notifications for the period from January to July 2023).
- The health and finance sectors remain the highest reporting industries. The health industry reported 104 breaches and finance 49 breaches. The insurance sector reported 45 data breaches.
- Malicious or criminal attacks remain the leading source of data breaches, accounting for 67% of the total (compared to 71% in the previous period).
- The top causes of human error breaches were personal information sent to wrong recipient by email (33%), unauthorised disclosure by unintended release or publication (20%), and personal information sent to wrong recipient by mail (10%).
- Phishing (compromised credentials) is the top source of cyber incidents with 28% of cyber incidents being a result of phishing. Compromised or stolen credentials followed as the second most common source of cyber incidents at 27%, along with ransomware at 27%.
- The OAIC reported a significant increase in the number of secondary notifications (121 notifications) from the previous reporting period (29 notifications).

If your organisation is required to comply with privacy law or has a privacy policy, refer to the 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 cyber security.

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. Our privacy guide also covers the Notifiable Data Breach Scheme.

Note – cyber security incident

Your organisation may need to notify the government agencies below in the event of a cyber security incident. You can report a cyber incident online. The Australian Cyber Security Centre will then forward the report to the Cyber and Infrastructure Security Centre or Australian Federal Police for involvement as needed:

- Australian Cyber Security Centre (**ACSC**)

  This is the Federal agency for cyber security. They may provide a position on whether payment should be made, especially if a foreign government is a potential threat agent.

- 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

  The Department provides advice if public health is at risk resulting from the ransomware attack.