



**SIBENCO**  
LEGAL & ADVISORY

# PRIVACY TRAINING

Susan Bennett  
Sibenco Legal & Advisory  
e: [susan.bennett@sibenco.com](mailto:susan.bennett@sibenco.com)  
p: +61 409 480 840  
[🐦 @sibenco](https://twitter.com/sibenco)

# Privacy



A strong **privacy culture** is critical for ensuring personal information security

**Privacy champions** essential for strong privacy culture

# Personal Information





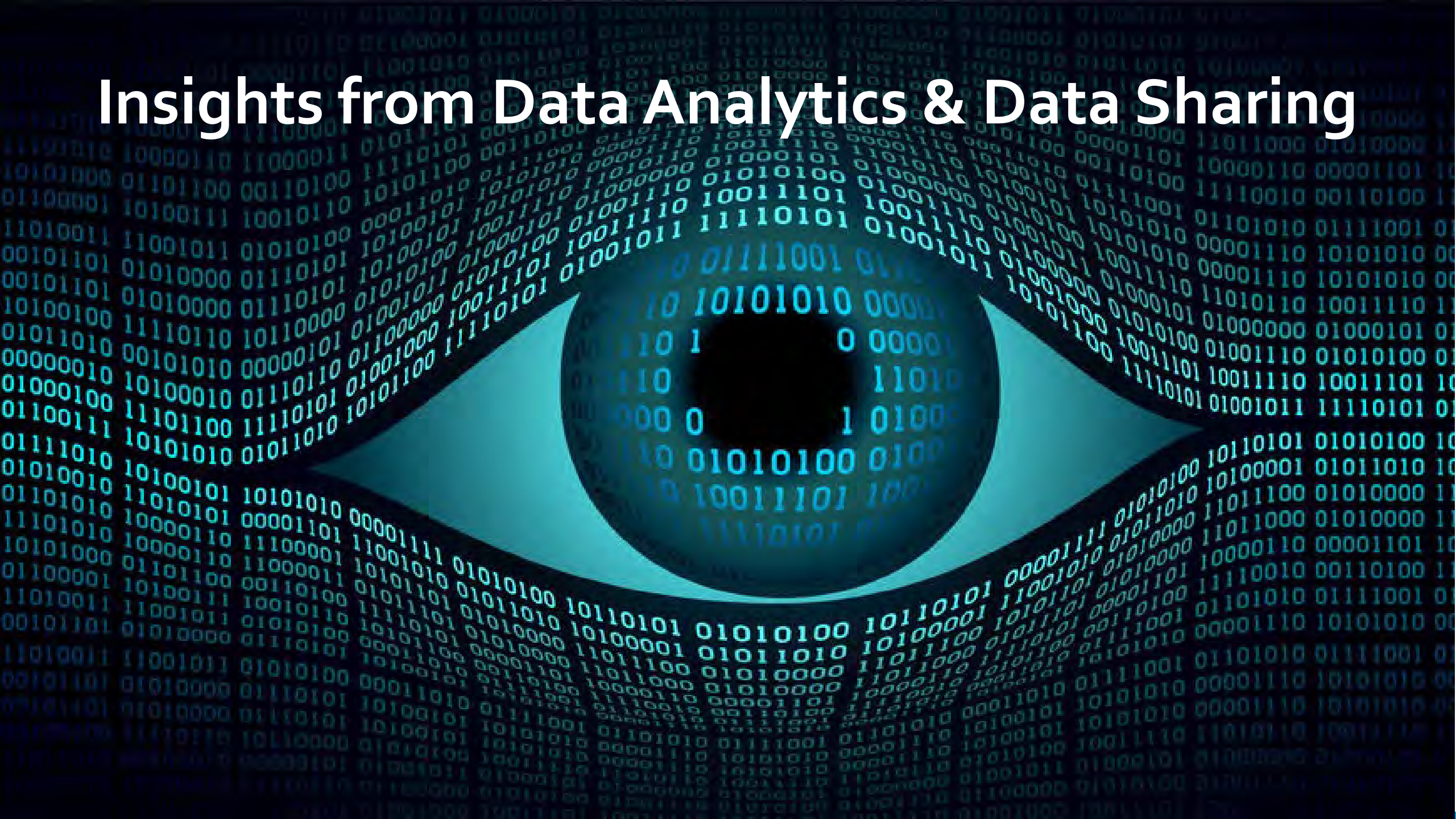
# Personal Information



# Global Digital Economy – data flows



# Insights from Data Analytics & Data Sharing



# Information

**Freedom of  
Information**

**FOI Act 1982**

**Privacy**

**Privacy Act 1988**





# Privacy now in focus



# Cambridge Analytica & Facebook

## Cambridge Analytica scandal: the biggest revelations so far

Since Christopher Wylie blew the whistle in the Observer, developments have been rapid. Here's what we know about the analytics firm, Facebook and Trump's election team



▲ Cambridge Analytica whistleblower: "We spent \$1m harvesting millions of Facebook profiles" - video

## Cambridge Analytica and Facebook: The Scandal and the Fallout So Far

Revelations that digital consultants to the Trump campaign misused the data of millions of Facebook users set off a furor on both sides of the Atlantic. This is how The Times covered it.



## Cambridge Analytica's Facebook data was accessed from Russia, MP says

by Donie O'Sullivan, Drew Griffin and Patricia DiCarlo @CNNTech  
July 27, 2018, 6:50 PM ET



Cambridge Analytica's Facebook data was accessed from Russia, MP says

The now infamous Facebook data set on tens of millions of Americans gathered by a Cambridge University scientist for a firm that went on to work for Donald Trump's 2016 campaign was accessed from Russia, a British member of parliament tells CNN.

## The Cambridge Analytica Files

A year-long investigation into Facebook, data, and influencing elections in the digital age



- Revealed / 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**
- The Brexit whistleblower / Did Vote Leave use me? Was I naive?**
- Facebook told me it would act swiftly on data misuse - in 2015**
- Revealed: Steve Bannon's psychological warfare tool: meet the data war whistleblower**
- Christopher Wylie goes on the record to discuss the role he played in exposing the profiles of millions of Facebook users in order to help the Conservative Party**
- Facebook's work of shame / The Cambridge Analytica fallout**
- Politicians can't control the digital giants with rules drawn up for the analogue era**
- Investigations spend seven hours at Cambridge Analytica HQ**
- Former Cambridge Analytica exec says she wants lies to stop**
- The Cambridge Analytica saga is a scandal of Facebook's own making**

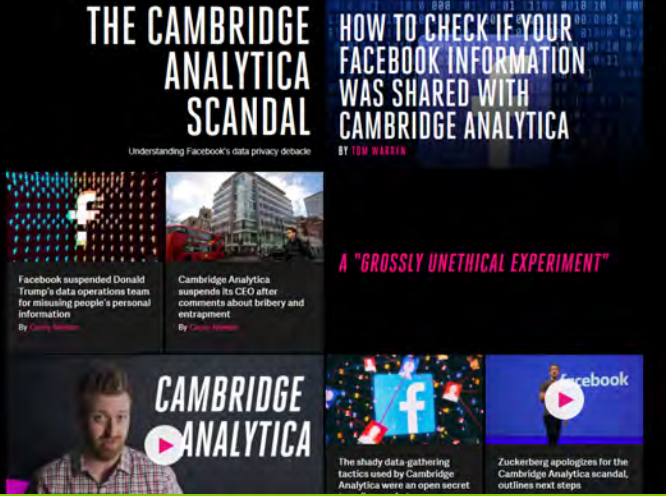
## THE CAMBRIDGE ANALYTICA SCANDAL

Understanding Facebook's data privacy debate

### HOW TO CHECK IF YOUR FACEBOOK INFORMATION WAS SHARED WITH CAMBRIDGE ANALYTICA

BY TOM WARREN

A "GROSSLY UNETHICAL EXPERIMENT"



- Facebook suspended Donald Trump's data operations team for misusing people's personal information
- Cambridge Analytica suspends its CEO after comments about bribery and entrapment
- The shady data-gathering tactics used by Cambridge Analytica were an open secret
- Zuckerberg apologizes for the Cambridge Analytica scandal, outlines next steps

## Facebook Cambridge Analytica Scandal: 10 Questions Answered

TECH • FACEBOOK



By BLOOMBERG April 10, 2018

# Cambridge Analytica & Facebook

How Cambridge Analytica Exploited the Facebook  
Data of Millions

New York Times

# PageUp – June 2018

NEWS

LOCATION: Sydney, NSW [Change](#)

[Home](#) [Just In](#) [Politics](#) [World](#) [Business](#) [Sport](#) [Science](#)

[Print](#) [Email](#) [Facebook](#) [Twitter](#) [More](#)

MUST READ: [MICROSOFT DECLARES WINDOWS 10 APRIL 2018 UPDATE READY FOR BUSINESS](#)

## PageUp could face class action over potential data mishandling

Centennial Lawyers is considering launching a class action lawsuit against the HR SaaS provider after it suffered a malware attack and possible resulting data breach.

## Bank details, TFNs, personal details of job applicants potentially compromised in major PageUp data breach

By Pat McGrath and Clare Blumer, ABC Investigations  
Updated 7 Jun 2018, 12:07pm

The personal details of thousands of Australians have potentially been compromised, with HR company PageUp, which counts Telstra, NAB, Coles, Australia Post, Aldi and Medibank as clients, revealing a massive data breach.

## How the PageUp Hack is Highlighting HR's Data Protection Problems

by Guest Contributor on June 14, 2018

FINANCIAL REVIEW

Home / Technology

Jun 8 2018 at 12:54 PM  
Updated Jun 8 2018 at 12:54 PM

[Save article](#) [My Saved Articles](#) [Print](#) [License article](#)

## PageUp data breach forces Coles, Aus Post and more to close careers websites

[G+](#) [f](#) [t](#) [in](#) [v](#)



Karen Cariss, co-founder and chief executive of PageUp, was forced to address a data breach on Wednesday.



## HR Software company PageUp victim of a Data Breach, experts fear a domino effect

June 6, 2018 By Pierluigi Paganini

[My Page](#) [Like 13](#)

[G+](#)

HR Software Firm PageUp is the last victim of a data breach, the company has 2.6 million active users across over 190 countries.

The Sydney Morning Herald

BUSINESS COMPANIES CYBER SECURITY

## PageUp data breach: ABC, Asahi, Myer, Macquarie pull jobs pages

By Jennifer Duke  
11 June 2018 – 4:52pm

Australians hoping to apply for a new job on the long weekend may have found their plans scuppered, with a swathe of businesses pulling down their careers pages after the PageUp data

BANK INFO SECURITY

[Breach Notification](#) [Breach Response](#) [Data Breach](#)

## HR Service Provider PageUp Discloses Data Breach

Customers Include Aldi, Lindt, Australia Post, Commonwealth Bank and Telstra

Jeremy Kirk (@Jeremy\_kirk) · June 7, 2018 · 0 Comments

[Email](#) [Print](#) [Twitter](#) [Facebook](#) [LinkedIn](#) [Credit Eligible](#)

[Get Permission](#)

## PageUp faces customer losses, lawsuits after data breach

[G+](#) [f](#) [t](#) [in](#) [v](#)



# PageUp - Universities

## Universities impacted

Universities victims of data breach at PageUp incl: Melbourne, RMIT, UNSW, Macquarie, ANU, Tasmania.

Reported that 'malicious code executed inside PageUp's systems'.

## Major universities hit by data breach affecting thousands of job applicants at top firms

By [Michael Koziol](#)

8 June 2018 - 4:54pm



5 [View all comments](#)

Leading universities including Melbourne and Macquarie have become the latest victims of a major data breach at human resources firm PageUp, forcing them to suspend their job boards and urge applicants to check their affairs for unusual activity.

PageUp People, which manages recruitment for ASX200 firms including AMP, Telstra and Coles, revealed it had detected "unusual activity" on its IT infrastructure last month and received "some indicators that client data may have been compromised".

The breach is under investigation by the government-run Cyber Security Centre. PageUp advised there was "no evidence that there is still an active threat, and the jobs website can continue to be used" - though many of its clients were being more cautious.





# ANU says 'sophisticated operator' stole data in new cyber breach

By [Max Koslowski](#) and [David Wroe](#)

Updated June 4, 2019 — 4:48pm, first published at 11:33am



36 [View all comments](#)

Up to 200,000 students and staff of the Australian National University have had personal data stolen in a "sophisticated" cyber attack that echoes a similar breach last year attributed to the Chinese government.

The university has admitted the hackers stole data stretching back 19 years that included bank details, passport information and academic records of current and former students and staff.



## TODAY'S TOP STORIES

### FEDERAL BUDGET

There's one thing politicians just can't resist when the economy goes bad



### MONEY APPS

Hours before Afterpay boss took to the stage, he was tapped over potential counter-terrorism breach



### TRUMP DIPLOMACY

On Iran, Trump tweets like a hawk but - thankfully - acts like a dove



## ANU data breach stretching back 19 years detected

Updated 4 Jun 2019, 5:02pm

**The Australian National University has been hit by a massive data hack, with unauthorised access to significant amounts of personal details dating back 19 years.**

A sophisticated operator accessed the ANU's systems illegally in late 2018 but the breach was only detected two weeks ago, the university said in a statement.

Based on student numbers over that time, as well as staff turnover, the university has estimated approximately 200,000 people were affected by the breach.

"We believe there was unauthorised access to significant amounts of personal staff, student and visitor data extending back 19 years," ANU vice-chancellor Brian Schmidt said.

"Depending on the information you have provided to the university, this may include names, addresses, dates of birth, phone numbers, personal email addresses and emergency contact details, tax file numbers, payroll information, bank account details, and passport details. Student academic records were also accessed."

However, Professor Schmidt said the hack had not accessed credit card details, travel information, medical records, police checks, workers' compensation information, vehicle registration numbers, and some performance records.



PHOTO: The hacker accessed personal details of staff, student and visitor data at Australian National University. (ABC News: Niki Challis)

**RELATED STORY:** [Doubts over data safety after ANU hack](#)

**RELATED STORY:** [Chinese hackers infiltrate systems at ANU](#)

**RELATED STORY:** [Where Australia ranks on the list of state-sponsored hackers](#)

## Key points:

- ANU vice-chancellor Brian Schmidt said the university had been made aware of the breach two weeks ago
- Professor Schmidt said there had been unauthorised access to "significant amounts" personal data
- IT upgrades put in place after a different breach last year helped detect the incident

# Australian Catholic University staff details stolen in fresh data breach

By [Carrie Fellner](#)

June 17, 2019 – 3.36pm



The Australian Catholic University has revealed the sensitive personal information of staff members has been stolen in a cyber attack, in the second significant security breach revealed in a month to have occurred at one of the country's tertiary institutions.

In an email circulated on Monday afternoon, the university confirmed a number of staff email accounts and some university systems had been compromised in a phishing attack on May 22.



Tuesday, 18 June 2019 08:50

## Attackers use phishing to gain access to ACU staff data ★

Featured

The Australian Catholic University has been hit by a data breach, with the attacker(s) using a phishing email to trick users into revealing their credentials on a fake ACU login page. The ACU has three public websites, with the main one running on Linux, while two others, which allow staff to log in, run on Windows Server 2008.



NEWS

# Laptops holding 30 years' worth of student data stolen from UWA



By George Nott

CIO |

29 JULY 2019 22:25 AEST

The laptops – which were taken in a break-in at a UWA administration building – contain the Tax File Numbers and student identification numbers of people who applied to study at the university between 1988 and January 2018.

“Separately, and in varying degrees of completeness, there are also details across the laptops from applicants who may have provided the University with information such as names, dates of birth and passport numbers to obtain a confirmation of enrolment,” Vice-Chancellor Professor Dawn Freshwater”

# 'Alarming' Data Breach Exposes 50,000 Students In Ticketing Website Bungle

NAME  
CONTACT DETAILS  
DATE OF BIRTH  
BANK DETAILS



Get, an online service used by a numerous clubs, societies, and student organisations around Australia, has suffered a major data breach, potentially





## Tech start-up investigating 'potential data leak' on online ticketing platform

By [Ben Nielsen](#) and [Rebecca Puddy](#)

Posted 10 Sep 2019, 7:10am

Student claims 'insane' amount of information available

Claims about the system vulnerability emerged over the weekend, after a University of Canberra software engineering student posted on social media.

The student, who asked to remain anonymous, told the ABC he found the data when applying for a club membership. "[The website] showed a list of all the people that were part of that society, which seemed a bit strange to me," the student said. He said a quick online search found the personal data of about 200,000 users dating back more than a year. "I looked at the information that was being sent from Get to my computer ... it's things like name, phone number, date of birth, addresses, student number.

# March 2020

Australia data breach: 90,000 staff, students, suppliers impacted at Melbourne Polytechnic

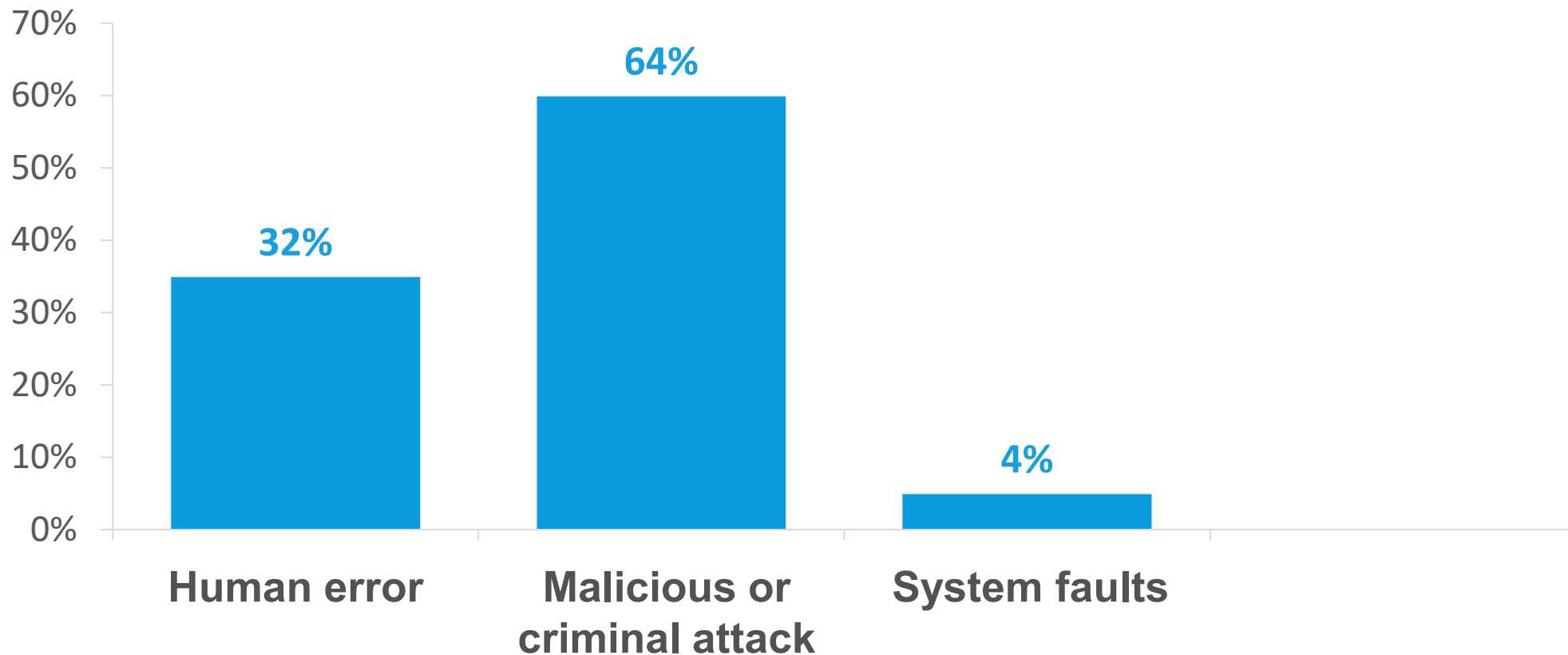


Personal data, including e-mail addresses, passwords, driver's license, passport details, and financial and health information of 90,000 staff, students and suppliers

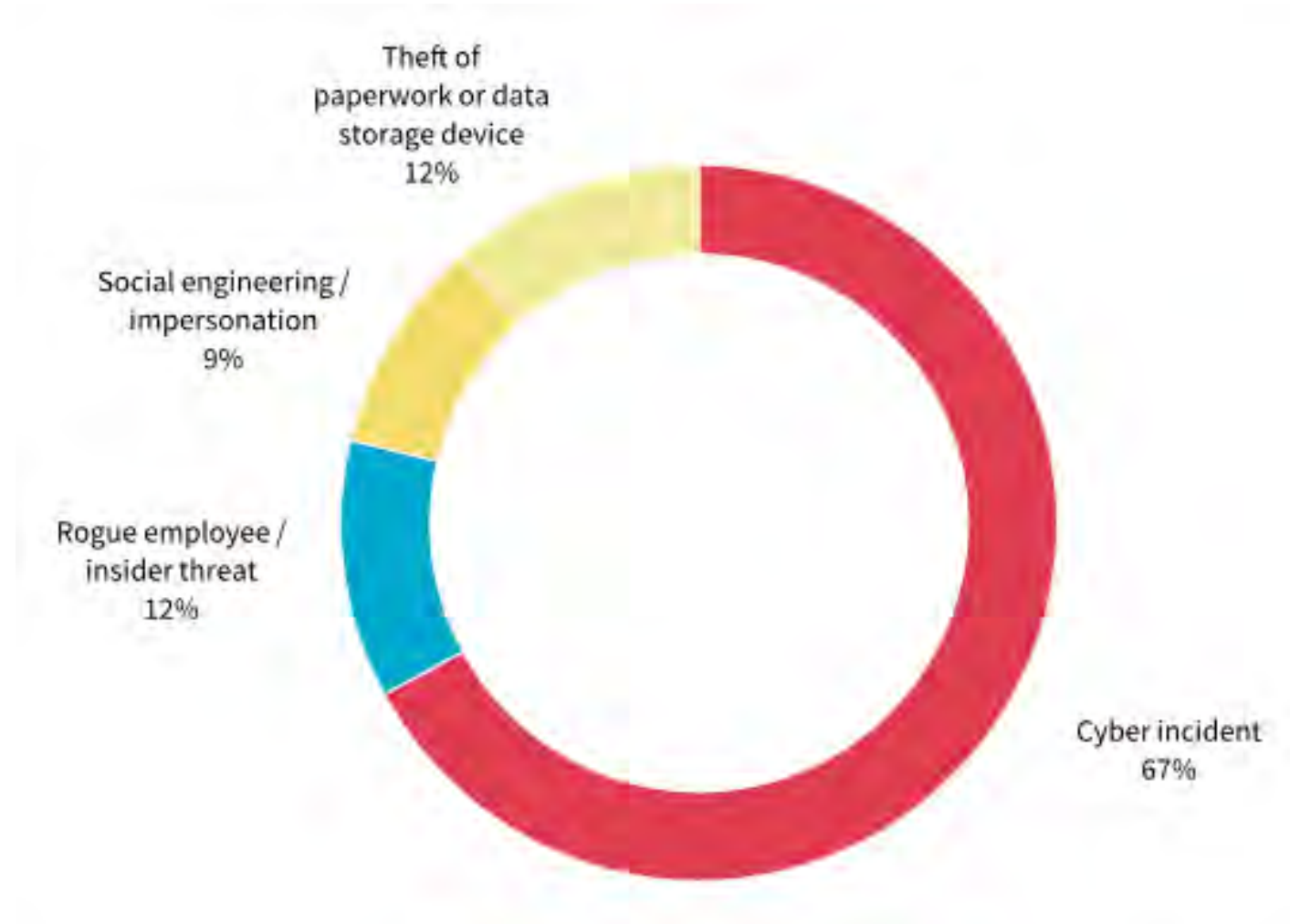


Victoria Police notified Melb Poytechnic that an individual who attended the campus in **late 2018** had 'obtained unauthorised access to Melbourne Polytechnic's computer systems by hard logging onto the network; overcoming security measures.'

# Data Breach Causes – OAIC, 28 Feb 2020

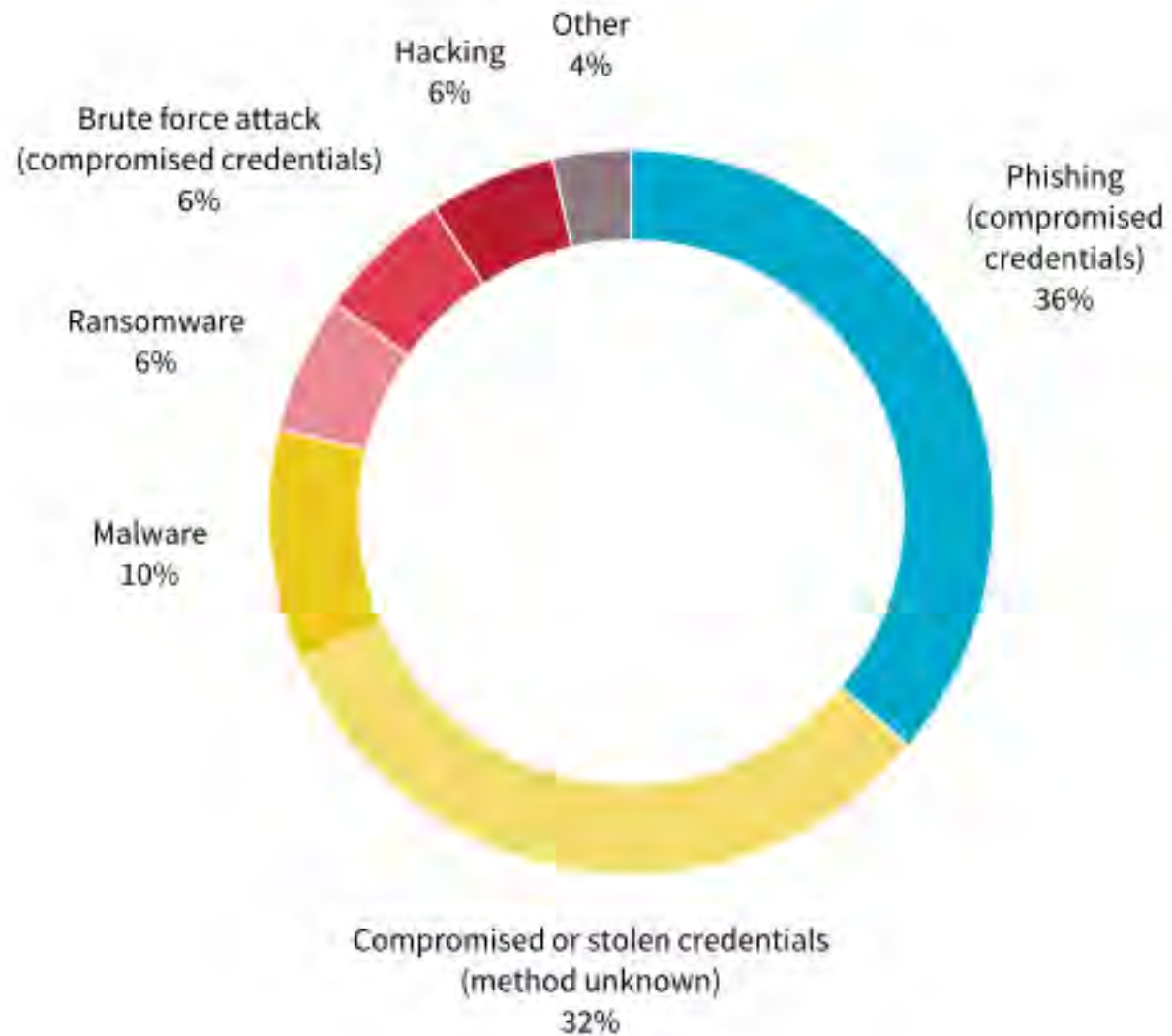


# Malicious or criminal attacks

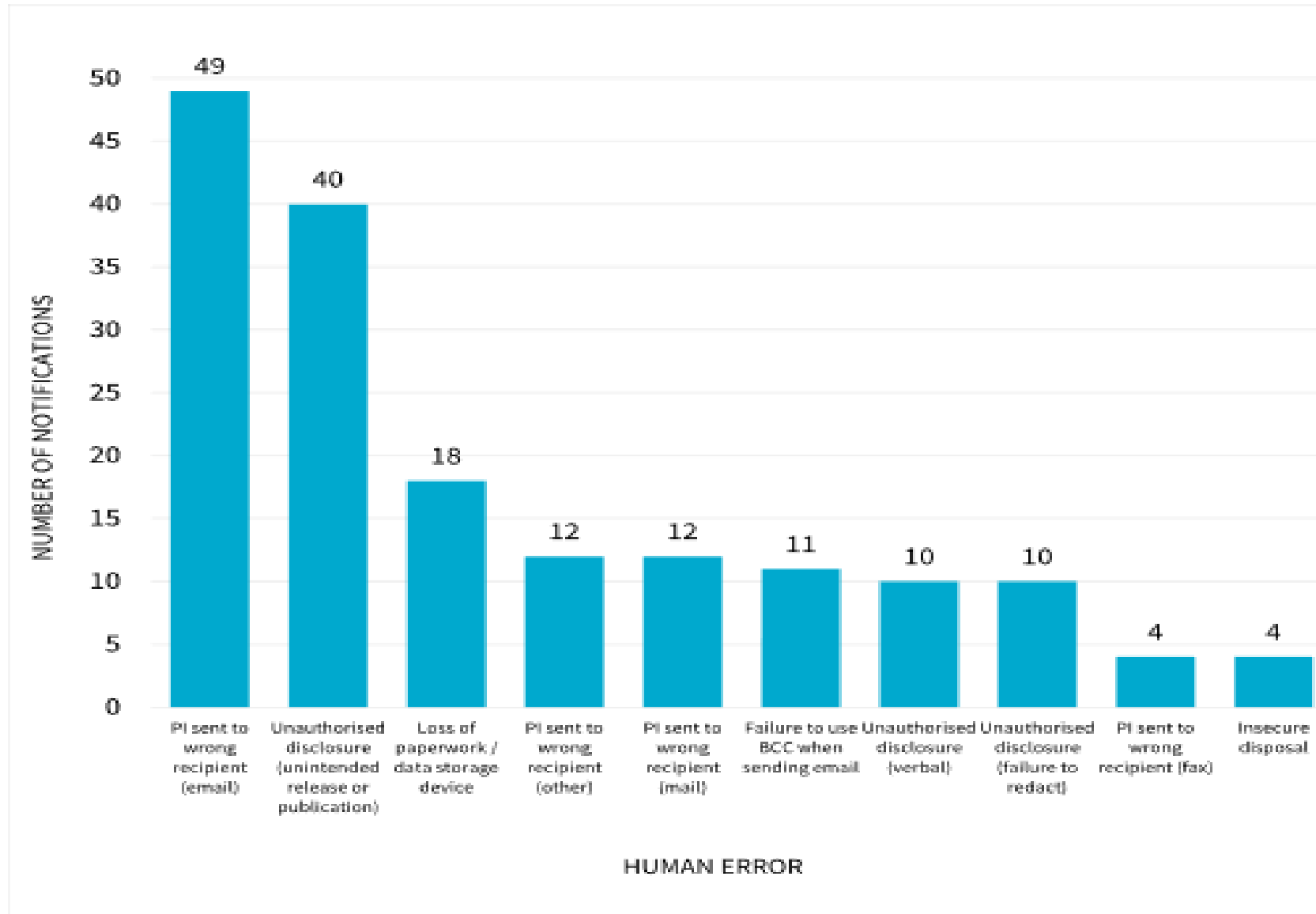




# Cyber incident



# Human Error Causes – OAIC, 28 Feb 2020

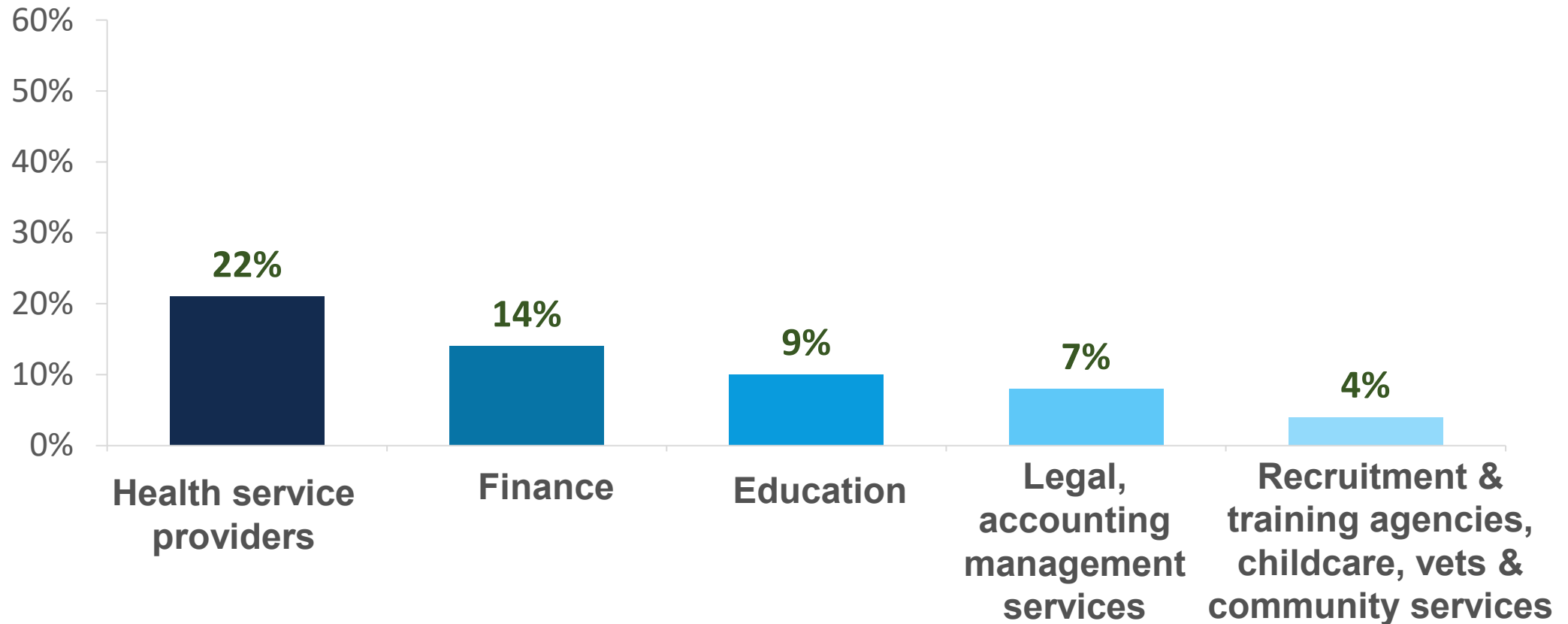


# Data Breach



- A data breach happens when personal information is accessed or disclosed **without** **authorisation** or is lost.

# Top 5 Sectors – July to Dec 2019





# OAIC report – 1<sup>st</sup> 12 months of NBD Scheme



- **964 data breach notifications**  
- From 1 April 2018 to 31 March 2019

- **114 data breach notifications**  
- for financial year 2016/2017

# OAIC report – 19% increase in 2019



- **537 data breach notifications**  
- From 1 July 2019 to 31 December 2019

- **460 data breach notifications**  
- From 1 January 2019 to 30 June 2019

**What do you do if you identify a data breach of personal information?**



# Notify the ANU Privacy Officer



# Data breach notification

You must notify affected individuals and OAIC when a data breach involving personal information is likely to result in serious harm



- Enables students, staff and affected individuals to take any steps required to protect themselves from risk that may occur as a result of the data breach.
- Assist to mitigate any damage and reflect positively on the University's reputation.



# Serious Harm



**The types of PI involved more likely to cause serious harm include:**

sensitive information – e.g. health

documents commonly used for ID fraud  
e.g. Medicare number, student number,  
driver license, passport details

financial information

a combination of types of PI that allows more  
to be known about the individuals

# Nature of Harm



**Examples likely to result in serious harm include:**

identity theft

significant financial loss

threats to an individual's physical safety

loss of business or employment opportunities

humiliation, damage to reputation or relationships

workplace or social bullying or marginalisation

# Notify the ANU Privacy Officer



# Process for managing a data breach



# **When are affected individuals and OAIIC notified of data breach?**





# Assessment - As Short a Time as Possible



**Section 26WH(2):** An organisation must take all reasonable steps to complete the assessment within 30 calendar days after the day it became aware of the grounds that caused it to suspect an eligible data breach.

**But....**

wherever possible entities to treat 30 days as a maximum time limit ..., and endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time.

# Assessing a Suspected Data Breach

The assessment:

Must be  
reasonable  
and  
expeditious

**and**

Entities may  
develop their  
own  
procedures for  
assessing a  
suspected data  
breach

# General Data Protection Regulation (GDPR)

## How Europe's GDPR will affect Australian organisations

Failure to comply with the data protection regulations could result in a €20 million fine, and Australian organisations with links to Europe will not be exempt.

By Asha McLean | July 12, 2017 -- 23:37 GMT (09:37 AEST) | Topic: Security

## Max Schrems files first cases under GDPR against Facebook and Google

European data protection bodies vow to work with Irish colleagues on complaints

© Fri, May 25, 2018, 08:03 | Updated: Fri, May 25, 2018, 18:15

Derek Scally in Berlin



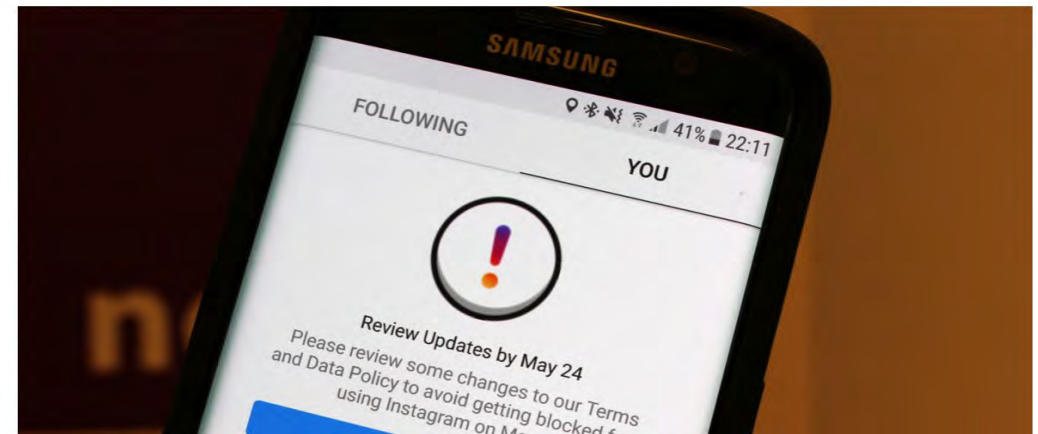
Privacy campaigner Max Schrems accused the tech giants of 'coercing' users to accept data policies

European data protection bodies have promised to work closely with their Irish colleagues on multi-billion-euro complaints filed by Austrian privacy campaigner Max Schrems against Facebook and Google.

## Facebook, Google face first GDPR complaints over 'forced consent'

Natasha Lomas @riptari / May 25, 2018

Comment



SECURITY

## The Game of Lawsuits – Another One Filed Against Facebook Over Data Misuse



By Rafia Shaikh

May 30, 2018

12  
SHARES

f SHARE

t TWEET

SUBMIT

# EU- GDPR



The biggest change to Europe's privacy laws in 20 years

Enforced from 25 May 2018

Penalties of up to 4% of global turnover or €20 million, whichever is higher

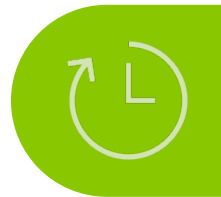




# Notification of Data Breach under GDPR



Under the GDPR, notification must be made where a data breach is likely to **'result in a risk for the rights and freedoms of individuals'**.






Notification must be made **within 72 hours** of first having become aware of the breach.



Data processors are required to notify their customers and the controllers **'without undue delay'** after first becoming aware of a data breach.



# GDPR applies to Australian orgs that -

-  are data processors or controllers with an establishment in the EEA
-  offer goods or services to individuals in the EEA
-  monitoring the behavior of individuals in the EEA, where that behavior takes place in the EEA

# Mandatory Data Breach Reporting



## NDB Scheme

Australia's notifiable data breach (NDB) scheme  
- 23 February 2018

APP entities – incl orgs with \$3m turnover, health care providers, ANU, private tertiary education providers, & breaches of TFNs



## Global trend

EU - General Data Protection Regulation (GDPR) - 25 May 2018

Australian orgs incl education providers, tertiary institutes if they are operating in the EU or offering goods & services to EU residents – i.e. prospective or current students or alumni residing in EU



# Notification of Data Breach under GDPR



Under the GDPR, notification must be made where a data breach is likely to **'result in a risk for the rights and freedoms of individuals'**.



Notification must be made **within 72 hours** of first having become aware of the breach.



Data processors are required to notify their customers and the controllers **'without undue delay'** after first becoming aware of a data breach.



# Rights of Individuals Under the GDPR

**Right of  
access**

**Right to  
be  
informed**



**Right to  
object**

**Right to  
withdraw  
consent**

**Right to  
rectification**

**Right  
to restrict  
processing  
(in certain  
circumstances)**

**Right  
to object  
to automated  
decision making  
(in certain  
circumstances)**

**Right to  
erasure / be  
forgotten**

**Right  
to data  
portability**

# Global Digital Economy – data flows



# Changes to Privacy Act ahead



Federal Government announcement in March 2019 that:

- OAIC will be provided with an additional \$25 million over three years to give it the resources it needs to investigate and respond to breaches of individuals' privacy
- Amendments to Privacy Act will be drafted for consultation.

# Privacy Check List

- Check - are you collecting PI?
- Check/think - do you need the PI, or all of the PI?
- Check before using and/or disclosing PI - i.e. is the use or disclosure permitted?
- Think before you send - avoid email address errors and/or wrong recipients
- Secure your computer and other devices; keep passwords safe
- Don't fall for phishing or other scams
- Be vigilant about information security



# The challenge of Shadow IT




Home » IT Leadership

**OPINION**

## Hillary Clinton is now the face of shadow IT

Even if the former secretary of state set up a private mail server purely for the convenience of using a single phone for both government work and personal use, Hillary Clinton is now the poster child for the dangers of rogue IT. Intentions aside, a move like Clinton's puts the security of confidential data at risk.

[Twitter](#) [Facebook](#) [LinkedIn](#) [Google+](#) [Reddit](#) [StumbleUpon](#) [Email](#) [Print](#)

 **By Tom Kaneshige**  
Senior Writer, CIO |  
MAY 12, 2015 10:55 AM PT

## What We Know About the Investigation Into Hillary Clinton's Private Email Server

By ALICIA PARLAPIANO | UPDATED OCT. 28, 2016

On Oct. 28, the F.B.I. director, James B. Comey, said that the bureau had recently uncovered new emails potentially related to the investigation into the private email server. The latest emails were found after the bureau seized at least one electronic device once shared by Anthony D. Weiner and his estranged wife, Huma Abedin, an aide to Mrs. Clinton. [RELATED ARTICLE](#)

**30,000** initially turned over by Mrs. Clinton's lawyers, deemed work-related, returned to the State Department in December 2014.

- **8 chains** included "**top secret**" information
- **36 chains** included "**secret**" information
- **8 chains** included "**confidential**" information, the lowest level of classification
- **2,000 emails** have since been classified "**confidential**"
- The F.B.I. director, James B. Comey, said that a very small number of emails had classified markings when they were sent.

**14,900** additional work-related emails that Mrs. Clinton did not turn over to the State Department, uncovered by the F.B.I. during the course of its investigation.



# Personal Information

# What is Personal Information?

**Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.**

What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances.



# Personal Information at the University



• Student/staff - name, address, ID number

• Family details, bank account details

• Medical Info incl medicare number

• Counselling notes

• Photographs, recorded images



# What are the risks?



- Risk to student and/or staff safety
- Financial loss to the student/family, and/or staff and/or University
- Reputational damage
- Loss of trust in University
- Regulatory investigation, litigation



# Personal information about an individual which is apparent or can reasonably be ascertained



## Redaction of name

*AIN v Medical Council of New South Wales* [2016] NSWCATAD 5



'While the Applicant's personal information was masked from the human eye, her personal information was able to be 'read' by the Google search engine. This resulted in a search for 'Dr [AIN]' (or similar) leading to a link to a copy of the (human eye redacted) Medical Tribunal's decision. The Respondent accepted, properly in my view, that a Google search for 'Dr [AIN]' would link the Medical Tribunal's decision to her'

# De-identification of Personal Information



De-identified information is information from which identifiers have been permanently removed, or where identifiers have never been included.

De-identified information cannot be re-identified.

# Personal information from linking with other information



'We have concluded that, depending on the circumstances, sources of information other than the information or opinion which contains the personal information, may be consulted to ascertain the person's identity.'

*APV and APW and Department of Finance and Services  
[2014] NSWCATAD 10 at [54]*

# Australia – Re-identification of dataset



## THE SIMPLE PROCESS OF RE-IDENTIFYING PATIENTS IN PUBLIC HEALTH RECORDS

In late 2016, doctors' identities were decrypted in an open dataset of Australian medical billing records. Now patients' records have also been re-identified - and we should be talking about it

By Dr Vanessa Teague, Dr Chris Culnane and Dr Ben Rubinstein, University of Melbourne

In August 2016, Australia's federal Department of Health published medical billing records of about 2.9 million Australians online. These records came from the Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) containing 1 billion lines of historical health data from the records of around 10 per cent of the population.

These longitudinal records were de-identified to protect a person's identity from being connected to the government's [open data website](#).



ENGINEERING & TECHNOLOGY

### Featured

 **Dr Vanessa Teague**  
School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne

 **Dr Chris Culnane**  
School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne

 **Dr Benjamin Rubinstein**  
Senior Lecturer, School of Computing and Information Systems, Melbourne School of Engineering, University of Melbourne

Engineering and IT

## Research reveals de-identified patient data can be re-identified

18 December 2017

## Health record details exposed as 'de-identification' of data fails

One in 10 Australians' private health records have been unwittingly exposed by the Department of Health in an embarrassing blunder that includes potentially exposing if someone is on HIV medication, has terminated a pregnancy, or is seeing a psychologist.

Unique patient records matching the online public information of seven prominent Australians, including three former or current MPs and an AFL footballer, were revealed in a study by the University of Melbourne's School of Computing and Information Systems.

A report published on Monday by the university's Dr Chris Culnane, Dr Benjamin Rubinstein and Dr Vanessa Teague outlines how de-identified historical health data from the Australian Medicare Benefits Scheme (MBS) and the Pharmaceutical Benefits Scheme (PBS) released to the public in August 2016 can be re-identified using known information about the person to find their record.

## Health pulls Medicare dataset after breach of doctor details

By Paris Cowan  
Sep 29 2016  
15:27 AEST

### [Updated] Researchers say govt encryption was poor.

The Department of Health has removed a research dataset based on Medicare and PBS claims from its open data portal after a team of Melbourne researchers pointed out that practitioner details could be decrypted.

The government today advised that the data was withdrawn yesterday following "an alert made in the public interest" by researcher Dr Vanessa Teague from Melbourne University on September 12.

Teague told the department that she and her colleagues had analysed 10 percent of the linked dataset and found it was possible to decrypt some of the service provider ID numbers attached to doctors.

"As a result of the potential to extract some doctor and other service provider ID numbers, the Department of Health immediately removed the dataset from the website to ensure the security and integrity of the data is maintained," the agency said in a statement.



Aussies born before 1962 with private health cover need to know this





# Australian Privacy Principles (APPs)



# 13 Australian Privacy Principles



There are **13 APPs** and they govern standards, rights and obligations around:

- **the collection, use and disclosure of PI**
- **ANU's governance and accountability**
- **integrity and correction of PI**
- **the rights of individuals to access PI**

# The Privacy Principles (APPs)

1

**Open and transparent management of PI** -  
incls having a clearly expressed and up to date privacy policy

2

**Anonymity and pseudonymity**

3

**Collection of PI** – outlines when you can collect PI

4

**Dealing with unsolicited PI** - outlines steps to be taken  
where unsolicited PI is received

# The Privacy Principles (APPs)

5

**Notification** – outlines what an individual must be informed

6

**Use or Disclosure** – outlines the circumstances in which PI may be used or disclosed

7

**Direct marketing** - may only use or disclose PI for direct marketing purposes if certain conditions are met

8

**Cross-border disclosure of PI** - outlines steps that must take to protect PI before it is disclosed overseas

# The Privacy Principles (APPs)

9

**Gov't related identifier** – outlines limited circumstances when a gov't identified may be adopted

10

**Accuracy** – reasonable steps must be taken to ensure PI is accurate, up to date and complete

11

**Security** - reas steps must be taken to protect PI from misuse, interference and loss, and from unauthorised access

12

**Access** – incls a requirement to provide access unless a specific exception applies

13

**Correction** – outlines the obligation to correct PI held about individuals



# Collection



# Collection of PI for lawful purpose



1. It must be lawful;
2. It must be directly related to a function or activity of the organisation; and
3. It must be reasonably necessary for that purpose.



# Disclosure of Personal Information

# Which of the following is correct?

- 1 The disclosure is directly related to the purpose of the collection and the University has no reason to believe this person would object.
- 2 The person is reasonably likely to be aware of the disclosure.
- 3 The disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the person or another person.

# Uses



**Sharing of information between Uni's Health Service,  
Counselling and Special Needs - 'uses'**

*CEU v University of Technology Sydney [2017] NSWCATAD 79*

# Reasonably expect



*CEU v University of Technology Sydney* [2017] NSWCATAD 79

The purpose of the disclosure from the GP to the Special Needs Unit of Student Services was 'to provide documentary evidence of ongoing medical conditions affecting her studies, so that she might access the services of the Special Needs Unit'.



# What security safeguards are reasonable for contractors?

- minimise the amount of personal information given out
- audit or monitor the performance of the service provider – eg contractor or tech system
- control the disposal of the information or demand the return of all personal information once the service is completed
- ensure contractual provisions minimising opportunities for misuse of personal information
- include appropriate contractual clauses incl indemnity clauses to pass on the costs of any compensation due to the actions of an outside contractor/service provider.



**Third party  
providers –  
technology,  
contractors  
&  
Privacy Impact  
Assessments**

# Privacy Impact Assessments - PIAs

A PIA identifies how a new or revised project or system can have an impact on an individual's privacy, and makes recommendations for managing, minimising or eliminating those privacy impacts.

A PIA is likely to be required if:

- personal information is collected in a new way;
- personal information is collected in a way that might be perceived as being intrusive;
- personal information will be disclosed to another agency, a contractor, the private sector or to the public; or
- there is a change in the way personal information is collected, disclosed, retained, stored or secured or handled.

- [Privacy Impact Assessment Guideline](#) available on ANU website
- Examples of PIA- [Graduate search](#)
- For assistance contact the ANU Privacy Officer - [privacy@anu.edu.au](mailto:privacy@anu.edu.au)



# Discussion

# Example

**EA to DVC calls HR and says there is an urgent need to call the staff member who is on leave and they need their personal mobile number, which they don't have. Should you provide the number?**





# Example

EA to General Manager of School calls and requests birthdays for staff in School for arranging of staff birthday morning teas. You can easily provide a list of names without the year of births, so do you provide the list?



# Example

Annabel's father calls Linda, who is Annabel's supervisor, and says he is concerned that he hasn't heard from Annabel for 6 weeks as she usually speaks with him regularly. He is worried as she suffers from depression and would like Annabel's contact details. Can you provide Annabel's mobile number or email address to her father?



# Example

ASIO contacts Dean of School asking for information about an academic who is suspected of being involved in a terror organisation. ASIO want access to attendance and travel destinations over the last 4 months, it is extremely urgent. The Dean hands this information over to ASIO. Should the Dean have done this?



# Example

Recent legislation changes have led to a need to change some processes in the HR system and Figtree system. This will require some further information to be collected from staff and technology changes to be made to both systems and can be used for insights for planning by ANU. What privacy issues does this raise? How would you approach making the system changes?



# Example

A detective contacts University HR staff member and for contact details for one of the University employees. They say that the disclosure is necessary a major fraud investigation, but is unwilling to provide further details in case it compromises the investigation.





# Example

A staff member is seriously injured and, due to their injuries, cannot give consent. Can the University disclose the individual's health information to the treating health service where the University reasonably believes that disclosure of the information is necessary to lessen the serious threat to the individual's life posed by those injuries?



# Example

Annabel is a staff member and wants to use the University's counselling service. She calls and is informed that she is required to give her name to use the service. The University say she can only use the service if she provides her name. Is this correct?



# Example: secondary purpose directly related to primary purpose of collection

A University counsellor collects health information about a staff member for the purpose of providing treatment, and then decides, for ethical and therapeutic reasons, that they cannot treat the individual. The health service provider then advises another provider at the counselling service of the individual's need for treatment and of the provider's inability to provide that treatment.



# Example – Anonymous letter

Anonymous letter alleges misconduct and corruption against senior executive Y. The University commences investigation. Senior executive Y alleges it is a breach of privacy.



# Example:

## Anonymising qualitative data

This shows how a piece of qualitative personal data – in this case an interview with a child - can be converted into an anonymised form which still contains valuable information but does not identify the child.

### Original text

**Interview recorded:** 3pm, 10 October 2011

**Interviewee:** Julius Smith

**DoB:** 9 September 2005

**School:** Green Lanes Primary School

*I live on Clementine Lane so I walk to school every day. I live in a flat with my parents and my Uncle Jermaine. When I get home from school I watch TV. I don't like reading but I like watching Harry Potter films. My favourite subject at school is art. My teacher is Mr Haines and he is very nice. I used to get bullied by Neil and Chris but I told Mr Haines and they stopped.*

*I play football for Junior Champs, and we are good. I play midfield.*

### Anonymised text

**Interview recorded:** October 2011

**Interviewee ref:** 2011/45

**School year:** Key Stage 1 School

**Local authority area:** City of Sydney Council

*I live in [LM51 postcode] so I walk to school every day. I live with [family members]. When I get home from school I watch TV. I don't like reading but I like watching Harry Potter films. My favorite subject at school is art. My teacher is Mr. [teacher's name] and he is very nice. I used to get bullied by [other pupils] but I told [the teacher] and they stopped.*

*I play football for [a local team], and we are good. I play midfield.*



# Personal Information



# Privacy Champions & Privacy Proactive

**Be proactive,  
Be prepared  
and able to  
quickly escalate  
and respond**

- **Be able to identify when there is a data breach**
- **Escalate and notify Privacy Office immediately**
- **Embed Privacy Culture – e.g team meetings**
- **Staff training – identifying, escalating and knowing what to do in breach event**
- **Ensure suppliers comply with contractual requirements incl privacy regulations**

# Privacy Check List

- Check - are you collecting PI?
- Check/think - do you need the PI, or all of the PI?
- Check before using and/or disclosing PI - i.e. is the use or disclosure permitted?
- Think before you send - avoid email address errors and/or wrong recipients
- Secure your computer and other devices; keep passwords safe
- Don't fall for phishing or other scams
- Be vigilant about information security



**SIBENCO**  
LEGAL & ADVISORY

**Thank you**

**Susan Bennett**

**Sibenco Legal & Advisory**

**e: [susan.bennett@sibenco.com](mailto:susan.bennett@sibenco.com)**

**p: +61 409 480 840**

**[www.sibenco.com](http://www.sibenco.com)**

** @sibenco**