Notifiable Data Breaches

Data breaches are occurring at an alarming rate and can be disastrously damaging for both an organisation and its customers. In just the first year of Australia's Notifiable Data Breach scheme, more than 800 data breaches were reported to the Office of the Australian Information Commissioner (OAIC).

For a business, data breaches can be detrimental to its brand, which can mean a loss of revenue and ultimately a loss of customer trust. We can just look at the knock-on effect of consumer credit reporting agency Equifax on credit markets around the world after 143 million of its personally identifiable customer records were successfully stolen.

For customers, the impact of a data breach is almost always irreconcilable. Based on a survey by the Australian Community Attitude to Privacy Survey (ACAPS) , conducted by the OAIC, 58 per cent of consumers said they would not deal with a business due to privacy or security concerns associated with data loss.

The risk is even higher for small-to-medium businesses (SMBs). Recent research revealed that 57 per cent of all SMBs with an annual turnover of $3 million have not undertaken any sort of IT security risk assessment in the last 12 months, putting their devices, data and documents at risk.

However, to ensure the protection of consumers and encourage greater transparency among Australian organisations in the event of a data breach, the country's first data breach notification law – dubbed the Notifiable Data Breach (NDB) scheme – came into effect on February 22, 2018.

What is the Notifiable Data Breaches Act?

Under the new law, officially known as the Privacy Amendment (Notifiable Data Breaches) Act 2017, any government agency, organisation or business with an annual turnover of $3 million or more in Australia that is covered by the Australian Privacy Act (1998) is obliged to notify individuals whose personal information is involved in a data breach, as soon as practicable after becoming aware of a breach.

Under the Act, a notifiable data breach is a data breach that is likely to result in serious harm to any of the affected individuals. The Act defines a data breach as occurring when any personal information held by an organisation is lost or subject to unauthorised access or disclosure.

[1] https://www.accenture.com/au-en/insight-cost-of-cybercrime-2017

[2] https://www.oaic.gov.au/engage-with-us/community-attitudes/

[3] http://www.zdnet.com/article/oaic-received-31-notifications-in-the-first-three-weeks-of-data-breach-scheme/

AT A GLANCE

The Notifiable Data Breaches Scheme

What is the Notifiable Data Breaches (NDB) Scheme?

The NDB scheme requires any organisation covered by the Australian Privacy Act (1988) to notify any individuals likely to be at risk of serious harm by a data breach.

When did it come into force?

The NDB scheme has been effective since February 22, 2018.

What are some examples of a data breach?

Examples of when a data breach includes in the event a device containing customers' personal information is lost or stolen; a database containing personal information is hacked; or personal information is mistakenly given to the wrong person.

What happens after a data breach?

An organisation that has suffered a data breach must notify the Office of the Australian Information Commissioner (OAIC) as well as affected members of the public. A notification must contain the identity and contact details of the organisation; a description of the data breach; the kinds of information concerned; and recommendations about what affected individuals should do.

The NDB scheme is overseen by the OAIC and brings Australia's privacy laws in line with other jurisdictions that have implemented similar legislations, including the United States and the European Union.

During the first year the NDB scheme, 812 incidents were reported. The OAIC confirmed in its most recent quarterly report (1 October to 31 December) that it received 262 data breach notifications. Industry sectors that reported the highest number of breaches during the quarter were health service providers, finance, and legal, accounting and management services. The education, and mining and manufacturing sectors were also key targets.

What is considered a data breach?

According to the OAIC, an eligible data breach arises when:

- A device containing a customer's personal information is lost or stolen
- A database containing personal information is hacked
- Personal information is mistakenly provided to the wrong person

What happens after a data breach?

When an organisation is aware of a data breach, the OAIC and the public must be notified as soon as possible. Information that needs to be provided includes:

- The identity and contact details of the affected organisation
- A description of the data breach
- The kinds of information concerned in the data breach
- Recommendations about the steps individuals should take in response to the data breach

However, there are some exceptions to the law – primarily in situations when two or more entities hold the same information, in which case only one organisation needs to notify of the breach, or in circumstances relating to law enforcement activities. There are also provisions relating to secrecy regarding national security.

[4] http://www.shredit.com.au/en-au/resource-centre/infographics/security-tracker-2016

[5] https://www.itnews.com.au/news/contractor-behind-australias-biggest-ever-data-breach-revealed-440339

How to protect your business from a data breach?

Regardless of the size of your business, it's important to recognise that you can be a target. It's equally important to illustrate to customers that current best practice security measures are in place to protect their data from nefarious attackers.

Taking a holistic and multilayered approach to protecting your business, combining both security measures and awareness training, is therefore key to successfully avoiding a data breach.

Although many SMBs have come to rely on a 'computer savvy' staff member to handle IT support, most now choose to partner with a trusted managed service provider (MSP) to not only support day to day IT, but to also protect a company from the latest cybersecurity threats, and assist with backup and disaster recovery. The key benefits for SMBs engaging an MSP is always knowing how critical information is stored and secured, how data is backed up in the event of a network failure or what impact a sudden disaster would have on the business.

Cyber awareness training can assist businesses and their staff to familiarise themselves with some of the most common causes of data breaches. The OAIC identified these as including human error as well as malicious or criminal attacks through avenues such as malware and system faults . Engaging employees in regular (and mandatory) cybersecurity training that enables them to spot and avoid potential phishing scams in their inbox, a leading entry point for ransomware, is one of the most effective ways to avoid an attack.

Conclusion

Since the introduction of the Privacy Amendment (Notifiable Data Breaches) Act 201 in February, it's even more vital for every organisation to do everything they can to ensure they prevent a data breach, or other forms of hacking.

Not only do they risk being penalised by the government for these breaches, it can also have a long-term impact on how a company is perceived in the market, which can be damaging to a company's revenue stream and reputation.

The reality is that most breaches come down to human error and in order to avoid it, education and is important. However, given that humans are inevitably fallible it's important to ensure there is an all-in-one backup, protection and disaster recovery system in place as a foundational protection piece against data breaches.

[6] https://www.itnews.com.au/news/contractor-breach-exposes-50k-aussie-govt-bank-staff-records-476650

[7] https://www.arnnet.com.au/article/629667/data-governance-focus-following-australia-second-largest-breach/

[8] https://www.datto.com/au/resources/apac-ransomware-survey-17

[9] https://home.kpmg.com/uk/en/home/insights/2017/06/2017-ceo-outlook.html

For more information please contact: Anton Nesbit | Business Development Manager | Phone: 0272686669 | Email: anton@silicon.co.nz | Silicon Systems Limited | https://www.silicon.co.nz/