Loop Secure

WHITE PAPER

PREPARING FOR THE NOTIFIABLE DATA BREACHES SCHEME

PUBLIC

Version: 1.0

29/11/2017

ABN 76 114 448 225

Document Control

Document Information

File Name	(P)_Loop Secure - Analysis - Australian Notifiable Data Breaches (NDB) Scheme.docx
Last Updated	Wednesday, 29 November 2017

Document Contributors

Name	Role	Email
Patrick Butler	Chief Executive Officer	pbutler@loopsec.com.au
Lyal Collins	Chief Information Security Officer	lcollins@loopsec.com.au

Contents

1 Executive Summary

Benjamin Franklin once said, 'an ounce of prevention is worth a pound of cure'. Today this can be aptly applied to the value proposition of protecting our important information.

Unfortunately, recent history shows that data breaches are a fact of life for many organisations – no-one knows who is going to be breached, or when.

That said, proven incident handling responses and breach impact minimisation through solid operations security has a significant return on investment when compared to the potential financial impact and brand damage of a breach.

The Notifiable Data Breaches (NDB) Scheme commencing on 22 February 2018 is a timely reminder to take stock of our approach to protecting information. The Scheme will require organisations covered by the Australian Privacy Act 1988 to notify all individuals likely to be at risk of serious harm if personal data is compromised by a data breach.

Legal advice should be sought by organisations wishing to clarify whether the Scheme applies to them and to the extent the obligations impacts existing processes and capabilities. That said, as with the Privacy Act 1998 and amendments, the NDB Scheme is concerned with information that is "About" the individual or information from which their identity can be reasonably ascertained.

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

Organisations covered by the Scheme should take the following immediate steps:

- Ensure their existing information incident response plan covers the reporting and notification requirements set out in the Scheme, in addition to detecting, containing and 'fixing' the breach. If no response plan is in place then one should be developed.
- Privacy impact assessments and information security risk assessments should be conducted where needed to understand where information is stored, the risks to your organisation from holding that data and what controls are required to manage these risks.

Having these processes and capabilities in place will enable you to respond to any breach in line with the requirements of the Scheme. Secondly and equally important, you need to understand the controls and risk treatments required to reduce the likelihood of a breach occurring in the first place.

If your current cyber security maturity is well developed, then the NDB may be 'business as usual'. If your cyber security maturity is still growing, then developing, implementing or refining your cyber security risk management program is the ideal way to enhance this while better protecting your firm, shareholders and its customers.

Risk management is the foundation for your maturity improvement program. Effective risk management will identify any gaps needed to address any new risks arising from the NDB Scheme. An inclusive risk management approach will also identify other cyber risks that have the propensity to impact on your organisation, particularly:

- Reputational / Brand Damage
- Failure to meet compliance and regulatory requirements
- Financial Loss from incident clean-up, loss of customers / market share, fines etc

2 Notifiable Data Breaches - Summary[1]

2.1 What is the Notifiable Data Breaches Scheme?

The passage of the Privacy Amendment (Notifiable Data Breaches) Act 2017 established a Notifiable Data Breaches (NDB) Scheme in Australia.

The NDB Scheme requires all organisations covered by the Australian Privacy Act 1988 to notify any individuals likely to be at risk of serious harm by a data breach, should the organisation suffer a data breach.

This notice must include recommendations about the steps that individuals should take in response to the data breach. The Australian Information Commissioner must also be notified.

Organisations will need to be prepared to conduct quick assessments of suspected data breaches to determine if they are likely to result in serious harm.

2.2 What is a Notifiable Data Breach?

Under this legislation, a data breach occurs when personal information held by an organisation is lost or subjected to unauthorised access or disclosure. "Personal information" includes items under the Privacy Act, or other information from which a person's identity could be guessed or inferred. Given the propensity of computers to correlate identity from small snippets of data, this term potentially means all data about customers – and it's up to your organisation to decide, and justify, otherwise.

A Notifiable Data Breach is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates. While this sounds subjective, the legal community has well-established views on how to interpret such legislation, often relying upon the "reasonable person" test i.e. would a reasonable person come to a similar conclusion about the potential for 'serious harm' to 'any' individual whose details are affected.

Examples of a data breach include when:

- A device containing customers' personal information is lost or stolen
- A database containing personal information is hacked
- Personal information is mistakenly provided to the wrong person or company.

[1] Information within this summary has been sourced from the OAIC website on 24/10/2017

2.3 Which entities are affected by the NDB Scheme?

Agencies and organisations already within the scope of the Privacy Act 1998 are required to comply with the NDB Scheme.

These include Australian Privacy Principle (APP) entities, health care providers, credit reporting bodies, credit providers, and tax file number (TFN) recipients.

Small Business Operators are mostly exempt from the NDB Scheme, providing annual turnover is under $3million pa and are not health care providers, credit reporting bodies, credit providers, and tax file number (TFN) recipients.

Foreign firms with interests in Australia are also responsible for complying with the NDB Scheme.

2.4 What data or information is subject to the NDB Scheme?

As with the Privacy Act 1998 and amendments, the NDB Scheme is concerned with information that is:

- **"About" the individual**; or
- **About an individual whose identity is apparent, or can reasonably be ascertained**, from the information or opinion.

The Privacy Act defines personal information as:

> *…information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.*

Common examples are an individual's name, signature, address, telephone number, date of birth, medical records, bank account details and commentary or opinion about a person.

Some legal opinions indicate that the purpose or reasons for generating the records and how the information is used play a part in determining if the information is "about" an individual.

Although there is a limited amount of legal determinations on the NDB scope, in some cases it will be obvious as to information on the scope of the NDB. If in doubt seek, legal advice.

2.5 Why is the NDB Scheme important?

The NDB Scheme provides an incentive for organisations to strengthen the protections afforded to everyone's personal information, and to provide transparency in the way that organisations respond to data breaches.

This in turn supports consumer and community confidence that personal information is being respected and protected, consequently increasing the economic value of the information based business models that most organisations employ today.

It also gives individuals the opportunity to take pro-active steps to minimise the damage that can result from unauthorised use of their personal information.

2.6 When does it take effect?

The NDB Scheme will commence on 22 February 2018. It only applies to eligible data breaches that occur on, or after, that date.

2.7 Frequently Asked Questions

1. What is personal information?

Section 6 of the Privacy Act defines 'personal information' as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable. This might include a person's name and address, medical records, bank account details, photos, videos and even information about what an individual likes, their opinions and where they work.

2. Which data breaches are notifiable?

Not all data breaches are notifiable — the NDB Scheme only requires organisations to notify when there is a data breach that is likely to result in serious harm to any individual to whom the information relates. Exceptions to the NDB Scheme will apply for some data breaches, meaning that notification to individuals or to the Information Commissioner may not be required.

Impact: Organisations need the ability to identify what information was compromised, can the compromised information lead to "serious harm to an individual", internal notification and escalation processes, and appropriately authorised roles who can notify individual and the Information Commissioner

3. How quickly must an assessment of a breach be performed?

An entity must take all reasonable steps to complete the assessment within 30 calendar days after the day the entity became aware of the grounds (or information) that caused it to suspect an eligible data breach.

Impact: Compromise detection, and time-effective escalation, analysis and notification processes are necessary under the NDB Scheme

4. How do I assess a suspected data breach?

Organisations that suspect an eligible data breach may have occurred are required to undertake a reasonable and expeditious assessment to determine if the data breach is likely to result in serious harm.

The Office of the Australian Commissioner (OAIC) expects that an entity's business as usual approach to data breach management, including its data breach response plan, will be reviewed and updated to incorporate the requirements of the NDB Scheme for assessing suspected eligible data breaches.

Impact: Responsible and Empowered personnel with the requisite skills and authority to make decisions about the potential for 'Serious harm" are required under the NDB Scheme.

5. What are the breach notification requirements?

Where an organisation becomes aware that there are reasonable grounds to believe an eligible data breach has occurred, they are obligated to notify individuals at likely risk of serious harm and the Commissioner as soon as practicable. This notification must set out:

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

Impact: Personnel empowered to act and communicate to affected individuals need to be designated in your organisation. Furthermore, the ability to quickly analyse potential protection steps for the affected individuals and make these recommendations is required.

3 Time to consider your Cyber Security Maturity

Those familiar with the Scout and Girl Guides movements will be familiar with the motto “Be Prepared”. Organisations wishing to prepare for the upcoming NDB Scheme should take the opportunity to re-assess their overall approach to cyber security - and if needed, undertake further preparations.

Typically, preparation includes having a mature cyber security program. In turn, an effective information security incident management process is fundamental to a cyber security program.

There are significant business risks associated with an immature or unprepared cyber security program. Often, the potential regulatory and compliance impacts arising from a data breach are outweighed by the following business risks:

- Reputational / Brand Damage;
- Financial Loss from incident clean-up, loss of customers / market share, fines etc and;
- Negative Shareholder Impact.

3.1 Cyber Security Maturity – Where to start

Loop recommends focusing on the following cyber security best practices to get started:

- Develop an Information Security Risk Management Policy and Procedure;
- Undertake a Risk Assessment across the organisation’s Information Assets and;
- Develop and Information Security Incident Management policy and procedure.

These lead to outcomes that inform the business about where your cyber risks are, are these risks managed, and place you in a position to minimise the impact of cyber security incidents in line with the NDB Scheme requirements.

Having an understanding of your cyber risks contributes to a cyber security roadmap to improve your overall maturity.

4 Preparing for the NDB Scheme

4.1 NDB Scheme – Securing Personal Information

The Privacy Act includes thirteen Australian Privacy Principles (APPs) that regulate the handling of personal information.

APP 11 requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information.

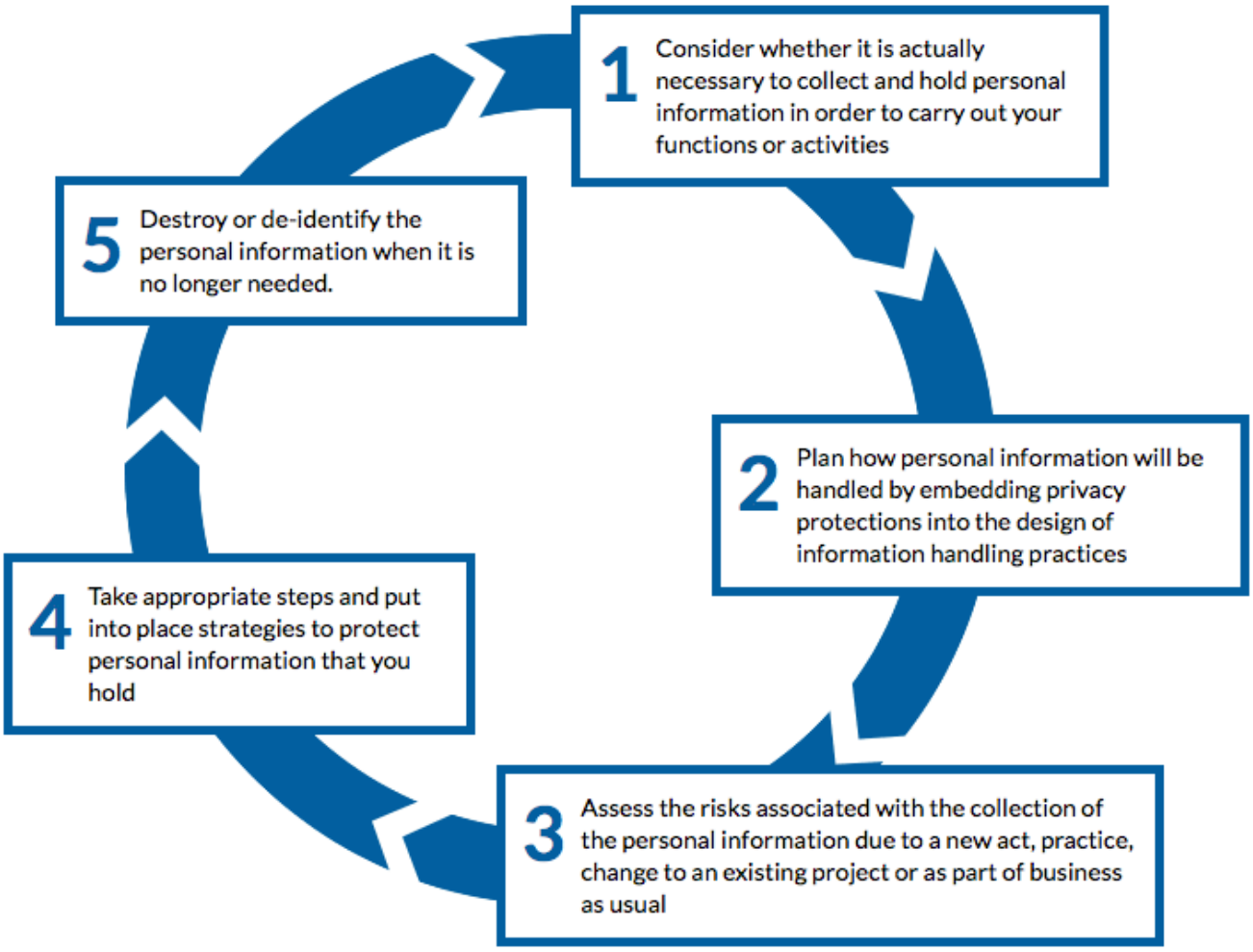
The principle will require an entity to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure[2].

4.2 The information Life-cycle[3]

If you handle personal information, you should consider how you will protect personal information during the stages of its lifecycle.

Personal information security throughout the lifecycle is illustrated as follows:

[2] Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 86.
[3] OAIC Guide to Securing Personal Information - Accessed 1/11/2017



To effectively protect personal information throughout its lifecycle, you will need to be aware of when and how you are collecting it and when and how you hold it. As noted above, your personal information holdings can be dynamic and change without any necessarily conscious or deliberate action.

All areas of the business need to be considered as "In-Scope" such as Disaster recovery, Software (SaaS) and Infrastructure as a Service (IaaS) environments, furthermore, the lifecycle may include the passing of personal information to a third party for storage, processing or destruction.

4.3 Assessing the Risk[4]

This is the key element required to ensure you can adequately protect your information.

To assess risk effectively with regards to personal information, you can conduct a privacy impact assessment (PIA) or information security risk assessment.

A PIA is a written assessment that identifies the privacy impacts of a proposal and sets out recommendations for managing, minimising or eliminating those impacts. Generally, a PIA should:

- Describe the personal information flows in a proposal;
- Analyse the possible privacy impacts of those flows;
- Assess the impact the project as a whole may have on the privacy of individuals and;
- Explain how those impacts will be eliminated or minimised.

You may also need to conduct an information security risk assessment (also known as a threat risk assessment) in conjunction with a PIA. An information security risk assessment is generally more specific than a PIA because it involves the identification and evaluation of security risks, including threats and vulnerabilities, and the potential impacts of these risks to information (including personal information) handled by an entity.

The findings of a PIA and information security risk assessment should inform the development of your risk management and information security policies, plans and procedures.

Once the risks have been identified, you should then review your information security controls within the Preventative, Directive, Detective, Corrective and Recovery domains to determine if they are adequate in mitigating the risks to tolerable level. Given that processes, information, personnel, applications and infrastructure change regularly, and the constantly evolving technology and security risk landscape, regular review and monitoring of personal information security controls is crucial.

4.4 NDB Scheme – 'Reasonable Steps'

Within the Privacy Act you will regularly hear the term 'reasonable steps' used to outline how you should be protecting personal information.

The issue of what qualifies as 'reasonable' varies from organisation to organisation based on varying circumstances. Legal advice should be sought to determine the circumstances that affect the assessment of reasonable steps. Note also that protections considered to be 'reasonable' today may

[4] OAIC – Assessing Risk - Accessed 2/11/2017

not meet that same threshold as the changes unfold to both your business and the external threat environment.

More information on these circumstances can be found here.

The security measures considered reasonable to take following the above assessment, are all covered within best practice information security standards such as ISO/IEC 27001. Steps and strategies[5] outlined by the OAIC include:

- Governance, culture and training.
- Internal practices, procedures and systems.
- ICT security.
- Access security.
- Third party providers (including cloud computing).
- Data breaches.
- Physical security.
- Destruction and de-identification.
- Standards.

Many of the steps and strategies outlined above may also assist you in protecting other types of information, such as commercially confidential information, and vice versa many of the best practices outlined in the ISO/IEC 27001 standard will contribute towards protecting personal information.

[5] OAIC Steps and Strategies - Accessed 30/10/2017

5 Loop Secure Profile

Loop Secure is a specialist cyber security firm delivering a wide range of services to manage cyber risk and protect business assets.

Solutions include:

- Managed Security Services
- Offensive Security Services
- Cyber Security Consulting
- A wide range of leading security controls.

Managed Security Services are controlled from our World Class Security Operations Centre in Melbourne, Australia. We have five core services focused on the business outcomes of managing cyber risk and maintaining compliance. These comprise of Continuous Security Monitoring and Incident Response, Vulnerability Management, Security Awareness Training as well as Endpoint and Network Protection.

Loop has significant expertise and certifications in cyber security consulting and offensive security.

Cyber Security Consulting is focused on the implementation and maintenance of effective Information Security Management Systems (ISMS), aligned with the ISO framework. To achieve this, we deliver Cyber Security Gap Assessments, Cyber Security Strategy and the implementation of specific policies and procedures to manage cyber risk and compliance obligations.

As an extension of our compliance capability, Loop is also a Qualified Security Assessor (QSA) certified by the PCI Council to review and certify companies to the PCI-DSS standard.

Our Offensive Security Services team assist customers in testing the effectiveness of their cyber defences through mimicking a broad range of attacker techniques in order to identify your organisations weak points. These services range from targeted Penetration Testing to full scale Red-Teaming engagements.

Loop also recognises the need for product based security controls, and partners with leading product vendors to provide our clients with the right security controls they need.