Notifiable Data Breach Scheme

New Australian data breach notification laws have come into effect.

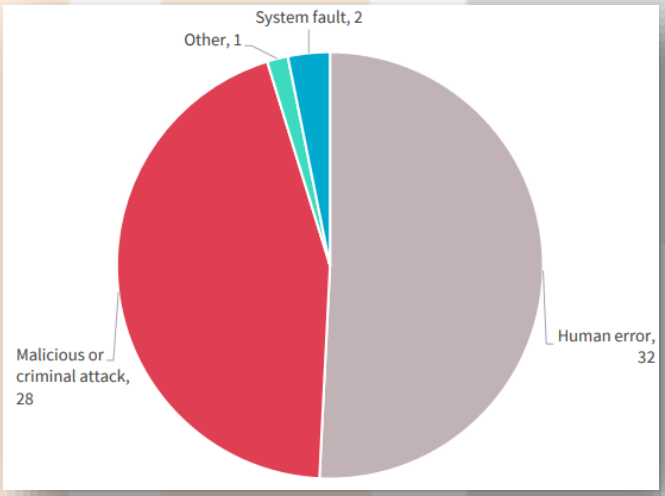
Is your business protected and aware of the consequences?

The NDB (Notifiable Data Breach) scheme only applies to data breaches involving personal information that are likely to result in **serious harm** to any individual affected. These are referred to as **eligible data breaches**.

Serious harm is not clearly defined by the Privacy Act. In the context of a data breach however, serious harm to an individual may include serious physical, psychological, emotional, financial or reputational harm.

Organisations are required to notify the Office of the Australian Information Commissioner (OAIC) in addition to notifying individuals affected by the **eligible data breach**. There are a few exceptions which may mean notification may not be required for certain data breaches.

In the first quarterly report for 2018 by the OAIC of the NBD scheme, human error was blamed for 50% of reported NDB, followed by malicious or criminal attacks at 44%.



Source: "Notifiable Data Breaches Quarterly Statistics Report", Office of the Australian Information Commissioner, Qtr1 2018

The top 5 industry sectors that reported breaches were:

- Healthcare service providers
- Legal, Accounting and Management services
- Finance
- Education
- Charities

Key points:

- New data breach notifications came into effect 22nd February 2018.
- The scheme only applies to businesses with an annual turnover in excess of $3M.
- Businesses must alert authorities and affected clients of an **eligible data breach**.
- Fines of up to $2.1M may apply for non-compliance with the new NDB scheme.

What can be done?

Businesses can consider several preventative actions to avoid the repercussions of a data breach:

- Increase awareness and improve education to help staff reduce risky behaviour that results in data breaches. Common risky behaviour includes:
  - Opening unknown links from unknown senders.
  - Entering information into an unqualified website.
  - Inadvertently sending documents containing personal information to the incorrect recipient.

  All these are extremely common and contribute to an **eligible data breach**.
- Assess and ensure your current IT systems provide sufficient protection against malicious attacks.
- Ensure that your business has the right backup and disaster recovery solution so that critical information can be retrieved.

Contact IPO Digital Solutions for more information on how we can help secure your business and reduce the chances of data breach.