Cyber alert: Introduction of the Notifiable Data Breaches scheme

Karen Searle
Senior Account Executive
+61 8 8385 3535

Background on legislative changes

On 22 February 2018 the *Privacy Amendment (Notifiable Data Breaches) Act 2017* came into effect. Prior to this legislation there was no statutory requirement in Australia, other than for eHealth data breaches, for businesses to notify either affected individuals or regulatory bodies of any data breach.

The Act introduces the Notifiable Data Breaches (NDB) scheme which establishes mandatory reporting protocols of all eligible data breaches for entities bound by the Australian Privacy Principles. These are any private sector and not-for-profit organisations with an annual turnover greater than $3m and all Commonwealth Government and Australian Capital Territory Government agencies.

An eligible data breach occurs:

1. When both of the following conditions are met:
   - there is unauthorised access to, or unauthorised disclosure of, personal information; and
   - the breach would lead a reasonable person to conclude that there is a likely risk of serious harm to any of the individuals to whom the breached information relates;

OR

2. The data is lost in circumstances when:
   - unauthorised access to, or unauthorised disclosure of, personal information is likely to occur; and
   - if the above were to occur, a reasonable person would conclude that there is a likely risk of serious harm to any of the individuals to whom the breached information relates.

Accidental errors in processing or transmitting personal information may also be deemed as eligible data breaches under the NDB scheme.

Following an increase in the penalty unit value, the *Privacy Act* now allows for the following civil penalty provisions:

- A serious or repeated interference with privacy of 2000 penalty units (current total is $420 000) or up to 2000 penalty units for a privacy breach.
- The maximum penalty that the court can order for a body corporate is five times the amount listed in the penalty provisions (current maximum $2.1m).

What details must a notification include?

Notification to the Office of the Australian Information commissioner (OAIC) should be made in the form of a Notification Data Breach statement, with the draft template available on the Australian Government website (www.oaic.gov.au).

There are three options to consider in notifying affected individuals:

Option 1: Notify all individuals

If it is practicable, an entity can choose to notify each of the individuals whose personal information was part of the eligible data breach.

Option 2: Notify only those individuals at risk of serious harm

If it is practicable, an entity can notify only those individuals who are at risk of serious harm from an eligible data breach.

Option 3: Publish notification

If neither option 1 or 2 are practicable, an entity must publish a copy of the statement prepared for the OAIC on their company website and also take proactive steps to publicise the core details of the eligible data breach to increase the likelihood it will come to the attention of individuals at risk of serious harm.

DATA BREACH CONSEQUENCE	FINANCIAL COST / LOSS	CYBER INSURANCE PROTECTION
IT forensic costs to assess and remediate the data breach	Expected	Yes
Notification costs incurred in advising affected individuals	Expected	Yes
Legal costs to notify regulators (breach coach)	Expected	Yes
Ongoing credit monitoring services to affected individuals	Expected	Yes
PR costs to assist in reducing damage to brand	Expected	Yes
Legal defence costs and damages for liability claims arising from affected individuals	Possible	Yes
Payment Card Industry (PCI) fines or assessments	Possible if breached data includes credit card information	Yes
Extortion demands	Possible	Yes

* The above summary represents a general overview of available insurance coverage and should not be relied upon in the event of a claim. Please refer to the specific terms and conditions of your insurance policy for full terms and conditions.