Incident Insights

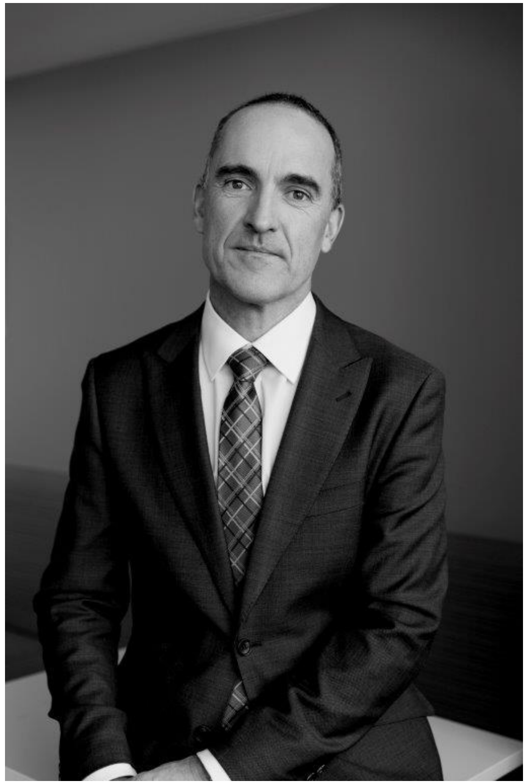
Victorian Information Security Network (VISN)
March 2023

OVIC
Office of the Victorian
Information Commissioner

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

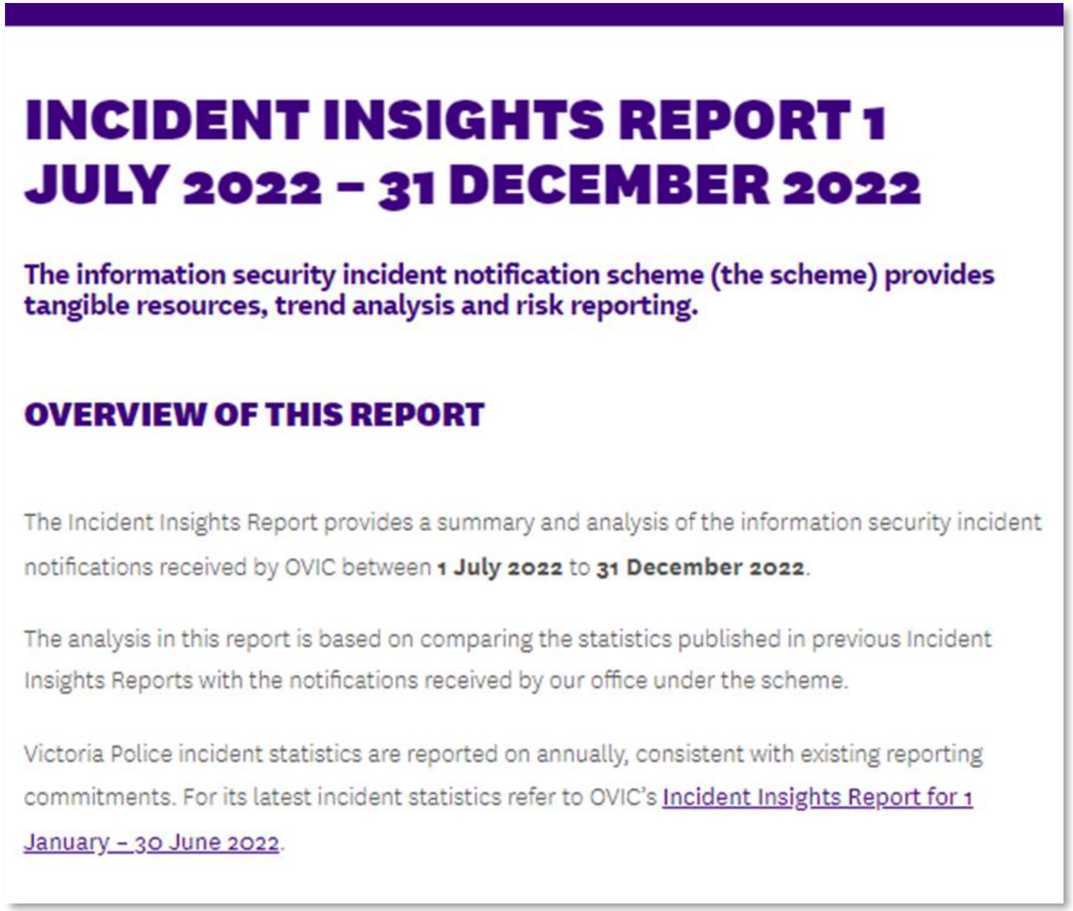
We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

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

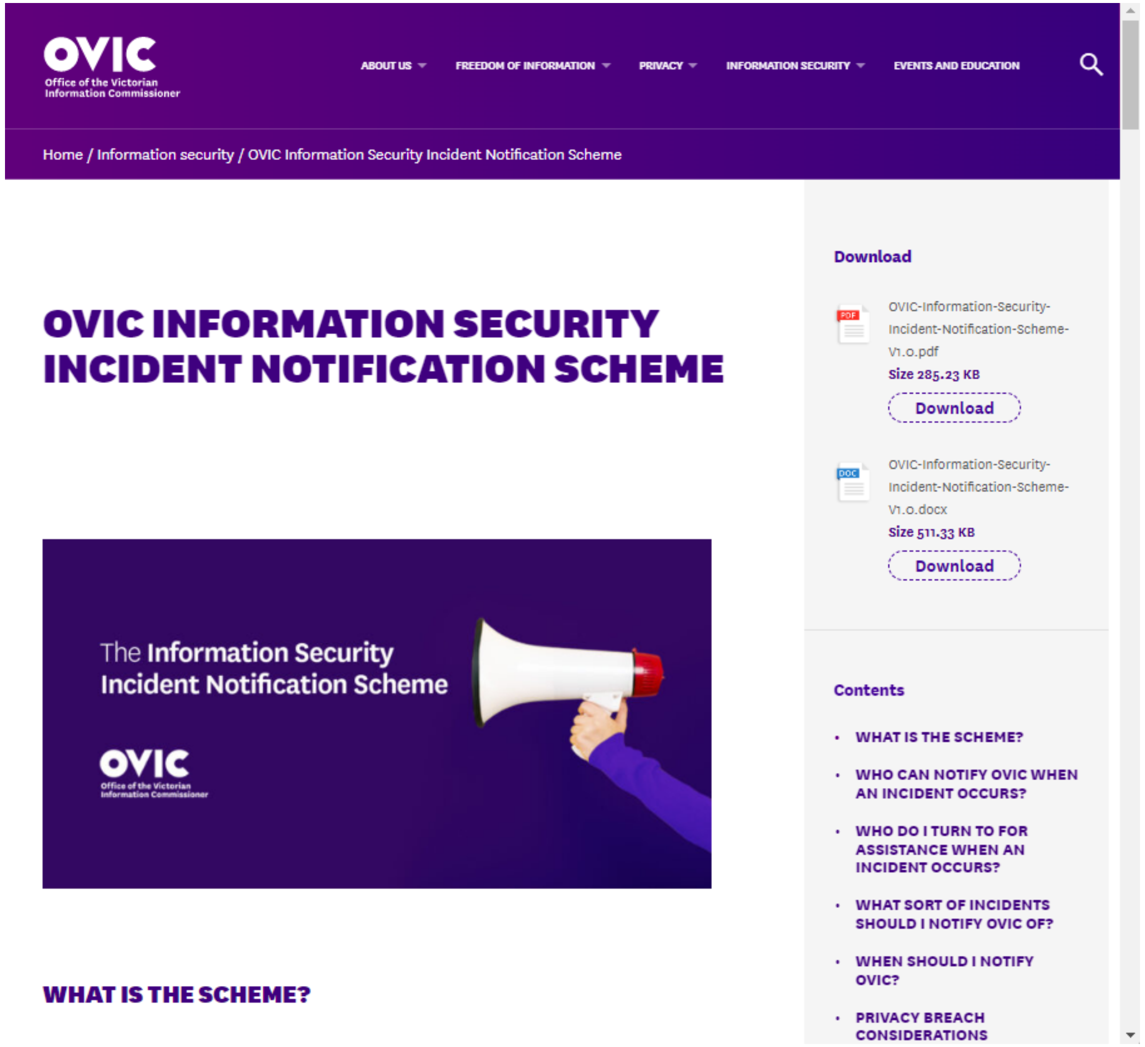
What is the Incident Notification Scheme?

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.


OVIC
Office of the Victorian Information Commissioner
ABOUT US
FREEDOM OF INFORMATION
PRIVACY
INFORMATION SECURITY
EVENTS AND EDUCATION
Home / Information security / OVIC Information Security Incident Notification Scheme
Download
Download
The Information Security Incident Notification Scheme
OVIC
Office of the Victorian Information Commissioner

OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME

Download

OVIC-Information-Security-Incident-Notification-Scheme-V1.0.pdf
Size 285.23 KB

OVIC-Information-Security-Incident-Notification-Scheme-V1.0.docx
Size 511.33 KB

Contents

- 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?
- PRIVACY BREACH CONSIDERATIONS

WHAT IS THE SCHEME?

The Latest Incident Insights Report
Themes and Trends

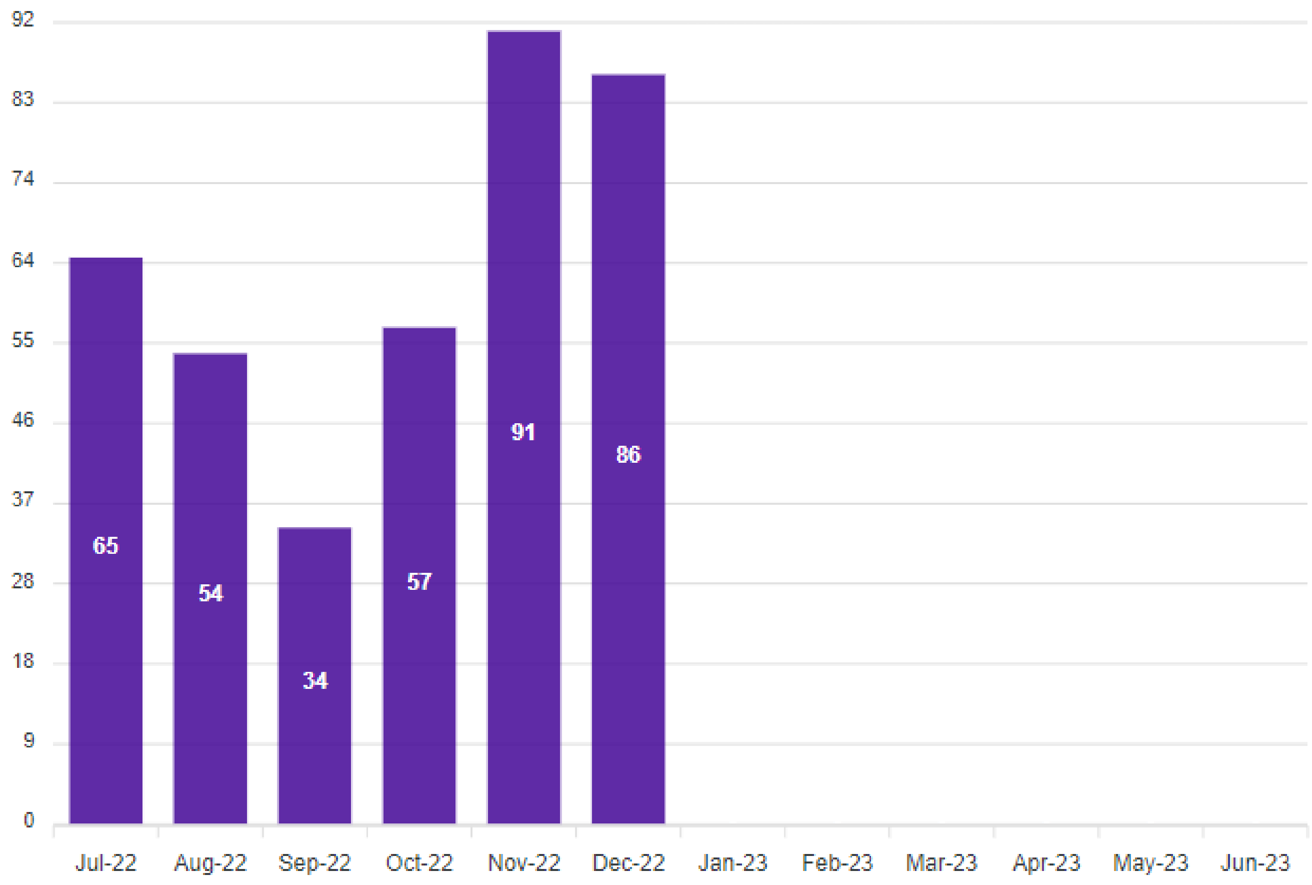
Anna Harris
Principal Advisor, Information Security - OVIC

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!

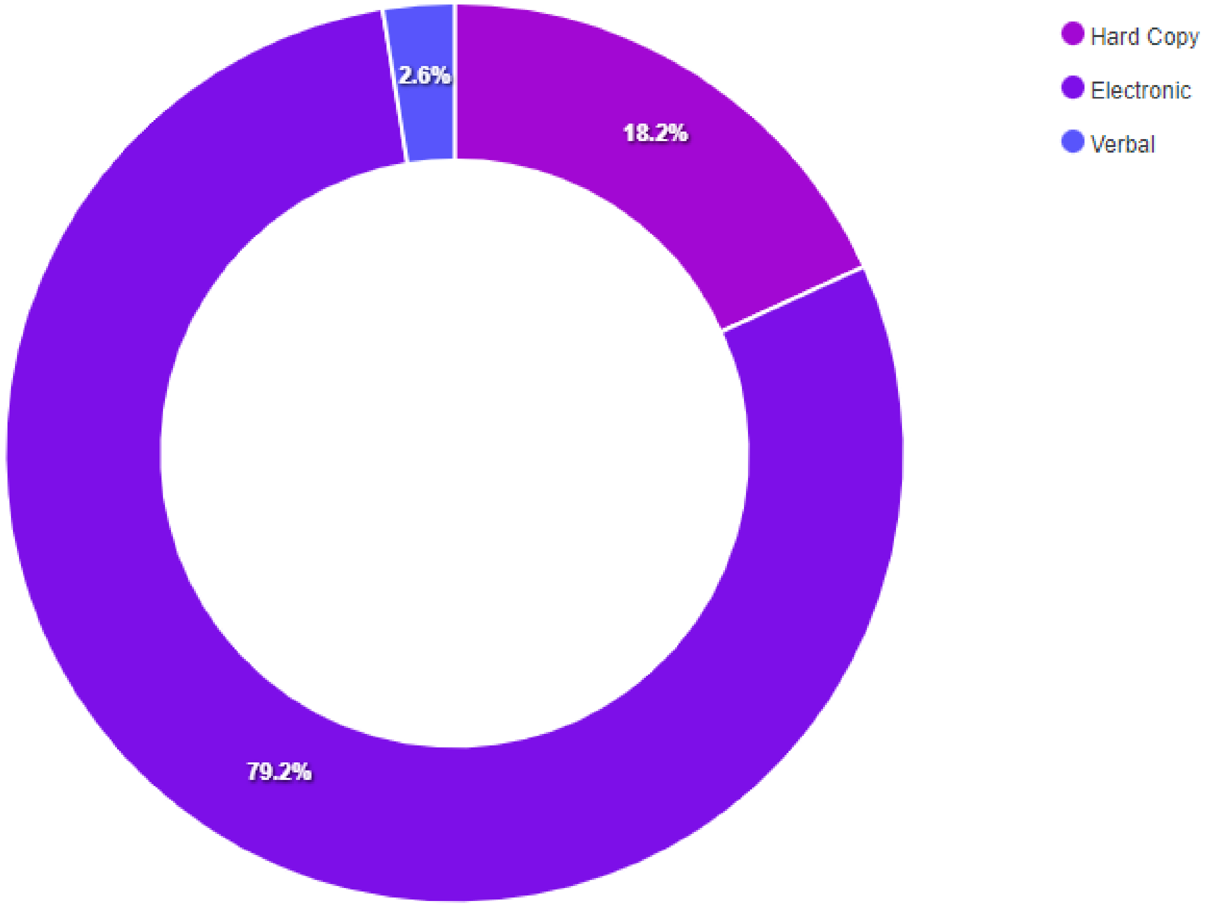
What was the most affected information format in the Jul-Dec reporting period?

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

Office of the Victorian
Information Commissioner

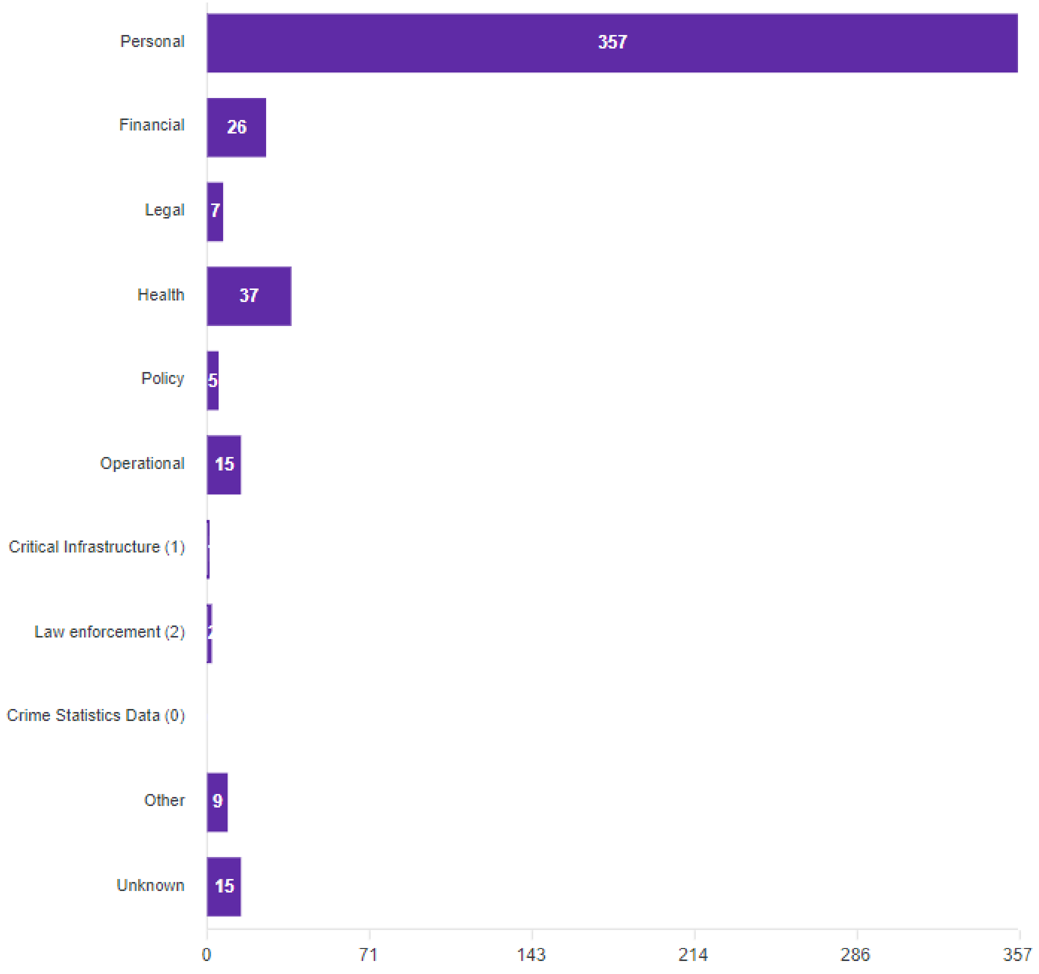
Information format

- **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**.



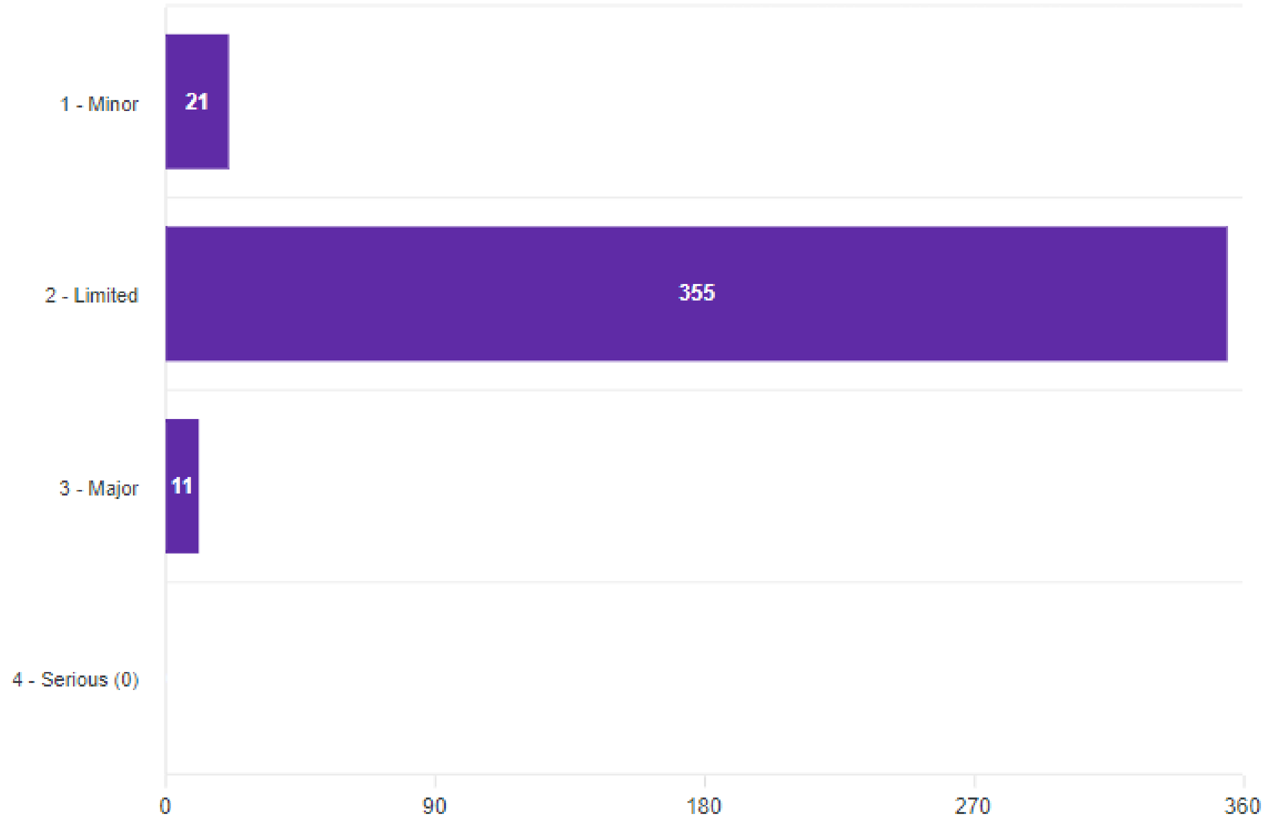
Information type

- **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.



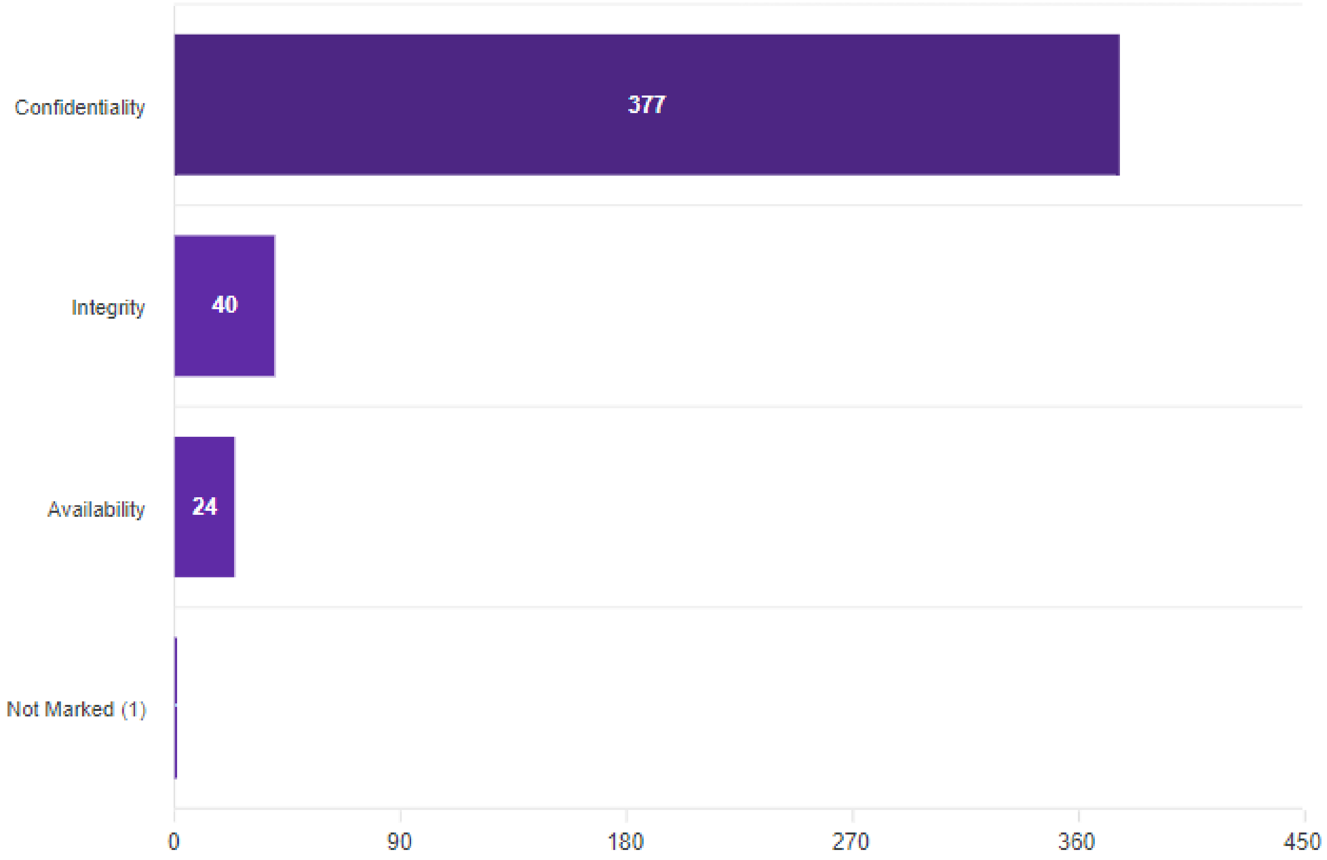
Quiz time!

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

A. Confidentiality
B. Integrity
C. Availability

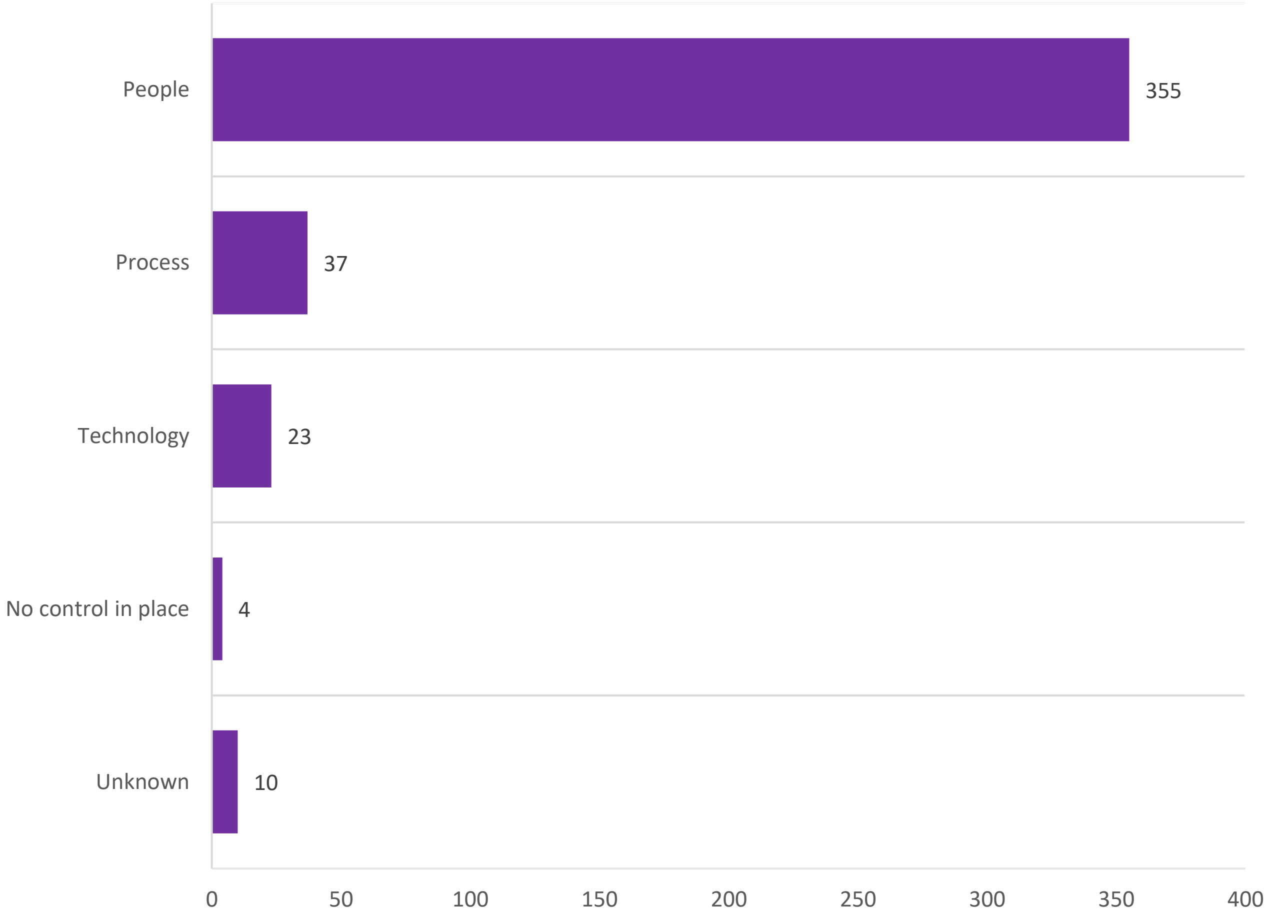
Security attributes

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



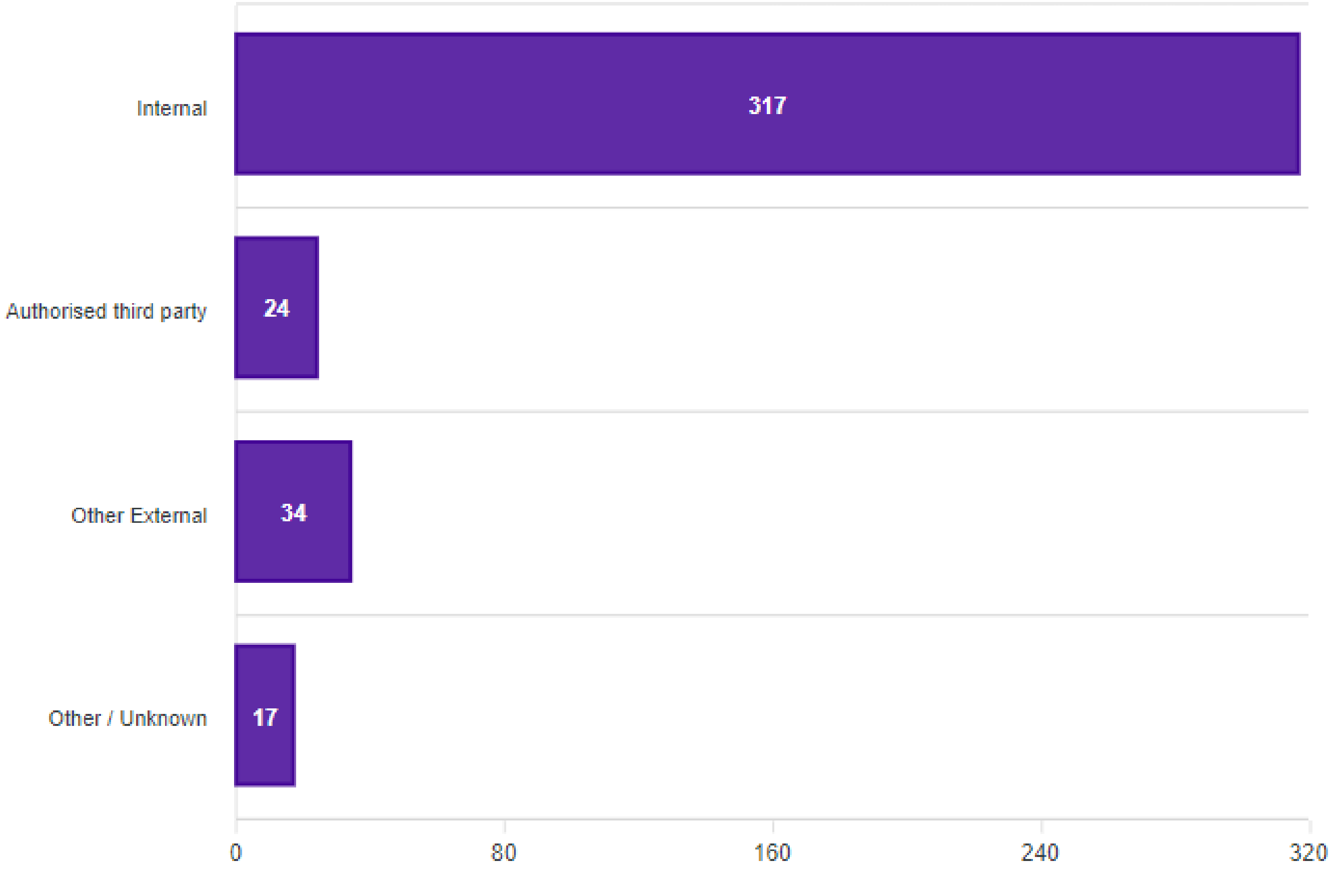
Control areas

- **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)**.



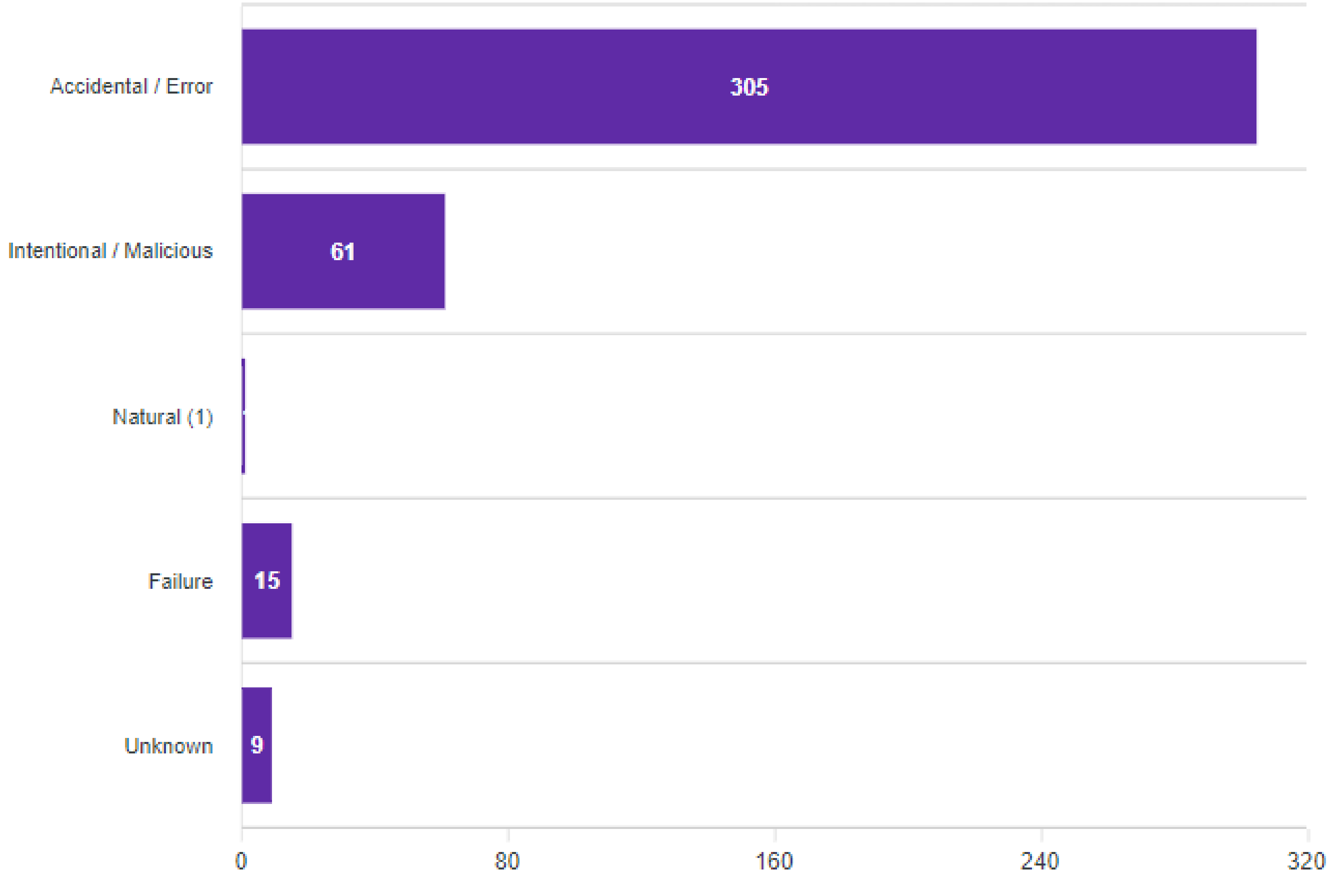
Threat actors

- **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…	caused by…	resulting in…	
Financial fraud	Internal staff intentionally accessing customer accounts and changing bank details	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

Recording to cease

Office of the Victorian
Information Commissioner

Incident Management

Victoria Police

Office of the Victorian Information Commissioner

Security Incident Registry (SIR)

- Security Incident Registry (SIR) was established in 2012.

- Focuses on isolation, containment and explores opportunities for remediation of security incidents.

Case Study 1

- A proactive audit was conducted identifying an employee exiting the organisation had moved sensitive information onto an external USB drive.

- A search warrant was conducted finding the employee had removed over 18,000 files.

- An arrest was made and person charged.

Case Study 2

- A proactive audit identified a sworn member conducted unauthorised checks whilst on extended leave.

- Criminal brief of evidence was prepared and the employee received disciplinary action.

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

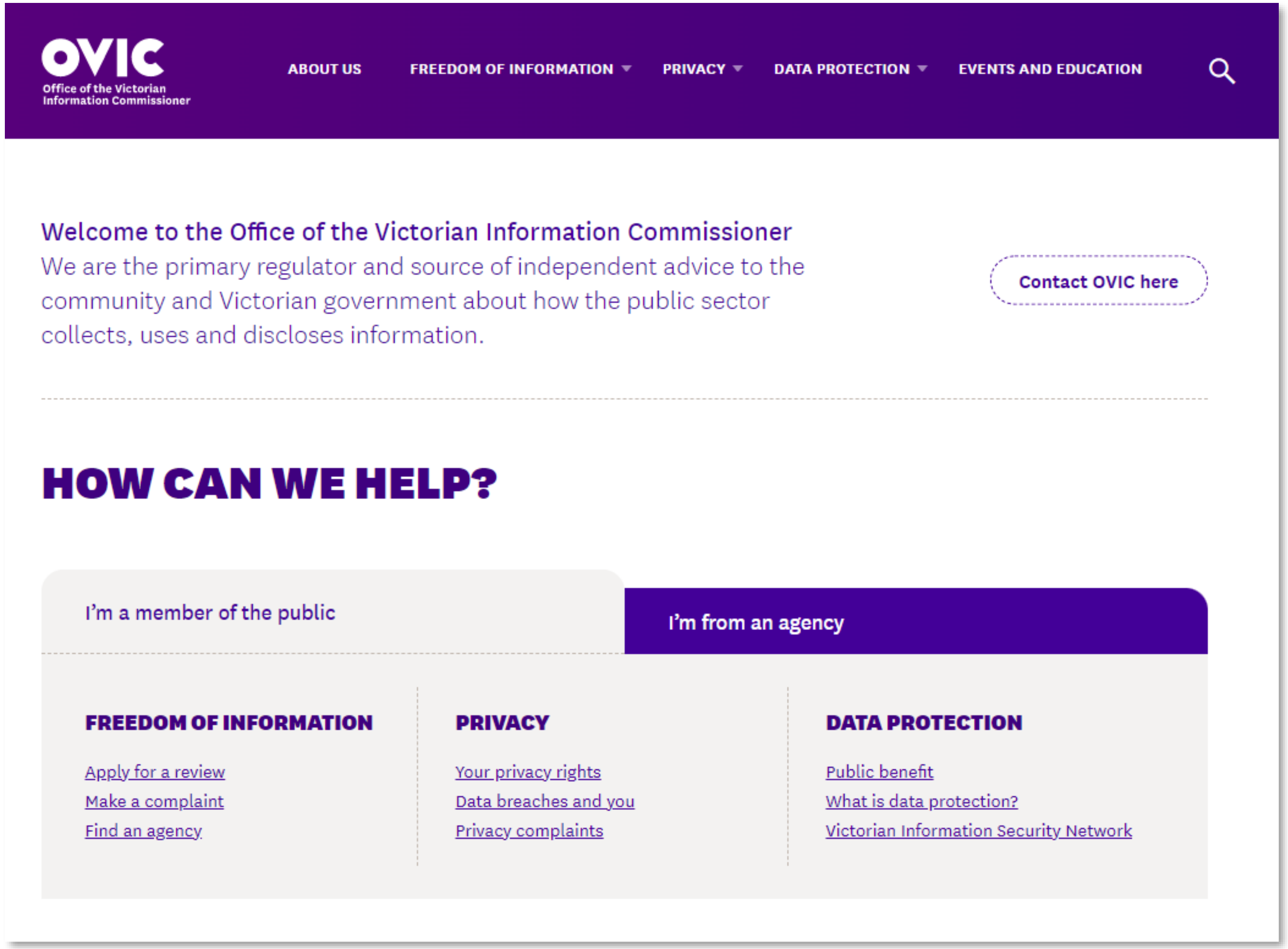
Find out more

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

ovic.vic.gov.au

Contact the Information Security Unit

security@ovic.vic.gov.au



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.

HOW CAN WE HELP?

FREEDOM OF INFORMATION

- Apply for a review
- Make a complaint
- Find an agency

PRIVACY

- Your privacy rights
- Data breaches and you
- Privacy complaints

DATA PROTECTION

- Public benefit
- What is data protection?
- Victorian Information Security Network