CyberRisk

Protecting your reputation

MANDATORY BREACH REPORTING AND PRIVACY. WHAT YOU NEED TO KNOW.

WAYNE TUFEK - DIRECTOR, CYBERRISK

APRIL 20, 2017

INTRODUCTIONS

- Wayne Tufek
- Director @ CyberRisk
- Information security, technology risk management and privacy
- Our goal is to help our clients to effectively manage their cyber risk
- We provide pragmatic practicable advice and expertise built on years of real world experience
- www.cyber-risk.com.au

AGENDA

- What is the Privacy Act?
- To whom does the Privacy Act apply?
- What will change in Feb 2018?
- What constitutes a data breach?
- If I have a data breach what will I need to do?
- Am I prepared?
- What does reasonable security look like?
- Next steps

DISCLAIMER

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation and facts.

WHAT IS THE PRIVACY ACT?

- The *Privacy Act 1988* (Privacy Act) regulates the handling of personal information about individuals.
- Personal information is information or an opinion 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.
- The Privacy Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information).
- Refer to the Office of the Australian Information Commissioner

  (https://www.oaic.gov.au/)

WHAT IS THE PRIVACY ACT?

- APP 1 — Open and transparent management of personal information
- APP 2 — Anonymity and pseudonymity
- APP 3 — Collection of solicited personal information
- APP 4 — Dealing with unsolicited personal information
- APP 5 — Notification of the collection of personal information
- APP 6 — Use or disclosure of personal information
- APP 7 — Direct marketing
- APP 8 — Cross-border disclosure of personal information
- APP 9 — Adoption, use or disclosure of government related identifiers
- APP 10 — Quality of personal information
- APP 11 — Security of personal information
- APP 12 — Access to personal information
- APP 13 — Correction of personal information

https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles

TO WHOM DOES THE PRIVACY ACT APPLY?

- Australian Government agencies and all businesses and not-for-profit organisations with an annual turnover more than $3 million have responsibilities under the Privacy Act, subject to some exceptions.

EXCEPTIONS

- Some small business operators (organisations with a turnover of $3 million or less) are covered by the Privacy Act including:
- private sector health service providers. Organisations providing a health service include:
    - traditional health service providers, such as private hospitals, day surgeries, medical practitioners, pharmacists and allied health professional
    - complementary therapists, such as naturopaths and chiropractor
    - gyms and weight loss clinic
    - child care centres, private schools and private tertiary educational institutions.
- businesses that sell or purchase personal information
- credit reporting bodies

The Privacy Act also covers specified persons handling your:

- consumer credit reporting information, including credit reporting bodies, credit providers (which includes energy and water utilities and telecommunication providers) and certain other third parties
- tax file numbers under the Tax File Number Guidelines
- https://www.oaic.gov.au/privacy-law/rights-and-responsibilities

WHAT WILL CHANGE IN FEBRUARY 2018?

- Privacy Amendment (Notifiable Data Breaches) Bill 2016 was passed in the Australian Parliament on 13 February 2017. The Bill amends the Privacy Act 1988 (Privacy Act) to introduce a mandatory data breach notification regime and comes into effect in February 2018.
- **The notification regime is a significant change to the data breach notification obligations of organisations holding personal information.**

WHAT CONSTITUTES A DATA BREACH?

Australian Privacy Principle 11 — security of personal information

- 11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:
    - from misuse, interference and loss; and
    - from unauthorised access, modification or disclosure.
- Applies even in situations where the personal information is provided to a third party as part of a managed service

WHAT CONSTITUTES A DATA BREACH? (CONT)

- An entity holds personal information AND there is a breach of APP 11.1
- There may be an "**eligible data breach**"
  - Where there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity;

    AND
  - A **reasonable person** would conclude that access or disclosure is **likely** to result in **serious harm** to any of the individuals to whom the information relates

WHAT CONSTITUTES A DATA BREACH? (CONT)

- **Likely to result in serious harm?**
  - the kind or kinds of information;
  - the sensitivity of the information;
  - whether the information is protected by one or more security measures;
  - if the information is protected by one or more security measures—the likelihood that any of those security measures could be overcome;
  - the persons, or the kinds of persons, who have obtained, or
  - who could obtain, the information;

IF I HAVE A DATA BREACH, WHAT WILL I NEED TO DO?

- ***What if there is suspected data breach?***
- If there are reasonable grounds to suspect that there may have been an eligible data breach

  The entity must:

  a) carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an eligible data breach of the entity; and

  b) take all reasonable steps to ensure that the assessment is completed within 30 days after the entity becomes aware

IF I HAVE A DATA BREACH, WHAT WILL I NEED TO DO? (CONT)

- There are exceptions!
  - If the entity takes action in relation to the access or disclosure
  - Before the access or disclosure results in serious harm
  - As a result of the action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm to the affected individuals

Then the access or disclosure will not be an eligible breach

IF I HAVE A DATA BREACH, WHAT WILL I NEED TO DO? (CONT)

- General notification obligations
- An entity must give a notification if:
    a) it has reasonable grounds to believe that an eligible data breach has happened; or
    b) it is directed to do so by the Commissioner.

- *Prepare a Statement that contains:*
    a) the identity and contact details of the entity; and
    b) a description of the eligible data breach that the entity has reasonable grounds to believe has happened; and
    c) the kind or kinds of information concerned; and
    d) recommendations about the steps that individuals should take in response to the eligible data breach that the entity has reasonable grounds to believe has happened.

IF I HAVE A DATA BREACH, WHAT WILL I NEED TO DO? (CONT)

- *Notification*
    - Notify the OAIC
    - If practicable **notify all affected individuals** using the normal method of communication

Or if not practicable

a) publish a copy of the statement on the entity's website (if any); and

b) take reasonable steps to publicise the contents of the statement.

- **As soon as practicable** after the completion of the preparation of the statement.

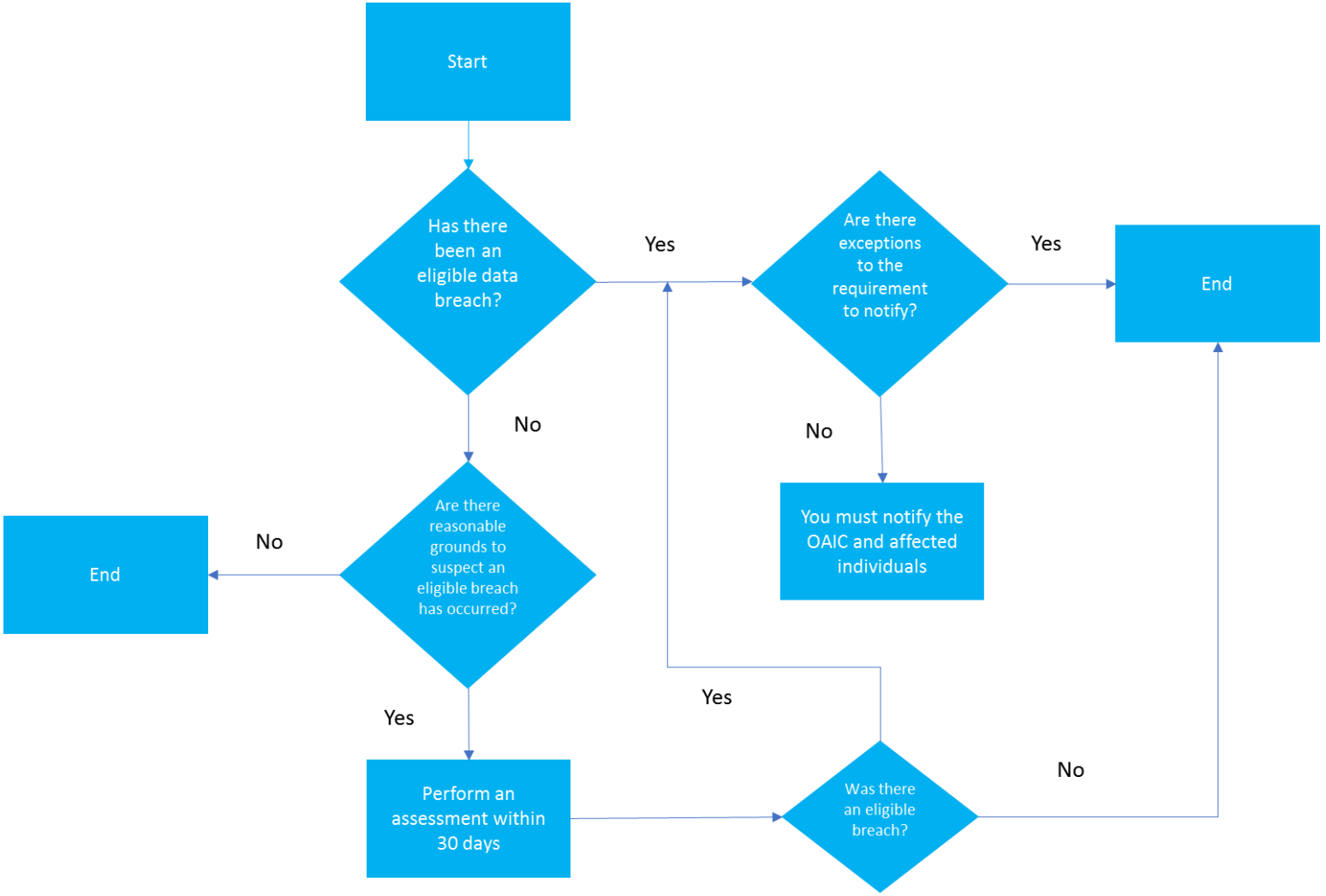
https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches

IF I HAVE A DATA BREACH, WHAT WILL I NEED TO DO? (CONT)

The Commissioner has a range of enforcement powers, including the power to:

- make a determination requiring the payment of compensation for damages or other remedies, such as the provision of access or the issuance of an apology (enforceable by the Federal Court or Federal Magistrates Court)
- accept an enforceable undertakings,
- Serious or repeated interferences with the privacy of an individual attract a maximum penalty of $360,000 for individuals and $1,800,000 for bodies corporate, and
- seek an injunction regarding conduct that would contravene the Privacy Act.

IF I HAVE A DATA BREACH, WHAT WILL I NEED TO DO? (CONT)



AM I PREPARED?

- An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information
- A Guide to Information Security – "Reasonable steps" to protect personal information
- https://www.oaic.gov.au/images/documents/privacy/privacy-guides/information-security-guide-2013_WEB.pdf

AM I PREPARED? (CONT)

- What are reasonable steps to ensure information security under the Privacy Act will depend on the circumstances, including the following:
  - the nature of the entity holding the personal information
  - the nature and quantity of personal information held
  - the risk to the individuals concerned if the personal information is not secured
  - the data handling practices of the entity holding the information
  - the ease with which a security measure can be implemented.

AM I PREPARED? (CONT)

- Reasonable steps include:
  - Privacy by design
  - Complete Privacy Impact Assessments (PIA) – The OAIC expects entities to undertake a PIA for any new acts, practices or projects that involve the handling of personal information.
  - https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments

AM I PREPARED? (CONT)

- Reasonable steps include:
  - Privacy policy
  - Information security governance – Security policies
  - Complete an inventory of your information assets
  - Risk management
  - Safeguards and security controls
  - Keep software up to date (patching)
  - Configure systems for maximum security
  - User authentication (Strong passwords and multifactor authentication)
  - Limit super user or system administrator level access
  - Encryption
  - End point protection (anti-virus)

AM I PREPARED? (CONT)

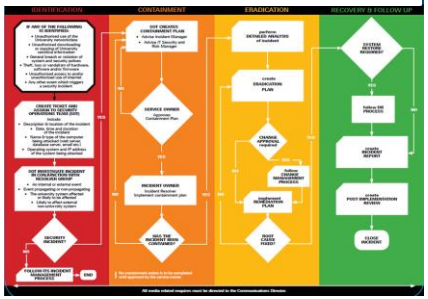
- Reasonable steps include:
  - Network security
  - Security monitoring
  - Security testing (Vulnerability assessments, penetration testing)
  - Data breach response plan
  - Physical security
  - Security training and awareness

NEXT STEPS

- Immediately:
  - The time to act is now
  - The best approach to data breaches is to try and prevent them in the first place
  - Begin reviewing and testing your security and privacy controls and safeguards
  - Where is your data?
  - Who has access to the data and do they need access?
  - Does your organisation have a “reasonable” level of security in place - how well is your data protected?
  - Do you comply with the Privacy Act?
  - Identify weaknesses and control gaps
  - Put in place a plan to remediate

NEXT STEPS (CONT)

- Within the next 6 months:
  - Review your data breach response plan
  - What processes do you have in place to identify an eligible data breach or to investigate an event that may be one?
  - How will you assess the likelihood of serious harm?
  - Your breach response plan must now include steps to notify those affected and the OAIC
  - Notification methods and message templates
  - Update your plan for the new requirements
  - Test the new plan
  - Ensure that all those involved understand their role
  - Don't forget your Crisis Management plan



PRIVACY AWARENESS WEEK

- 15-19th of May
- https://www.oaic.gov.au/paw2017/

QUESTIONS?

Questions

PASSION • INTEGRITY • EXPERIENCE • RESULTS