



Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches scheme

Insights from 12 months in operation

Amie Grierson, Principal Director

30 May 2019

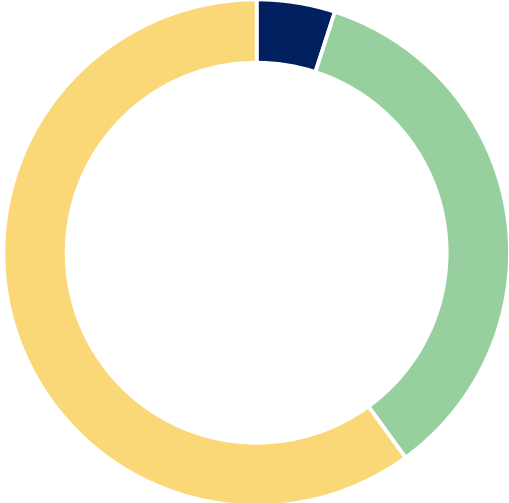
OAIC

Notifiable Data Breaches scheme

- Commenced 22 February 2018
- Requirements go to the core of good privacy practice —transparency and accountability:
- Incentivises proactive security practices to protect personal information
- Ensures individuals can act to prevent harm
- Allows consumers to make informed choices

Sources of data breaches

April 2018-March 2019



■ System fault ■ Human error ■ Malicious or criminal attack

Key statistics

964

Eligible data breaches



580

Malicious or criminal attack



153

Phishing



340

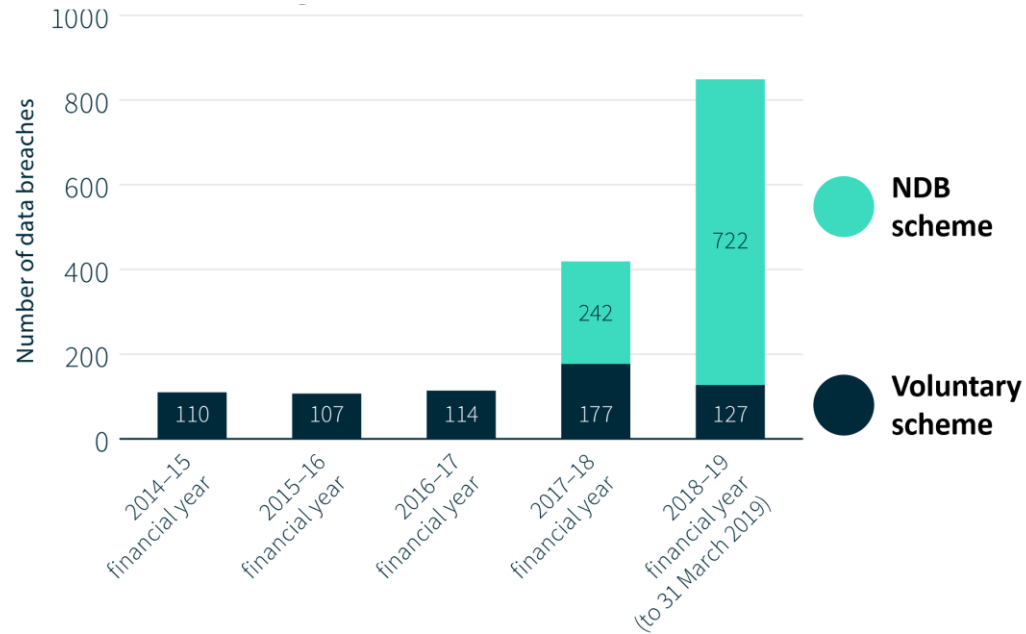
Human error



Mandatory and voluntary notifications

712%

Increase in notifications compared to voluntary scheme



Best practice recommendations

1. Effective training
2. Invest in better security measures
3. Prepare a data breach response plan
4. Understand your data holdings
5. Put the consumer first

Our regulatory approach

- Driving awareness of NDB scheme
- Ensuring breach contained and rectified, steps taken to prevent reoccurrence, notification to individuals
- Proportionate and evidence-based regulatory approach
- Will use enforcement powers where necessary

Useful resources

Guide to managing data breaches:

<https://www.oaic.gov.au/agencies-and-organisations/guides/data-breach-preparation-and-response>

Quarterly statistics report on the NDB scheme:

<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/>

12 month Insights Report on NDB scheme:

<https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme/quarterly-statistics-reports/notifiable-data-breaches-scheme-12-month-insights-report>

Responding to a privacy incident

- Checklists, guides and templates
- Establish Board and Executive positions regarding responses
- Establish key relationships in advance

Essential templates

- Risk Assessment - individuals and business
- Response Plan
- Notification eligibility
- Notification Documents

Timing of Response – Slow down to speed up

- Useful information for impacted individuals
- Dealing with questions from impacted individuals
- Regulator is busy too!
- Look after your staff