

# Community Legal Centres Queensland

## Privacy and data breaches

—  
**Cathy Lyndon**  
Special Counsel  
—

25 October 2019

### What we will cover

Context



What is personal information?



Mandatory Data Breach regime



Practical steps CLCs can take

# PERSPECTIVES ON CYBER RISK 2019



MinterEllison

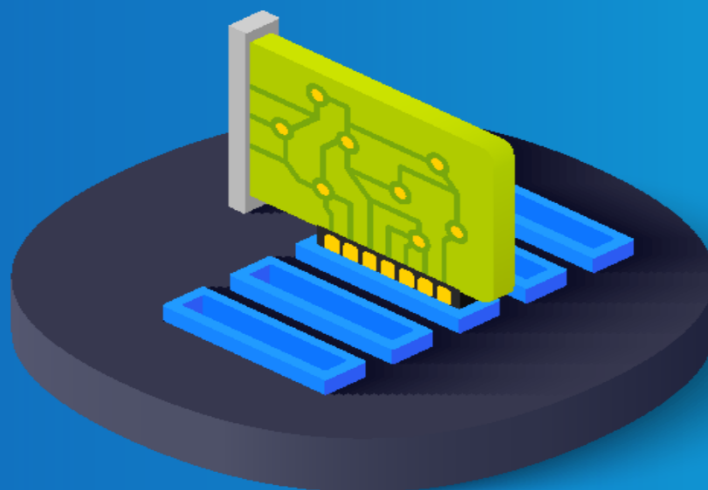
## Part one

### Our findings in the evolving privacy landscape

In late 2018, we conducted our fourth annual cyber security survey, to assess how Australian organisations are responding to cyber risk in an environment of increasing regulation.

Our survey results indicate a marked increase in awareness and understanding of cyber risk, with more organisations than ever appreciating the importance of adequately addressing an ever growing cyber threat.

However, an increase in understanding is not always translating into the practical steps that organisations must take to effectively mitigate against this threat.



## Part two

### Regulation upped the ante in 2018

Last year saw some of the most significant regulatory developments in Australian and overseas privacy and data protection regimes in many years.



## Part three

### Looking ahead

As we navigate the challenges of the fourth industrial (digital) revolution, we find ourselves at the crossroads of current and developing data-related rights: information privacy rights, consumer rights, intellectual property rights, and human rights.



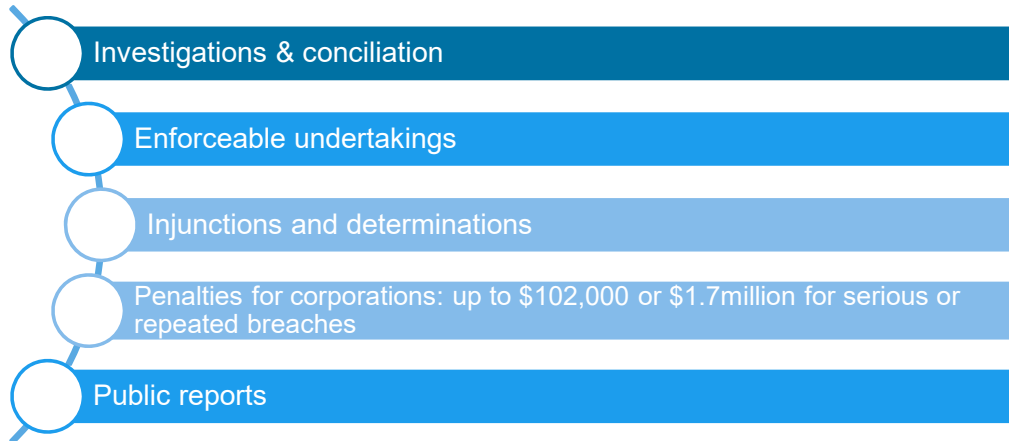
# Overview of privacy obligations

## Privacy law framework

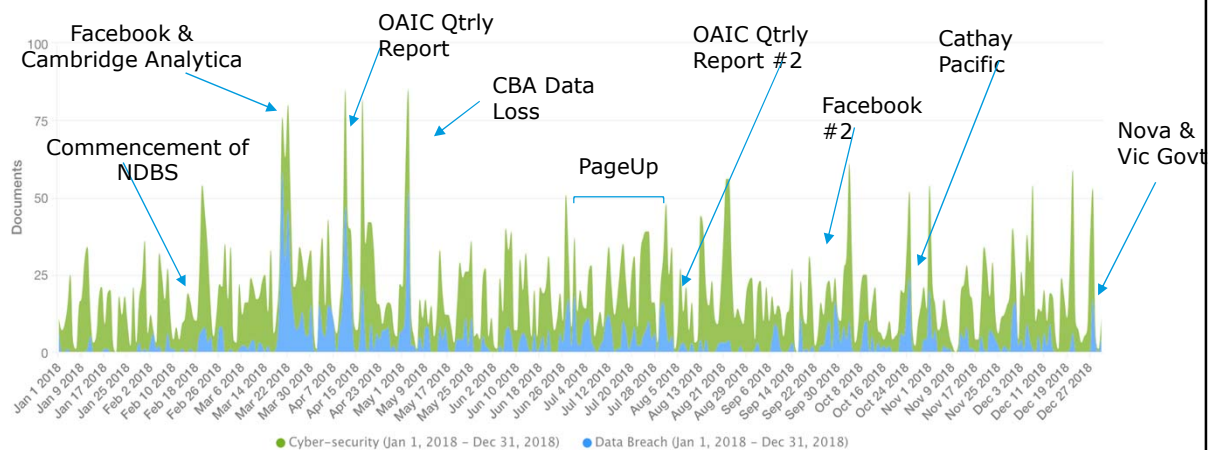


## Privacy Act enforcement

OAIC enforcement toolkit includes:



MinterEllison






MinterEllison

### Lessons learned – causes of breaches

- Inadequate password protection
- Little control over privileged accounts
- Poor user account management, especially de-provisioning of unused accounts
- Inadequate controls over remote access
- Lack of security monitoring for suspicious and malicious activity

## Mandatory data breach regime



### What is serious harm?



- **Objective test** – entities are not generally expected to make enquiries about the circumstances of each affected individual
- Reasonable person means a **person in the entity's position**:
  - Properly informed;
  - Based on information:
    - immediately available
    - following reasonable enquiries OR
    - an assessment of the breach

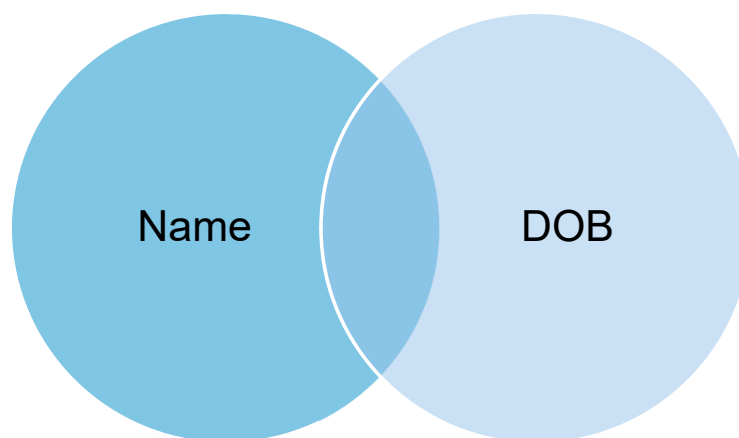


## Relevant matters (a non-exhaustive list)

- Kind or kinds of information
- Sensitivity of information
- Whether protected by one or more security measures
- The likelihood those security measures may be overcome
- The person or persons who have (or could) obtain the information
- Whether security measures render unintelligible or meaningless
- The likelihood those security measures could be overcome
- The nature of the harm ...

MinterEllison

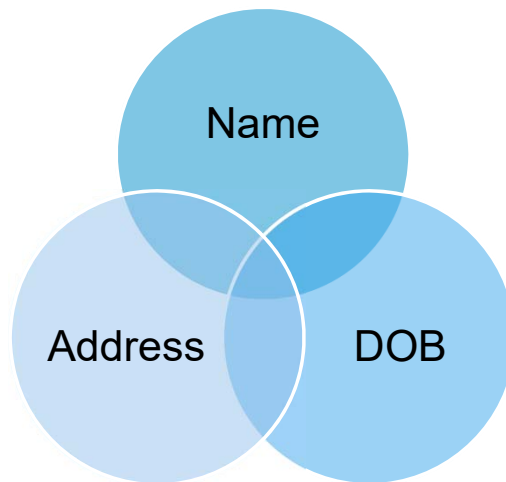
## Example 1



MinterEllison

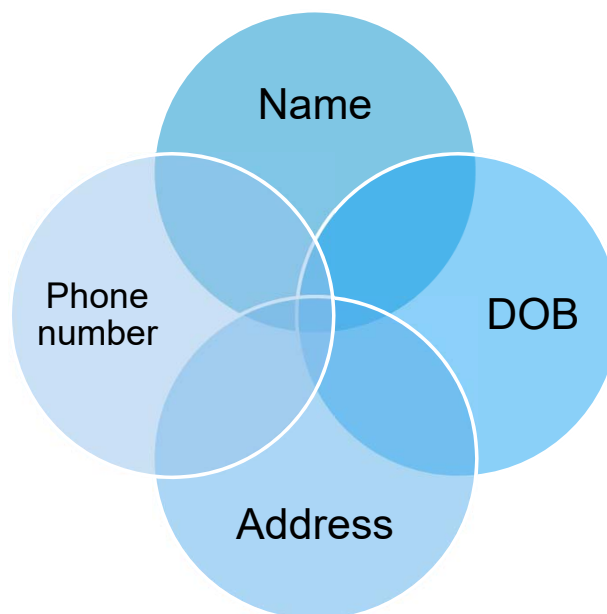


## Example 2



MinterEllison

## Example 3



MinterEllison

## High risk credentials



MinterEllison

## Potential impacts

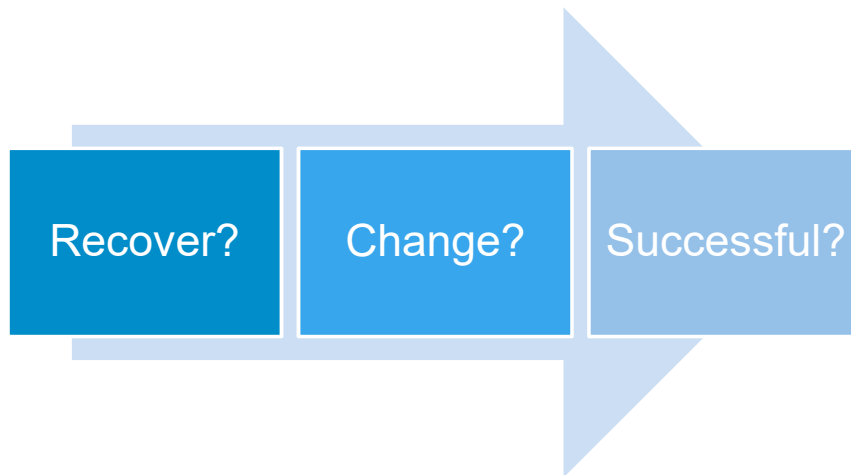
~ 23% of individual will experience emotional harm from a data breach notification

~ 2% of individuals believe they have experienced a phishing or telephone scam resulting from the data breach

< 0.5% experience actual misuse

MinterEllison

## Remedial Action



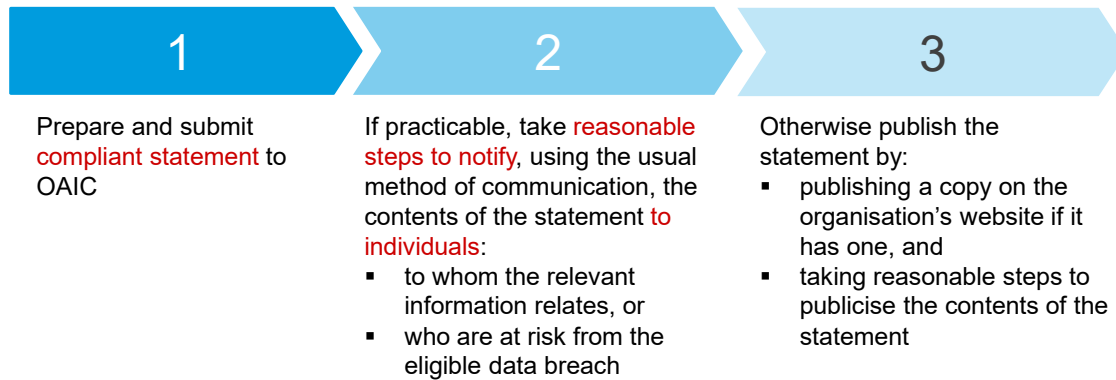
MinterEllison

## Assessment and notification steps

	Step 1 - Assessment	Step 2 – Notify Commissioner	Step 3 – Notify individuals
Obligation	<p>Positive duty to investigate (once suspect)</p> <p>Determine if there are reasonable grounds to believe that there has been an eligible data breach</p> <p>(must be reasonable and expeditious assessment)</p>	<p>Prepare statement about breach and provide to Privacy Commissioner</p>	
Timing	<p>30 days to make assessment if unsure if eligible data breach</p>	<p>As soon as practicable after becoming aware that there are reasonable grounds to believe eligible data breach</p>	<p>As soon as practicable after statement (step 2) is prepared</p>

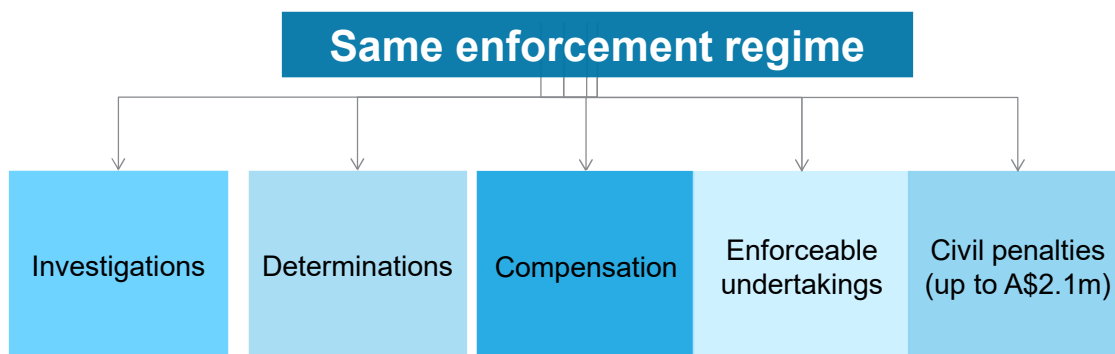
MinterEllison

## Notification of eligible data breach



MinterEllison

## Consequences of failing to notify



MinterEllison

## Data breach scenario



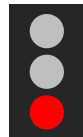
## Ready, set... notify?



Contain



Assess/Remediate



Notify

MinterEllison

## Checklist – assessing the data breach

Is the personal information likely to have been lost or accessed?

Type and volume of personal information?

Individuals who are or may be affected (are they vulnerable)?

Cause of the breach?

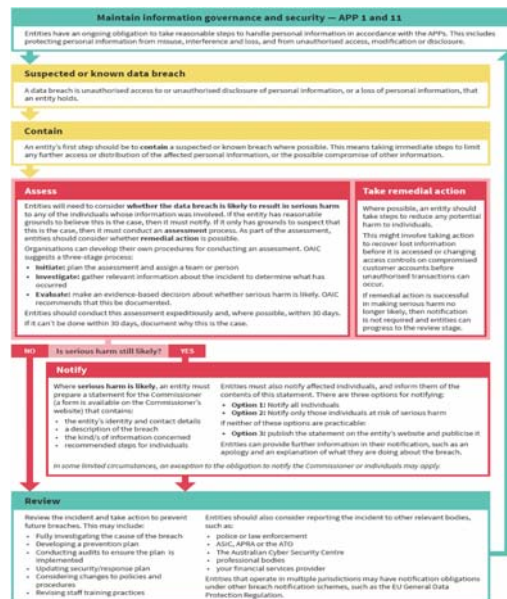
Extent of the breach?

Was it caused by third party (hacker) and are motives malicious?

Possible harm(s) that may occur to individuals affected?

How can breach be contained and remediated or how can PI be secured or recovered?

MinterEllison



MinterEllison

## How to prepare

MinterEllison





## To do

Train your employees and volunteers on identifying, escalating and actioning breaches

Identify data breach response team

Develop a data breach response plan

- Contain, Assess, Notify, Review
- Communications

Review IT security, recovery options and insurance

MinterEllison

## Questions?



## Contact



**Cathy Lyndon**  
Special Counsel

**T** +61 7 3119 6474  
**M** +61 408 284 825  
**E** [cathy.lyndon@minterellison.com](mailto:cathy.lyndon@minterellison.com)