

# *Incident Insights*

Victorian Information Security Network (VISN)  
March 2023

*We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.*

*We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.*

# Commissioner's welcome



**Sven Bluemmel**  
Information Commissioner

## **INCIDENT INSIGHTS REPORT 1 JULY 2022 – 31 DECEMBER 2022**

The information security incident notification scheme (the scheme) provides tangible resources, trend analysis and risk reporting.

### **OVERVIEW OF THIS REPORT**

The Incident Insights Report provides a summary and analysis of the information security incident notifications received by OVIC between **1 July 2022** to **31 December 2022**.

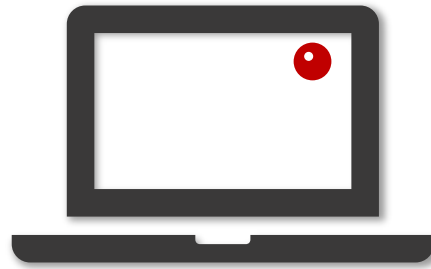
The analysis in this report is based on comparing the statistics published in previous Incident Insights Reports with the notifications received by our office under the scheme.

Victoria Police incident statistics are reported on annually, consistent with existing reporting commitments. For its latest incident statistics refer to OVIC's [Incident Insights Report for 1 January – 30 June 2022](#).

# Housekeeping



**Cameras and mics are muted.**  
If your Teams is running slow, try disconnecting from your VPN.



The first half of today's session is being **recorded** and will be made available after the session.



**slido**



Join the conversation using **#Incidents** at **slido.com** or using the chat feature in **MS Teams**.

# What we'll explore today

- What is the Incident Notification Scheme?
- The latest Incident Insights Report – themes and trends
- Incident management at Victoria Police
- Session close

*What is the Incident Notification Scheme?*

# What is the Incident Notification scheme?

Victorian government agencies or bodies are required to notify OVIC of incidents that compromise the **confidentiality, integrity, or availability** of public sector information in all forms.



What sort of incidents need to be notified to OVIC?

Incidents that reach the threshold of a business impact level (BIL) of 2 (limited) or higher.

A screenshot of the OVIC website page titled "OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME". The page features a purple header with the OVIC logo and navigation links: ABOUT US, FREEDOM OF INFORMATION, PRIVACY, INFORMATION SECURITY, and EVENTS AND EDUCATION. Below the header is a breadcrumb trail: Home / Information security / OVIC Information Security Incident Notification Scheme. The main content area has a large heading "OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME" and a banner image showing a hand holding a megaphone with the text "The Information Security Incident Notification Scheme" and the OVIC logo. To the right of the banner is a "Download" section with two links: "OVIC-Information-Security-Incident-Notification-Scheme-V1.o.pdf" (Size 285.23 KB) and "OVIC-Information-Security-Incident-Notification-Scheme-V1.o.docx" (Size 511.33 KB), each with a "Download" button. Below the download section is a "Contents" section with a list of links: "WHAT IS THE SCHEME?", "WHO CAN NOTIFY OVIC WHEN AN INCIDENT OCCURS?", "WHO DO I TURN TO FOR ASSISTANCE WHEN AN INCIDENT OCCURS?", "WHAT SORT OF INCIDENTS SHOULD I NOTIFY OVIC OF?", "WHEN SHOULD I NOTIFY OVIC?", and "PRIVACY BREACH CONSIDERATIONS".

*The Latest Incident Insights Report  
Themes and Trends*

Anna Harris  
Principal Advisor, Information Security - OVIC



# Themes and Trends



Volume



Information  
format



Information  
type



Business  
Impact  
Level (BIL)



Security  
attributes



Control  
areas



Threat  
actors

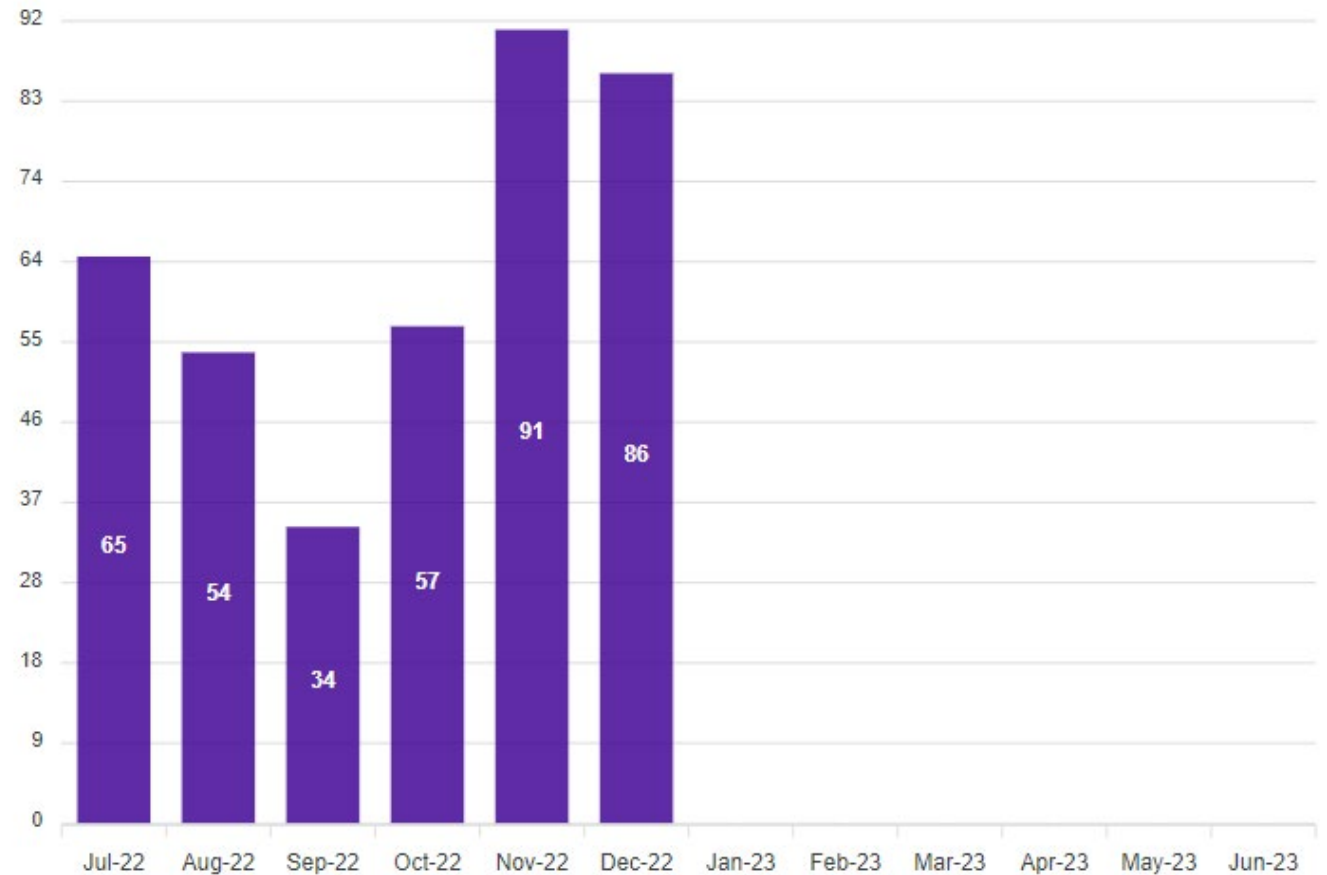


Threat  
types

# Volume - Notifications by month



- OVIC received **387** notifications between **1 July to 31 December 2022** (inclusive).
- This is a **12%** increase compared to the same time last year.



*Quiz time!*

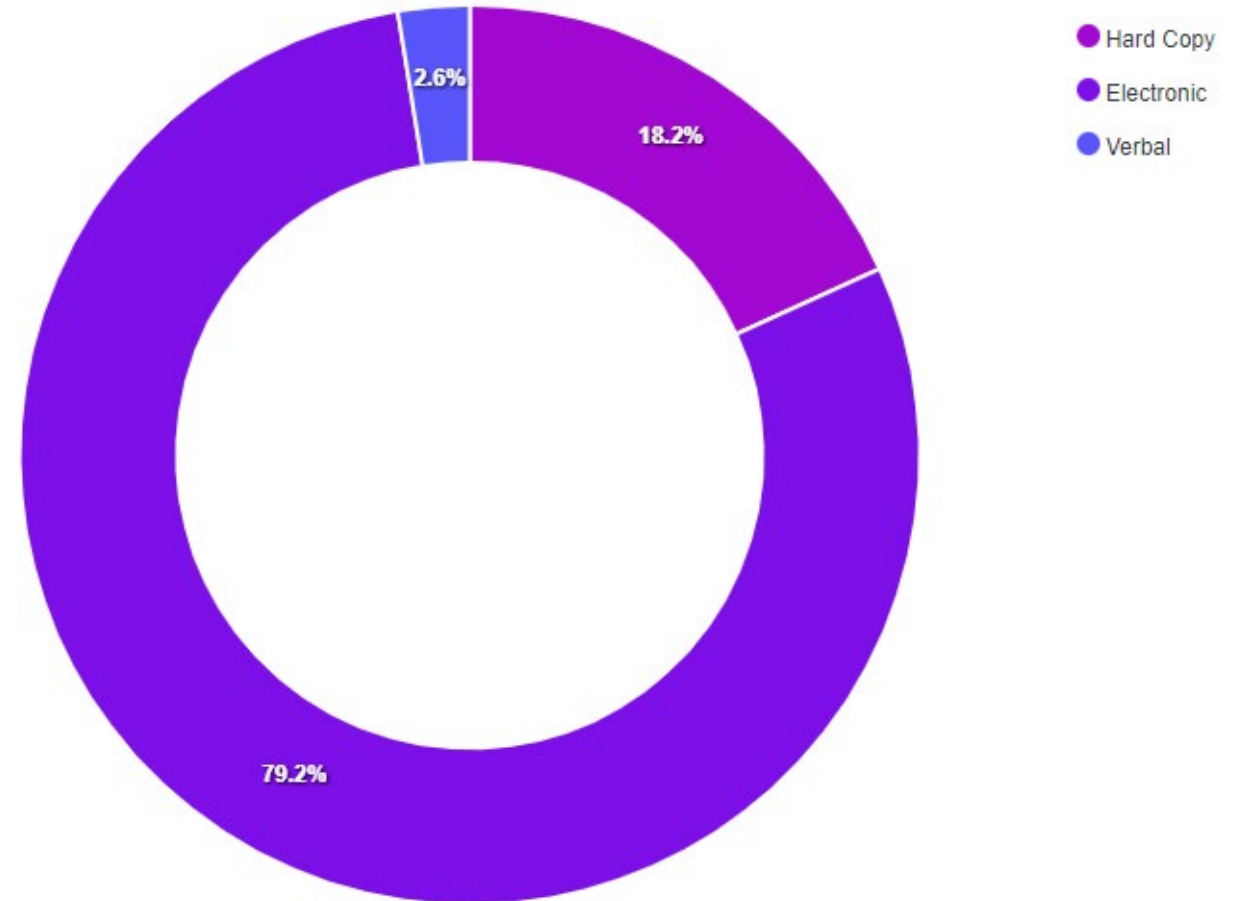
What was the most affected information format in the Jul-Dec reporting period?

- A. Electronic information
- B. Hard copy information
- C. Verbal information

# Information format



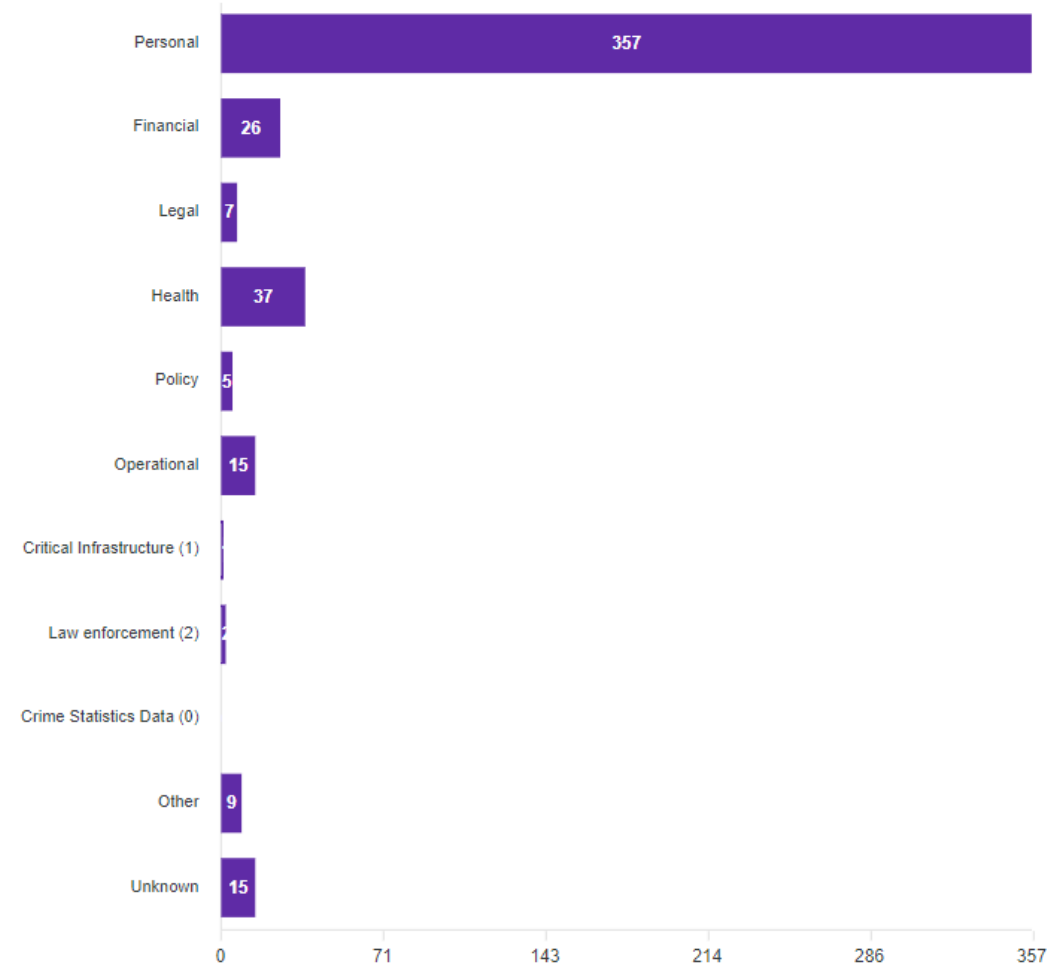
- 309 notifications indicate compromises of **electronic information**.
- Half of the incidents affecting electronic information related to emails - predominantly **sending emails to the incorrect recipient**.
- **Half** of incidents involving hard copy information were related to **mail**.



# Information type



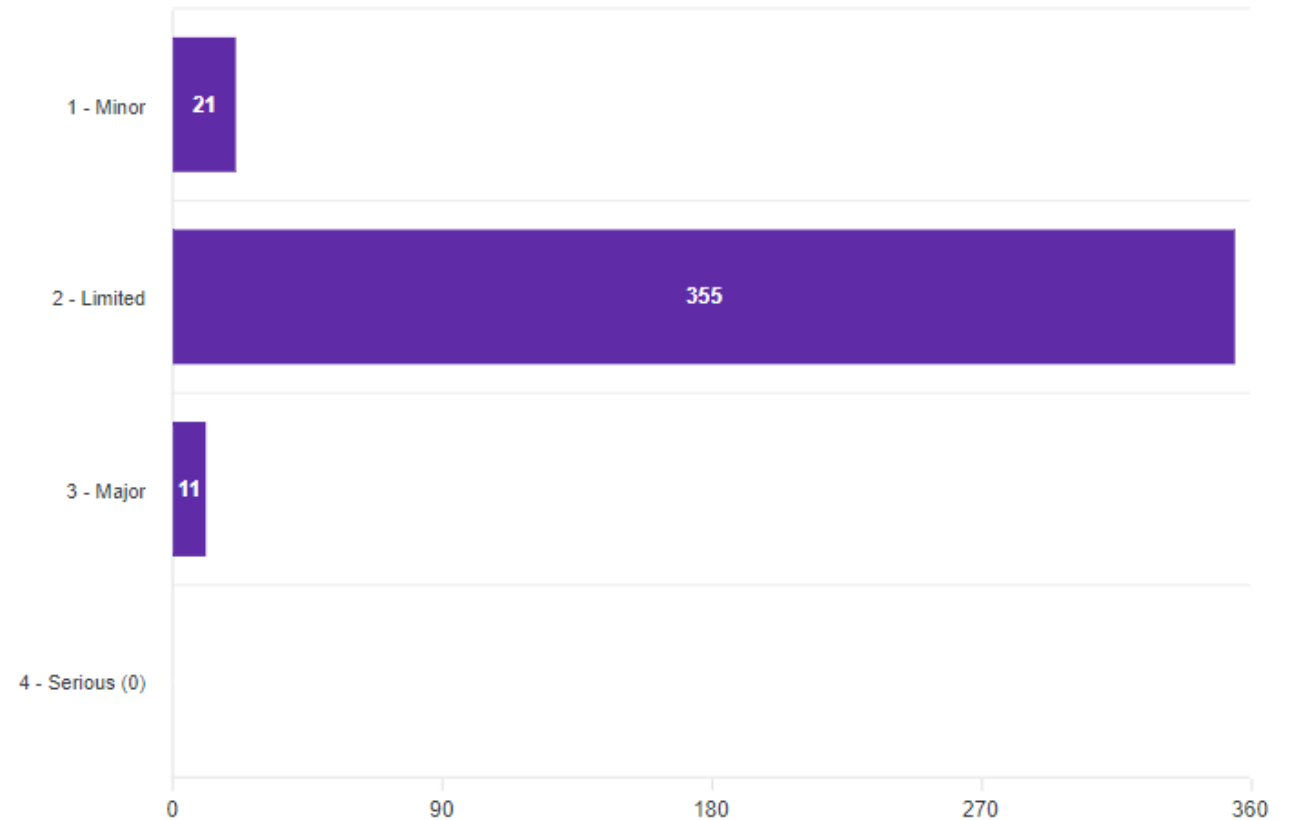
- 92% incident notifications indicate compromises of **personal** information.
- 15 incident notifications where the type of information involved was **Unknown**.
- A recent update to the notification form added two new information types: **law enforcement** and **crime statistics** information.



# Business Impact Level (BIL)



- **92%** of incidents were assessed as impacting BIL 2 / Limited information.
- **3%** nominated BIL 3.
- If in doubt just notify.



*Quiz time!*

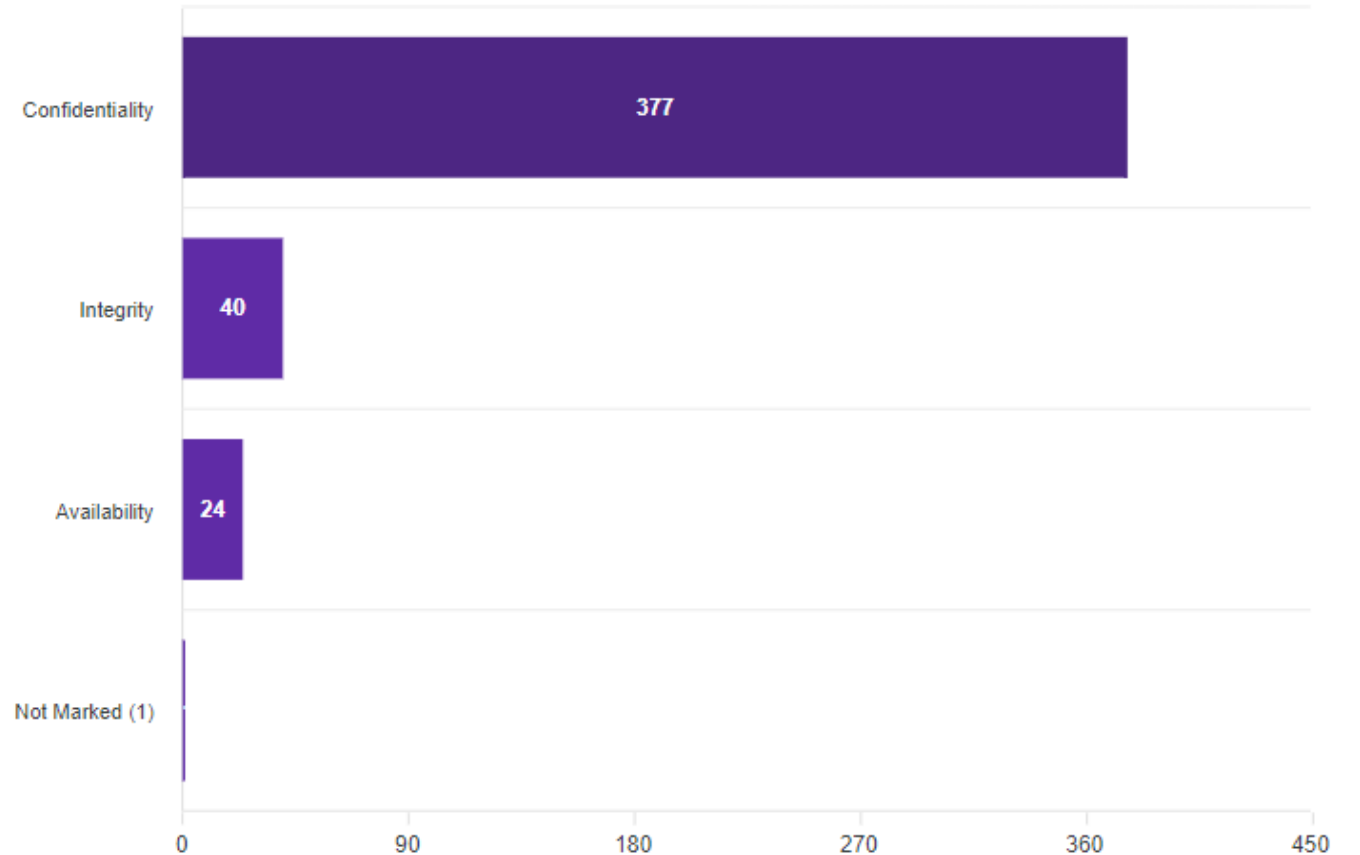
What was the most affected security attribute in the Jul-Dec reporting period?

- A. Confidentiality
- B. Integrity
- C. Availability

# Security attributes



- **98%** of incident notifications indicate compromises of the **confidentiality** of information.
- **12%** of notifications selected more than one option for this field.

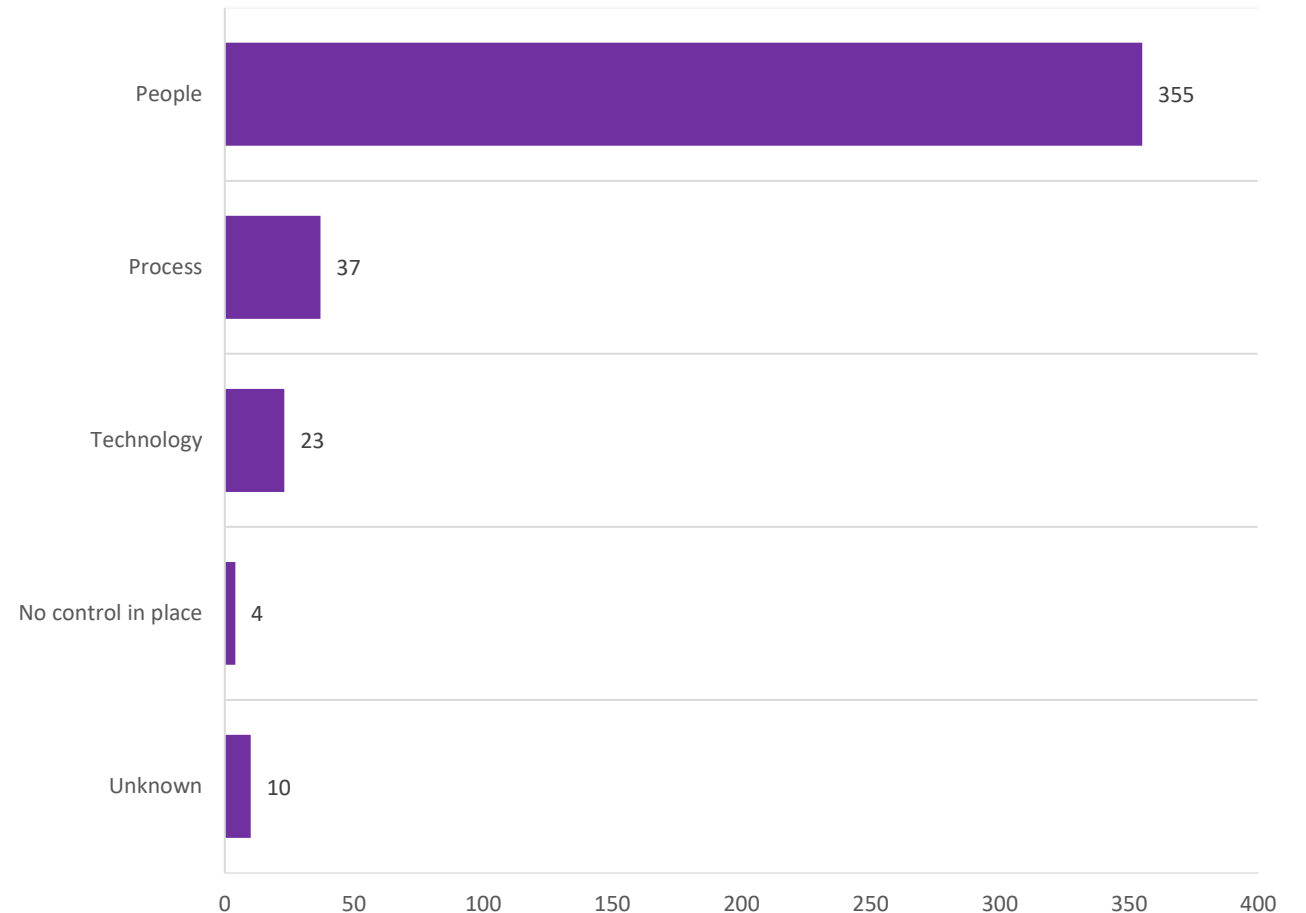




# Control areas



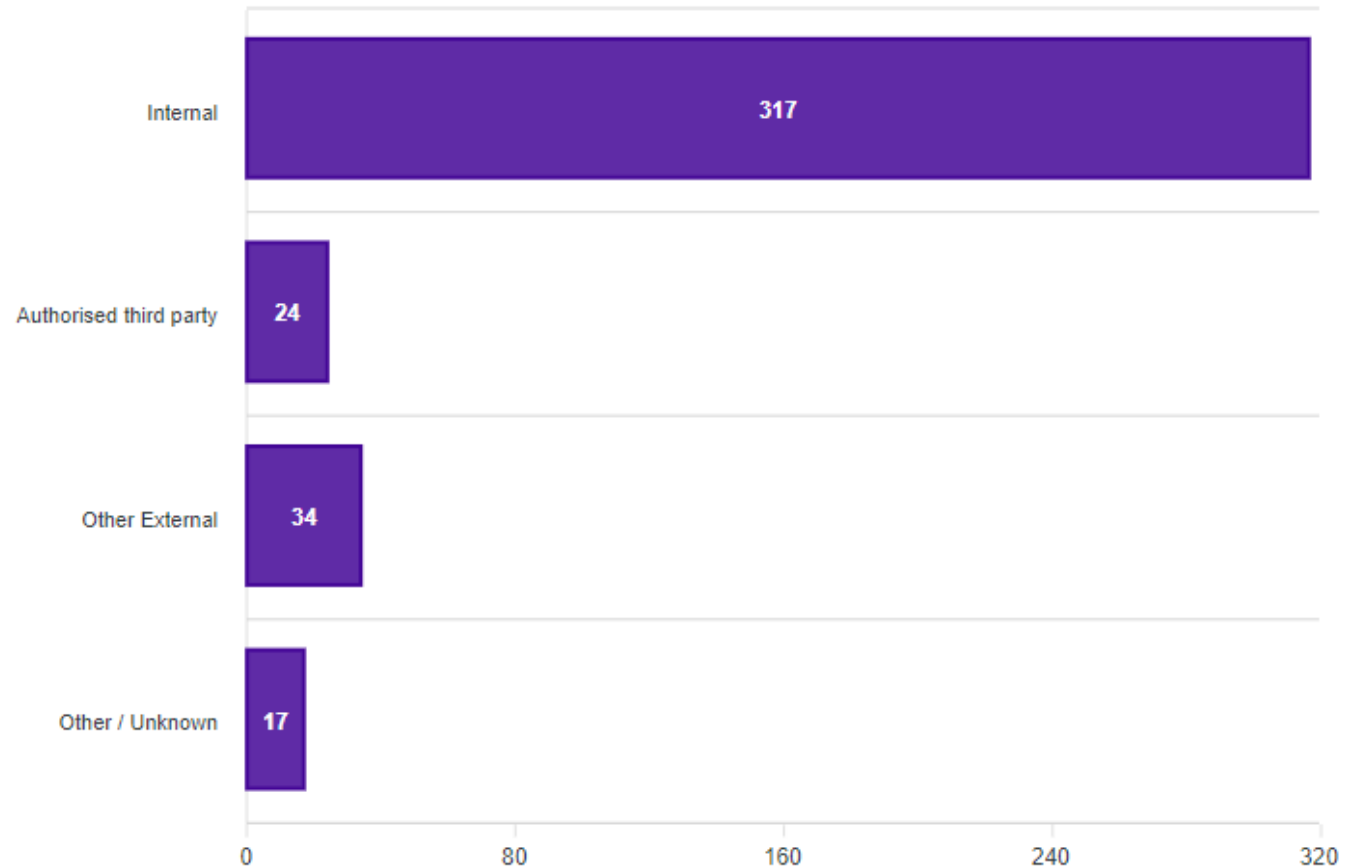
- **92%** of notifications related to **people**.
- The number of incidents caused by deficiencies in **process** was **10%**.
- In most (**83%**) occurrences where **process** was selected, **people** was also selected.
- **14** notifications where **technology** was selected on its own.
- **4** notifications (**1%**) where the incident occurred due to a **missing control(s)**.



# Threat actors



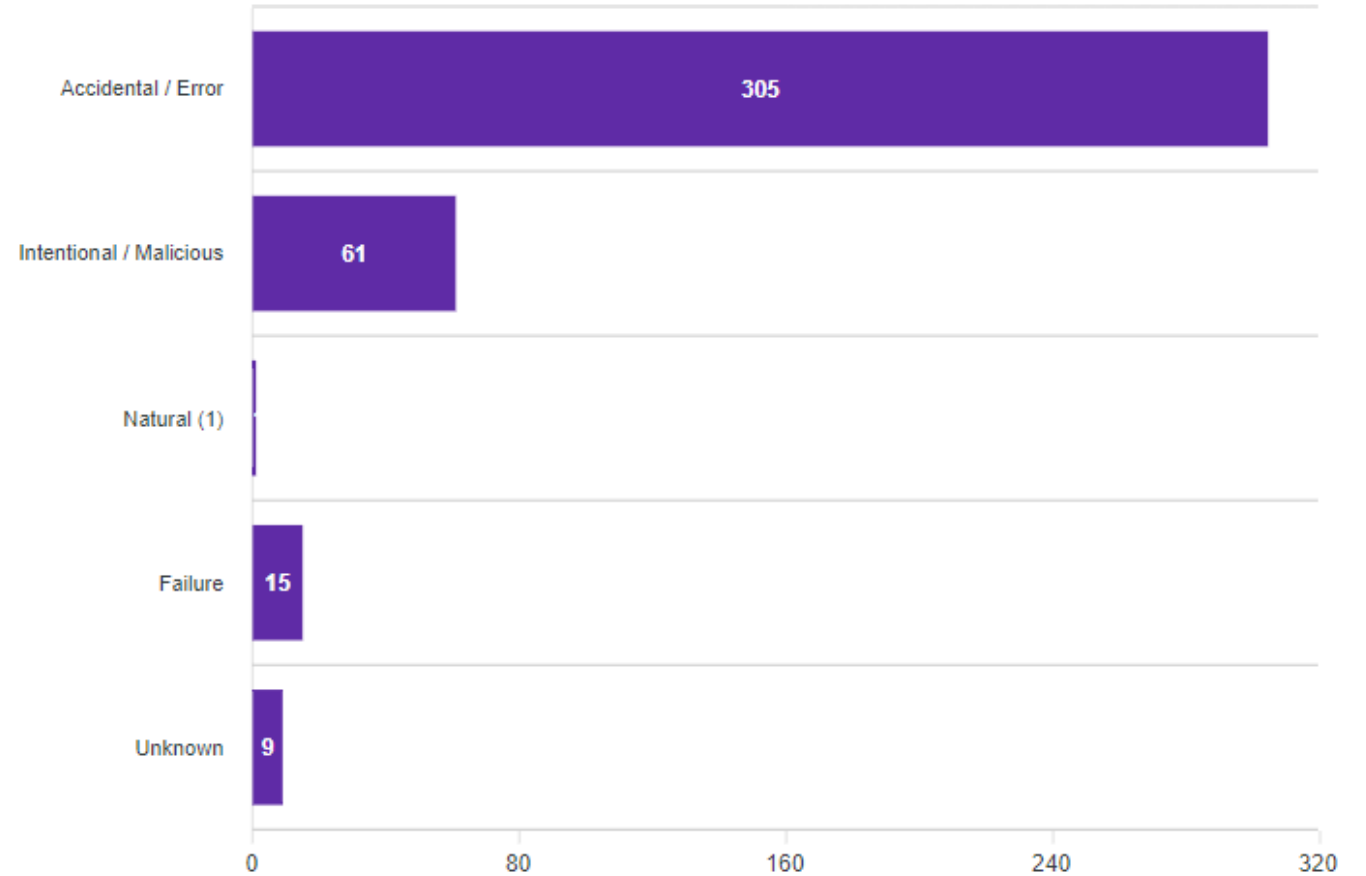
- 82% of notifications related to **internal staff**.
- 24 notifications related to **authorised third parties** such as contracted service providers.
- 17 notifications indicated that the threat actor could not be ascertained.



# Threat types



- 79% of notifications related to accidental actions.
- 16% of notifications related to intentional actions.



# Risk statements

The risk of...

Financial fraud

caused by...

Internal staff intentionally accessing customer accounts and changing bank details

resulting in...

Impact on organisation's finances  
Impact to individuals whose personal information was affected

CI

Unauthorised access to sensitive information

Malicious threat actor launching a cyber-attack on an authorised third-party who retained public sector information longer than the required timeframe

Impact on public services (reputation of, and confidence in, the organisation)  
Impact to individuals whose personal information was affected

C

Unauthorised access to/inability to access public sector information

Lost back up tapes during transit from authorised third party to public sector organisation

Impact to individuals whose personal information was affected  
Impact on service delivery

C  
A

*Questions?*

Contact the Information Security Unit  
[security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)

# Deputy Commissioner's Final Thoughts



**Rachel Dixon**

Deputy Commissioner  
Privacy and Data Protection



Please provide your feedback on the session via  
the Poll in MS Teams

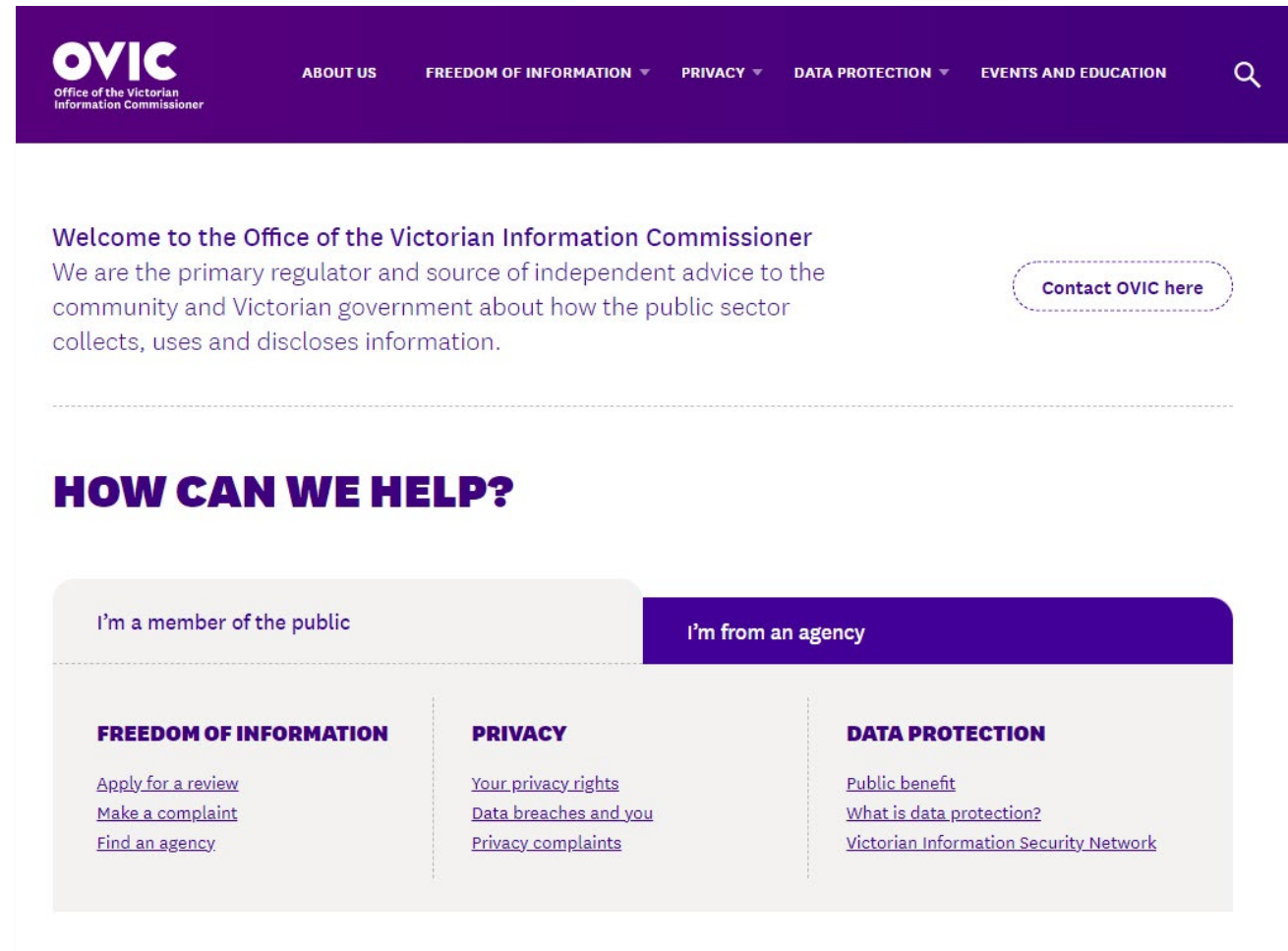
# Find out more

Visit the OVIC website to download our guidance material, read our examination reports, and find out more!

[ovic.vic.gov.au](https://ovic.vic.gov.au)

Contact the Information Security Unit

[security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)



The screenshot shows the OVIC website homepage. At the top is a purple navigation bar with the OVIC logo and the text 'Office of the Victorian Information Commissioner'. The navigation menu includes 'ABOUT US', 'FREEDOM OF INFORMATION', 'PRIVACY', 'DATA PROTECTION', and 'EVENTS AND EDUCATION', each with a dropdown arrow. A search icon is on the right. Below the navigation bar, the main content area has a white background. It starts with a welcome message: 'Welcome to the Office of the Victorian Information Commissioner. We are the primary regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses and discloses information.' To the right of this text is a button that says 'Contact OVIC here'. Below this is a section titled 'HOW CAN WE HELP?' in large purple letters. Underneath this title are two tabs: 'I'm a member of the public' (which is currently selected and highlighted in purple) and 'I'm from an agency'. Below the tabs are three columns of links. The first column, under 'FREEDOM OF INFORMATION', includes links for 'Apply for a review', 'Make a complaint', and 'Find an agency'. The second column, under 'PRIVACY', includes links for 'Your privacy rights', 'Data breaches and you', and 'Privacy complaints'. The third column, under 'DATA PROTECTION', includes links for 'Public benefit', 'What is data protection?', and 'Victorian Information Security Network'.