22 February 2017

MANDATORY NOTIFICATION LAWS - THE IMPACT ON YOUR ORGANISATION

The *Privacy Amendment (Notifiable Data Breaches) Bill 2016 (Cth) (*Bill) has been passed by both Houses of Parliament. After gaining Royal Assent, which is seen as a formality, the new laws will come into effect within the next 12 months.

So what does this mean for your organisation and how can you prepare?

Who is governed under these new obligations?

Any entities or agencies regulated by the Privacy Act.

Known as an 'APP Entity', this includes most federal government agencies, credit providers, credit reporting agencies and tax file number recipients. More importantly for the private sector, it extends to organisations with an annual turnover of $3m or more. However, if the organisation is involved in the following, they will be considered an 'APP Entity' regardless of their size.

An organisation that:

- provides a health service and holds health information other than an employee record; or
- discloses personal information about another individual for a benefit, service or advantage, or provides a benefit, service or advantage to collect personal information; or
- is a contracted service provider for a Commonwealth contract.

It is also becoming more common for smaller organisations (i.e. less than $3m in revenue) to actively '*Opt In'* to the Privacy Act and hence send a clear message to their clients that they are committed to strong privacy practices.

What is an 'eligible' data breach?

Unauthorised access or disclosure of personal information that a reasonable person would conclude will likely result in *serious harm* to those individuals, constitutes an *eligible* data breach. Although not explicitly defined, *serious harm* refers generally to serious physical, emotional, financial and reputational harm.

When must notification occur?

Organisations are able to carry out an assessment to confirm whether an *eligible* data breach has occurred. This assessment must be completed within 30 days of the organisation first becoming aware of a possible breach. If there are reasonable grounds to believe an *eligible* breach has occurred, then notification to each affected individual must occur as soon as practicable.

Notification must also be made to The Australian Privacy & Information Commissioner ('Privacy Commissioner'). The organisation must provide a statement which contains the entity and its contact details, a description of the breach and the information at risk, along with recommendations about what individuals can do to minimise their risk.

If each individual is unable to be notified due to a particular set of circumstances, the organisation must publish the notification statement on their website and take reasonable steps to publicise its content.

What does this mean for organisations?

No longer can organisations look to 'cover up' data breaches. Proactive and positive steps are now required by organisations to be transparent with the Privacy Commissioner and affected individuals, to ensure those individuals can take the necessary steps required to mitigate the risk of *serious harm*.

This will force organisations and their Boards to give serious consideration to the data they hold and the protection mechanisms they implement around that data. A large scale data breach has the potential to be more costly than ever and may have serious ramifications for the organisation's reputation.

If an organisation fails to comply with the notification requirements, the Privacy Commissioner has a broad range of powers, which includes seeking enforceable undertakings and issuing fines and penalties against individuals (up to $340,000) and organisations (up to $1.7m).

How can organisations prepare?

Preparation is best broken down into two categories, being *prevent* and *respond*.

Prevent

Organisations and their Boards should be taking a proactive approach to cyber risk. Organisations should be conducting regular security health checks around where and how their data is secured, what applications are in use within their network and who has access to what areas of the network. Engagement with third party IT security vendors can be helpful as they can implement enterprise wide vulnerability and penetration testing programs.

Organisations should also ensure that when managing cyber risk, their sights are focused on educating their workforce. Training programs around cyber risk should be implemented with particular attention given to training employees on identifying and protecting their organisation from cyber attacks.

Respond

Organisations must respond swiftly in the event of a breach. A well-documented and annually tested business continuity and disaster recovery plan should be in place and understood by key members of the organisation who are required to act at the time of an incident.

A **cyber insurance policy** should also be in place and form part of the organisation's overall insurance programme. The proactive nature of the first party cover provided within a cyber policy will ensure that the costs associated with responding to an *eligible* data breach are met via a panel of expert vendors arranged by the insurer. Such costs include important notification related costs such as legal costs, forensic IT costs, public relations costs and credit monitoring related expenses.

If an organisation **does not** have a cyber insurance policy, these costs will need to be met by the organisation themselves and will likely impact the organisation's balance sheet. Questions will also be asked as to whether the directors and officers of the organisation have correctly discharged their duties under the Corporations Act by not insuring against such risks.