PREPARING FOR THE MANDATORY NOTIFIABLE DATA BREACH SCHEME

BECOMING STATE-OF-THE-ART

Cyberthreats are getting more sophisticated and prevalent, affecting society and economies. Consequently, government regulation is evolving to reflect this risk and drive confidence in the digital space. **From 22 February 2018**, Australian organisations that are subject to the Privacy Act will need to report data breaches to the affected parties and to the Office of the Australian Information Commissioner (OAIC). As businesses grapple with new requirements on data protection, aligning with the Notifiable Data Breach (NDB) scheme is essential. Managing this alignment successfully means not just ticking boxes, but holistically addressing their cyber risks and becoming state-of-the-art.

WHY IS THE AUSTRALIAN GOVERNMENT TAKING ACTION?

Australia's Privacy Act has been in place since 1988 and it regulates how personal information is handled. It demands that organisations collecting personally identifiable information take all reasonable steps to protect that information. Given the increasing reliance on digital technology and the growing risk of cybercriminals accessing personal information, the NDB scheme has been developed to encourage a higher standard of personal information security, help individuals minimize harms resulting from a data breach and improve transparency on how agencies respond to serious data breaches.

Recent estimates by the Attorney-General's department indicate that identity crime costs Australia more than $1.6 billion each year, with around $900 million lost by individuals through credit card fraud, identity theft, and scams. The NDB scheme was designed to empower people to protect themselves if their personal information has been breached.

This makes strong cybersecurity an increasingly important priority for everyone.

WHO IT APPLIES TO

The NDB scheme applies to all government agencies and businesses that are required to comply with the Privacy Act. This includes, among others, businesses and not-for-profit organisations with an annual turnover of more than $3 million.

Other businesses may also be subject to the scheme, even if their turnover is less than $3 million. This includes organisations that collect personal data, as well as individuals that handle personal information for a living such as:

- private sector health service providers including gyms,
- weight-loss consultants, and alternative medicine practitioners
- schools, colleges, universities, and childcare centres
- businesses that sell or purchase personal information
- credit providers and credit reporting bodies
- those who handle tax file numbers or health records.

[1] https://www.afp.gov.au/what-we-do/crime-types/fraud/identity-crime

WHAT THIS MEANS FOR BUSINESS

- Businesses need to ensure their information systems are secure and prevention is key.
- Organisations can take four key steps to ensure compliance with the NDB scheme:

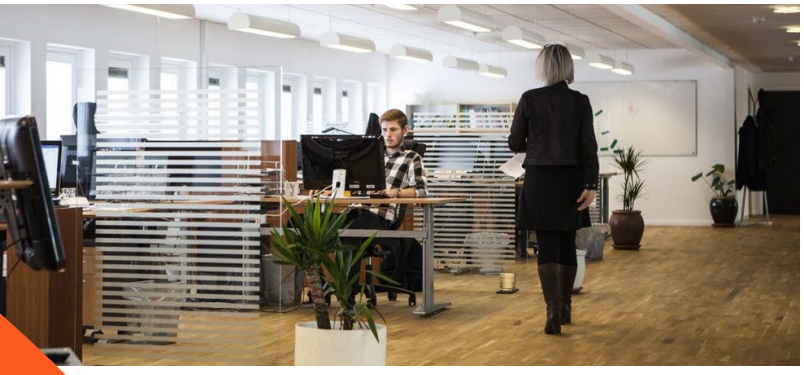
1. **Embed a culture of privacy.** Teach employees to treat information as a valuable asset, protecting it with strong passwords and being mindful of who they share data with.
2. **Focus on prevention.** Data breaches cost time and money, as well as affecting the organisation's reputation. It's more cost- and time-effective to prevent them than to respond to them. This depends on being aware of what data is being collected, where it's being stored, what it's being used for, and who has access to it.
3. **Test and review.** Cyberthreats are constantly evolving so businesses need to make sure their security approach is also evolving to stay ahead of threats. This involves regularly testing security systems and processes to ensure they're still relevant and effective.
4. **Improve.** Organisations should seek continual improvement when it comes to protecting personal data.

RECOMMENDATIONS FOR BUSINESSES

- Many businesses will already be prepared for the NDB scheme through their regular privacy and security measures. Others will need to work to get ready. Businesses should work with their Chief Information Security Officer and their General Counsel to develop a plan for addressing cybersecurity incidents.
- Businesses should build a senior technical team to identify and manage cybersecurity risks as part of their overall risk management strategy.
- Business should also work with senior leaders to develop and practice incident prevention strategies and response plans.

KEY DEFINITIONS

- A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals whose information was breached.
- Serious harm isn't confined to financial losses; it can include reputational damage or embarrassment, as well as emotional distress.
- A data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure.



PREVENTION

CURRENT STATUS

The NBD scheme becomes effective on 22 February 2018.

PREVENTION VERSUS TICK-THE-BOX COMPLIANCE

"Cybersecurity continues to evolve at a rapid pace, yet it's very easy to slip into the habit of taking the same security measures that worked in the past. Ask yourself when you last changed a security process, or reviewed your capabilities, and whether they remain state-of-the-art. More rudimentary is: how do you measure success; just what is the yardstick that allows you to validate the need for change? In the dynamic cybersecurity arena, continuing to do the same old things because they worked in the past typically means you are slowly slipping away from state-of-the-art capabilities."

– Greg Day, VP & CSO, Palo Alto Networks

STATE-OF-THE-ART PREVENTION PLATFORM

State-of-the-art security begins by facing cyberthreats with an understanding that prevention is crucial. One of the historical points of failure has been to cling onto old security practices when new more effective methods have evolved. Cybersecurity is incredibly dynamic, and businesses should not wait for attackers to show them they have slipped from state-of-the-art. Fully addressing the evolving cyber policy and threat environment requires a combination of the right people and processes, advanced technology, and information sharing, all working in concert.

1. The right processes make people more efficient at managing risk, by using training to reduce human error.
2. Advanced technology knows the network and responds automatically to new threats.
3. Sharing information as a community helps businesses respond to new attacks faster than they can be launched, building a network effect of defence.

The MSS name is synonymous with industry-leading practice in cybersecuirty solutions, offering pro-active protection, reactive solutions and ongoing audit services for clients across Australia. Our Perth cybersecurity specialists expertly provide tailored solutions for your organisation's security requirements. Find out how to make your security state-of-the-art by visiting www.mssit.com.au

mss

679 Murray St, West Perth WA 6005 | 1300 MSS4IT (677 448) | sales@mssit.com.au | mssit.com.au