DUAL

CYBER – MANDATORY BREACH NOTIFICATION

What is a data breach?

A data breach happens when personal information is accessed and disclosed without authorisation, or is lost. For example:

- **a mobile phone that holds an individual's personal information is stolen**
- **an individual's personal information is sent to the wrong person**
- **a hacking of a database containing personal information**

What is the Notifiable Data Breach (NDB)?

On 23rd February 2018, the Privacy Act 1988 was amended to include the Notifiable Data Breaches (NDB) Scheme. The NDB scheme sets out mandatory notification and control requirements for all data breaches involving serious harm to an individual's personal data is to be reported to the Office of the Australian Information Commissioner (OAIC) if the company falls within the reporting criteria.

Previously, companies were simply encouraged to report data breaches and were not legally required to report to the OAIC or inform customers of any potential breaches.

What is 'Personal Information?'

Personal information includes a broad range of information, that could identify an individual.

For example, personal information may include:

- an individual's name, signature, address, phone number or date of birth
- sensitive information
- credit information
- employee record information photographs
- internet protocol (IP) addresses
- voice print and facial recognition biometrics (because they collect characteristics that make an individual's voice or face unique)
- location information from a mobile device (because it can reveal user activity patterns and habits).

What is sensitive information?

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin
- political opinions or associations
- religious or philosophical beliefs
- trade union membership or associations
- sexual orientation or practices criminal record
- health or genetic information
- some aspects of biometric information.

Examples of 'Serious Harm'

Examples of serious harm can include:

- identity theft, which can affect your finances and credit report
- financial loss through fraud
- a likely risk of physical harm, such as by an abusive ex-partner
- serious psychological harm
- serious harm to an individual's reputation.

How long to notify a data breach?

Companies will have 30-day's to investigate an incident from the time they become aware of the breach to assess whether an incident is an 'eligible data breach' and if so, report it to the OAIC.

Who does it affect?

The Privacy Act 1988 affects every organisation with an annual turnover more than over $3 million and small businesses that handle personal information.

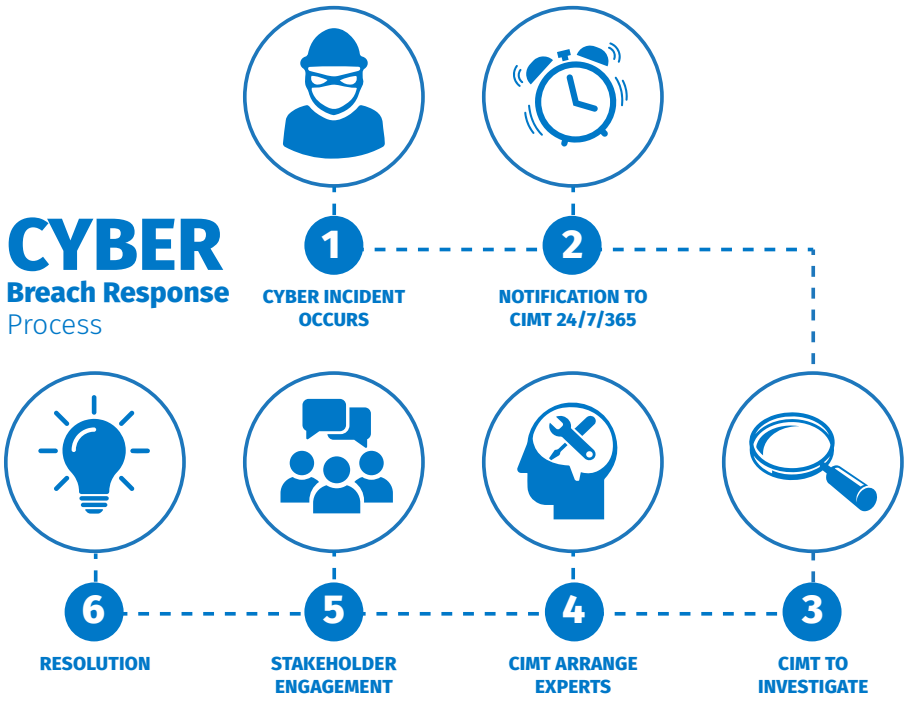
What is the fine and penalty?

Failure to act and report a breach will see fines and penalties up to approximately $400k for individuals and $2m for organisations. However, a new penalty regime is expected to be introduced with penalties to be increased up to $10 million for organisations.

What to do if you think there has been a breach?

In the first instance, notifications should be made via the following methods to ensure that security/privacy breaches are managed efficiently and effectively:

1. phone Cyber Incident Management Team in the first instance on +64 4 831 0243 or
2. send an email to cyber.incident@canopius.com



DUAL's WebRater Cyber Product

Offering is targeted towards the SME market.

- Cyber Platinum is DUAL's original Cyber offering and is aimed towards SME clients with up to $50m turnover
- DUAL offer limits from $250,000 - $2,000,000.
- DUAL's Cyber product includes: First party, third party and Business Interruption coverage.
- For larger clients, please contact your local DUAL underwriter to discuss.