Office of the Victorian Information Commissioner

Managing the privacy impacts of data breaches

Dermot Dignam, Manager, Privacy Guidance

Privacy Awareness Week 2019

The plan

Part 1: Introduction

- What is a data breach? What are the consequences?

Part 2: Privacy legislation and data breaches

- *PDP Act; NDB Scheme; and GDPR*

Part 3: Preparing for a data breach

- Data breach response plans

Part 4: Responding to a data breach

- Guiding principles and 4 step process

After: Overview of Vic Govt Cyber Incident Response Service

- Shaun Price, Senior Advisor, CIRS

But first, a plug!

- Updated OVIC guidance on Managing the privacy impacts of a data breach.

- Will be available this week via OVIC website .

Part 1: Introduction

Office of the Victorian Information Commissioner

What is a data breach?

- We are concerned with **privacy** impacts: effect on **individuals**.
- A data breach occurs when **personal information** that is held by a public sector organisation is subject to **misuse or loss or to unauthorised access, modification or disclosure.**
- They can be caused by a deliberate malicious act; human error; or inadequate systems/processes.
- They are not just IT-related.

TOP STORY

Medical records at Victorian hospital get hacked

ABC NEWS

Just In | Australia Votes | World | Business | Sport | Science | Health

Print | Email | Facebook | Twitter | More

Data breach sees Victorian Government employees' details stolen

Posted 1 Jan 2019, 12:04pm

EXCLUSIVE NATIONAL VICTORIA CYBER SECURITY

Catholic Church, major super fund and Toyota hit by cyber attacks

Patient **data breach** after **bag** stolen at Poole Hospital

BBC News - 25 Jul 2018

Lenovo staff loses company-issued laptop... and colleagues' data

Their names, salary figures and bank account numbers are now at risk.

Queensland police 'breached privacy' of domestic violence victim by leaking her details

Freedom of Information | Privacy | Data Protection

Consequences of a data breach

- Privacy is a human right – it "enables" other rights.
  UDHR; ICCPR; Vic Charter
- Some impacts will be minor but some can be serious.
- Examples of potential harm:

- ❑ Reputational damage
- ❑ Embarrassment/humiliation
- ❑ Emotional distress
- ❑ Identity theft or fraud
- ❑ Financial loss
- ❑ Loss of employment
- ❑ Family violence
- ❑ Other physical harm
- ❑ Intimidation
- ❑ Disruption of govt services

A recent reminder

Like 0

Tweet

Improper disclosure leads to ostracism, death

Sam Williams
21 February 2019

The Human Rights Review Tribunal recently found that the Parole Board breached the Privacy Act when it disclosed an offender's parole address, with tragic consequences.

Read the full decision: Tapiki and Eru v New Zealand Parole Board [2019] NZHRRT 5 (external link)

The Board agreed to release the offender from prison in large part because his mother, Ms Tapiki, committed to giving her son a fresh start. Ms Tapiki and her friend Ms Eru put careful thought and preparation into a plan to give the offender "a real chance for reintegration into the community and the best possible opportunity for a positive future," according to the Tribunal decision.

As part of the plan, Ms Tapiki gave up her small flat and Ms Eru agreed to have the offender and Ms Tapiki live with her. A probation officer assessed and approved Ms Eru's address and the Parole Board made living there a condition of the offender's release.

The Board disclosed the offender's release conditions to his victim, as the Parole Act requires. It redacted some information identifying Ms Tapiki, but it didn't redact the parole address.

After the disclosure, Ms Tapiki and Ms Eru started receiving threats and somebody smashed their letterbox. The Department of Corrections had to move the offender to another town, where he had no support system. He later took his own life.

Consequences for organisations

- Impact on reputation as a trusted custodian of personal information.

- Privacy complaints.

Part 2: Privacy legislation and data breaches

Office of the Victorian Information Commissioner

PDP Act and the 10 IPPs

- A data breach may involve a failure to comply with one or more of the IPPs (particularly IPPs 2 & 4).

- We encourage organisations to report data breaches to OVIC despite being no mandatory requirement (more on reporting to OVIC later.

Other obligations – NDB Scheme

- Serious data breaches must be notified to OAIC and affected individuals.
- A serious breach is one with a 'likely risk of serious harm' to the people the information is about.
- **BUT VPS agencies are exempt from NDB, except for data breaches involving tax file numbers.**

Other obligations – GDPR

Obligation on data controllers to report data breach to 'supervisory authority' and data subjects where there is a "high risk to their rights and freedoms".

BUT only likely to affect VPS organisations in rare circumstances because it applies where:

- the organisation offers goods and services to people in the EU;
- the organisation monitors the behaviour of people in the EU; or
- if the organisation has a physical or legal establishment in the EU.

Part 3: Preparing for a data breach

Office of the Victorian Information Commissioner

Data Breach Response Plan

- Sets out how the organisation will respond to a data breach by walking through what will be done and by whom in the event of a breach.

- **All Staff Awareness –** Explain to staff how they can identify a breach and to whom it should be reported.

- **Breach Response team** – Explain membership of team that will carry out response steps and roles of each member.

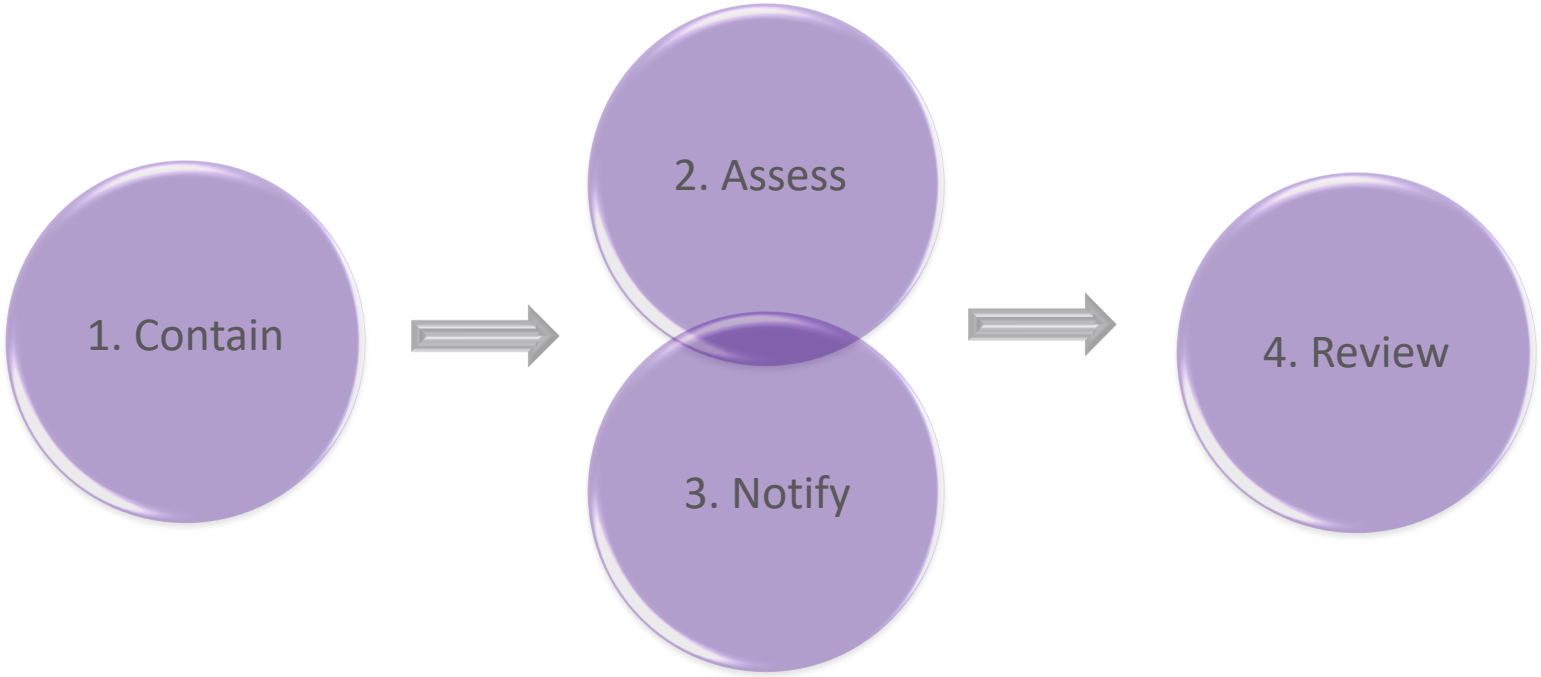
Part 4: Responding to a data breach

OVIC
Office of the Victorian Information Commissioner

Responding to a data breach - Overview

- Response will depend on exact circumstances.
- BUT – Act quickly and treat it as a priority.
- **Key principle = Minimising potential harm to affected individuals**

Responding to a data breach – 4 Steps



Where an organisation identifies potential harm while carrying out these steps, it should make **remediation** attempts at the **earliest opportunity** to minimise the chances of harm eventuating (e.g. by relocating an individual where there is a serious threat of physical harm).

Step 1: Contain

- First take steps to **confirm** that a breach has occurred.
- When confirmed, refer to your data breach response plan - **What needs to be done and by whom?**
- Try to **limit the extent** of the breach.
  - Some common actions are: stopping the unauthorised practice, recovering records and shutting down the system that was breached.

Step 1: Contain – Example scenarios

1. An organisation discovers that an ex-employee still has access to the organisation's system and has been accessing the system.

To contain the breach the organisation should immediately stop the employee's access.

2. Employee intends to send an email (containing personal information of clients) to a specific group of colleagues who work in the same team. But accidentally also sends to other employees who are not part of the team.

Options to contain:

- **Recall email;**
- **Ask IT if email can be deleted from unintended accounts; or**
- **Ascertain who accessed the email and instruct them to delete.**

Step 2: Assess the risk of harm

- Consider risk of harm to affected individuals.
- Risk = **likelihood** and **severity** of harm.
- Assess for the purpose of working out:
  - Whether to **notify** individuals and OVIC.
  - What other steps to take to **remediate** potential harm.
- This will require an **investigation** of the cause of the breach and the surrounding circumstances.

Step 2: Assess the risk – What factors?

The nature, sensitivity and volume of personal information

- The more sensitive/delicate, the higher the risk.
- The greater the amount, the higher the risk.

The circumstances of the data breach, including cause and extent

- How did it occur? Malicious or accidental?
- What is the relationship between recipient and affected individual?
- Has containment/remediation lessened the risk?

The nature of the potential harm to the affected individuals

- Remember different types of harm from earlier.
- Consider the particular characteristics of the individuals – vulnerabilities?

Step 2: Assess the risk of harm - Examples

Which of the two scenarios in each example involves higher risk?

1. Petition inadvertently posted online

a. List of residents petitioning for extra recycling facilities.

b. List of victims of historical sexual abuse petitioning for prosecution of perpetrators.

2. Individual's name and address disclosed to third party

a. Individual is the victim of a violent crime and third party is the alleged perpetrator.

b. Individual is client of govt agency and details disclosed to another govt agency.

3. List of contact details disclosed

a. Relates to work contact details of executive staff of a government agency.

b. Relates to addresses of elderly residents that require home care services.

Step 3: Notify individuals

- Whether to notify?
  - Largely determined by risk assessment at step 2.
  - If there is a foreseeable risk you should usually notify.
  - But not if notification reasonably likely to cause more harm than it would alleviate.

Step 3: Notify individuals - examples

1. A University sends an email to a specific group of students for a specific purpose. However, accidentally attached to the email is a spreadsheet with the personal and sensitive information of other students.

   Notify – risks include identity theft and reputational harm.

2. Council employee loses a bag on Council premises. The bag contains documents with personal information of an individual that receives council services. The Council reports the missing bag to the police but the bag is retrieved around an hour later by another Council employee.

   Don’t notify – no foreseeable risk of harm.

Step 3: Notify individuals – When and how?

When?

- As soon as reasonably practicable BUT make sure you have sufficient information.

How?

- Preferably directly unless not practicable.

Content of Notification

- Individuals should understand what has occurred and associated risks.
- Recommended steps to reduce risk of harm.
- Contact person at organisation.

Notifying OVIC

- We encourage voluntary notification of breaches that may involve a foreseeable risk of harm (or where organisation is unsure) as soon as reasonably possible.
- New template for those who wish to use.
- Flexible – no set format. Can be phone call with follow-up depending on seriousness.
- Report via 1300 006 842 or privacy@ovic.vic.gov.au.

Step 4: Review

- Assess the root cause of the breach to identifies how to prevent a similar incident occurring again.

  E.g. Audit of processes; review of policies; review of training; review of contractual obligations on providers.

- There may be several causes of the breach.

- Also review organisation's handling of the incident – did the breach response plan work?

Step 4: Review - Example

A staff member loses a USB stick containing clients' personal information resulting in some of those clients becoming a victim of identity fraud.

Involves human error BUT non-encryption contributed to breach.

Organisation could change policy so that staff are required to use USB sticks that are encrypted.

Victorian Government
Cyber Incident Response Service

Provides **expert cyber incident response and coordination services** to all Victorian Government organisations.

Funded by the Department of Premier and Cabinet under the *Cyber Security Strategy.*

Provides a **2nd line of defence** for cyber incident response.

Coordinates Victoria's response to significant cyber incidents and major emergencies.

VIC

CYBER_INCIDENT
RESPONSE_SERVICE

The service provides all Victorian Government organisations with access to:

- preparing an effective breach response strategy
- technical investigations and forensic services
- communications and engagement support via iDcare

When you experience a data breach….

Contact 1300 CSU VIC (24/7) or cybersecurity@dpc.vic.gov.au for assistance responding to cyber data breaches.

VIC

CYBER_INCIDENT
RESPONSE_SERVICE

Questions?