Preventing data breaches

Presented by:
Greg Lewis, Board Member, Tax Practitioners Board
Connor Dilleen, Director, Office of the Australian Information Commissioner

Technical guidance

Click this icon on the top right of your screen to join the chat

Click this icon for technical support

- Call Redback Support for technical problems: 1800 733 416.
- We'll provide a copy of the presentation and some helpful links after the webinar.
- You can claim CPE/CPD for attending this webinar. We don't issue attendance certificates.

What we will cover today

- What is a cyber-attack
- Your obligations
- Notifiable Data Breaches scheme
- Sufficient controls
- What to do in the event of a breach
- Where to get help
- Questions

Meet your presenters

Connor Dilleen

Director

OAIC

Greg Lewis

Board Member

TPB

What is a cyber-attack

Types of cyber-crime

Common types of cyber crime include:

- hacking
- online scams and fraud
- identity theft
- attacks on computer systems
- email spam and phishing
- illegal or prohibited online content.

First party losses from a cyber-attack

First party losses can include:

- business interruption losses
- the costs of repairing and restoring systems, or improving cyber security
- reputational damage
- extortion costs.

Third party losses from a cyber attack

Third party losses can include:

- liability in negligence for failing to properly protect client information
- fines imposed by regulators.

Tax practitioner obligations

Code item 6

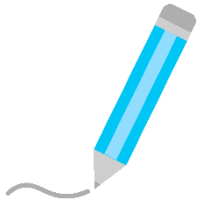
Code Item 6 - You must not disclose any information relating to a client's affairs to a third party unless you have:

- obtained the client's permission; or
- there is a legal duty to do so.

Code item 7

- Code item 7 - You must ensure that a tax practitioner service that you provide, or that is provided on your behalf, is provided competently.
- Sanctions for breaches of the Code can range from a written caution to termination of registration.

Consequences for failing to comply



Written caution

Order

Suspension

Termination

Notifiable Data Breaches scheme

Notifiable Data Breaches scheme

Organisations covered by the Privacy Act are legally required to quickly assess actual or suspected data breaches

If serious harm is likely to result, they must notify affected individuals

They must also notify the OAIC

Notifiable Data Breaches framework

The Notifiable Data Breaches scheme is intended to:

- provide a safer and more transparent environment
- improve compliance with privacy obligations
- provide entities with a framework for responding to data breaches
- provide an evidence base that can inform both government policy and industry practice.

What is an eligible data breach

Three criteria must be satisfied before a data breach is considered ‘eligible’:

1. unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information has occurred

2. the breach is likely to result in serious harm* to one or more individuals

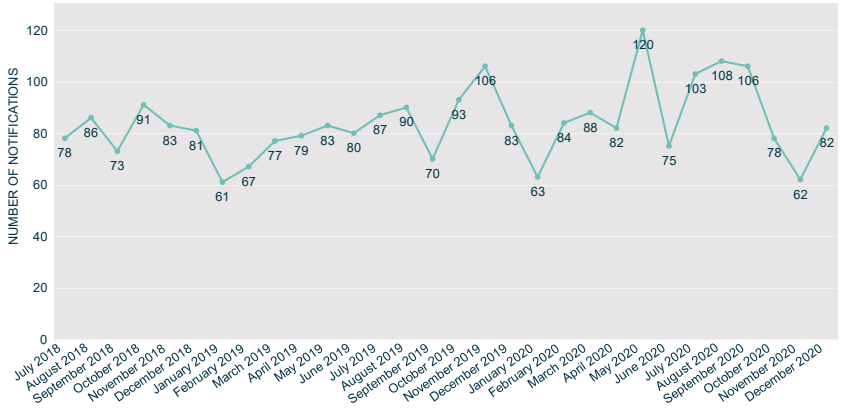
3. the entity has not been able to prevent the likely risk of serious harm with remedial action.

There is no strict definition of **serious harm**. It may include serious physical, psychological, emotional, financial or reputational harm

Trends in NDB notifications

The OAIC regularly publishes statistics about notifications received under the NDB scheme to help organisations and the public understand the operation of the scheme.

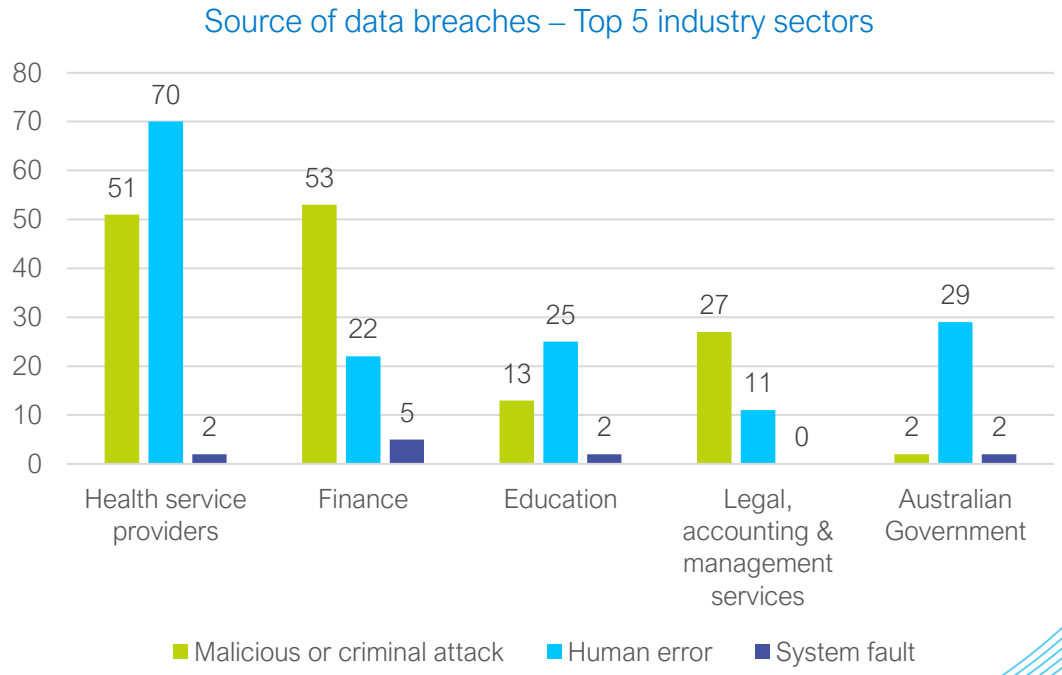
Number of notifications received by month



Source: NDB Report July-December 2020

Top reporting industry sectors

Health and finance have been the top two sectors to notify data breaches since the scheme began.



Source: NDB Report July-December 2020

Malicious or criminal attacks

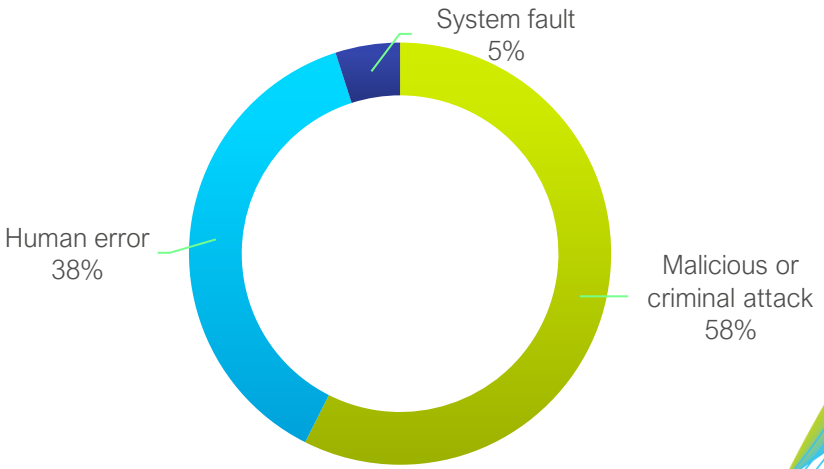
Malicious and criminal attacks are the leading source of data breaches reported to the OAIC.

The majority of breaches in this category involve cyber security incidents such as phishing, compromised or stolen credentials and ransomware.

This category also includes:

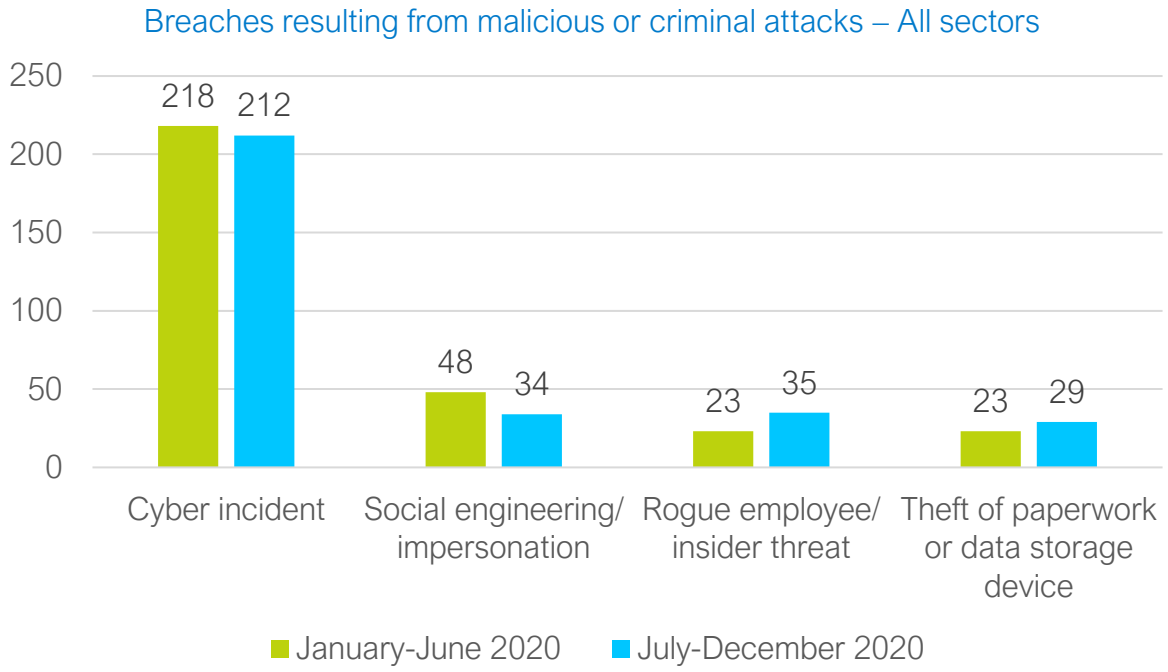
- social engineering/impersonation
- rogue employee/insider threat
- theft of paperwork or data storage device.

Source of notifiable data breaches



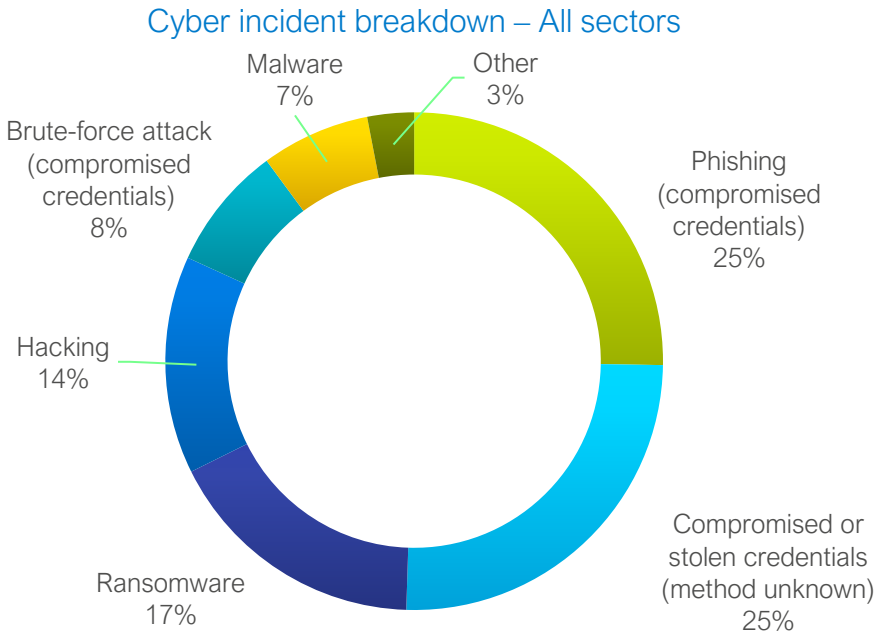
Source: NDB Report July-December 2020

Deep dive – malicious or criminal attacks



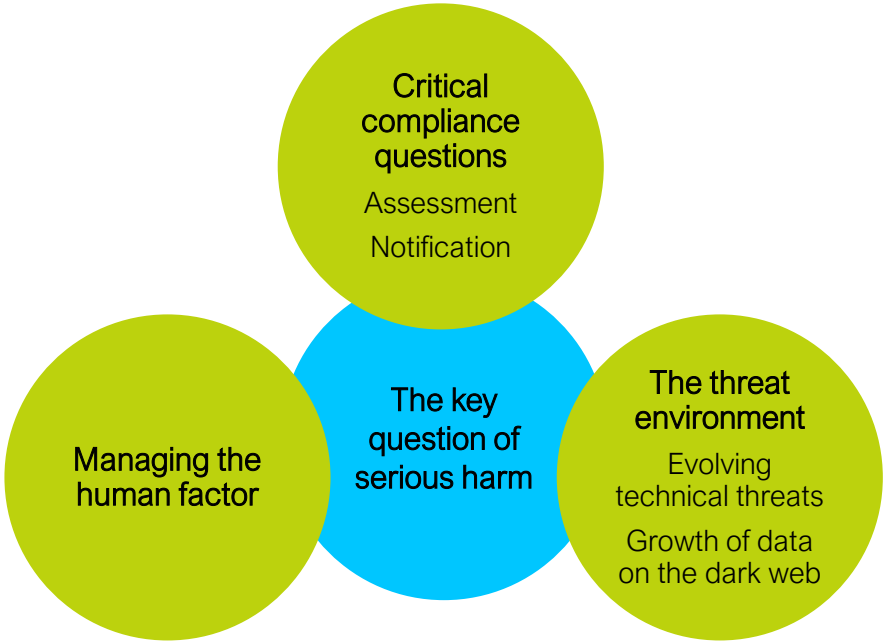
Source: NDB Report July-December 2020

Deep dive – cyber attacks



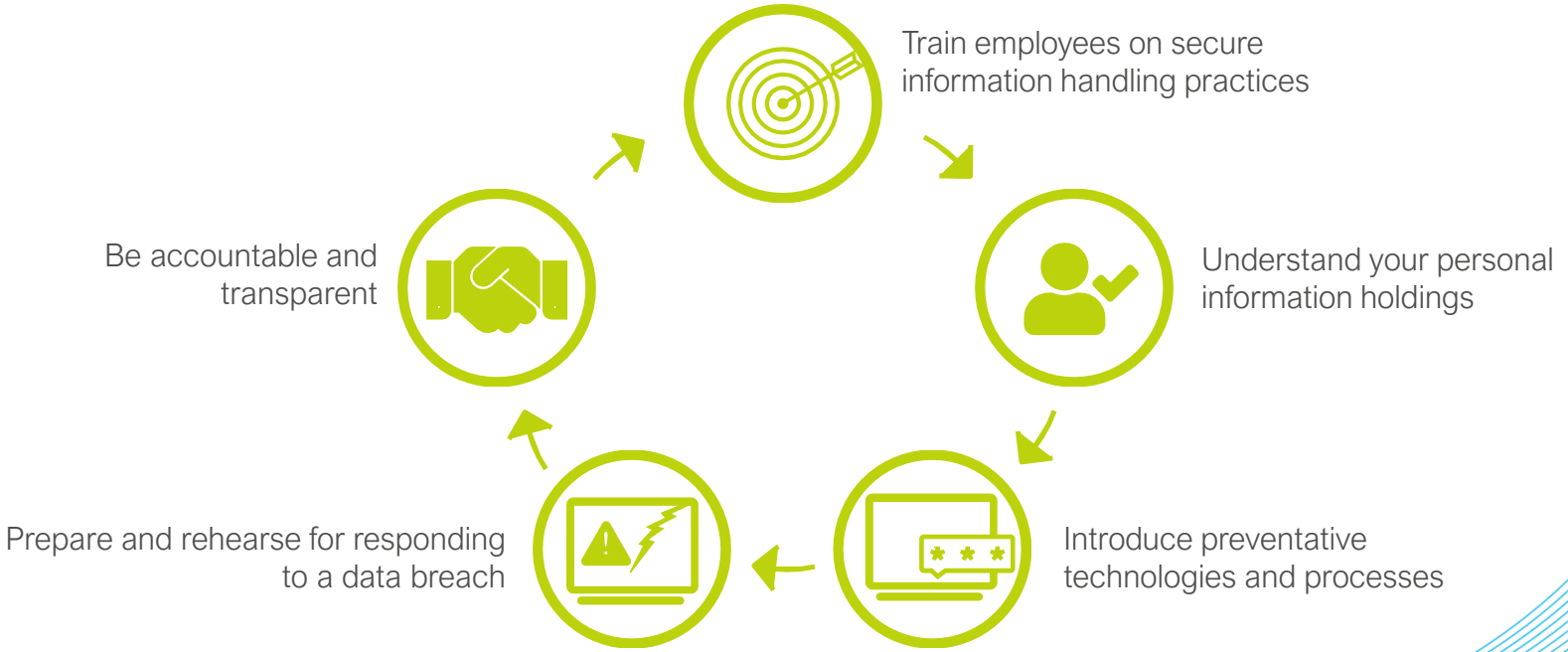
Source: NDB Report July-December 2020

Emerging themes and challenges



Sufficient controls

Data breach preparation and response

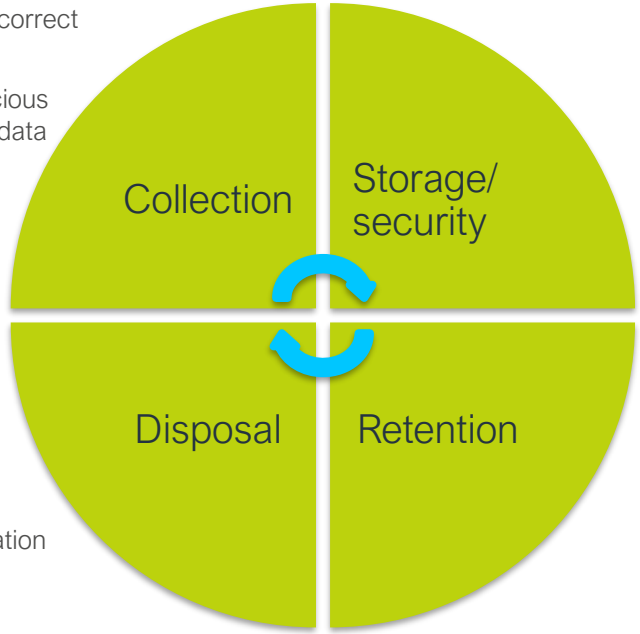


Managing the information lifecycle

Do we need to collect the information?

Are we collecting the information in the correct manner?

Can we limit the attack surface for malicious actors by limiting the amount or type of data we collect?



Are we storing and protecting the information appropriately?

Do we know where sensitive information is stored?

Do we have additional technical security measures in place for highly sensitive information?

Is access logging/auditing enabled?

Do we use managed service providers?

Do these MSPs hold data on our behalf?

Have we vetted their infrastructure?

Do we have a plan for the disposal of information when we no longer need it?

What are the thresholds?

Does this plan take into account information held on our behalf by managed service providers?

Do we need to retain the information?

How long do we need to retain it?

Do we periodically audit our information holdings?

Who is responsible for decisions on data retention?

Professional indemnity insurance

- One of your responsibilities under the Code is to maintain PI insurance that meets our requirements.
- The TPB does not recommend specific policies.
- Assess the risk of a cyber attack and consider if you need to take out additional professional indemnity insurance cover to assist with first party losses.

PI insurance: example

- A company had a $2 million turnover and 8 employees.
- Their server and client records were locked by ransomware software.
- The company had the files released after paying a ransom of $50,000 to hackers.
- Their insurance company paid them $150,000 to cover the loss of income, the ransom demand, consultant costs, and costs to restore the network.

Continuing professional education

- You can undertake cyber security awareness training via an online course, a webinar or through professional or technical reading.
- We will recognise cyber security awareness training as relevant CPE.
- CPE activities should be provided by persons or organisations with suitable qualifications and/or practical experience in the relevant subject area.

What to do in the event of a breach

Responding to a data breach

Generally, the actions taken following a data breach should follow four key steps:

1. Contain the data breach to prevent any further compromise of personal information.
2. Assess the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
3. Notify individuals and the OAIC if required. If the breach is an ‘eligible data breach’ under the NDB scheme, it may be mandatory for the entity to notify.
4. Review the incident and consider what actions can be taken to prevent future breaches.

What to do in the event of a data breach

If you have experienced a breach, you should:

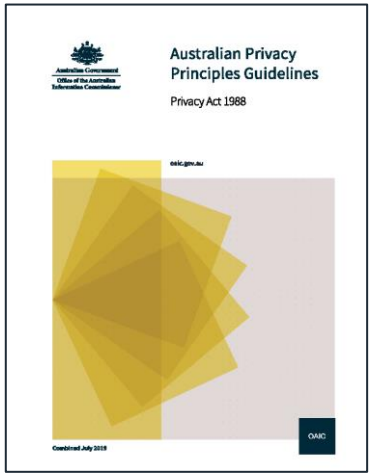
- contact the ATO
- advise any of your affected clients
- contact your software provider
- take steps to secure your information.

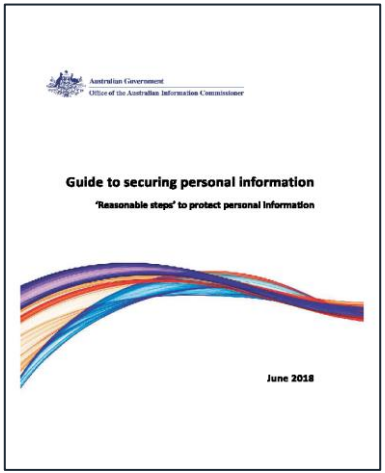
Where to get help

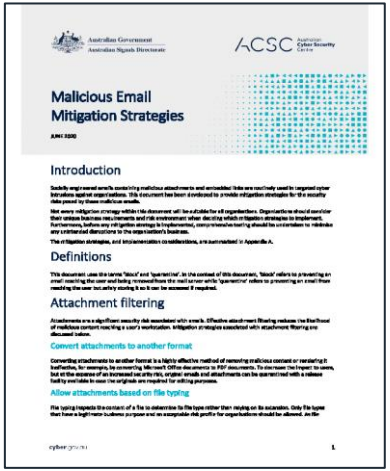
Where to get help

- In the event of a data breach, contact the ATO on **1800 467 033**
- TPB website **tpb.gov.au/protect-your-practice**
- Subscribe to TPB eNews at **tpb.gov.au/newsroom**
- ATO website **ato.gov.au/tpnews**
- OAIC website at **oaic.gov.au**

OAIC resources and materials







oaic.gov.au/privacy/guidance-and-advice

cyber.gov.au/acsc/view-all-content/publications

Questions

Stay in touch with OAIC

oaic.gov.au

oaic.gov.au/contact-us

1300 363 992
(Mon-Thu 10am-4pm AEST)

facebook.com/OAICgov

twitter.com/OAICgov

youtube.com/user/OAICgov

linkedin.com/company/office-of-the-australian-information-commissioner

oaic.gov.au/sign-up

MAKE PRIVACY A PRIORITY

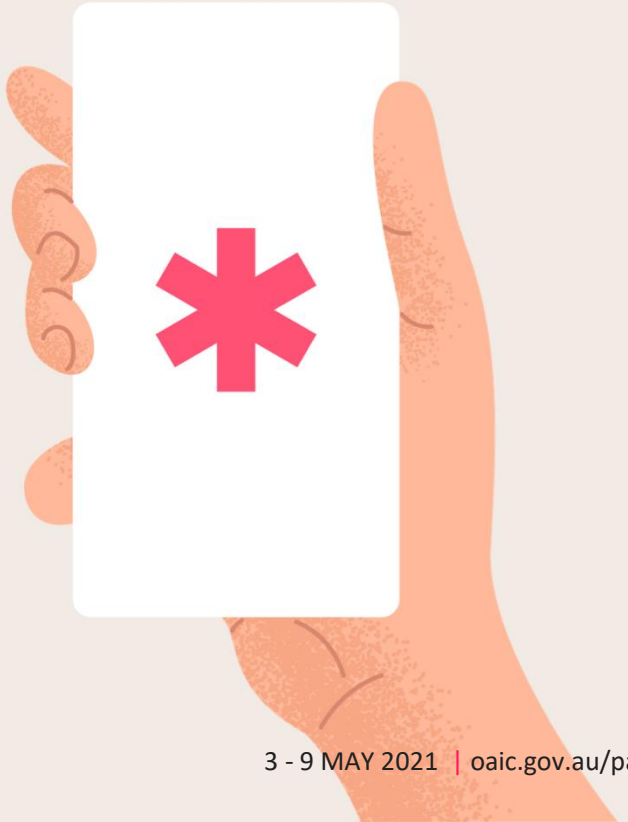
Privacy Awareness Week

Privacy Awareness Week is an annual initiative run by the OAIC as part of a joint effort with state and territory privacy regulators and members of the Asia Pacific Privacy Authorities forum.

The Privacy Awareness Week 2021 theme is:

Make privacy a priority

Businesses and government agencies are encouraged to keep personal information safe by building in privacy protections from the start of a new project, training staff to be privacy aware and taking steps to prevent data breaches.



PRIVACY AWARENESS WEEK

3 - 9 MAY 2021 | oaic.gov.au/paw

Stay in touch with the TPB

tpb.gov.au

tpb.gov.au/**contact**

1300 362 829
(Mon-Fri 9am-5pm AEDT)

facebook.com/**TPB.gov**

linkedin.com/**tax-practitioners-board**

twitter.com/**TPB_gov_au**

youtube.com/**TPBgov**