Monthly Newsletter

February 2018

charter partners
accounting + business advisors

New data breach laws come into effect

New data breach rules in affect from 22 February 2018 place an onus on businesses to protect and notify individuals whose personal information is involved in a data breach that is likely to result in serious harm.

In October last year, almost 50,000 employee records from Australian Government agencies, banks and a utility were exposed and compromised because of a misconfigured cloud based 'Amazon S3 bucket'. AMP was reportedly one of the worst affected with 25,000 leaked employee records. ITNews reports that the data breach was discovered by a Polish researcher who conducted a search for Amazon S3 buckets set to open, with "dev", "stage", or "prod" in the domain

name. One contractor appears to be behind the breach.

In October 2016, the details of over half a million Red Cross blood donors were inadvertently exposed after a website contractor created an insecure data backup. In the US, a massive data breach exposed credit records (including social security records) of over 145 million Americans – all because an IT worker didn't open an email about a critical patch for their software.

Regardless of how good your existing systems are, data breaches are a reality either through human error, mischief, or simply because those looking for ways to disrupt are often one step ahead. But it's not all about IT, there have been numerous cases of hard copy records being disposed of inappropriately, employees allowing viruses to penetrate servers after opening the wrong email, and sensitive data on USBs lost on the way home.

Who is covered by the data breach scheme?

The Notifiable Data Breach (NDB) Scheme affects organisations covered by the Privacy Act – that is, organisations with an annual turnover of $3 million or more. But, if your business is 'related to' another business covered by the Privacy Act, deals with health records (including gyms, child car centres, natural health providers, etc.,), or a credit provider etc., then your business is also affected. Special responsibilities also exist for the handling of tax file numbers, credit information and information contained on the Personal Property Securities Register.

What you need to do

It's important to keep in mind that complying with these new laws means more than notifying your database when something goes wrong. Organisations are required to take all reasonable steps to prevent a breach occurring in the first place, put in place the systems and procedures to identify and assess a breach, and issue a notification if a breach is likely to cause 'serious harm'.

Taking all reasonable steps - assessing risk

The Privacy Act already requires organisations to take all reasonable steps to protect personal information. The new data breach laws merely add an additional layer to assess breaches and notify where the breach poses a threat. For example, if you have not already, you should assess issues such as:

- How personal information flows into and out of your business.
  - What information do you gather?
  - What information do you provide?
  - Where private information is stored – map out what systems you use, where these systems store data, what level of security is provided within those systems, and what level of access each team member has.
- How private information is handled by your business across its lifecycle and who has access at each stage.
- Possible impacts on an individuals' privacy.
- The policies and procedures in place to manage private information, including risk management and mitigation, whether these are adhered to, and actively managed.
- The policy review process – review policies and procedures at least annually but again with the introduction of new systems and technology. Remember, you can't just

have a policy sitting somewhere, it needs to be actively reinforced and adopted by team members.
- Interstate new project protocols for ensuring privacy where personal information is at risk.
- Document everything including your reviews and procedural updates even if nothing changed. If there is ever an issue where your business's culpability is assessed, your capacity to prove that you took all reasonable steps will be important.

When it comes to data breaches, all organisations must have a data breach response plan. The data breach plan covers the:

- Actions to be taken if a breach is suspected, discovered or reported by a staff member, including when it is to be escalated to the response team.
- Members of your data breach response team, and
- Actions the response team is expected to take.

The Office of the Australian Information Commissioner provides a sample breach response plan.

Identifying a serious breach

So, what is a serious breach? A breach has occurred when there is unauthorised access to or disclosure of personal information or a loss of personal information that your business holds. Whether a breach is serious is subjective but may include serious physical, psychological, emotional, financial, or reputational harm. If a breach occurs, you need to think through how that information could be used for identity theft, financial loss, threats to physical safety, job loss, humiliation or reputational damage, or workplace bullying marginalisation.

If you suspect a breach has occurred, your business is obliged to take "reasonable" and "expeditious" action regardless of whether you think it is serious or not (under the NDB scheme you have a maximum of 30 days to assess the damage and respond but in general, the first 24 hours is often crucial to the success of your response). Ignorance is not a defence. A lack of systems to identify system breaches fails the Privacy Act's requirement to take all reasonable steps to protect personal information. As soon as a breach is identified anywhere in the business, whether it is IT based or physical, steps needs to be taken – if it is simply noting that no further action is required.

If you suspect a data breach has occurred that may meet the threshold of 'likely to result in serious harm', you must conduct an assessment. Sounds simple right? But the problem for business is often that there are initially no definitive answers about the extent of the breach or its seriousness for the assessment to take place. Take the example of a retail business with an online store. A hacker exploiting an unpatched vulnerability in your customer relationship management (CRM) system gains access to the customer database for your online store, which includes customer purchase histories and contact details. IT calls you and tells you there is a problem but can't tell you how, what customer records are affected, and if the records have been compromised. The first step is generally to contain the damage – isolate or shutdown the affected system to prevent further potential loss – then assess the scenario – not just because of the NDB scheme but because your business's reputation is on the line.

Notifying a breach

If a breach is assessed to potentially result in serious harm, you are obliged to advise affected individuals and the Australian Information Commissioner. You have the option to:

- Notify all individuals whose personal information is involved in the eligible data breach;
- Notify only the individuals who are at likely risk of serious harm; or
- Publish your notification, and publicise it with the aim of bringing it to the attention of all individuals at likely risk of serious harm.

You advise the Australian Information Commissioner of a serious potential breach using the Notifiable Data Breach statement – Form.

And it's not just Australia. Does your business have international connections?

Data breaches are common and many countries have moved to ensure that the personal information of individuals is protected. If your business operates overseas or has customers overseas you need to be aware of the requirements in those countries.

Most US states have compulsory data breach requirements. The European Union's General Data Protection Regulation (GDPR) comes into effect from 25 May 2018. If you operate through a local distributor in the European Union or have direct supply into those countries, then it's likely your business will be caught by Regulation.