datto | UNIFIED CONTINUITY

Notifiable Data Breaches

(Updated 9 January 2020)

Data breaches have become an almost daily occurrence and can be disastrously damaging for both an organisation and its customers. The most recent statistics available[1] show that in the 12 months to June 2019, Australia's Notifiable Data Breach scheme saw over 900 data breaches reported to the Office of the Australian Information Commissioner (OAIC).

For a business, a data breach can be detrimental to its brand, which can mean a loss of revenue and ultimately a loss of customer trust. They can even prove to be terminal. For example, US-based clinical laboratory, Quest Diagnostics, announced in June last year[2] that an unauthorised user had gained access to data on almost 12 million patients, including their credit card details and social security numbers. The company that was blamed for the breach was American Medical Collection Agency, a debt collection agency that handled patient data. AMCA's downfall was swift. Almost immediately, it lost four of its largest clients, including Quest Diagnostics, and filed a Chapter 11 petition for bankruptcy on June 17[3].

For customers, the impact of a data breach is almost always irrevocable. Based on a survey by the Australian Community Attitude to Privacy Survey (ACAPS)[4], 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.

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[5].

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

The most recent statistics available on the NDB scheme show that in the year to June 2019, 967 incidents were reported. The OAIC confirmed in its most recent quarterly report (1 April to 30 June 2019)[6] that it received 245 data breach notifications. The industry sectors that reported the highest number of breach notifications during the quarter were health service providers, finance (including superannuation), and legal, accounting and management services. The education and retail sectors were also key targets.

[1] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/

[2] https://www.washingtonpost.com/business/economy/quest-diagnostics-discloses-breach-of-patient-records/2019/06/03/aa37b556-860a-11e9-a870-b9c411dc4312_story.html

[3] https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach/

[4] https://www.oaic.gov.au/engage-with-us/research/2017-australian-community-attitudes-to-privacy-survey/report/

[5] https://www.lifehacker.com.au/2018/02/australias-notifiable-data-breaches-scheme-starts-next-week/

[6] https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-statistics-report-1-april-to-30-june-2019/

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.

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.

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 be notified of the breach, or in circumstances relating to law enforcement activities. There are also provisions relating to secrecy in regard to national security.

Recognising the impact of human error

There is a misconception that hackers are the cause of most data breaches. This is mainly because we are often exposed to media reports about large hacking cases, such as when mobile game producer Zynga announced in October 2019, that a hacker had accessed account log-in information, usernames, Facebook IDs, and phone numbers of customers who play its popular 'Draw Something' and 'Words with Friends' games[7]. Around 218 million customers who installed iOS and Android versions of the games before September 2 last year were affected.

This myth has largely been debunked with the OAIC identifying human error as the cause of one-third of all data breaches.

The data breach impacting around 50,000 Optus customers in October last year is a prime example[8]. Optus informed those customers that their names, addresses, and phone numbers were mistakenly published in the White Pages online directory, run by Sensis, as well as some hard copy local White Pages directories.

An administrative error was blamed for the leak, with Optus and Sensis laying the blame for the breach at each other's door.

In another case that also came to light in October last year, the names, phone numbers and email addresses of almost 50,000 Australian university students were exposed by online events promotion company, Get[9]. The company's mobile app, which is used by university clubs and societies to sell tickets to events, had an error in its search option that provided an opportunity to anyone to access the personal details of anyone who had used the app to buy tickets in the last two years.

Human error can also be blamed when someone unintentionally opens a well-crafted phishing email, resulting in ransomware infiltrating a business's systems. In the 2019 State of the Channel Ransomware Report[10], 91% of MSPs reported attacks against ANZ small-to-medium-sized businesses in the last two years – the highest rate globally. Yet, somewhat worryingly, there is a disconnect between the perceived threat of ransomware amongst MSP's and the SMBs themselves, with 89% of MSPs saying that SMBs should be very concerned about the threat, but only 28% of MSPs reported that SMBs were very concerned about ransomware.

The core issue of human error comes down to a lack of education and awareness around how to maintain good IT security posture. The need for companies to invest in security measures and the right people to implement those measures effectively was highlighted in the State of Industrial Cybersecurity 2019 report by security firm Kaspersky[11], which found that employee errors or unintentional actions accounted for 52% of incidents affecting operational technology (OT) and industrial control system (ICS) networks in the past year.

What can be done?

There are several preventative actions that businesses can take to avoid data breaches.

As human factors are often the weakest links in the cybersecurity chain, it is worthwhile paying close attention to strengthening this aspect of an organisation's security posture.

Cyber awareness training is key.

Effective and regular awareness training can get end users to think before they click on an email or a malicious URL or provide requested details. Educated users will make far better decisions and fewer mistakes.

Knowing humans are fallible and make mistakes, it is important for organisations to look at the technology layer of their business to ensure there are solutions in place that can offer both backup and protection if something does go wrong; in addition to implementing an awareness training program for end-users.

Automatic backups ensure systems can be restored no matter what happens, plus critical information can be recovered if it happens to fall in the wrong hands.

Preparation also means having a disaster recovery plan in place. Businesses with a disaster recovery plan report increased savings, enhanced system reliability, improved security, and reduced insurance premiums – even without disaster.

[7] https://www.cnet.com/news/words-with-friends-hack-reportedly-exposes-data-of-more-than-200m-players/

[8] https://www.smh.com.au/national/thousands-of-optus-mobile-numbers-mistakenly-published-in-white-pages-20191025-p5346z.html

[9] https://www.theguardian.com/education/2019/sep/10/data-breach-may-affect-50000-australian-university-students-using-get-app

[10] https://www.datto.com/au/resources/dattos-global-state-of-the-channel-ransomware-report-au

[11] https://ics.kaspersky.com/the-state-of-industrial-cybersecurity-2019/

What does the NDB scheme mean for my business?

The NDB scheme may now be in effect but MSPs should not feel limited.

Anything concerning security is usually viewed as a block on innovation because there are often regulations and policies in place to the protect data. But the relentless parade of data breaches over the last few years has created a real revenue opportunity for MSPs to provide additional cybersecurity services for clients.

KPMG's 2019 Global CEO Outlook[12] found that 71 per cent of CEOs viewed cyber security as a strategic function and a source of competitive advantage, rather than an overhead cost — something Australian CEOs can really learn from.

Customers are increasingly more attracted to those companies willing to provide them with a newly increased assurance that their data is safe. By ensuring customers the utmost protection, MSPs can build trusted customer relationships that will drive loyalty and retention. This is why we see companies, such as Apple, constantly reinforcing the security aspect of its operating platform as one of its standout features and how it is superior against cyber criminals when compared to competitors, such as Samsung, whose smartphones operate on an open-platform.

In fact, there is an opportunity for companies to turn their ability to be secure into a corporate social responsibility as a way to assure customers they will protect and fairly use their personal data and any other sensitive information.

This will help reassure the trust factor in the business customer relationship. If businesses can guarantee that their security tools are more superior compared to a competitor's, the opportunity presents itself to charge for premium pricing, increasing revenue and customer growth.

Conclusion

Since the Privacy Amendment (Notifiable Data Breaches) Act came into effect in February 2018, 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.

[12] https://home.kpmg/xx/en/home/campaigns/2019/05/global-ceo-outlook-2019.html

datto

Corporate Headquarters
Datto, Inc.
101 Merritt 7
Norwalk, CT 06851
United States
partners@datto.com
www.datto.com
888.294.6312

Global Offices

USA:	888.294.6312
Canada:	877.811.0577
EMEA:	+44 (0) 118 402 9606
Australia:	+61 (02) 9696 8190
Singapore:	+65-31586291