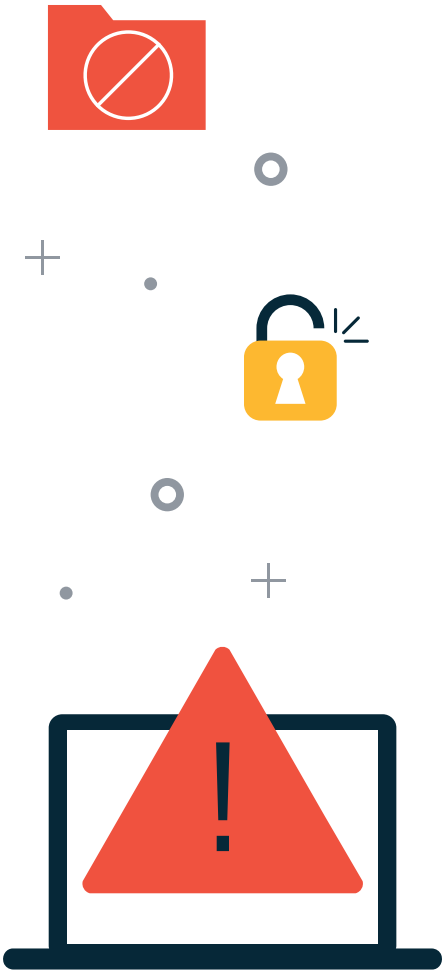
datto



DATTO NOTIFIABLE DATA BREACHES WHITE PAPER

Data breaches are accelerating and can be disastrously damaging for both an organisation and its customers. According to research by Accenture , the global average number of security breaches each year is 130, which has risen annually by 27.4 per cent.

For a business, data breaches can be detrimental to its brand, which will mean a loss of revenue and ultimately a loss of customer trust. For example, 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 Office of the Australian Information Commissioner (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.

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.

The OAIC confirmed three weeks after the NDB Scheme came into effect it had received 31 data breach notifications .

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.

The notice must also include recommendations about the steps affected individuals need to take in response to a data breach.

[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/

datto

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 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.

Data breach myths busted

There is a huge misconception that hackers are the number one cause of data breaches. This is mainly because we are often exposed to media reports about large hacking cases, such as the Sony hack in 2014 where hackers stole huge swaths of confidential documents – including those belonging to Hollywood celebrities – before leaking them online.

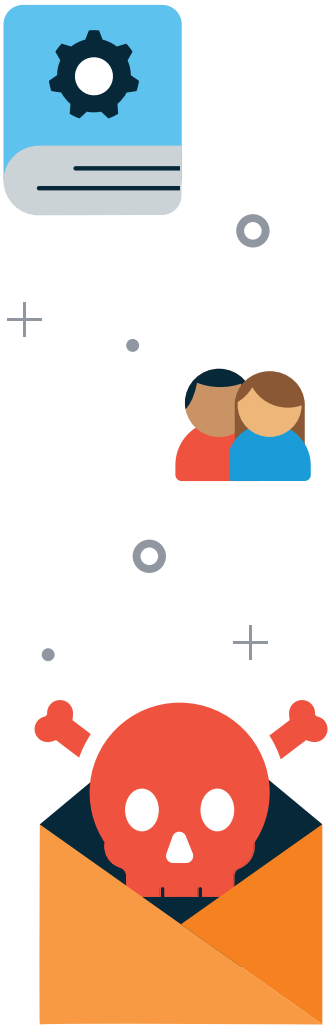
The actual leading cause of data breaches -- and often the most detrimental because it can disrupt business continuity -- has been identified as unintentional human error.

Information security firm Shred-It's survey of more than 1,100 businesses in Australia admitted that human error is a larger threat to information security than deliberate theft or sabotage by a third party .

The data breach of the Red Cross Blood Service in August 2017 is a prime example. This involved sensitive personal and medical records of 550,000 potential donors being exposed online. According to news reports , what was considered at the time Australia's largest data breach was caused by an error made by one of the Red Cross Blood Service's contractor's technical team members, who accidentally leaked a database backup containing all the significant information donors enter as part of the booking process including name, gender, physical and email address, phone number, date of birth, country of birth, blood type and instances of high-risk sexual behaviour.

[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



In a separate case, the personal details – including full names, passwords, IDs, phone numbers, email addresses, credit card numbers and details on staff salaries – of almost 50,000 Australian employees of several government agencies, banks and a utility were leaked online . In that instance, according to media reports , Australia's Labor Party Shadow Minister of Digital Economy Ed Husic conceded that "more often than not it's not the tech that lets you down, it's the people and the processes", suggesting that this leak was also due to human error.

Human error can also be blamed when someone unintentionally opens up a well-crafted phishing email, resulting in the infiltration of ransomware into a business' systems. The 2017 State of the Channel Ransomware Report found an estimated 6 per cent of small-to-medium-sized businesses paid a total of $12.6 million in ransomware as a result of these attacks.

The core issue of human error comes down to a lack of education and awareness around how to maintain good IT security posture. The Shred-It survey found while 38 per cent of c-suite executives and 46 per cent of small business owners recognise human error is identified as the biggest source of a potential data breach, almost two-thirds of small to medium businesses and 5 per cent of larger organisations said they had either never trained their staff on information security policies or didn't have these policies in place.

What can be done?

There are several preventative actions that businesses can take to avoid the repercussions of a data breach.

As human factors are often the weakest links in the cybersecurity chain, it pays to focus on strengthening an organisation's security posture.

Increasing awareness and enhancing education are key, but increasing awareness does not equate to knowledge. Therefore, businesses need to enhance an end-user's awareness, as well as provide education.

Awareness can get end users to think before they act, so rather than clicking on anything and everything, it will trigger them to think about why they may or may not need to click that next button. Education can give end users the knowledge they need to change the way they act. Educated users will make far better decisions and fewer mistakes than those who are less educated.

Ultimately, unlike machines that are programmed to carry out tasks, humans are fallible and can make mistakes.

It is therefore important to look at the technology layer of the business to ensure there are solutions in place that can offer both backup and protection if something does go wrong, in addition to educating and raising awareness among end-users. All-in-one solutions can ensure that if you get hit with a data breach you are able to recover from it as quickly as possible.

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.

[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

Part of planning 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.

What does the NDB scheme mean for my business?

The NDB scheme may now be in effect but it is not a limiting law.

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 businesses – if there is a well-designed cybersecurity program in place.

The KPMG CEO Outlook 2017 asked 150 CEOs in the UK for their thoughts about security and found that 70 per cent viewed it as a chance to unearth fresh revenue streams and innovate, 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, businesses 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 by enforcing security controls that 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 ensure that their security is more superior compared to a competitor's, the opportunity presents itself to charge for premium pricing, increasing revenue and customer growth.

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.

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

About Datto

At Datto, our mission is to empower the world's small and medium sized businesses with the best in enterprise-level technology. We do it by equipping our unique community of Managed Service Provider partners with the right products, tools and knowledge to allow each and every customer to succeed. It's an approach that's made us the world's leading provider of MSP delivered IT solutions. Datto is headquartered in Norwalk, CT, with offices worldwide.

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