

Cyber security

Legal information for community organisations

This fact sheet covers:

- ▶ common cyber security risks
- ▶ protecting systems and information
- ▶ preparing for and responding to cyber incidents
- ▶ the Cyber Security Act
- ▶ privacy and data breach obligations



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.

Cyber security involves protecting an organisation's systems, networks, devices and information from unauthorised access, disruption, damage or misuse.

A cyber incident can interrupt services, expose personal or confidential information, cause financial loss and damage community trust.

Cyber security and privacy are closely connected, but they are not the same. Cyber security focuses on protecting systems and information from cyber threats, while privacy laws regulate how organisations collect, hold, use, disclose and protect personal information.

Strong cyber security practices can help an organisation meet its privacy obligations and reduce the likelihood and impact of a data breach. However, it is not possible to eliminate every cyber risk.



Read this fact sheet together with [our Privacy Guide](#), which explains privacy obligations and the Notifiable Data Breaches scheme.

The [Cyber Security Act 2024 \(Cth\)](#) (**Cyber Security Act**) introduced Australia's first standalone cyber security legislation.

Terminology

Some key terms used in this fact sheet are explained below.

Australian Signals Directorate (ASD) and Australian Cyber Security Centre (ACSC)	<u>ASD</u> is an Australian Government agency responsible for cyber security and other national security functions. The <u>ACSC</u> operates within ASD and provides cyber security advice, assistance and reporting channels.
Business email compromise (BEC)	BEC is a form of cybercrime in which a criminal uses email or a compromised email account to impersonate a trusted person or organisation. The criminal may seek money, credentials, confidential information or changes to payment details.
Cyber incident	This is an event or series of events that compromises, or may compromise, the confidentiality, integrity or availability of an organisation's systems, networks, devices or information. A specific statutory definition may apply to particular obligations under the Cyber Security Act or other legislation.
Cyber Incident Review Board (CIRB)	The CIRB is the independent statutory body established under the Cyber Security Act to conduct no-fault reviews of significant cyber security incidents and make recommendations to reduce the likelihood or impact of future incidents.
Distributed Denial of Service (DDoS)	This is an attack that overwhelms a system, service or network with traffic so that legitimate users cannot access it.
Firewall	This is hardware or software that monitors and controls incoming and outgoing network traffic according to security rules.
Logging	This is recording activity within a system, network or application. Logs can help an organisation detect suspicious activity, investigate an incident and understand what occurred.
Malware	This is software designed to disrupt, damage, monitor or gain unauthorised access to a system, device or information.
Multi-factor authentication (MFA)	This is a security measure that requires a user to provide two or more types of evidence before gaining access. For example, a password and a code generated by an authentication application.
National Cyber Security Coordinator	The National Cyber Security Coordinator is the Australian Government official responsible for coordinating whole-of-government responses to significant cyber security incidents.
Phishing	This is a fraudulent communication designed to persuade a person to disclose information, transfer money, open a malicious attachment or visit a malicious website.
Ransomware	This is malicious software or activity that prevents access to systems or information, or threatens their misuse or disclosure, to obtain money or another benefit.
Ransomware or cyber-extortion payment	This is where money or another benefit provided in response to a demand connected with a cyber security incident. Mandatory reporting only applies where a covered entity makes a payment or

	becomes aware that a payment was made on its behalf. A demand without payment does not trigger the mandatory reporting obligation.
Smart devices	A smart device is an internet-connected or network-connected product, sometimes called an Internet of Things device . Examples include smart televisions, smart watches, home assistants, security cameras and baby monitors. Mandatory standards apply to most in-scope consumer-grade smart devices manufactured on or after 4 March 2026.
Social engineering	These are techniques that manipulate people into disclosing information, transferring money, granting access or acting against normal security procedures.
Threat actor	This is a person, group or organisation that carries out, or attempts to carry out, malicious cyber activity.

Common cyber risks

Cyber risks can arise from within an organisation, from external threat actors or through third-party providers. For example, a phishing attack may originate outside the organisation but succeed because a staff member opens a malicious attachment or discloses login credentials.

This fact sheet groups cyber risks into:

- **internal risks**, involving personnel or internal systems
- **external risks**, involving cybercriminals and other threat actors
- **third-party risks**, involving service providers, software platforms and cloud services

A cyber incident can cause service disruption, information loss, financial loss, legal consequences and reputational damage.

Charities and not-for-profits commonly face threats including phishing, business email compromise and ransomware. The [Australian Signals Directorate recommends](#) measures such as staff training, multi-factor authentication, independent verification of payment requests and tested backups.



Current data breach trends

Data breach notifications remain at historically high levels. The Office of the Australian Information Commissioner (**OAIC**) received 1,205 notifications under the Notifiable Data Breaches scheme during 2025, the highest annual number since the scheme began in 2018.

Current statistics are available through the OAIC's [Notifiable Data Breach statistics dashboard](#).



Cyber insurance

Cyber insurance may help manage some of the consequences of a cyber incident, but it is not a substitute for appropriate cyber security. Before purchasing or renewing cyber insurance, review what the policy covers, any security requirements, notification obligations and whether incidents involving third-party providers are covered.

For more information about cyber liability insurance, see [our webpage on managing insurance and risk](#).

People and internal cyber risks

Cyber incidents are not always caused solely by external threat actors. They can also result from mistakes, inadequate processes, inappropriate access or deliberate conduct by people within an organisation.

For the purposes of this fact sheet, **personnel** includes board or committee members, employees, volunteers, contractors, and other people with access to the organisation's systems or information.

Everyone with access to systems or information should understand their cyber security responsibilities and know how to report a suspected incident promptly.

Organisations should make sure personnel know:

- how to recognise suspicious emails, messages and payment requests
- where to report suspicious activity
- what to do after accidentally disclosing information
- how to escalate a suspected cyber incident or data breach
- why prompt reporting is important

The [Australian Signals Directorate recommends](#) regular training on phishing and scams, as well as independent verification of requests to make urgent payments or change bank account details.



Human error and data breaches

The [OAIC reported](#) that human error accounted for 37% of all data breach notifications received from January to June 2025, or 193 notifications. This was an increase from 29% in the previous reporting period. These figures reinforce the importance of regular training, clear procedures, appropriate access controls and prompt reporting of mistakes.

Training and awareness

Regular, role-appropriate training can help personnel recognise cyber risks and respond appropriately.

Training should reflect the organisation's activities, the systems and information a person can access, the person's responsibilities, current cyber threats, and the organisation's reporting procedures.

Training alone is not enough and should be supported by clear procedures, appropriate access controls and technical safeguards.



Tip

Make it easy for personnel to report suspected incidents and mistakes. Prompt reporting gives an organisation the best opportunity to contain an incident and reduce harm.



Example

Danielle accidentally emails a spreadsheet containing personal and health information to more than 100 unintended recipients. Although Danielle notices the mistake immediately, she does not report it until several days later.

The delay reduces the organisation's opportunity to contain and assess the incident. The organisation cannot assume the risk has been addressed simply because recipients are asked to delete the information.

The organisation should promptly assess whether the incident is an eligible data breach under the Notifiable Data Breaches scheme.

Examples of internal cyber risks

Risk	Potential consequences
A person deliberately takes or publishes organisational information	Disclosure of confidential or personal information, legal liability and loss of community trust
Personnel access information without a legitimate reason	Privacy breaches, harm to affected individuals and regulatory consequences
A portable device containing information is lost or stolen	Unauthorised access, service disruption and possible notification obligations
An email is sent to the wrong recipient or addresses are exposed by failing to use BCC	Unauthorised disclosure and possible privacy law consequences
Former personnel retain access to accounts or systems	Unauthorised access, alteration or disclosure of information
Information is accidentally made publicly accessible because of a configuration or publishing error	Public disclosure, privacy law consequences and reputational damage

Reducing internal risks

Organisations can reduce internal cyber security risks by:

- limiting access to systems and information based on role and operational need
- regularly reviewing and removing access when a person's role changes or involvement ends
- implementing security measures such as multi-factor authentication
- providing regular cyber security training and awareness activities
- establishing clear procedures for verifying payment requests and other high-risk transactions
- encouraging prompt reporting of suspected incidents, mistakes and suspicious activity
- testing incident response procedures to ensure personnel understand their responsibilities

Third-party and supply-chain risks

Most organisations rely on third-party providers for services such as cloud storage, software, accounting systems and website hosting.

While these services can improve efficiency, they can also create cyber security risks, and an organisation may be affected by a cyber incident involving a provider even where its own systems have not been compromised.

Some cyber incidents affect multiple organisations at the same time. These are sometimes referred to as **multi-party breaches** and often arise when a cloud, software or managed service provider experiences a cyber incident that affects its customers. Examples include the [MediSecure](#) and [Outabox incidents](#).



Example

Damian works for an accounting firm that manages billing information on behalf of a not-for-profit organisation. The accounting firm's systems are compromised in a cyber incident, exposing information relating to the organisation and its clients. The organisation becomes aware of the incident only after media reports emerge.

Although the incident occurred within the provider's systems, the organisation may still face operational disruption, reputational harm and privacy law obligations.

Managing third-party risks

Boards and management should actively oversee cyber security risks associated with third-party providers. Regulators have identified third-party providers as a significant source of cyber security risk and expect organisations to take reasonable steps to assess and manage those risks.

Before engaging a third-party provider, organisations should consider:

- what information the provider will access, store or process
- whether the provider has appropriate cyber security measures in place
- how cyber incidents will be identified and reported
- whether the provider is permitted to engage subcontractors
- where information will be stored and processed

Contractual arrangements should also clearly address:

- cyber security obligations
- privacy obligations
- incident reporting requirements
- responsibilities following a cyber incident
- information retention and destruction requirements at the end of the arrangement



Tip

Conduct appropriate due diligence before engaging a third-party provider and review key providers periodically. A cyber incident involving a provider may still have significant consequences for your organisation.

Privacy impact assessments

Where a project involves collecting, using or disclosing personal information, organisations may wish to conduct a privacy impact assessment.

A privacy impact assessment is a structured process used to identify privacy risks and possible measures to address them.



For more information, see the [OAIC's guide to undertaking privacy impact assessments](#).

External cyber risks

External cyber risks arise from people or groups outside an organisation, including cybercriminals and other threat actors.

Common examples include:

- phishing emails and messages
- business email compromise
- ransomware
- distributed denial-of-service (**DDoS**) attacks
- credential theft
- malware and spyware
- social engineering attacks

External cyber risks can result in service disruption, financial loss, unauthorised access to systems and the loss, alteration or disclosure of information.

While technical safeguards are important, organisations are best protected through a combination of technical measures, staff training, clear procedures and effective incident response planning.

Examples of external cyber risks

Risk	Potential consequences
A phishing email tricks a staff member into disclosing login credentials	Unauthorised access to systems or information
A ransomware attack encrypts important files	Loss of access to systems, operational disruption and extortion demands
A business email compromise attack convinces staff to transfer funds	Financial loss and reputational damage
A DDoS attack overwhelms a website or online service	Service interruption and loss of access for users
Malware is installed through a malicious attachment or website	System compromise, data loss or information theft

Training remains important

External cyber threats continue to evolve, and cybercriminals regularly adapt their methods to bypass technical controls.

Regular training helps personnel recognise suspicious activity and respond appropriately. Training should include topics such as phishing, fraudulent payment requests, social engineering and incident reporting.



Tip

Encourage personnel to verify unusual requests independently, particularly requests involving payments, banking details, passwords or sensitive information.

Privacy law obligations

A cyber incident may also trigger obligations under privacy laws, including obligations under the *Privacy Act 1988* (Cth) and the Notifiable Data Breaches scheme.

For more information, see [our Privacy Guide](#).

Protecting information from data breaches

Strong cyber security involves more than responding to incidents after they occur. Organisations should take proactive steps to reduce the likelihood of a cyber incident and minimise its impact if one occurs.

There is no single measure that can eliminate cyber risk. Effective cyber security requires a combination of technical controls, clear procedures, staff training and ongoing review.

What your organisation can do	Examples
Protect your systems	Use measures such as multi-factor authentication, strong passwords, software updates, malware protection and appropriate access controls.

Identify risks	Understand what information your organisation holds, where it is stored, who can access it and which systems are critical to your operations.
Detect suspicious activity	Monitor systems for unusual activity, make use of logging and audit functions where available, and ensure personnel know how to report suspicious behaviour.
Respond to incidents	Establish clear cyber incident and data breach response procedures and ensure personnel understand their responsibilities.
Recover from impacts	Maintain and test backups, restore systems where necessary and review incidents to identify improvements.



Tip

Cyber security measures are most effective when they are reviewed regularly.

Controls that were appropriate several years ago may no longer provide adequate protection against current threats.

The Essential Eight – cyber security strategies

The Australian Cyber Security Centre (**ACSC**) recommends the [Essential Eight Risk Maturity Framework](#), a set of cyber security strategies designed to help organisations protect themselves against common cyber threats.

Not every organisation will implement the Essential Eight in the same way. Organisations should consider which measures are appropriate having regard to their size, resources, systems and risk profile.



For more information, see the ACSC webpages [Essential Eight Maturity Model](#) and [Essential Eight Assessment Process Guide](#).

Creating a cyber incident response plan

No organisation can eliminate every cyber risk. A cyber incident response plan helps an organisation respond quickly and effectively when a cyber incident occurs.

A cyber incident response plan should:

- identify how incidents will be reported and escalated
- clearly allocate responsibilities for managing the response
- outline the steps for containing, investigating and recovering from an incident
- identify when external technical, legal or communications assistance should be sought
- address any legal, contractual or regulatory reporting obligations

The plan should reflect the organisation's size, resources, systems and the nature of the information it holds.

For example, a small volunteer-run organisation may require a relatively simple response plan, while a larger organisation handling significant volumes of personal or health information may require more detailed procedures.

**Tip**

A response plan is only useful if personnel know it exists and understand their responsibilities. Consider reviewing and testing the plan periodically to ensure it remains effective.



The Australian Cyber Security Centre (**ACSC**) provides guidance, templates and checklists to help organisations prepare a cyber incident response plan. For more information, see the [ACSC's guidance 'Cyber security incident response planning'](#).

Reporting cyber incidents

Following a significant cyber incident, organisations may need to report the incident to, or seek assistance from, one or more government agencies.

Cyber incidents, cybercrime and cyber security vulnerabilities can be reported through the Australian Cyber Security Centre's (ACSC) [Report page](#).

Relevant agencies may include:

- **[Australian Cyber Security Centre \(ACSC\)](#)**, which provides cyber security advice, assistance and reporting services
- **[Australian Federal Police \(AFP\)](#)**, which investigates and disrupts cybercrime
- **[Cyber and Infrastructure Security Centre \(CISC\)](#)**, where obligations relating to critical infrastructure may arise
- other regulators or government agencies, depending on the nature of the incident and the information affected

**Tip**

Organisations should consider whether reporting obligations arise under privacy laws, funding agreements, contractual arrangements or other legal requirements following a cyber incident.

The Cyber Security Act

The [Cyber Security Act 2024 \(Cth\)](#) introduced Australia's first standalone cyber security legislation.

The Cyber Security Act includes measures relating to ransomware and cyber-extortion payment reporting, voluntary information sharing during significant cyber security incidents, the Cyber Incident Review Board and security standards for certain smart devices.

**Note**

Some organisations may also have obligations under the [Security of Critical Infrastructure Act 2018 \(Cth\)](#). The Security of Critical Infrastructure Act contains separate obligations for certain operators of critical infrastructure assets. This fact sheet focuses on the Cyber Security Act and does not cover those obligations.

Ransomware and cyber-extortion payment reporting

From 30 May 2025, certain entities have been required to report ransomware and cyber-extortion payments to the Australian Government.

The reporting obligation applies to certain entities carrying on business in Australia, including entities with annual turnover of at least \$3 million in the previous financial year. Reports must generally be made within 72 hours after the payment is made or the entity becomes aware that a payment has been made on its behalf.

The reporting obligation is triggered by a payment, not merely because a ransom or extortion demand has been received.



For more information, see the Australian Government's [fact sheet on the mandatory ransomware payment reporting obligation](#).

Voluntary information sharing and the National Cyber Security Coordinator

The Cyber Security Act allows organisations to voluntarily share information with the National Cyber Security Coordinator in relation to significant cyber security incidents.

The National Cyber Security Coordinator is responsible for coordinating the Australian Government's response to significant cyber security incidents.

The Cyber Security Act also includes protections that regulate how specified information shared with the National Cyber Security Coordinator may be used and disclosed. These protections are intended to support information sharing during significant cyber security incidents.



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

The Cyber Incident Review Board

The Cyber Security Act established the Cyber Incident Review Board, an independent body that conducts no-fault reviews of significant cyber security incidents.

The Board's role is to identify lessons learned and make recommendations to improve Australia's cyber resilience and preparedness for future incidents.

Security standards for smart devices

The Cyber Security Act also establishes a framework for mandatory cyber security standards for certain smart devices.

Security standards now apply to most in-scope consumer-grade smart devices manufactured on or after 4 March 2026. The standards are intended to improve the baseline security of products such as smart televisions, smart watches, home assistants, security cameras and other connected devices.



For more information about the *Cyber Security Act 2024* (Cth), see the Australian Government's cyber security resources and guidance available through <https://www.cyber.gov.au/>.

Privacy law and the Notifiable Data Breach Scheme

Cyber security and privacy are closely connected. A cyber incident may involve the loss, unauthorised access, unauthorised disclosure or alteration of personal information.

Depending on its activities and size, an organisation may be subject to obligations under the *Privacy Act 1988* (Cth) and other Commonwealth, state or territory privacy laws. If your organisation is subject to privacy laws, its cyber incident response plan should align with its privacy obligations and procedures for responding to data breaches.

Where a cyber incident affects personal information, organisations should consider whether:

- privacy law obligations apply
- the incident may constitute an eligible data breach
- notification obligations arise

Responding to a data breach

If a cyber incident affects personal information, organisations should generally:

Step	Action
1.	Contain the incident
2.	Assess the risks associated with the incident
3.	Consider notification obligations
4.	Review the incident and implement improvements to reduce the risk of future breaches

The Notifiable Data Breaches scheme

The Notifiable Data Breaches (**NDB**) scheme requires certain organisations to notify affected individuals and the Office of the Australian Information Commissioner (**OAIC**) when they reasonably believe an eligible data breach has occurred.

An eligible data breach generally occurs where:

- personal information is lost, or accessed or disclosed without authorisation
- serious harm is likely to result to one or more affected individuals, and
- remedial action has not prevented the likelihood of serious harm

Not every cyber incident will trigger the NDB scheme. However, organisations should assess potential privacy impacts whenever a cyber incident involves personal information.



Tip

A cyber incident may trigger privacy obligations even if there is no evidence that personal information has been misused. Organisations should assess incidents promptly and document the steps taken to investigate and respond.



Current data breach trends

The OAIC received 1,205 notifications under the Notifiable Data Breaches scheme during 2025, the highest annual number since the scheme began in 2018. Most notifications were attributed to malicious or criminal activity.

Current information about reported breaches is available through the [OAIC's Notifiable Data Breach statistics dashboard](#).



Further information

This fact sheet provides a high-level overview only.

For detailed guidance on privacy obligations, the Notifiable Data Breaches scheme, eligible data breaches, notification requirements and responding to data breaches, read our [privacy guide](#).

The [OAIC website](#) also contains guidance on privacy compliance and data breach response, while the [ACSC website](#) contains practical cyber security resources and support.