

## WEBINAR: Learning from others' mistakes – privacy and cyber security update

Welcome! We will be starting the live webinar at 1.00 pm AEST.



**Craig Subocz**  
Senior Associate



**Stephanie Quatela**  
Associate

If during the webinar you have any questions or comments please use the chat box to type.

If at any time you experience any technical problems, please refresh the page (F5) or use the 'Reconnect' button

CONNECTION PROBLEMS?

RECONNECT



**Russell Kennedy**  
Lawyers



# Webinar Housekeeping

---

- This webinar runs best using Google Chrome as your browser, if at any time you experience any technical problems, please refresh the page (F5) or use the *'Reconnect'* button

CONNECTION PROBLEMS?

RECONNECT

- Throughout the webinar if you have any questions or comments please use the chat box, we will endeavour to answer as many as we can at the end of the presentation
- We will have multiple pop ups during the webinar, including some live polls and documents for you to download. Feel free to interact!
- Feedback survey made available at the end of the webinar

Download PDF handout



Click to download the webinar handout

Download

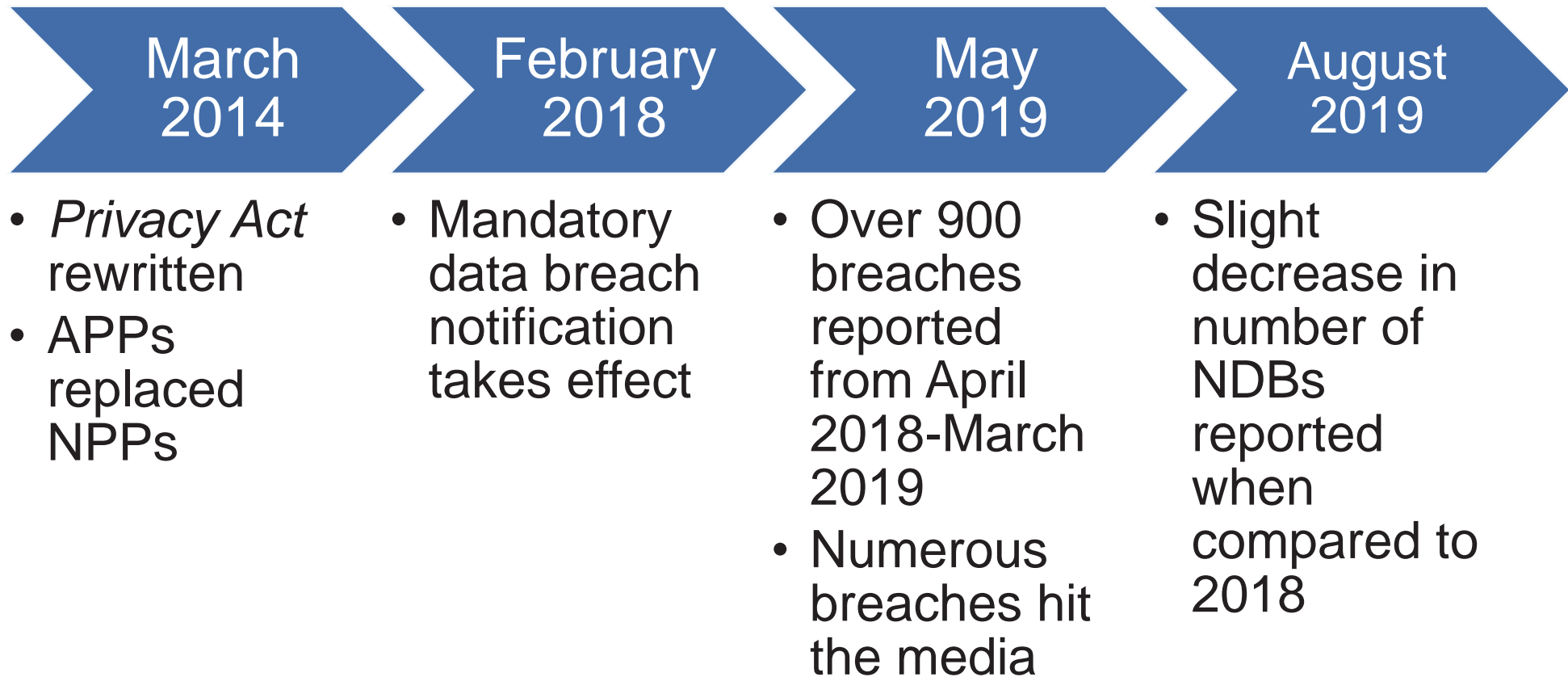
---

## Disclaimer

The information contained in this presentation is intended as general commentary and should not be regarded as legal advice. Should you require specific advice on the topics or areas discussed please contact the presenter directly.

# Where we have been

---



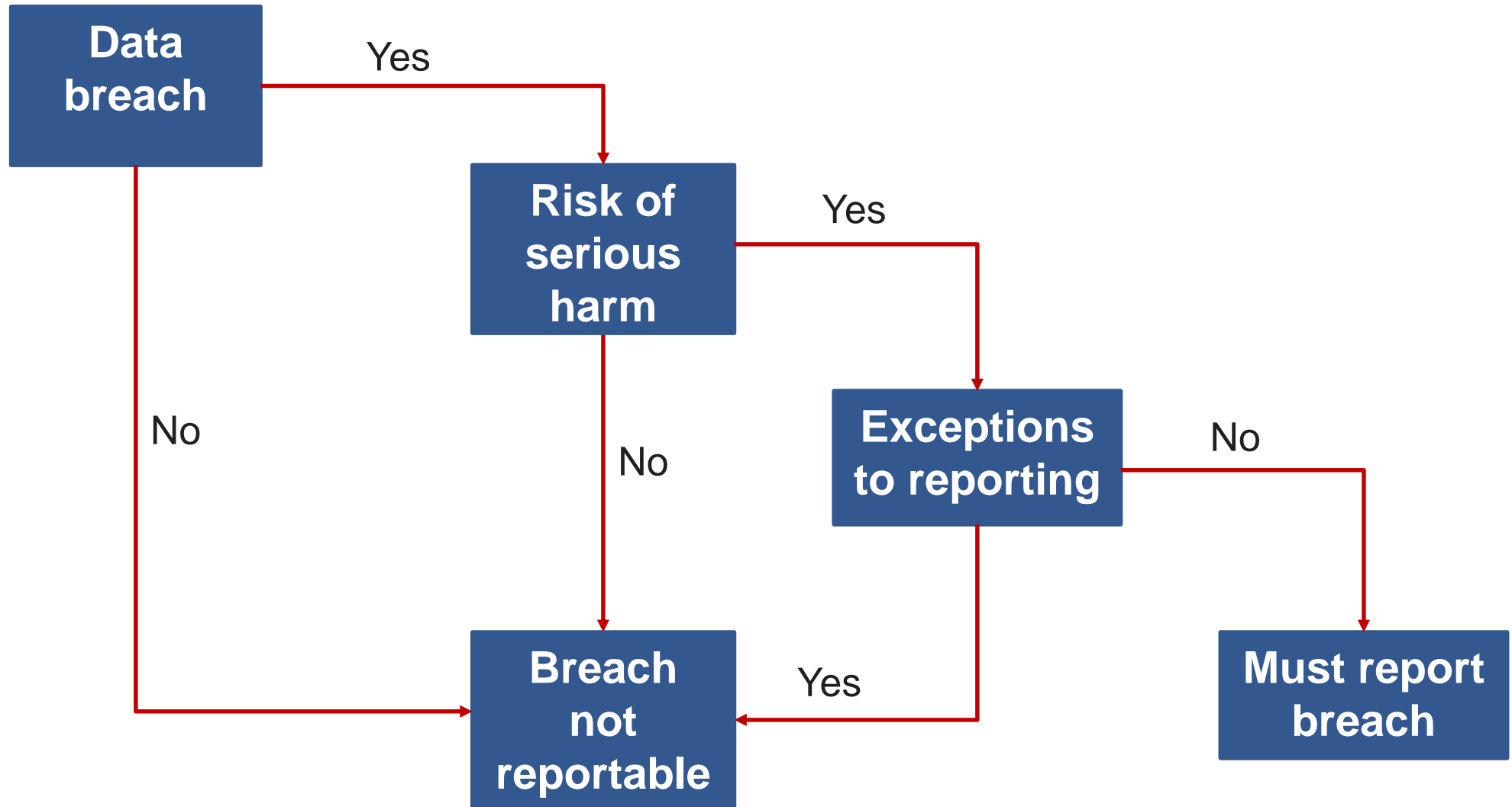
# What's the big deal about privacy?

---

- > Any Australian entity turning over \$3+ million a year must comply with the *Privacy Act*
- > Entities handling 'health information' must also comply, regardless of turnover
- > Compliance won't make you money
- > Get it wrong, it will cost you money
- > 22 February 2018 – new data breach notification laws

# When should a breach be reported?

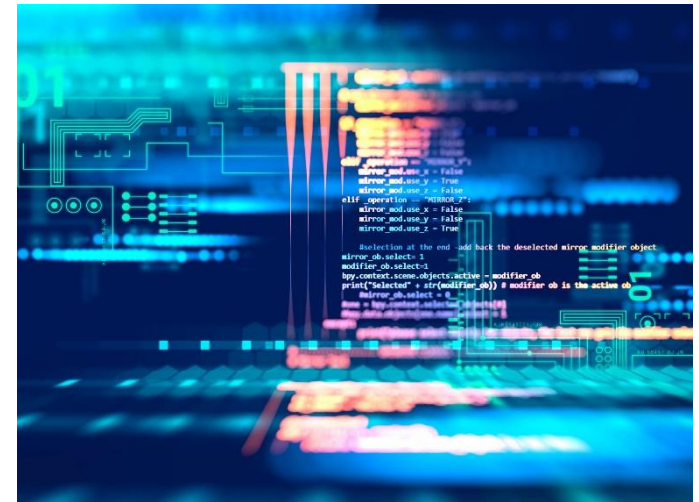
---



# What's happened so far?

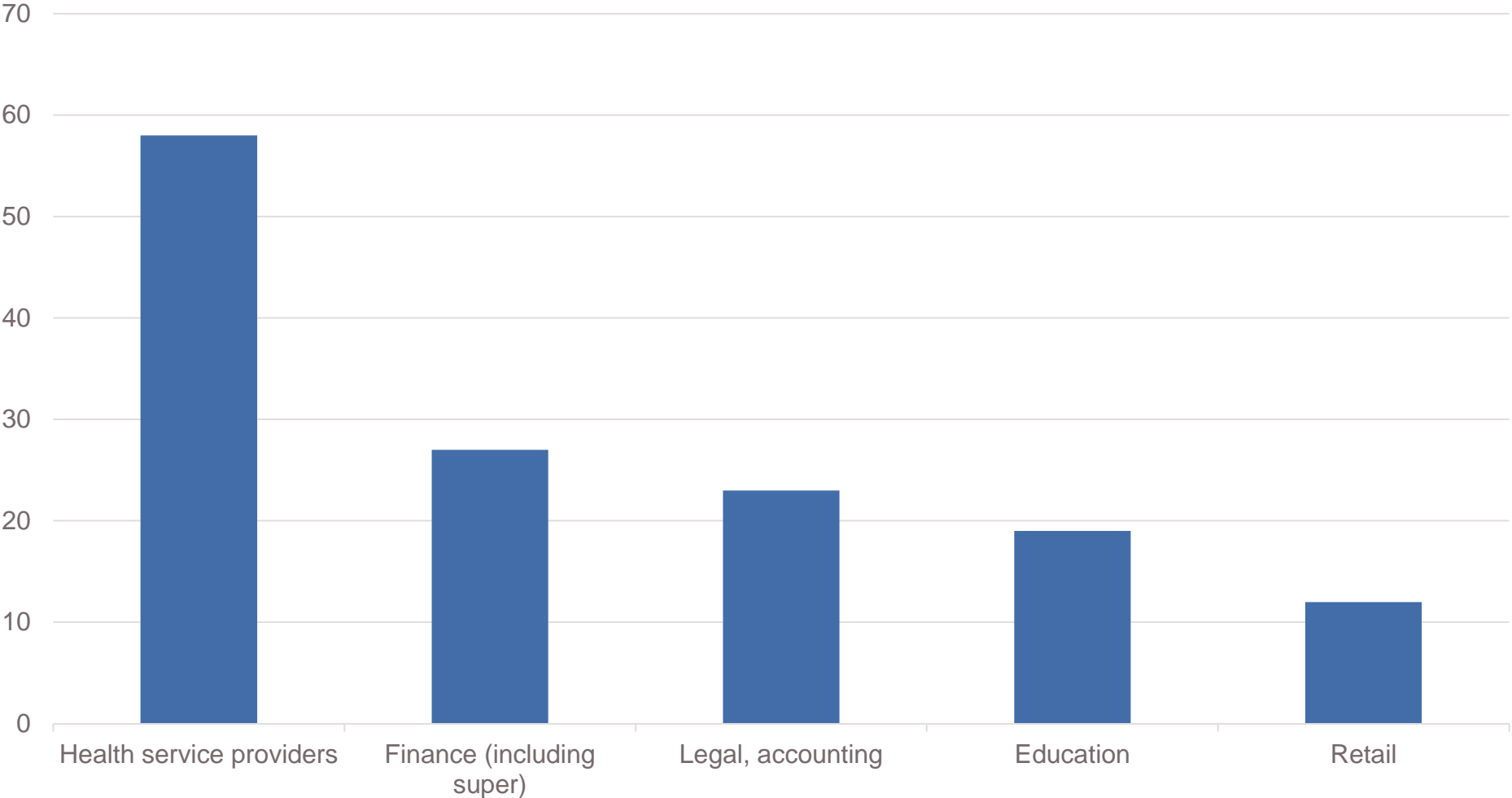
---

- > Every quarter, OAIC publishes data on breaches reported during the quarter
- > Reports accessible via OAIC website
- > Now have data for 2018 and 1 Jan to 31 March 2019
- > Over 800 breaches reported (averaging about 250 breaches per quarter)



# Industry sectors reporting breaches (Q1, 2019)

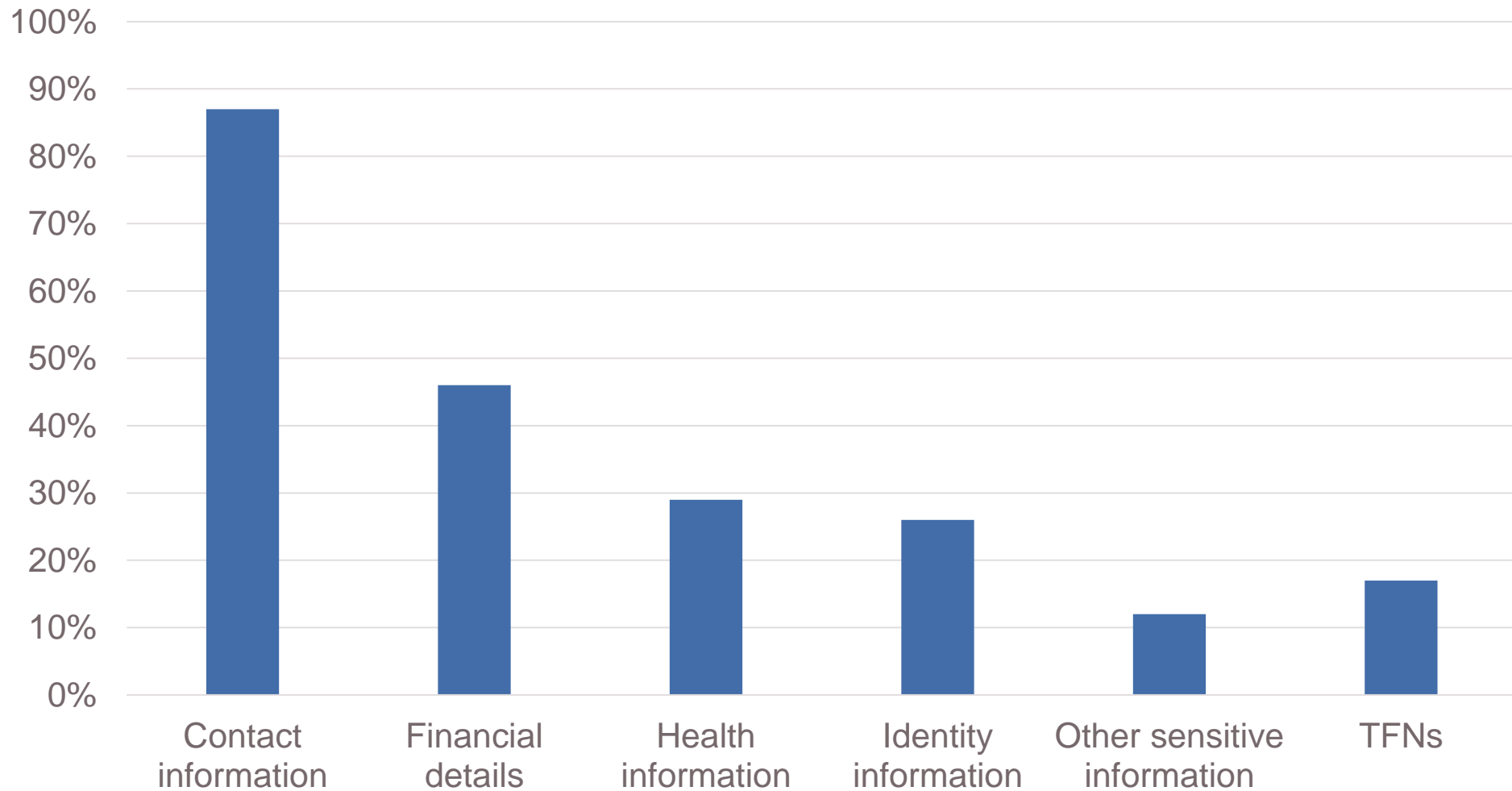
---





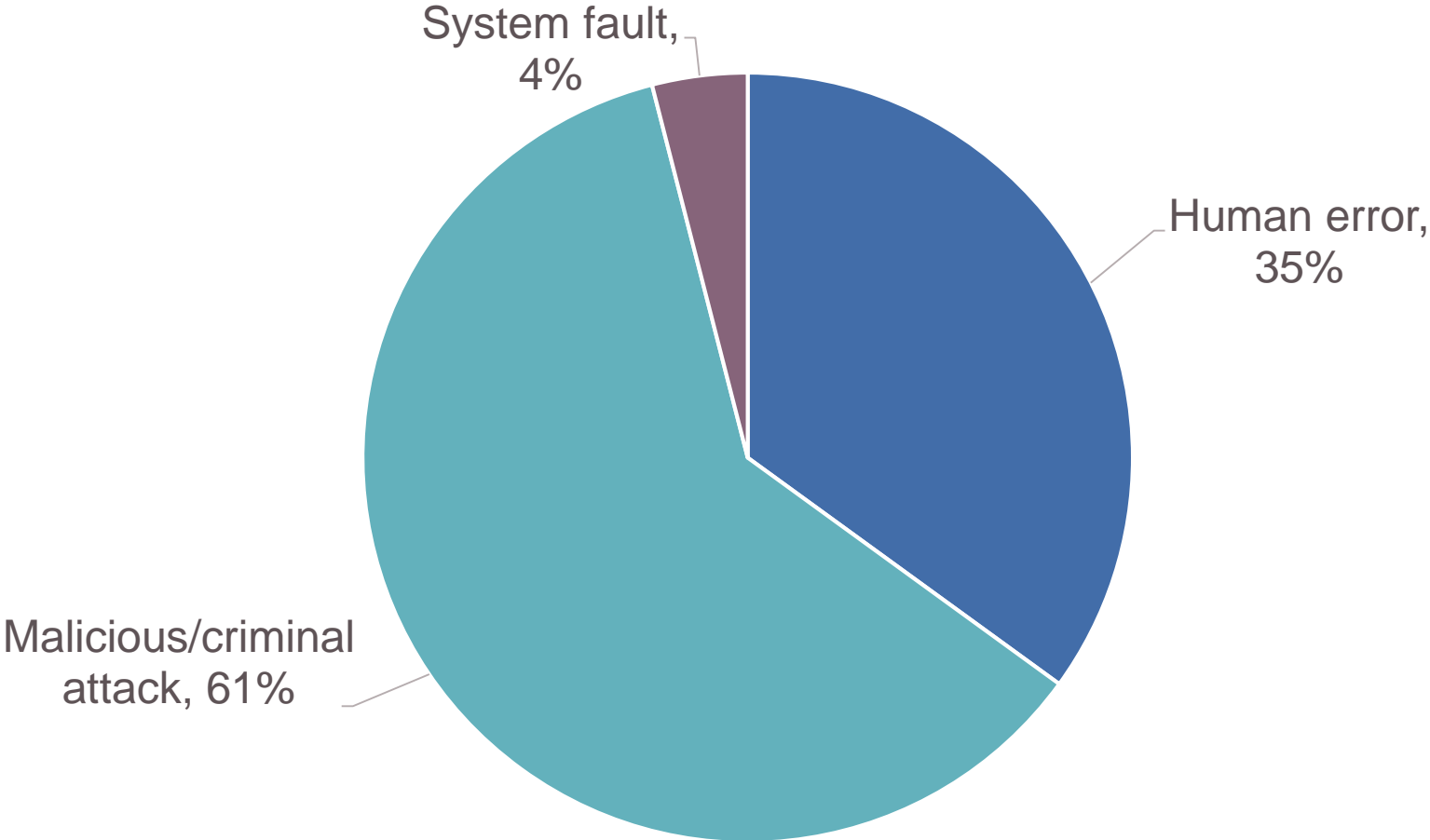
# Types of information involved (breaches reported Q1, 2019)

---

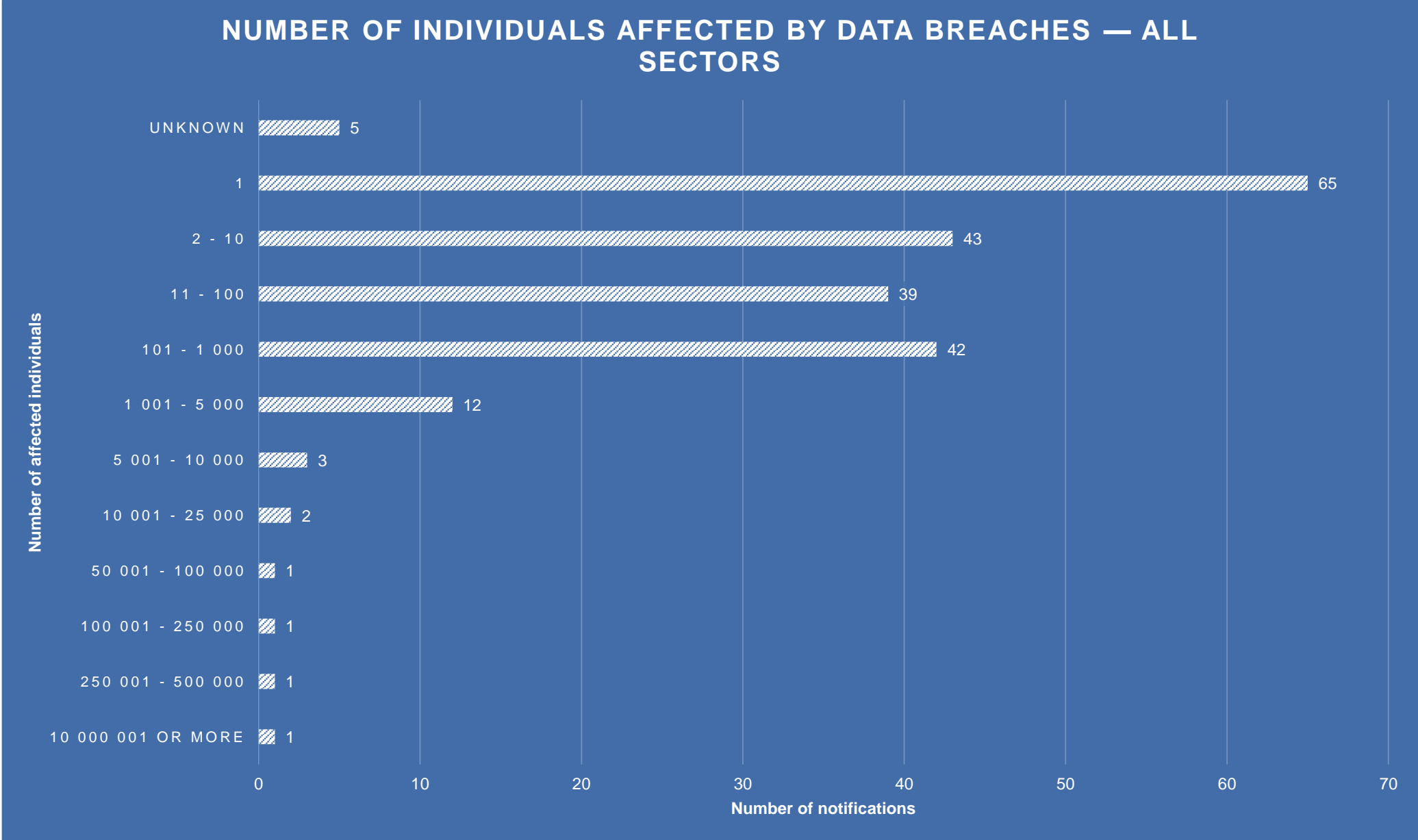


# Sources of breaches reported – 1 January to 31 March 2019

---



# Number of people affected – Q1, 2019



**Reminder for questions**



# February 2019: Australian Parliament IT system breached

---

> 8 February 2019:

## Security breach strikes parliament's IT network

By Justin Hendry  
Feb 8 2019  
10:29AM

All passwords reset.



> 18 February 2019:

## Scott Morrison reveals foreign government hackers targeted Liberal, Labor and National parties in attack on Parliament's servers

By political reporter Brett Worthington

Updated 18 Feb 2019, 3:03pm

> 10 April 2019:

## ASD confirms data stolen in Parliament IT breach

By Justin Hendry  
Apr 10 2019  
12:37AM

But exfil only netted non-confidential data.



# February 2019: Australian Parliament IT system breached

---

- > Department of Parliamentary Services conceded that not all elements of the Essential Eight (<https://www.cyber.gov.au/publications/essential-eight-explained>) had been implemented
- > Balance between flexibility for parliamentarians and cyber resilience



# February 2019: Australian Parliament IT system breached

---

## Take precautions

- > the sensitivity of your data
- > the consequences if your data is exposed
- > your budget
- > balance between tight security and user experience

# Public Transport Victoria (now Department of Transport) – July 2018

---

- > Found to have breached privacy laws – PTV released a dataset containing 15 million partially redacted public transport passenger details online
  - > Dataset included 1.8 billion records of touch-on and touch-off activity from 15 million myki cards
- > Actual breach - exposure of myki user's histories that could be used to identify individuals
  - > Information Commissioner: “Your public transport history can contain a wealth of information about your private life. It reveals your patterns of movement or behavior, where you go and who you associate with.”
- > DoT Issued with a compliance notice requesting it to strengthen its policies and procedures, including around data governance.



# February 2019: LandMark White breach

---


> **Sydney Morning Herald, 12 February 2019**

## Home loan details of 100,000 customers hacked in major data breach

By [Carolyn Cummins](#)

February 12, 2019 – 6.24pm



 0 [Leave a comment](#)

The nation's biggest banks are scrambling to contact up to 100,000 customers who may have been caught up in a major data breach at property valuation firm, LandMark White.

The breach, which LandMark White first revealed late on Friday, could include property valuations and personal contact information of home owners, residents, and property agents, including first and last names, residential addresses and contact numbers.

# February 2019: LandMark White breach

---

- > LMW published a detailed explanation of the breach on its website
- > Blamed the leak of data on a security vulnerability in its IT network
- > Took steps to close the leak once discovered
- > But the breach affected data collected over multiple years

> 21 February 2019

## Toyota Australia Statement Re-Attempted Cyber Attack

The Toyota corporate logo, consisting of the word "TOYOTA" in a bold, red, sans-serif font.

Toyota corporate logo.

Toyota Australia can confirm it has been the victim of an attempted cyber attack.

At this stage, we believe no private employee or customer data has been accessed.

The threat is being managed by our IT department who is working closely with international cyber security experts to get systems up and running again.

At this stage we have no further details about the origin of the attack.

We apologise for any inconvenience caused and thank customers for their patience.

# February 2019: Toyota Australia breach

---

- > Toyota likely would have been required to assess the circumstances of the breach to determine whether it was an eligible breach
- > 30 days to complete the assessment
- > If confirmed to be an eligible breach, an entity must notify OAIC and affected individuals as quickly as possible

# February 2019: Toyota Australia breach

---

- > Toyota not compelled to publicise any information about the breach if it is not an 'eligible data breach'
- > Eligible breach = if the breach would give rise to a risk of serious harm
- > Serious harm decided by weighing a number of factors



# February 2019: Toyota Australia breach

---

## > **Factors include:**

- > the nature of the data
- > the sensitivity of the data
- > whether security measures protect the data
- > who did or could have obtained access to the data
- > the nature of the harm

# February 2019: Toyota Australia breach

---

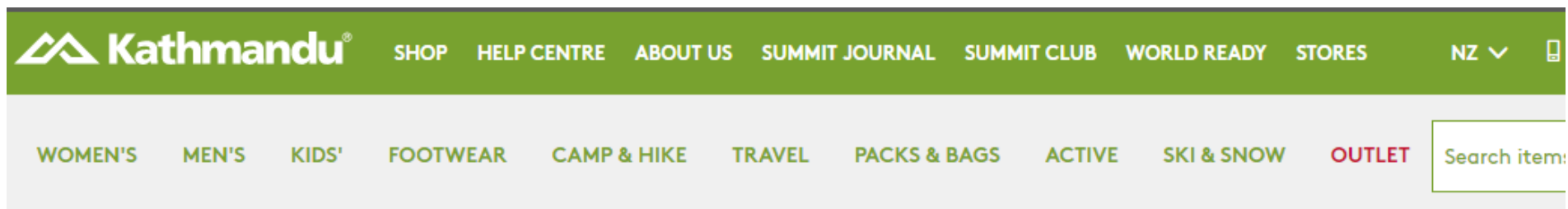
- > Evidently, Toyota Australia assessed the circumstances of the breach as such that it would not require reporting (i.e. it was not an eligible data breach)
- > Either individuals affected by the breach were not at risk of serious harm or Toyota Australia had taken remedial action to remove the risk of harm



# March 2019: Kathmandu breach

---

- > Unauthorised online store access by 3<sup>rd</sup> party
- > From Kathmandu's own website:



## Website Data Security Incident

[HOME](#) / [WEBSITE DATA SECURITY INCIDENT](#)

13 March 2019

We have recently become aware that between 8 January 2019 NZDT and 12 February 2019 NZDT, an unidentified third party gained unauthorised access to our website. During this process, the third party may have captured customer personal information and payment details entered at check-out for potential fraudulent use.

As soon as we became aware of this incident, we took immediate steps to confirm that our online store and our wider IT environment was secure. Since this time, we have been working closely with leading external IT and Cyber Security consultants to fully investigate the circumstances of the incident and confirm which customers may have been impacted.



## March 2019: Kathmandu breach

---

- > Kathmandu notified potentially affected customers directly
- > Given the nature of the breach, it was obviously reportable under the *Privacy Act* and under the Corporations Act 2001 (Cth) and ASX Listing Rules

# Mitigating against a data breach

---

- > Resources are available to help a company reduce the risk of a breach
- > ASIC publishes a good practice guideline on cyber resilience, as well as a list of questions directors should ask management about cyber resilience
- > APRA requires regulated entities to comply with a prudential standard on cyber resilience



# Dealing with a data breach

---



**DON'T PANIC!**

# Dealing with a data breach

---

- > Prevention better than cure
- > Assess and update privacy policy
- > Review contracts with key suppliers
- > Train staff
- > Develop and test data breach response plan
- > Insurance?

# Data breach response plan

---

- > Sometimes the best prevention won't stop the breach
- > Have a plan to deal with a breach
- > Being caught without a plan is a recipe for losing control of the message
- > Lose control of the message; lose your reputation



# Data breach response plan

---

The plan is an important tool to manage a breach

It sets a structure for managing your response to a breach and to comply with statutory obligations

- > Senior management oversight and board approval

Includes:

- > the actions to take if a staff member suspects or discovers a data breach
- > the members of the data breach response team (internal/external)
- > the actions the response team should take
- > a communications strategy

# Response team membership

---

- > If a data breach is detected, important to respond promptly
- > Reporting to a team leader and ultimately CEO, comprises:
  - > **Privacy officer**
  - > **Legal**
  - > **Risk management support**
  - > **ICT and HR support**
  - > **PR/Communications support – ideally with media training**

# Dealing with a data breach – Do's and Don't's

---

## DO

Act expeditiously

Be proactive

Be honest

Get assistance

Everything necessary to contain the breach

Evaluate risk to individuals exposed

Determine if notification is necessary

Take steps to prevent the breach from occurring again

Communicate with empathy and transparency

Investigate and obtain insurance

## DON'T

Panic

Ignore the issue

Be dishonest

Let concerns about being sued stop you from complying with your obligations

Be reactive



# How to craft a notification

---

- > The *Privacy Act* states that a public notification posted to a company's website satisfies the statutory requirement
- > Both Kathmandu and LandMark White published notification of their breach on their respective websites
- > Worth reading to see how a data breach notification works in practice

# Thanks and Q & A

---



**Craig Subocz**  
Senor Associate  
(03) 9609 1646

[csubocz@rk.com.au](mailto:csubocz@rk.com.au)



**Stephanie Quatela**  
Associate  
(03) 8602 7216

[squatela@rk.com.au](mailto:squatela@rk.com.au)

**Please use the chat box to type any questions you may have.**

**Please complete the feedback survey.**





Russell Kennedy Pty Ltd  
info@rk.com.au  
russellkennedy.com.au

**Melbourne**

Level 12, 469 La Trobe Street  
Melbourne VIC 3000  
PO Box 5146  
Melbourne VIC 3001 DX 494 Melbourne  
**T** +61 3 9609 1555 **F** +61 3 9609 1600

**Sydney**

Level 7, 75 Elizabeth Street  
Sydney NSW 2000  
Postal GPO Box 1520  
Sydney NSW 2001  
**T** +61 2 8987 0000 **F** +61 2 8987 0077

An international member of

**AllyLaw**

Liability limited by a scheme approved under Professional Standards Legislation.

[russellkennedy.com.au](http://russellkennedy.com.au)