

Incident Insights Forum

Victorian Information Security Network (VISN)
November 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



Rachel Dixon

Acting Information Commissioner

INCIDENT INSIGHTS REPORT: 1 JANUARY 2023 – 30 JUNE 2023

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 January 2023** to **30 June 2023**.

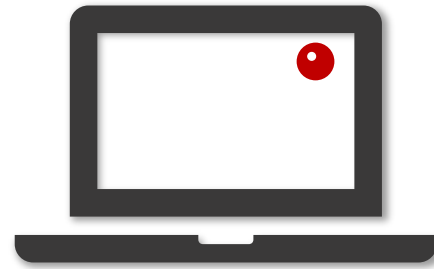
The analysis in this report is based on comparing the statistics published in previous Incident Insights Reports with the notifications received by our office under the scheme.

Victoria Police incident statistics are reported on annually, consistent with existing reporting commitments. These have been included towards the end of this report with comparisons made from our [Incident Insights Report for 1 January – 30 June 2022](#).

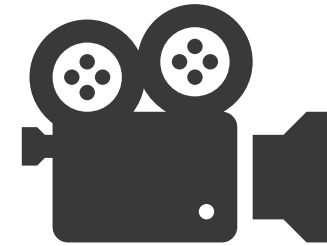
Housekeeping



Cameras and mics have been muted for **attendees**. If your Teams is running slow, try disconnecting from your VPN.

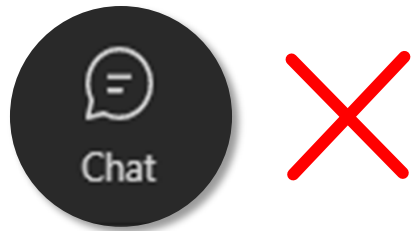
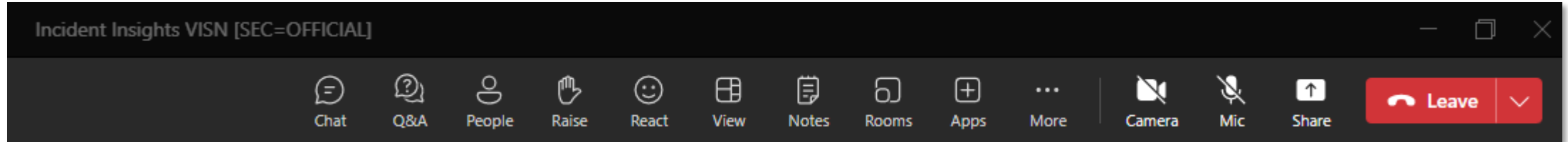


Today's session **is being recorded**.

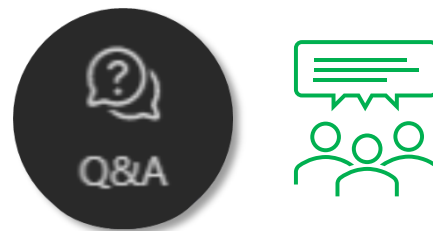


A copy of OVIC's **slides** and the **recording** will be made available in the coming days on OVIC's website.

Join the conversation



Regular **chat** functionality in Teams has been **disabled** in this forum.



Type your question into the
Teams Q&A channel.
You can choose to be **anonymous** or
leave your name displayed.



Each speaker will answer questions
following their presentation.
If you prefer to ask your question
verbally **raise your hand**.

What we'll explore today

- What is the Incident Notification Scheme?
- The latest Incident Insights Report – themes and trends
- AUSCERT
- ID CARE
- 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?

Under element E9.010, VPS organisations are required to notify OVIC of any **compromise of public sector information that may cause 'limited' (BIL 2) or higher** harm/damage to government operations, organisations, or individuals.

This includes information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET.

A screenshot of the OVIC website's 'Information Security Incident Notification Scheme' page. The page has a purple header with the OVIC logo and navigation links. The main content area features the title 'OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME' in large purple letters. Below this is a banner image showing a hand holding a megaphone against a dark background with the text 'The Information Security Incident Notification Scheme' and the OVIC logo. A 'Download' section on the right lists two PDF documents for download. A 'Contents' section on the right lists the page's structure. The footer of the page includes the text 'WHAT IS THE SCHEME?'

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

OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME

Download

OVIC-Information-Security-Incident-Notification-Scheme-V1.o.pdf
Size 285.23 KB
[Download](#)

OVIC-Information-Security-Incident-Notification-Scheme-V1.o.docx
Size 511.33 KB
[Download](#)

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?

*Themes and trends from the latest Incident
Insights Report*

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

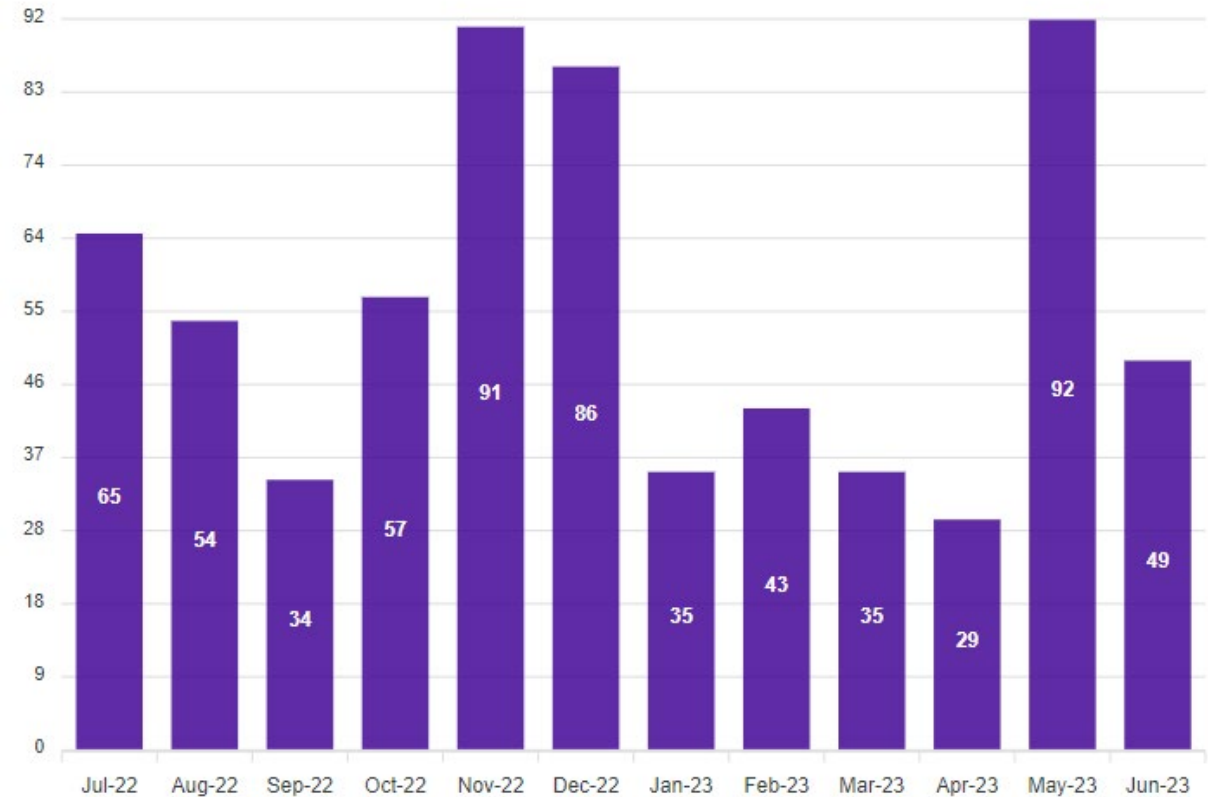


Threat
types

Volume - Notifications by month



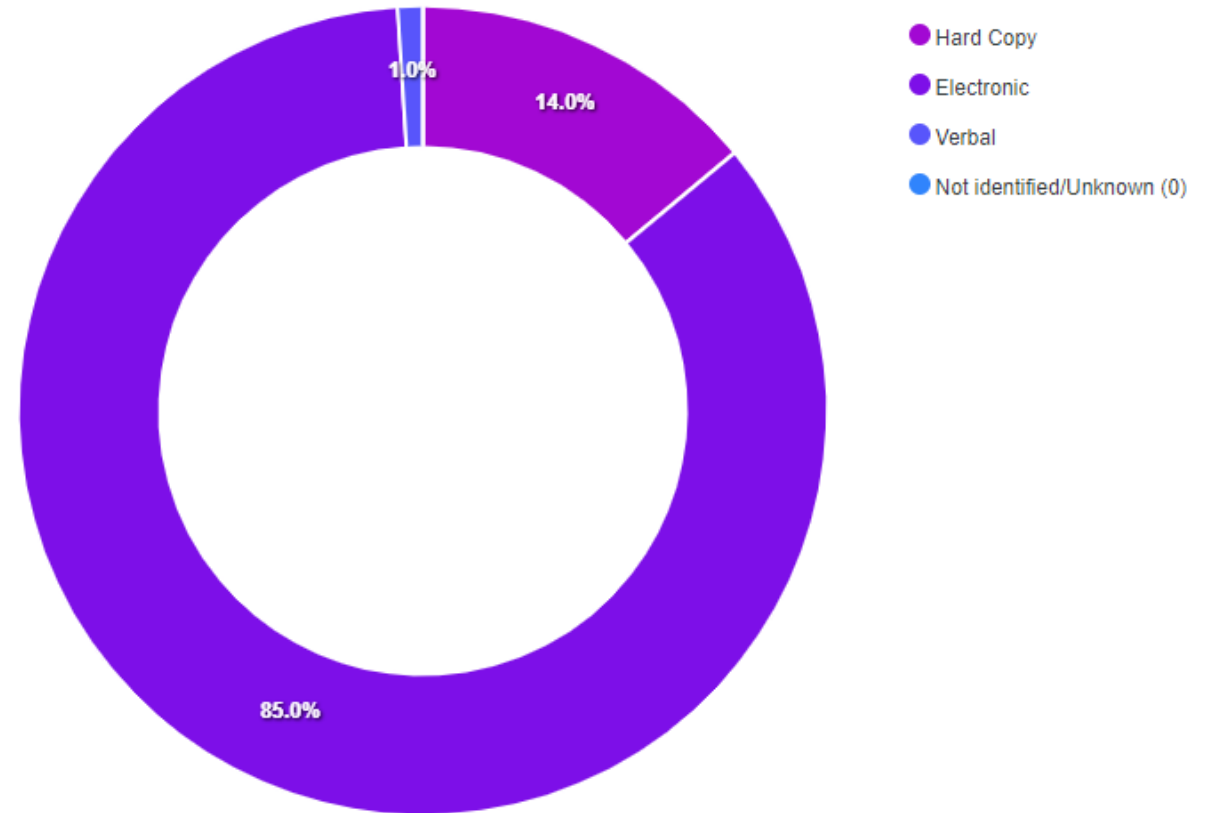
- OVIC received **283** notifications between **1 January to 30 June 2023** (inclusive).
- This is a **2%** decrease compared to the same time last year.



Information format



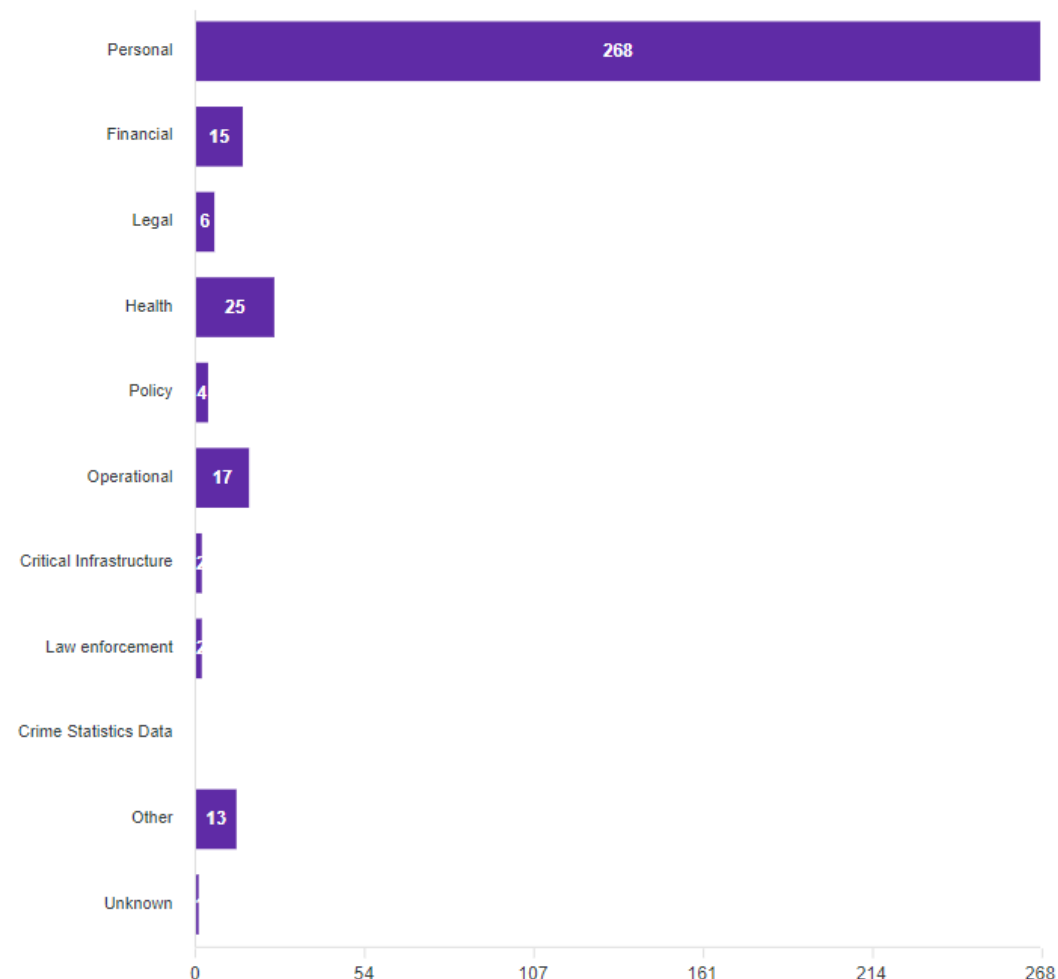
- 242 notifications indicate compromises of **electronic information**.
- More than half of the incidents affecting electronic information related to emails - predominantly **sending emails to the incorrect recipient**.
- **60%** of incidents involving hard copy information were related to **mail**.



Information type



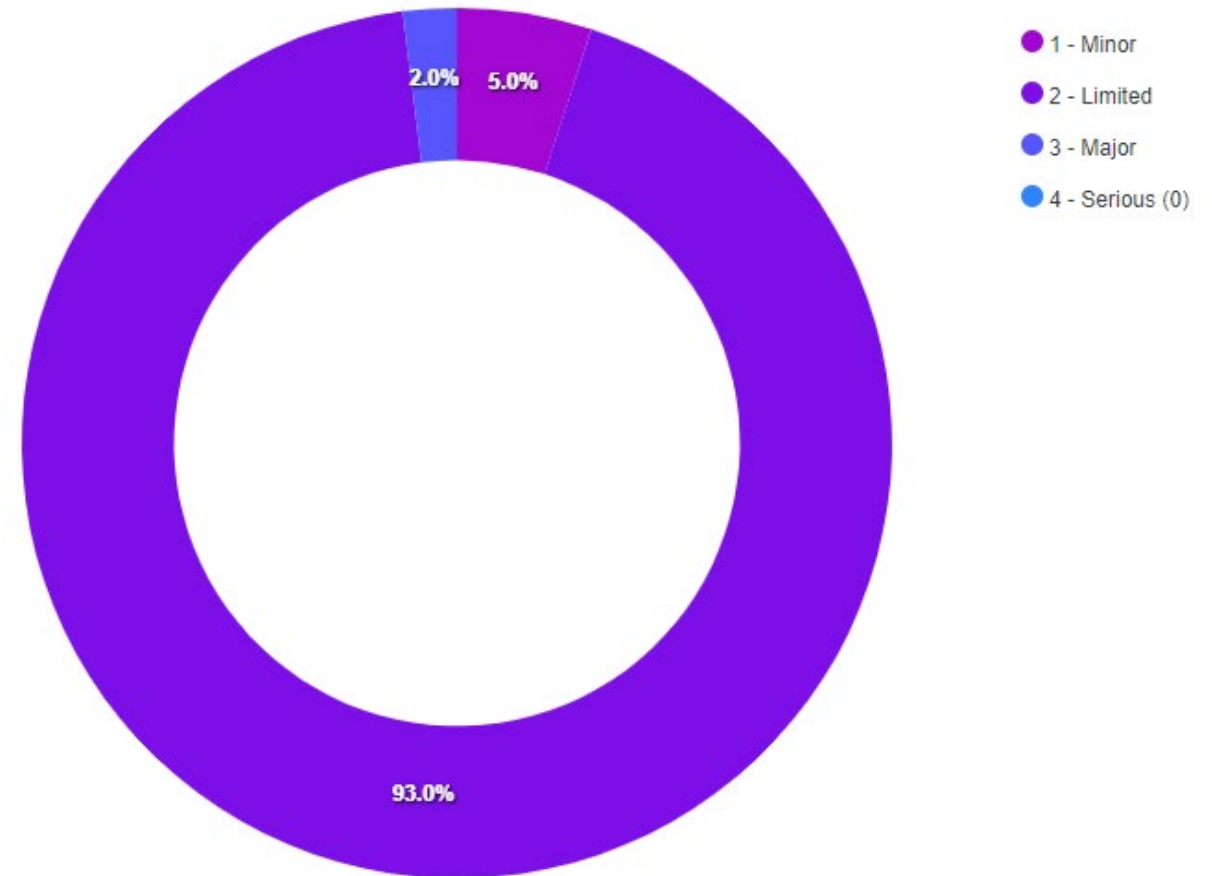
- **95%** incident notifications indicate compromises of **personal** information.
- **15%** incident notifications involved more than one information type.
- There were **13** notifications that selected **Other** e.g., cabinet information, credentials, or claim numbers.



Business Impact Level (BIL)



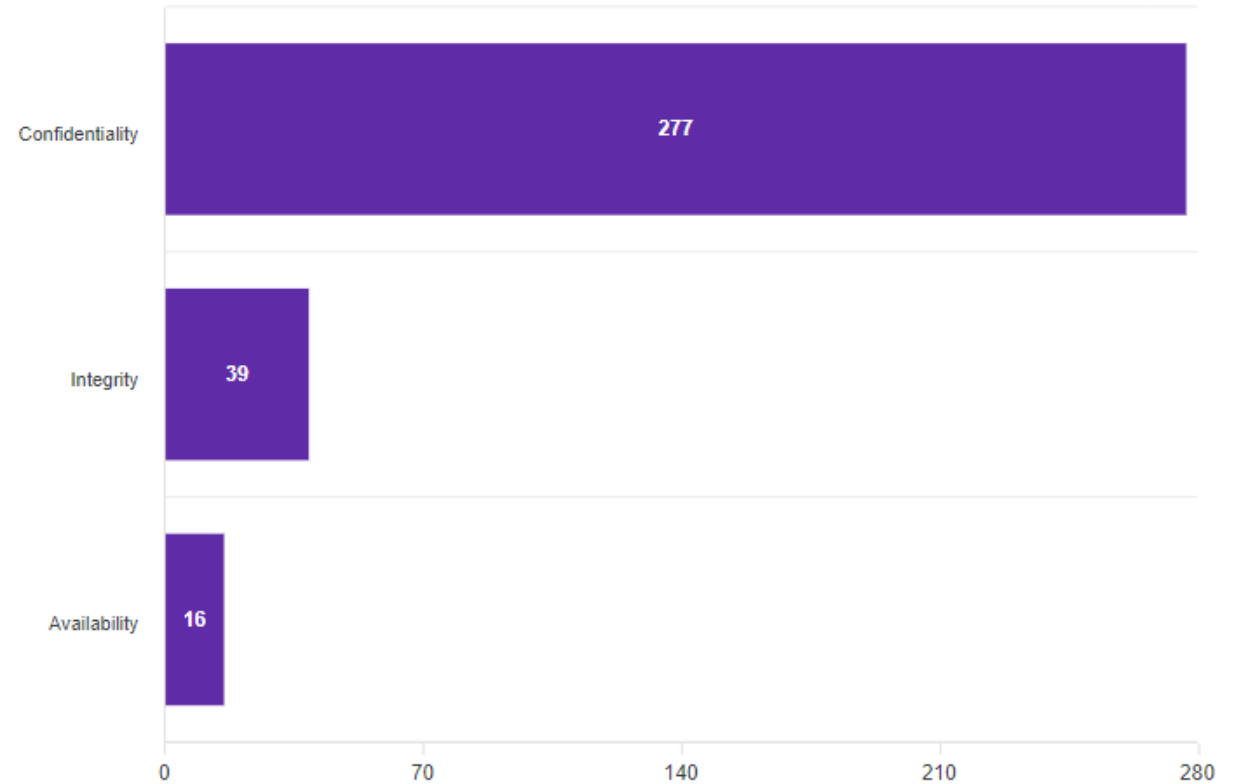
- **93%** of incidents were assessed as impacting BIL 2 (Limited harm or damage) to information.
- **6** incident notifications nominated BIL 3. Just half compared to the last reporting period.
- If in doubt of the BIL just notify.



Security attributes



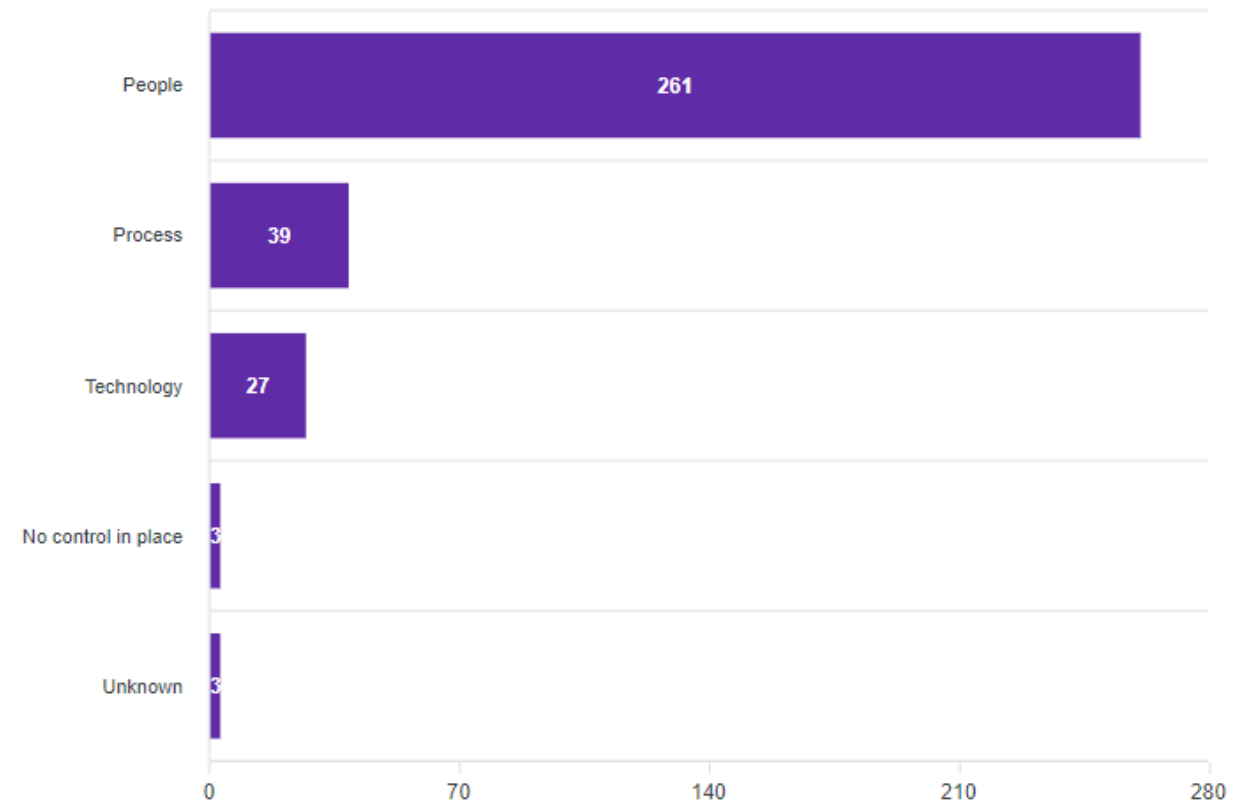
- **98%** of incident notifications indicate compromises of the **confidentiality** of information.
- **16%** of incident notifications selected more than one option for this field.



Control areas



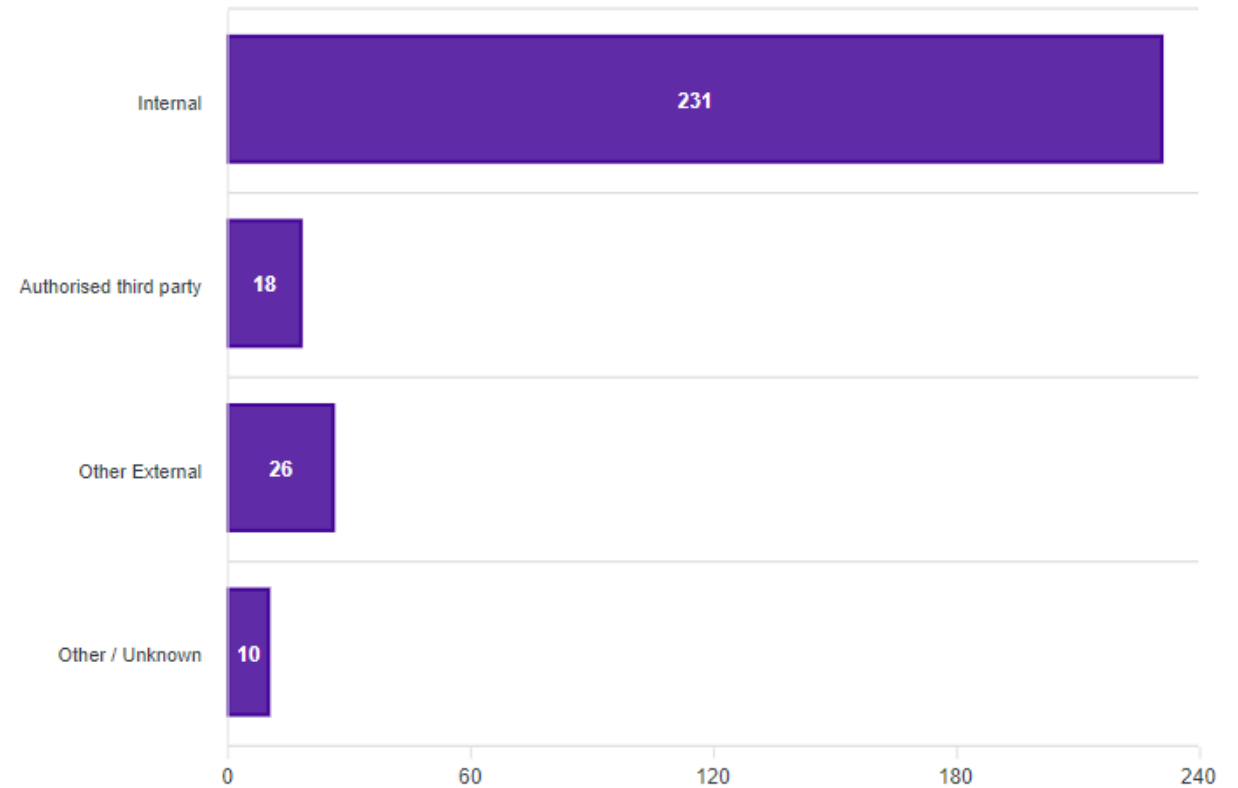
- 92% of notifications related to **people**.
- 9 notifications where **process** was selected on its own.
- 8 notifications where **technology** was selected on its own.
- 8 notifications where all three control areas were nominated as causal factors.
- 3 notifications (1%) where the incident occurred due to a **missing control(s)**.



Threat actors



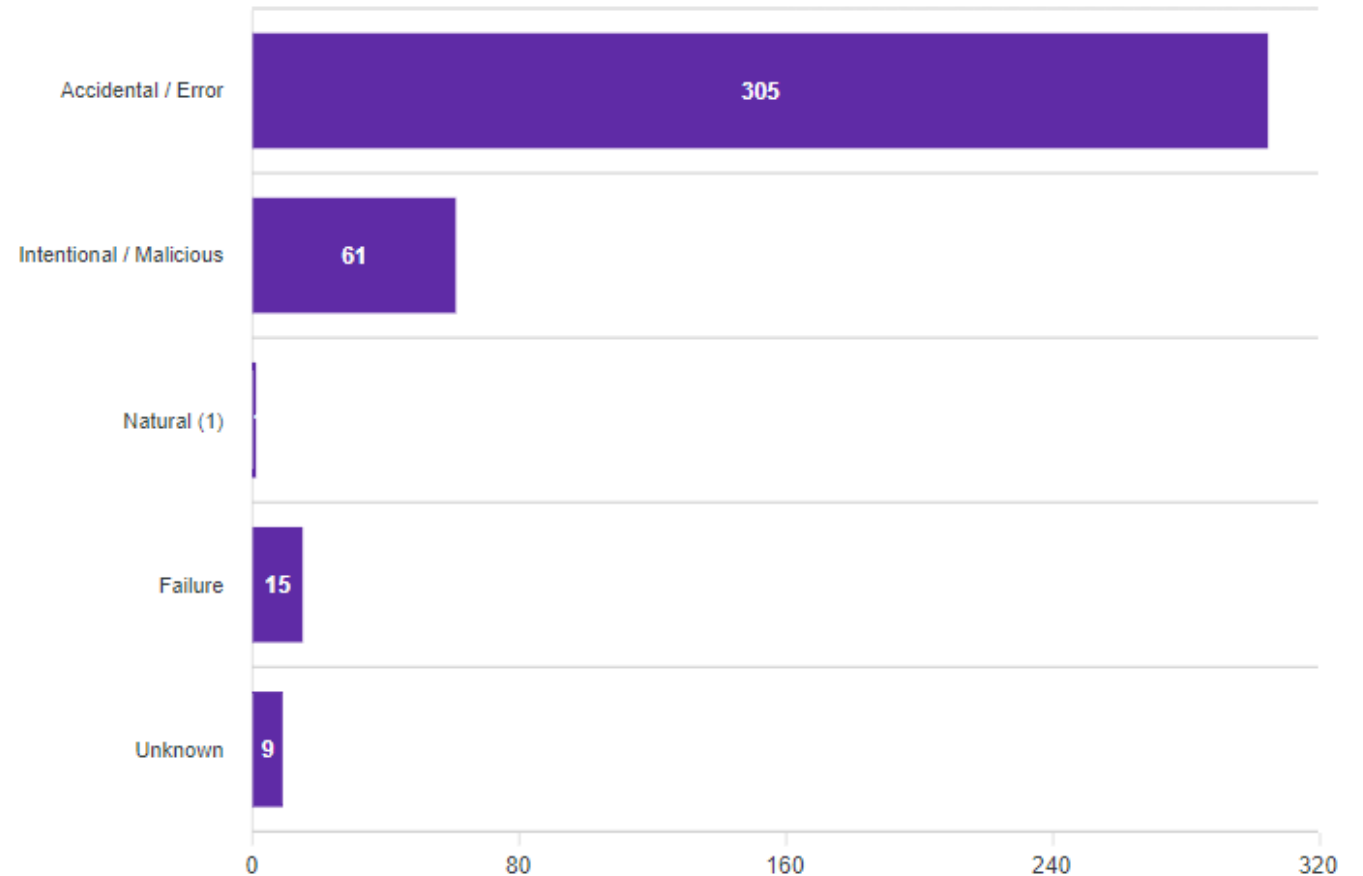
- 82% of notifications related to **internal staff**.
- **18** notifications related to **authorised third parties** such as contracted service providers.
- **10** notifications indicated that the threat actor could not be ascertained.



Threat types



- 82% of notifications related to accidental actions.
- 14% of notifications related to intentional actions.



Risk statements

The risk of...

caused by...

resulting in...

Poor data quality

Internal staff manually processing an application and inadvertently linking it to the wrong case

Impact on public services (reputation of, and confidence in, the organisation)

Impact to individuals whose personal information was affected

I

Unauthorised access to / inability to access public sector information

Thieves breaking into an authorised third-party premises and stealing a book / hard copy files and hard drive

Impact on service delivery

Impact on public services (reputation of, and confidence in, the organisation)

C
A

Unauthorised access to public sector information

Malicious threat actor hacking third party application account credentials that are the same as credentials used on VPS systems to either access public sector systems or publish on dark web

Impact on public services (reputation of, and confidence in, the organisation)

Impact on service delivery

Impact to individuals whose personal information was affected

CI
A

Questions for OVIC?

Contact the Information Security Unit
security@ovic.vic.gov.au



Mike Holm
AusCERT – Senior Manager

Note: The AUSCERT slides captured in the video recording of this session, reference the Traffic Light Protocol (TLP) which impose similar conditions to protective markings. TLPs indicate what information can be shared with different audiences and use four colours to communicate this.

*Some slides are marked **TLP:AMBER**, which typically restricts the sharing of contents to participants' organization and its clients. In this setting, AUSCERT have subsequently confirmed that this means "the public of Victoria and wider Australia"*



Prita Jobling-Baker
ID CARE – Team leader, Complex Cases and Incident
Response

Note: The IDCARE slides are captured in the video recording of this session.

Deputy Commissioner's Final Thoughts



Cara O'Shanassy

Acting Deputy Commissioner
Privacy and Data Protection



Find out more

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

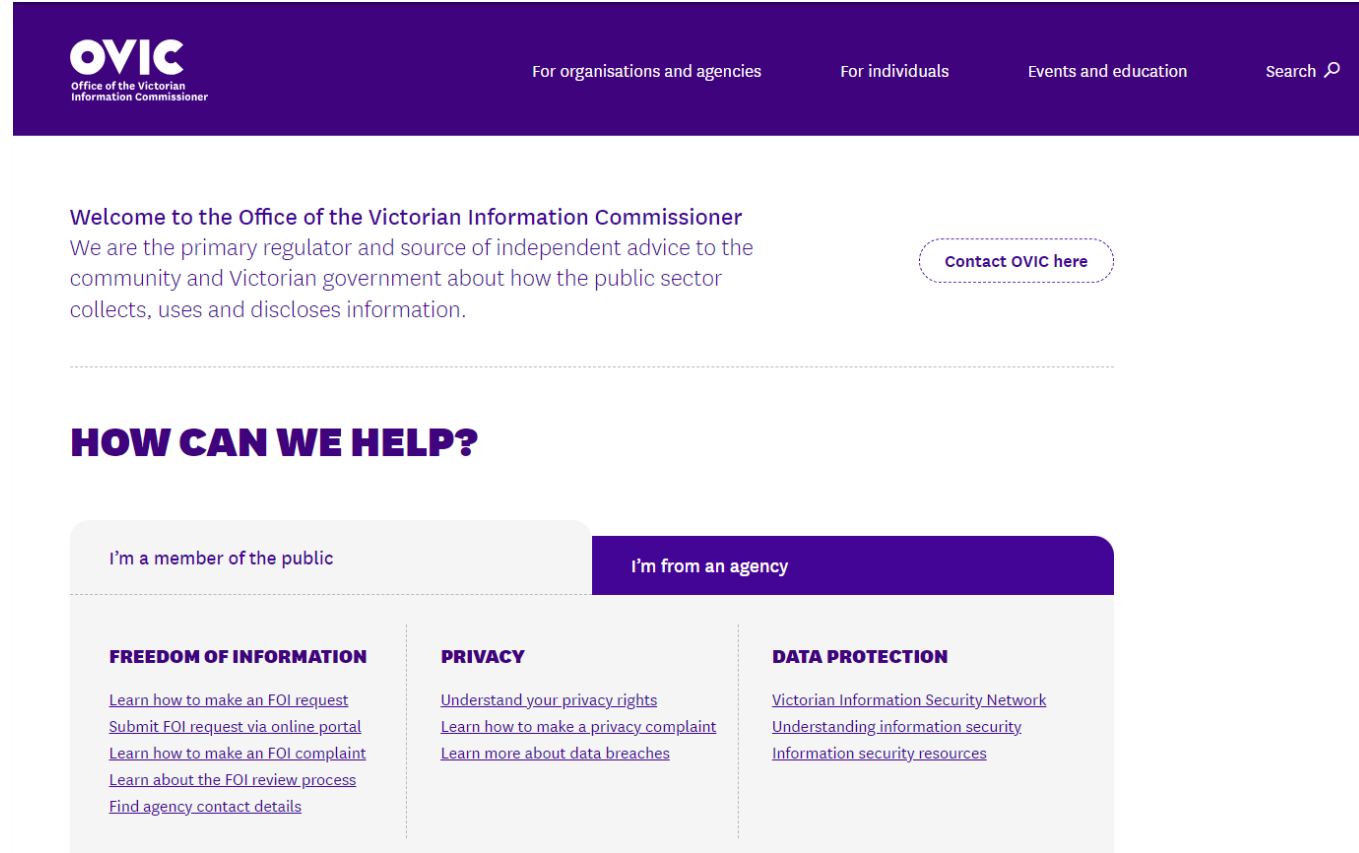
ovic.vic.gov.au

Contact the Information Security Unit by emailing

security@ovic.vic.gov.au

incidents@ovic.vic.gov.au

Or call 1300 00 OVIC



The screenshot shows the OVIC website homepage. The header is dark blue with the OVIC logo (Office of the Victorian Information Commissioner) on the left and navigation links for 'For organisations and agencies', 'For individuals', 'Events and education', and a search icon on the right. The main content area is white. It features a welcome message from the Office of the Victorian Information Commissioner, stating they are the primary regulator and source of independent advice. A 'Contact OVIC here' button is located to the right of the welcome message. Below this is a section titled 'HOW CAN WE HELP?' with two tabs: 'I'm a member of the public' (selected) and 'I'm from an agency'. Under the 'I'm a member of the public' tab, there are three columns: 'FREEDOM OF INFORMATION' with links to learn how to make an FOI request, submit FOI request via online portal, learn how to make an FOI complaint, learn about the FOI review process, and find agency contact details; 'PRIVACY' with links to understand privacy rights, learn how to make a privacy complaint, and learn more about data breaches; and 'DATA PROTECTION' with links to the Victorian Information Security Network, understanding information security, and information security resources.

OVIC
Office of the Victorian
Information Commissioner

For organisations and agencies For individuals Events and education Search

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.

Contact OVIC here

HOW CAN WE HELP?

I'm a member of the public I'm from an agency

FREEDOM OF INFORMATION
[Learn how to make an FOI request](#)
[Submit FOI request via online portal](#)
[Learn how to make an FOI complaint](#)
[Learn about the FOI review process](#)
[Find agency contact details](#)

PRIVACY
[Understand your privacy rights](#)
[Learn how to make a privacy complaint](#)
[Learn more about data breaches](#)

DATA PROTECTION
[Victorian Information Security Network](#)
[Understanding information security](#)
[Information security resources](#)