Is your organisation ready for Australia's new Mandatory Data Breach Laws?

Whether it's your customer lists, customer preferences, patient medical records or client financials, personal information and data is the all-important 'DNA' of any organisation. Alarmingly, serious data breaches are increasing, both in frequency and impact, as recent high-profile news stories illustrate.

And soon organisations will have no choice but to report data breaches which meet certain criteria, increasing the risk of a public relations disaster. Such serious data breaches will be the subject of mandatory data breach reporting obligations (**Mandatory Data Breach Laws**) under the *Australian Privacy Act 1988* (Cth) (the **Privacy Act**). Potential fines for a failure to notify an eligible data breach are large. The maximum penalty for corporations will be a newly minted AUD$2.1 million from 1 July 2017 (up from the previous maximum penalty of AUD$1.8 million).

In this fact sheet, data protection and management experts **Commvault** and privacy and cyber security law experts **Maddocks** join forces to give you an overview of the Mandatory Data Breach Laws and outline their simple **Review** – **Refine** – **Retest** – **Respond** strategy, to help your organisation prepare for the Mandatory Data Breach Notification Laws, mitigate risks and respond appropriately in the case of a serious data breach.

What is an eligible data breach?

An eligible data breach occurs where:

- there is **unauthorised access** to, or **unauthorised disclosure of information**; or
- **information is lost** in circumstances where unauthorised access or disclosure is likely to occur; and
- a reasonable person would conclude that the unauthorised access or disclosure would be **likely to result in serious harm** to any of the individuals to whom the information relates.

Importantly, where data is accessed, disclosed or lost but **robust encryption** is in place, your organisation will ordinarily **not be required to notify the breach**.

What must my organisation do if there is a breach?

Where an eligible data breach has occurred, both the **affected individual(s)** and the Office of the Australian Information Commissioner (**OAIC**) **must be notified**, using a statement which includes certain mandatory information.

As soon as your organisation becomes **aware** of an eligible data breach, it must notify the affected individual(s) and the OAIC **as soon as practicable**.

If such a breach is **suspected only**, then your organisation is still required to **take all reasonable steps to ensure an assessment is completed within 30 days**.

What should my organisation be doing? Review – Refine – Retest – Respond

Given the **demanding timeframes**, it is important for organisations to be **well-prepared** for a breach when it occurs. Maddocks and Commvault recommend organisations adopt a simple Review – Refine – Retest – Respond strategy as depicted below.

Respond

- in the case of a breach, activate your data breach response plan
- immediately notify relevant stakeholders to assess the breach (e.g. compliance, legal). Your lawyer should take steps to maintain privilege
- call in the experts (e.g. forensic consultants) to contain the risk and assist in assessing the breach and advising on the response
- consider whether mandatory notification of individuals and the OAIC is required
- make any other communications (e.g. with insurers, vendors, customers, public announcements, etc.)
- go back to the Review stage.

Review

- review security risks to personal information held by your organisation and the consequences of a breach of security
- review contractual arrangements with vendors, particularly in terms of the IT security policies and practices that each service provider has in place
- review information and data handling policies and procedures within your organisation, and develop a data breach response plan.

Retest

- if a defect has been identified and fixed, rigorously retest
- adopt a holistic approach to securing your data, consider and test the flow of data through the entire system rather than just individual points
- monitor your practices and preparedness through periodic audits.

Refine

- fix any security risks identified in the Review process (e.g. consider encryption)
- update policies and procedures (including to adopt a compliant response plan)
- refine your team of experts (forensic and technical experts, third party vendors, legal advisors).

If you would like to learn more about the new Mandatory Data Breach Laws and adopting a Review – Refine – Retest – Respond strategy, please contact Commvault or Maddocks.

Michael Bishop | Commvault
APAC Lead Counsel
61 2 8243 9815
mbishop@commvault.com

Brendan Tomlinson | Maddocks
Special Counsel
61 2 9291 6121
brendan.tomlinson@maddocks.com.au

Sonia Sharma | Maddocks
Senior Associate
61 2 9291 6143
sonia.sharma@maddocks.com.au

For more insight into the new laws visit maddocks.com.au/blog/explaining-australias-mandatory-data-breach-notification-laws/