OVIC
Office of the Victorian Information Commissioner

Information Security Incident Insights Forum

Victorian Information Security Network (**VISN**)
November 2024

A reminder – Some of today's session
is being recorded.

Acknowledgment of Country

Sean Morrison

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

Sean Morrison

Information Commissioner

Incident Insights Reports

Report for 1 July 2023 to 31 December 2023

Report for 1 January to 30 June 2023

Report for 1 July to 31 December 2022

Report for 1 January to 30 June 2022

Report for 1 July 2021 to 31 December 2021

Report for 1 January 2021 to 30 June 2021

Report for 1 July 2020 to 31 December 2020

Report for 29 October 2019 to 30 June 2020

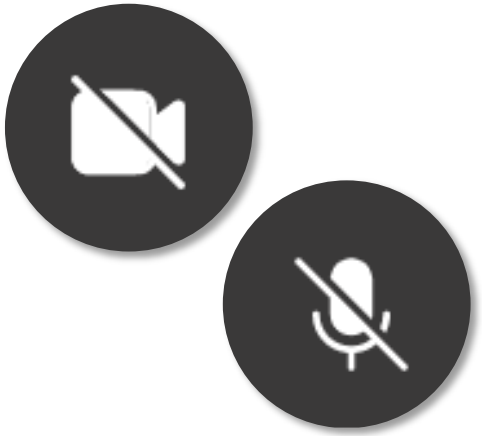
https://ovic.vic.gov.au/information-security/security-insights/

Information Security Unit

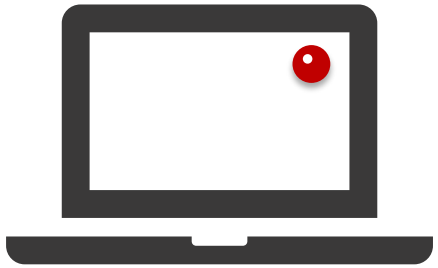
Anthony Corso

Assistant Commissioner – Information Security

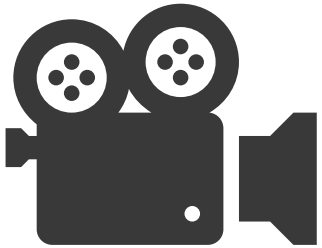
Housekeeping



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

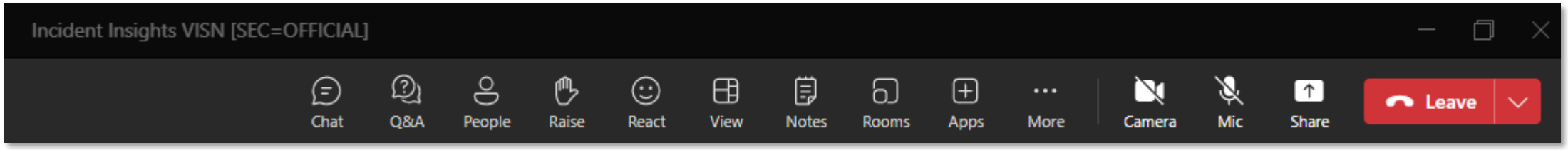


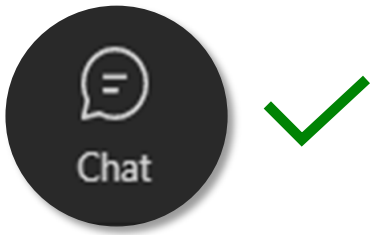
Today's session **is being recorded.**



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 is **enabled** in this forum. Your name will be displayed against any questions you post.

If you want to ask an **anonymous question,** type your question into the **Teams Q&A channel**.

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

What we'll explore today

- A bit about the Information Security Incident Notification Scheme
- The latest Incident Insights Report – themes and trends
- Guest speaker from Victoria Police – Cybercrime Division
- Session close

Information Security 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.

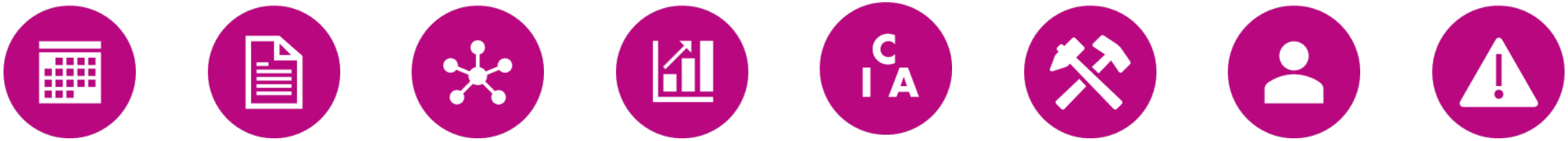
What sort of incidents need to be notified to OVIC?

- Under VPDSS element E9.010, VPS organisations are required to notify OVIC of any adverse impact on the **confidentiality, integrity, or availability** of public sector information with a **business impact level (BIL) of 2 (limited) or higher**.
- This includes information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET.

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

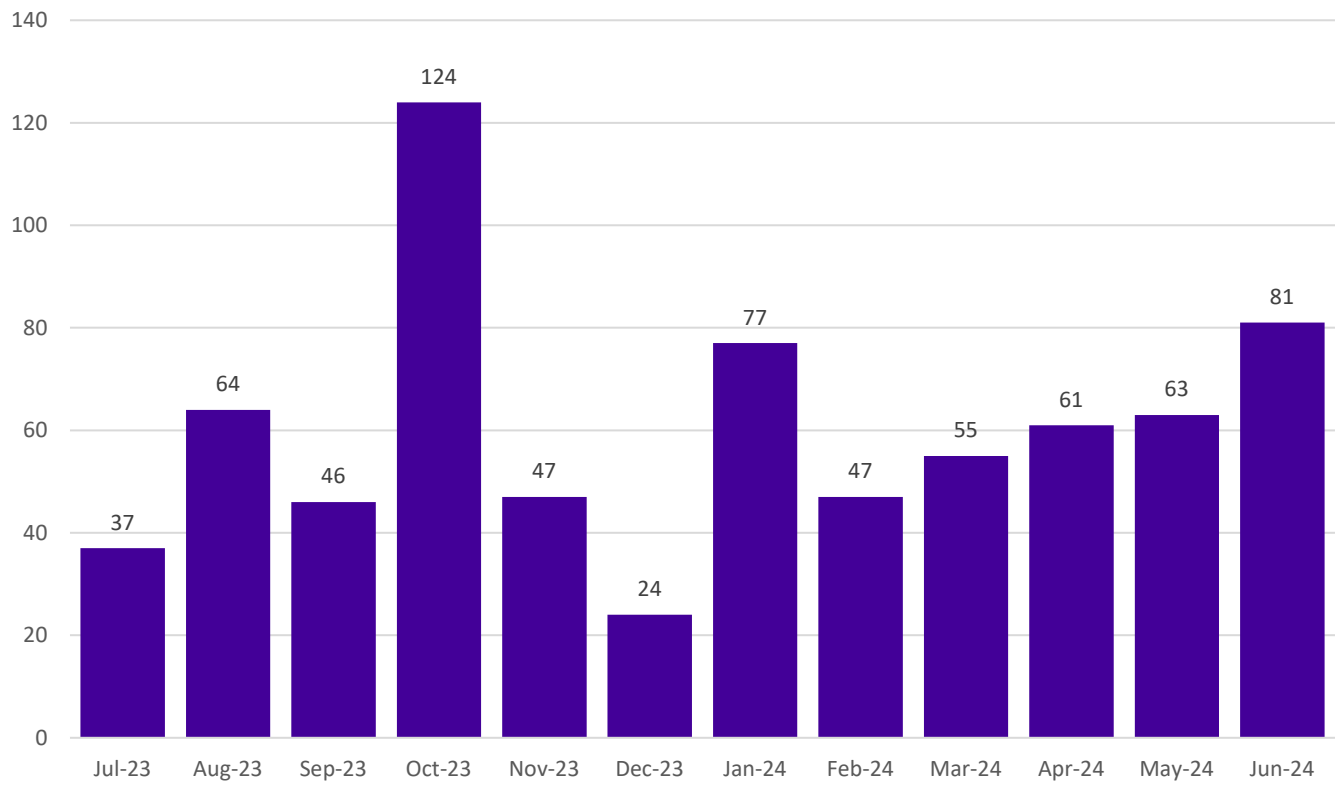
Control areas

Threat actors

Threat types

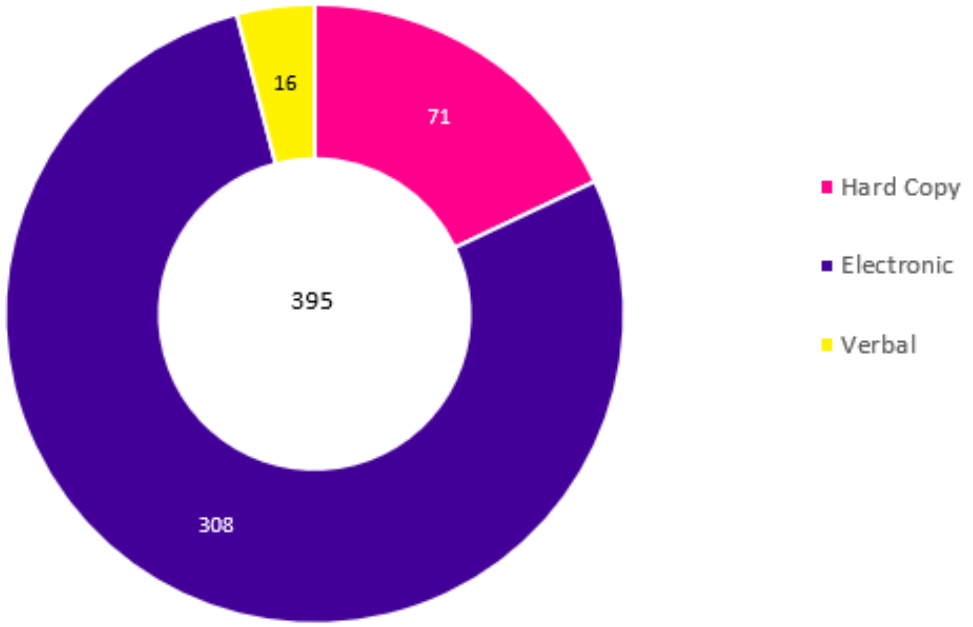
Volume – Notifications by month

- OVIC received **384** notifications between **1 January** to **30 June 2024**.
- This is a **12%** increase compared to the previous notification period.



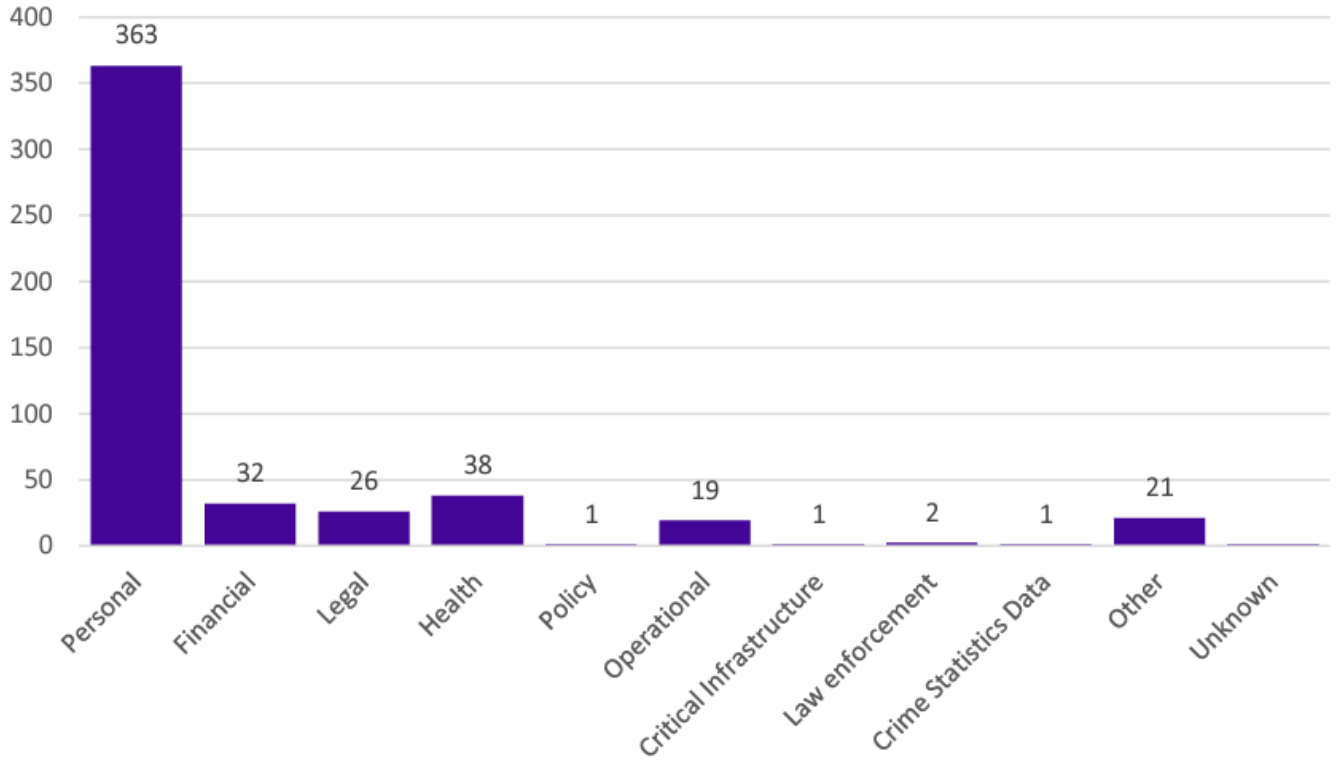
Information format

- **308** 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**.
- **69%** of incidents involving hard copy information were related to **mail**.



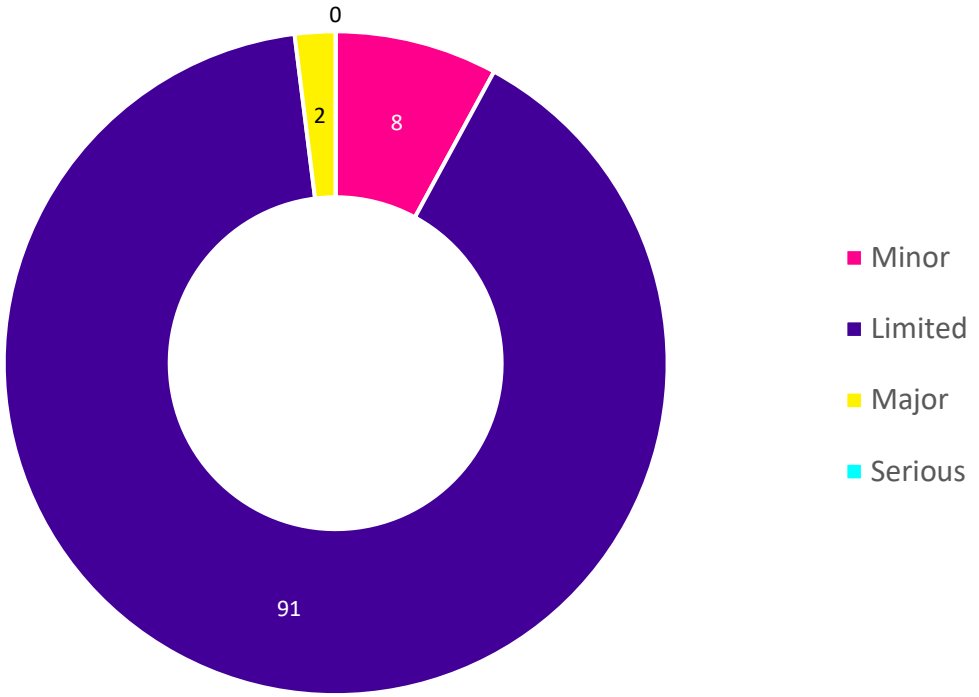
Information type

- **95%** incident notifications indicate compromises of **personal** information.
- **18%** incident notifications involved more than one information type.
- There were **21** notifications that selected **Other** e.g., claim numbers, DNS records, investigation reports.



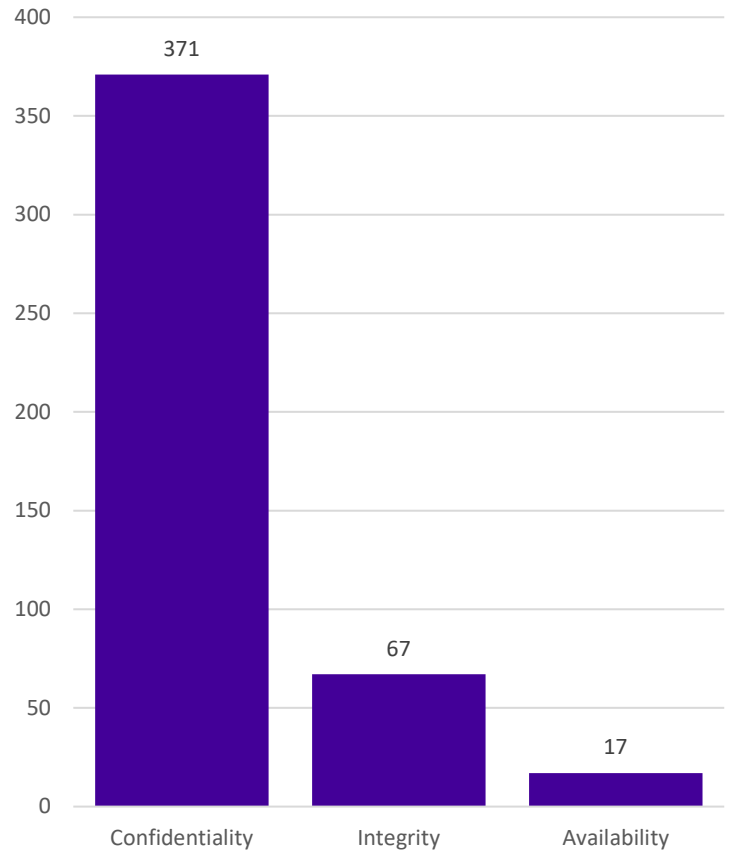
Business Impact Level (BIL)

- **91%** of incidents were assessed as impacting BIL 2 information (Limited harm or damage).
- **6** incident notifications nominated BIL 3.
- If in doubt of the BIL just notify.



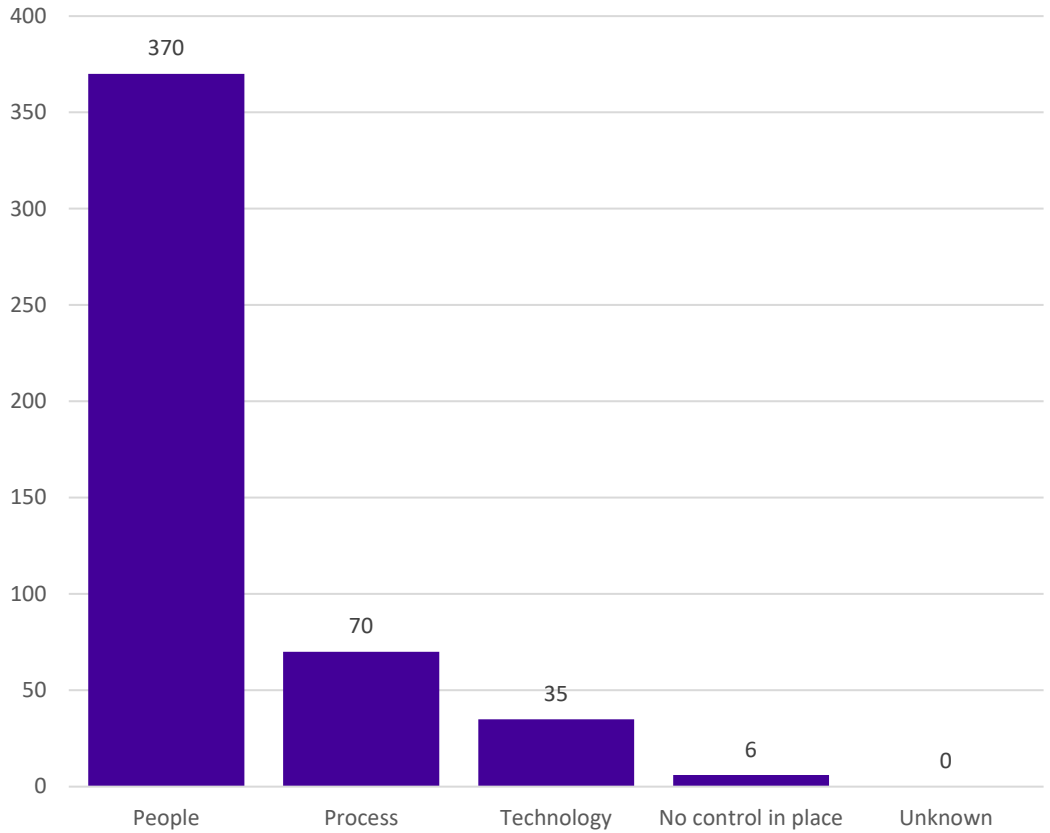
Security attributes

- **371** incident notifications indicate compromises of the **confidentiality** of information.
- **17%** of incident notifications selected more than one option for this field.



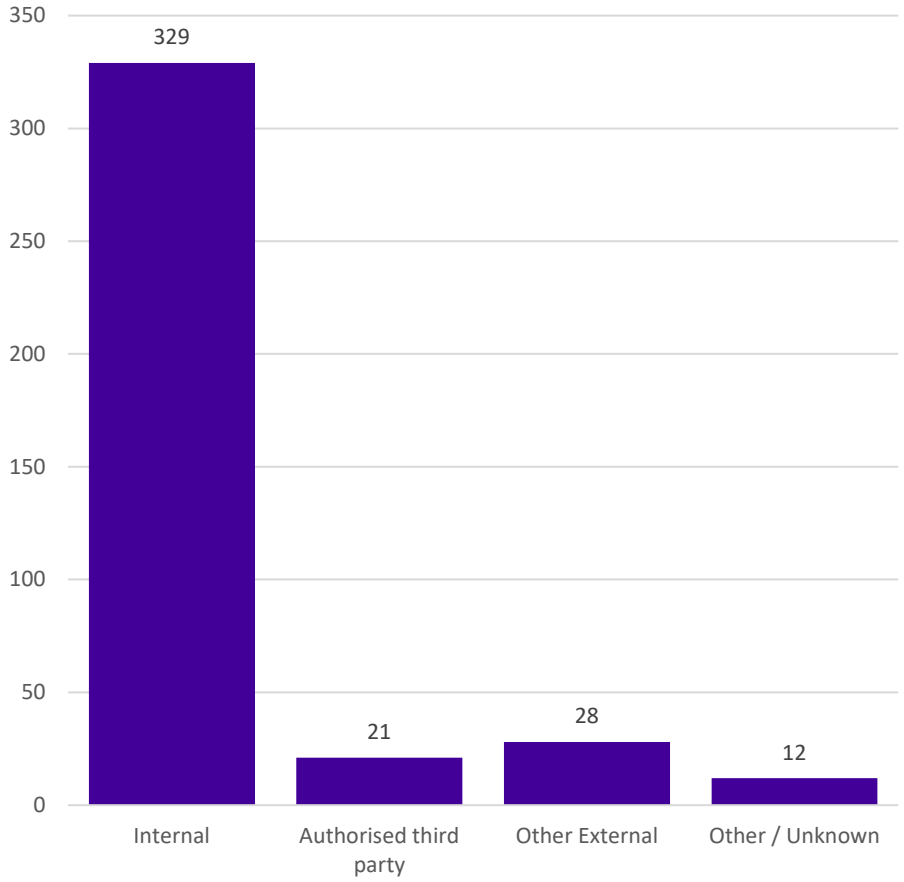
Control areas

- **96%** of incidents were caused by **people**.
- **70** incidents were caused by **process** issues.
- **35** incidents were caused by **technology**.
- **10** notifications nominated all three control areas as causal factors.



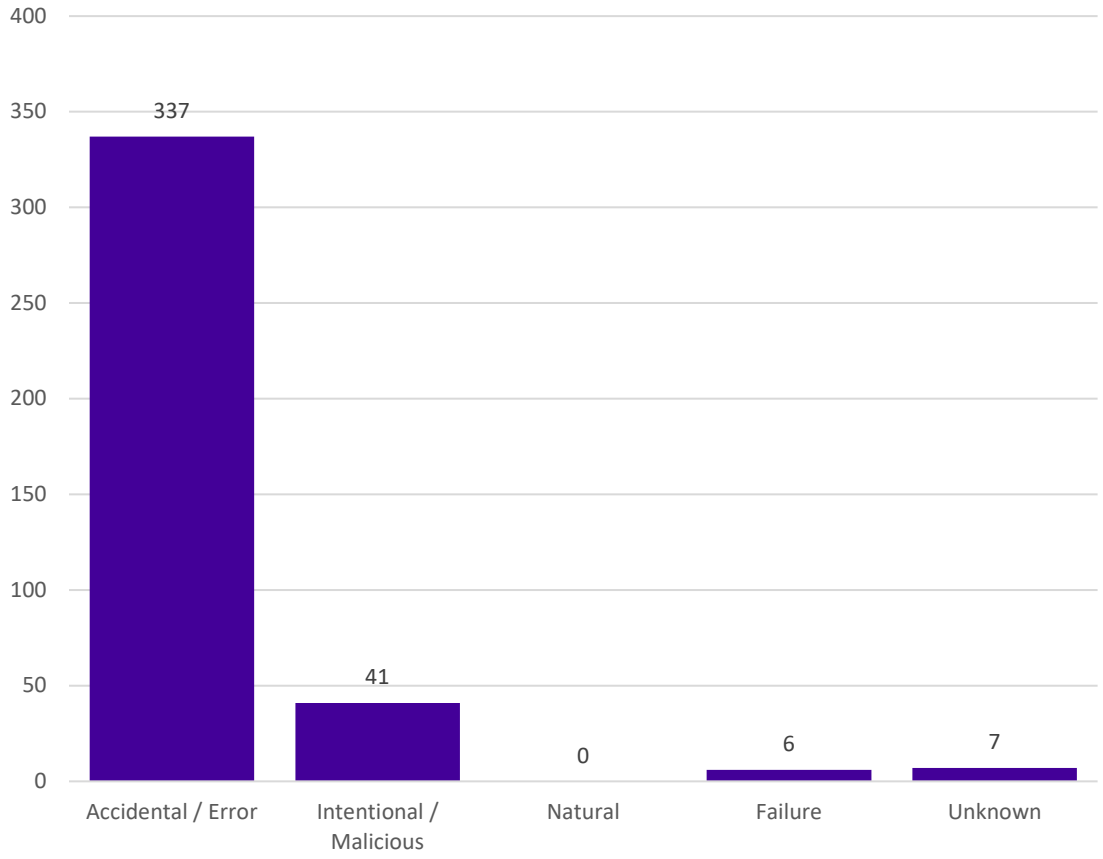
Threat actors

- **86%** of incidents were caused by **internal staff**.
- **21** incidents were caused by **authorised third parties** such as contracted service providers.
- **12** notifications indicated that the threat actor could not be ascertained.



Threat types

- **88%** of incidents were caused by **accidental actions**.
- **11%** of incidents were due to **intentional actions**.



Risk statements

The risk of…	caused by…	resulting in…	
Inappropriate handling and disclosure of payment information	Storing unredacted credit card information	Impact on legal and regulatory compliance requirements e.g. payment card industry data security standards (PCI-DSS) Impact to individuals whose personal information was affected	C I
Inability to make phone calls or conduct electronic monitoring	Telecommunications provider outage	Impact on service delivery Impact on public services (reputation of, and confidence in, the organisation)	A
Unauthorised access to customer ticketing data	Malicious threat actor compromising fourth-party supply chain	Impact on public services (reputation of, and confidence in, the organisation) Impact to individuals whose personal information was affected	C

Questions for OVIC?

Contact the Information Security Unit

security@ovic.vic.gov.au

Final thoughts

Rachel Dixon
Deputy Commissioner, Privacy and Data Protection

Deputy Commissioner's Final Thoughts

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

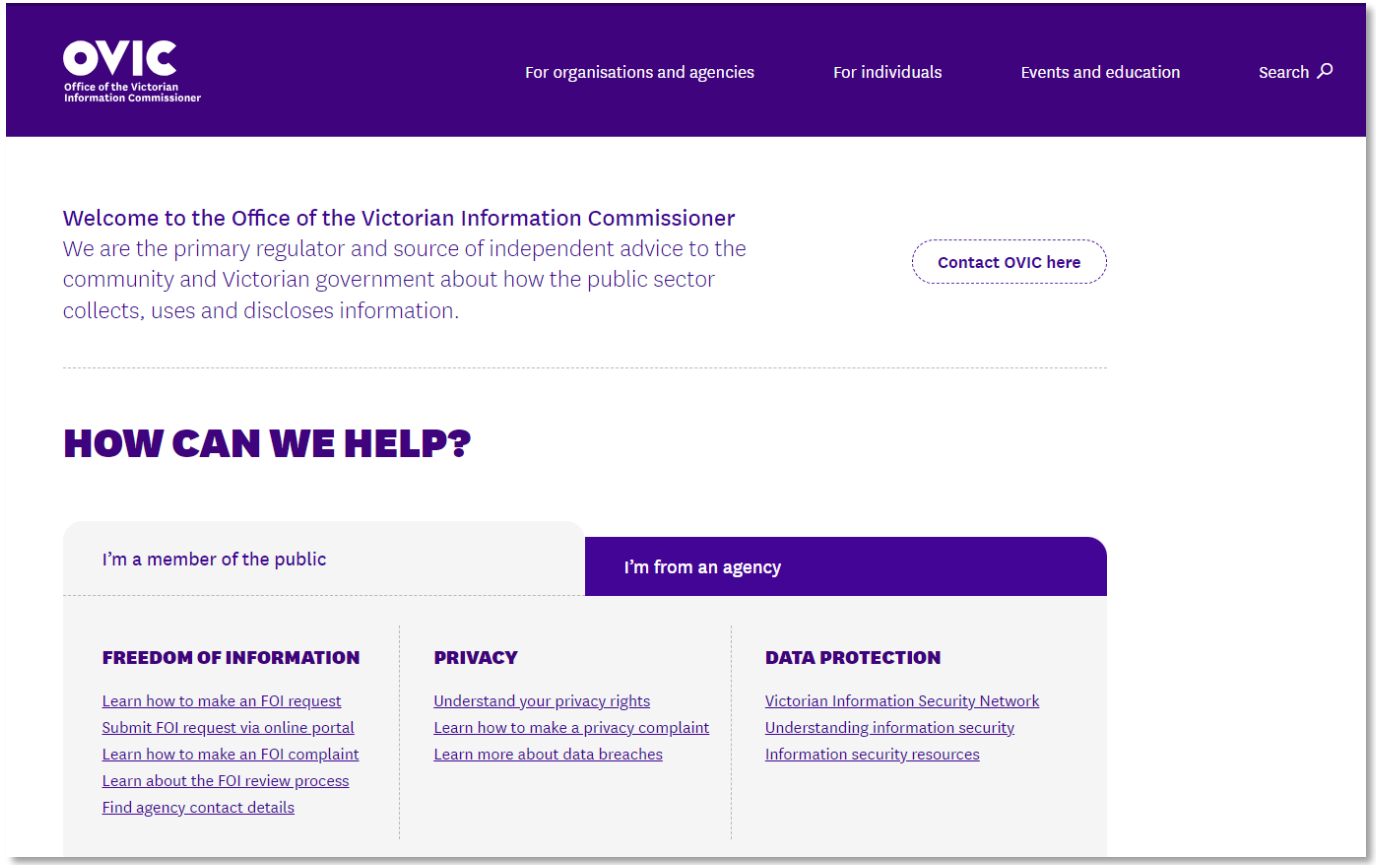
Contact the Information Security Unit by emailing

security@ovic.vic.gov.au

incidents@ovic.vic.gov.au

Or call

1300 00 OVIC



ovic.vic.gov.au