MARSH

February 2017

CLIENT ALERT

MANDATORY DATA BREACH NOTIFICATION LAWS PASS THE LOWER AND UPPER HOUSES OF PARLIAMENT

On 13 February the Federal Parliament passed the *Privacy Amendment (Notifiable Data Breaches) Bill 2016* into law (subject to royal assent) which has been three years in the making.

WHO DO THE PROPOSED MANDATORY NOTIFICATION LAWS APPLY TO?

The new laws, which will come into operation 12 months after the day royal assent is received (or earlier by proclamation), apply to most Australian government agencies, all private sector and not-for-profit organisations with a turnover of more than $3 million.

WHAT IS A NOTIFIABLE DATA BREACH?

The legislation considers a notifiable data breach as one that would lead a reasonable person to conclude that there is a likely risk of serious harm to any of the individuals the breached information relates to.

Such information includes personal details, credit information and tax file numbers.

Examples of when a data breach notification will be required include:

- Unauthorised access to, or unauthorised disclosure of, personal information about one or more individuals.
- Breach of a secure storage and handling of information.
- Accidental loss.
- Improper disclosure of information.

REPORTING BREACHES

Any organisation that becomes aware they have been breached or have lost data will need to report the incident to the Office of the Australian Information Commissioner (OAIC) "as soon as practicable" and notify the affected individuals immediately.

The requirements of notification include:

- Description of the data breach.
- Kind of information concerned.
- Number of affected records.

FINANCIAL IMPLICATIONS OF NOT COMPLYING

Under the new laws, those that fail to notify and are deemed to have committed a serious or repeated non-compliance with the mandatory notification requirements could be faced with penalties of up to $360,000 for individuals and $1.8 million for organisations.

PRACTICAL CONSIDERATIONS OF MANDATORY NOTIFICATION

The introduction of the new laws requires a change in approach when responding to breaches for all organisations.

Even organisations with well-developed breach reporting procedures may need to make amendments to ensure they comply with the new requirements.

The costs arising out of complying with the new legislation could be significant. In addition to costs of the actual notification process, organisations need to consider how they will deal with enquiries from affected individuals and what assistance these individuals require to deal with the fall out of the data breach, which may include credit monitoring.

Examples of costs incurred arising out of a breach might include employing a crisis communication team including legal advisers, public relations consultants and accountants to provide guidance on:

- Drafting accurate messages for the media (where appropriate).
- Frequency and timing of updates to the media regarding rectification of the breach.
- Determining overseas notification requirements if the organisation has global operations, e.g. if its data is in a cloud outside Australia.
- IT assistance to create a contact database of affected individuals.
- Establishment of a call centre to communicate with affected individuals.
- Provision of credit monitoring for affected individuals.

The new legislation means that all organisations need to have a greater level of sophistication when considering this issue. We recommend that all organisations have a dedicated breach committee established to:

- Understand the requirements within the new legislation.
- Ensure that current breach procedures, protocols and systems adequately address these requirements.
- Where gaps exist, project-manage improvements to systems.
- Monitor continued compliance with the new laws on an ongoing basis.
- Consider the risk of costs associated with responding to breaches under the new laws, and the appropriateness of transferring this risk via insurance.

CYBER INSURANCE AS A SOLUTION

The costs involved in notifying affected people, employing a crisis communication team, establishing a call centre and providing credit monitoring can be substantial. Additional costs may also be faced from third party claims made following a breach notification.

Marsh has developed a range of tools and cyber insurance policies to help our clients identify, manage, and transfer the risk associated with cyber breaches.

SUMMARY

The change in legislation requires immediate action from all organisations to ensure the ability to comply with the new requirements. Compliance with the requirements following a breach could be costly – all organisations need to assess and understand the risk of these potential costs and to consider how best to manage and transfer them.

KELLY BUTLER
Cyber Leader
+61 3 9603 2194
kelly.butler@marsh.com

ABOUT MARSH

Marsh is a global leader in insurance broking and risk management. Marsh helps clients succeed by defining, designing, and delivering innovative industry-specific solutions that help them effectively manage risk. Marsh's approximately 30,000 colleagues work together to serve clients in more than 130 countries. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), a global professional services firm offering clients advice and solutions in the areas of risk, strategy, and people. With annual revenue of US$13 billion and approximately 60,000 colleagues worldwide, Marsh & McLennan Companies is also the parent company of Guy Carpenter, a leader in providing risk and reinsurance intermediary services; Mercer, a leader in talent, health, retirement, and investment consulting; and Oliver Wyman, a leader in management consulting. Follow Marsh on Twitter; LinkedIn; Facebook; and YouTube.