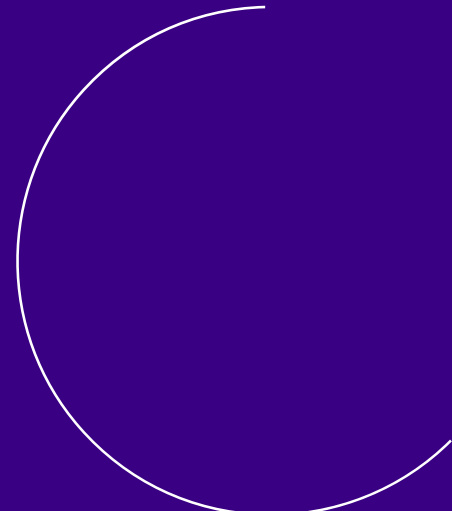
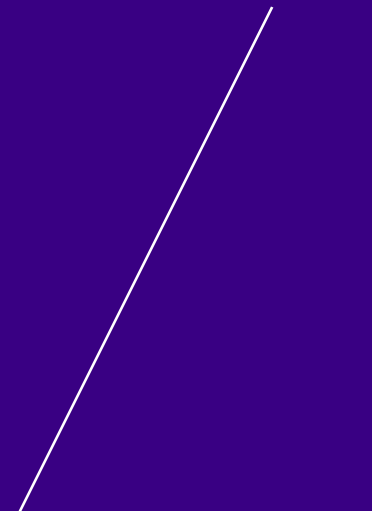
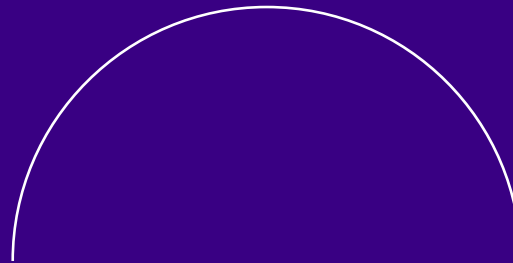


# *Information Security Incident Insights Forum*

Victorian Information Security Network (VISN)  
October 2025



A reminder – Today's session  
is being recorded.



## Acknowledgement of Country

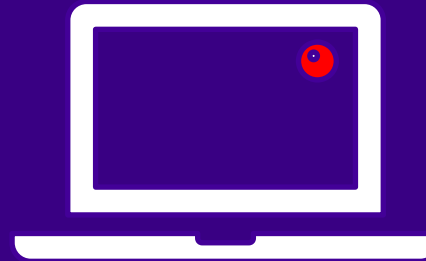
*We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.*

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

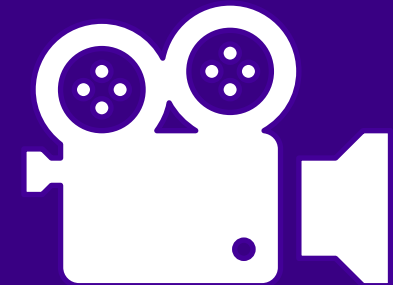
# Housekeeping - What to be aware of



Please turn off your **camera** and ensure your **mic is on mute** to minimise disruptions.

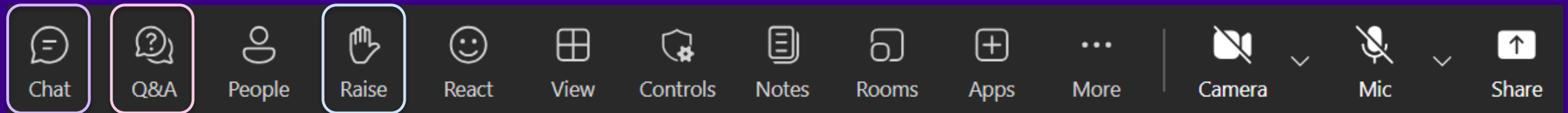


Today's session is **being recorded**.



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

# Housekeeping – How to engage



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



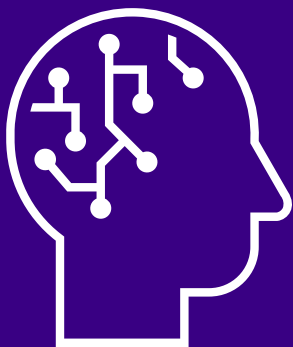
If you want to ask an **anonymous question**, type your question into the **Teams Q&A channel**.



Each speaker will answer questions following the presentation. If you prefer to ask your question verbally, **raise your hand** and **come off mute when called upon**.



# Housekeeping – Use of AI tools



Slides and a recording of this session will be made available in the coming days.

As such, we ask for that no Generative AI tools are used to take notes or record this event. We will remove users/tools who do so.

## OVIC's position on the use of generative AI in meetings with OVIC

A PDF document of this information is available to view and download [here](#).

This article outlines the Office of the Victorian Information Commissioner's (**OVIC**) position on the use of generative AI tools including AI notetakers, in meetings between OVIC's staff and OVIC's stakeholders.

OVIC's stakeholders may include Victorian public sector organisations, local councils, contracted service providers, consultants, Members of Parliament, interstate and international colleagues, and members of the public.

OVIC's staff includes OVIC employees and statutory office holders.

<https://go.vic.gov.au/4fM3O3t>

# What we'll explore today

- The Information Security Incident Notification Scheme
- The latest Incident Insights Report – themes and trends
- Hear from our guest speaker from the Office of the Australian Information Commissioner
- Questions

# *Information Security Incident Notification Scheme*

# The Incident Notification Scheme

**OVIC**  
Office of the Victorian  
Information Commissioner

For organisations and agencies

Home / Privacy / Resources for organisations / Information security and privacy incident notification form

## Information security and privacy incident notification form

Organisations that are subject to the Victorian Protective Data Security Standards (**VPDSS**) should notify OVIC of certain information security incidents. In addition, organisations that are subject to Part 3 of the PDP Act are encouraged to notify OVIC of incidents involving personal information that could cause harm to affected individuals.

**Any organisation that is subject to the PDP Act can therefore use this form to report incidents to OVIC, whether voluntarily or by obligation.**

Please use [our online form to notify us of information security incidents](#).

Information security incidents routinely impact **all types of public sector information**, held in a variety of formats.

## What sort of incidents are captured under the Scheme?

The Scheme falls from VPDSS element E9.010, under which VPS organisations should notify OVIC of incidents that have an adverse impact on the **confidentiality, integrity** and/or **availability** of public sector information assessed as having a ‘limited’ business impact or higher (**Business Impact Level of 2** or above).

Information assessed as being a BIL 2 or higher includes material with a **protective marking of:**

- OFFICIAL: Sensitive
- PROTECTED
- Cabinet-In-Confidence, or
- SECRET



# Avenues to notify OVIC

Organisations can notify OVIC of information security or privacy incidents in a number of ways.

## Option 1

### Online Incident Notification Form (webform)

The screenshot shows the 'Incidents Notification Form' with a progress bar at the top indicating five steps: 1. Introduction, 2. Information about the incident, 3. Privacy incidents, 4. Incident notification scheme, and 5. Thank you. The current step is 1. Below the progress bar, there is a 'Start the form' button. To the left of the button, there is text stating: 'Information security and privacy incident notification form'. Below this, it says 'What you should know before using this form'. Further down, it mentions 'Any organisation that is subject to the Privacy and Data Protection Act 2014 (Vic) (PDP Act) can use this form to report incidents to OVIC, whether voluntarily or by obligation.' and lists two bullet points: 'This form should not be used by members of the public to report incidents, data breaches or alleged wrongdoing by VPS employees or organisations to OVIC.' and 'Individuals wishing to do so, should instead use OVIC's Privacy Complaint Form.' Below this, it says 'Organisations that are subject to:' and lists two bullet points: 'Part 4 of the PDP Act and the Victorian Protective Data Security Standards (VPDSS) should notify OVIC of certain information security incidents, and'.



## Option 3

Send an email to  
[incidents@ovic.vic.gov.au](mailto:incidents@ovic.vic.gov.au)

## Option 2

### Downloadable Incident Notification form

The screenshot shows the 'Downloadable Incident Notification form'. At the top, it says '[CHOOSE A PROTECTIVE MARKING]'. Below this is the OVIC logo and the text 'Office of the Victorian Information Commissioner'. The title of the form is 'Information Security and Privacy Incident Notification Form'. Below the title, it says 'Organisations that are subject to the Victorian Protective Data Security Standards (VPDSS) must notify OVIC of certain information security incidents. In addition, organisations that are subject to Part 3 of the PDP Act are encouraged to notify OVIC of incidents involving personal information that could cause harm to affected individuals.' and 'Any organisation that is subject to the PDP Act can therefore use this form to report incidents to OVIC, whether voluntarily or by obligation.' Below this, it says 'Send the completed form to [incidents@ovic.vic.gov.au](mailto:incidents@ovic.vic.gov.au) or [privacy@ovic.vic.gov.au](mailto:privacy@ovic.vic.gov.au).' Below this is 'SECTION 1: General Details' which is a table with two columns: 'Field' and 'Details (if known)'. The table has rows for 'Name of organisation', 'Contact name and position', 'Contact phone number', 'Contact email address', 'What happened?', 'When did it happen?', and 'When did organisation become aware of it?'. At the bottom of the form, it says 'www.ovic.vic.gov.au OVIC ref: D22/11438' and '[CHOOSE A PROTECTIVE MARKING]'.

# *Themes and trends from the latest Incident Insights Report*

**Anna Harris**

*Principal Advisor, Information Security (OVIC)*

## Themes and trends



Volume



Information  
format



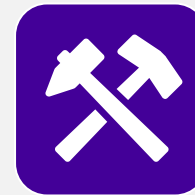
Information  
type



Business  
Impact Level  
(BIL)



Security  
attributes



Control  
areas



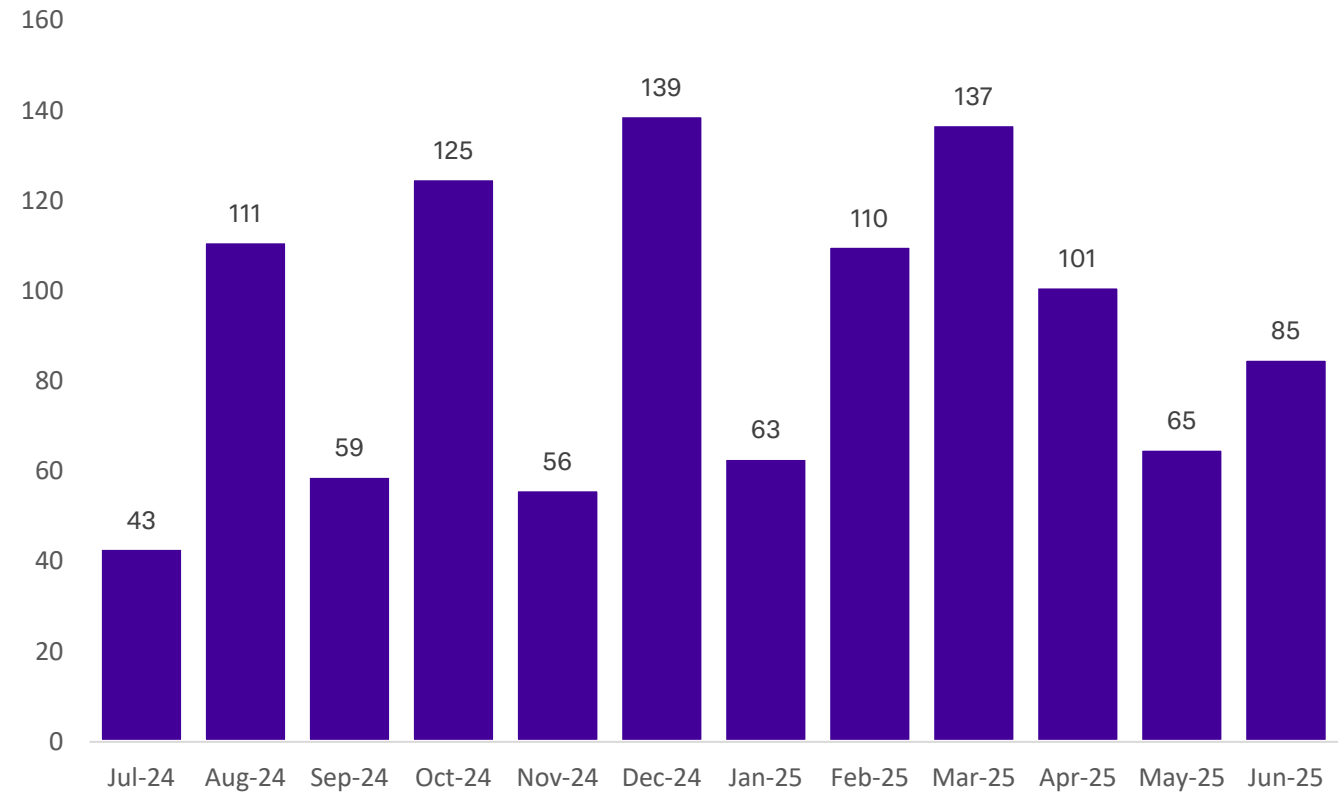
Threat  
actors



Threat  
types

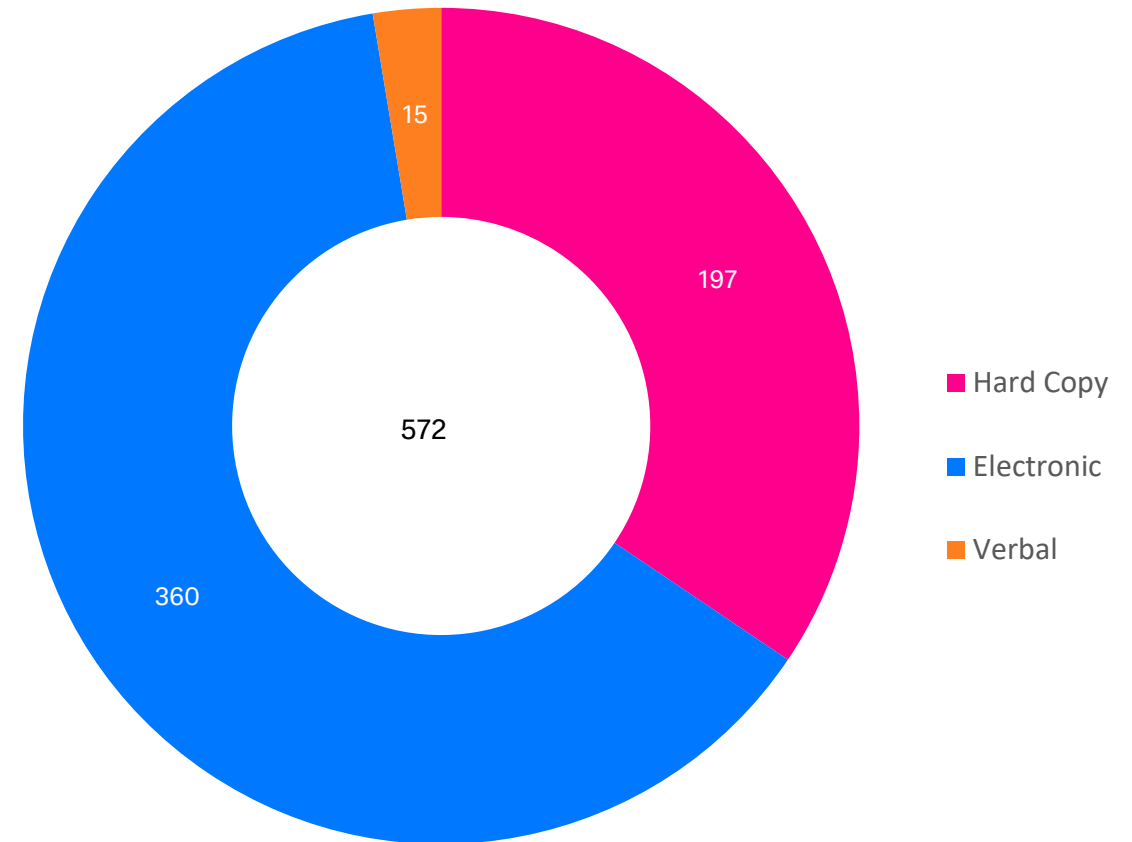
## Volume – Notifications by month

- OVIC received **561** notifications between 1 January to 30 June 2025.
- This is a **5%** increase compared to the previous notification period.



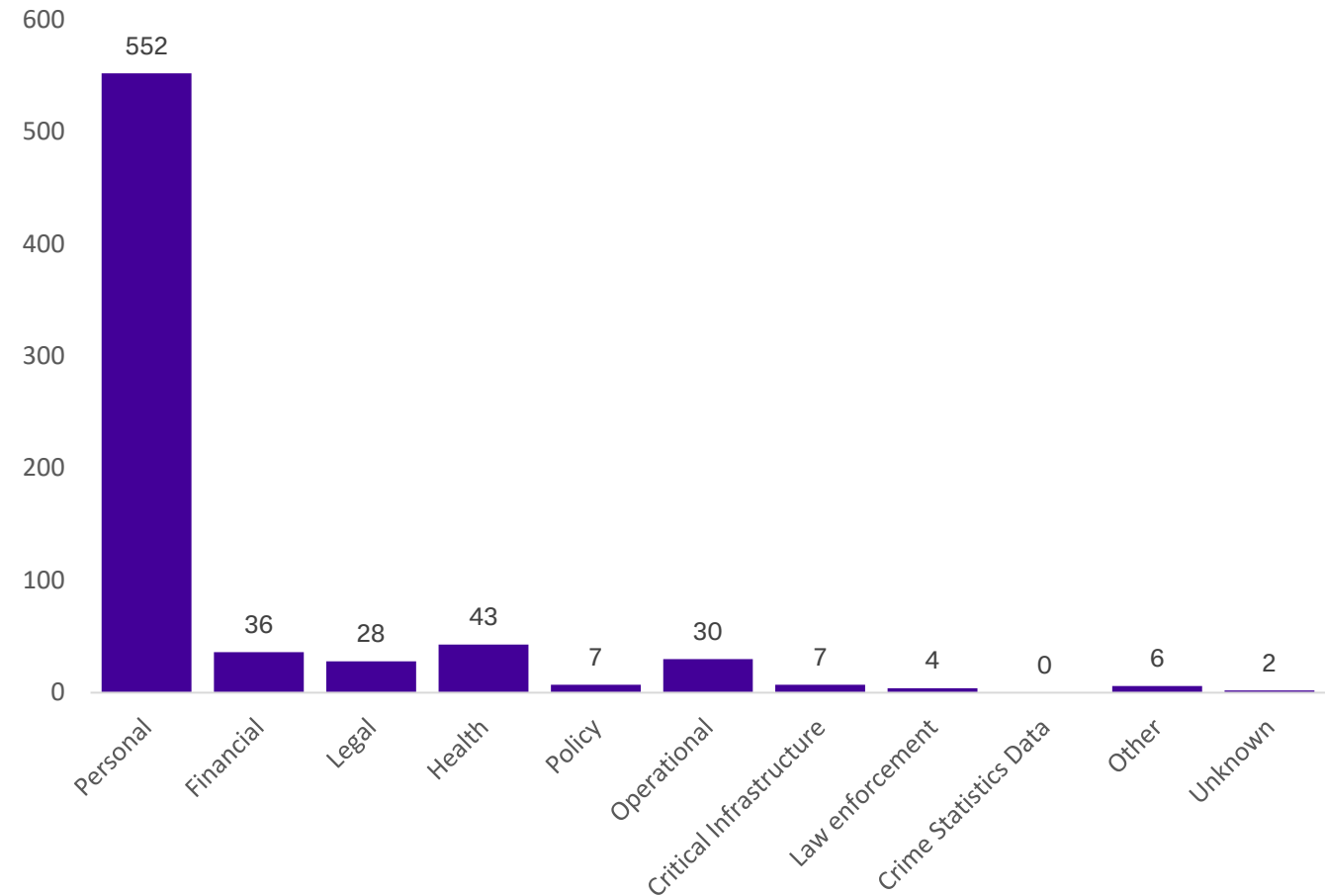
## Information format

- 360 incidents relate to compromises of **electronic information**.
- Over half of the incidents affecting electronic information related to email errors (**64%**).
- 79% of incidents involving hard copy information were related to **mail**.



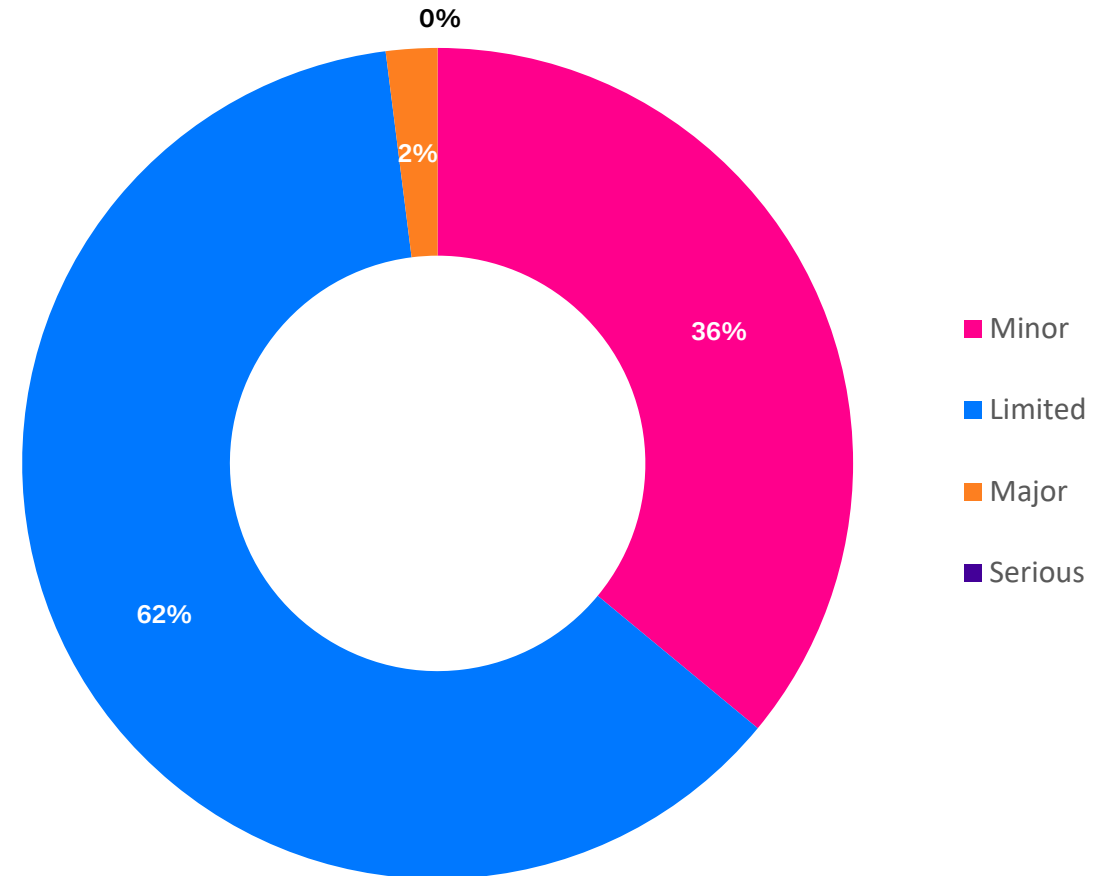
## Information type

- **98%** incidents indicate compromises of **personal** information.
- **21** incidents involved three or more information types.
- There were **8** incidents that selected **Other** e.g., commercially sensitive information, safety and wellbeing reports, incident trends and theme analysis.



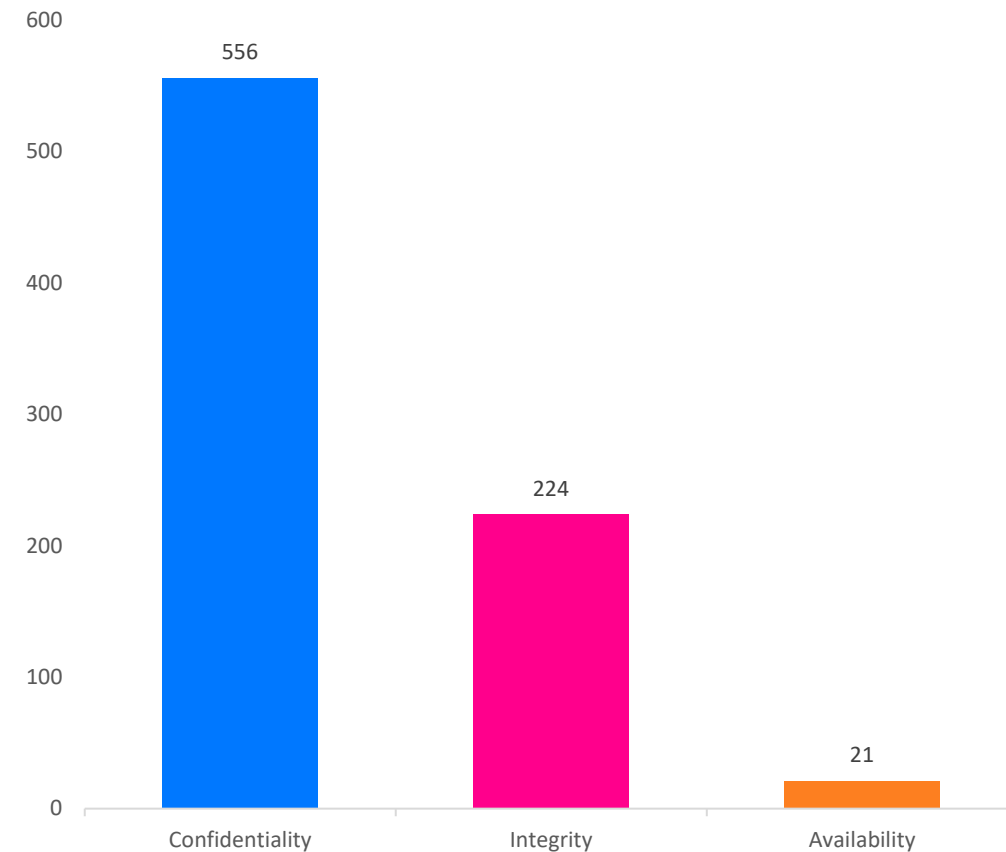
## Business Impact Level (BIL)

- **62%** of incidents were assessed as impacting **BIL 2** information (Limited harm or damage).
- **11** incidents affected **BIL 3** information.
- **36%** of incidents were assessed as **BIL 1** which is a **5% increase** from the last period.
- If in doubt of the BIL, just notify.



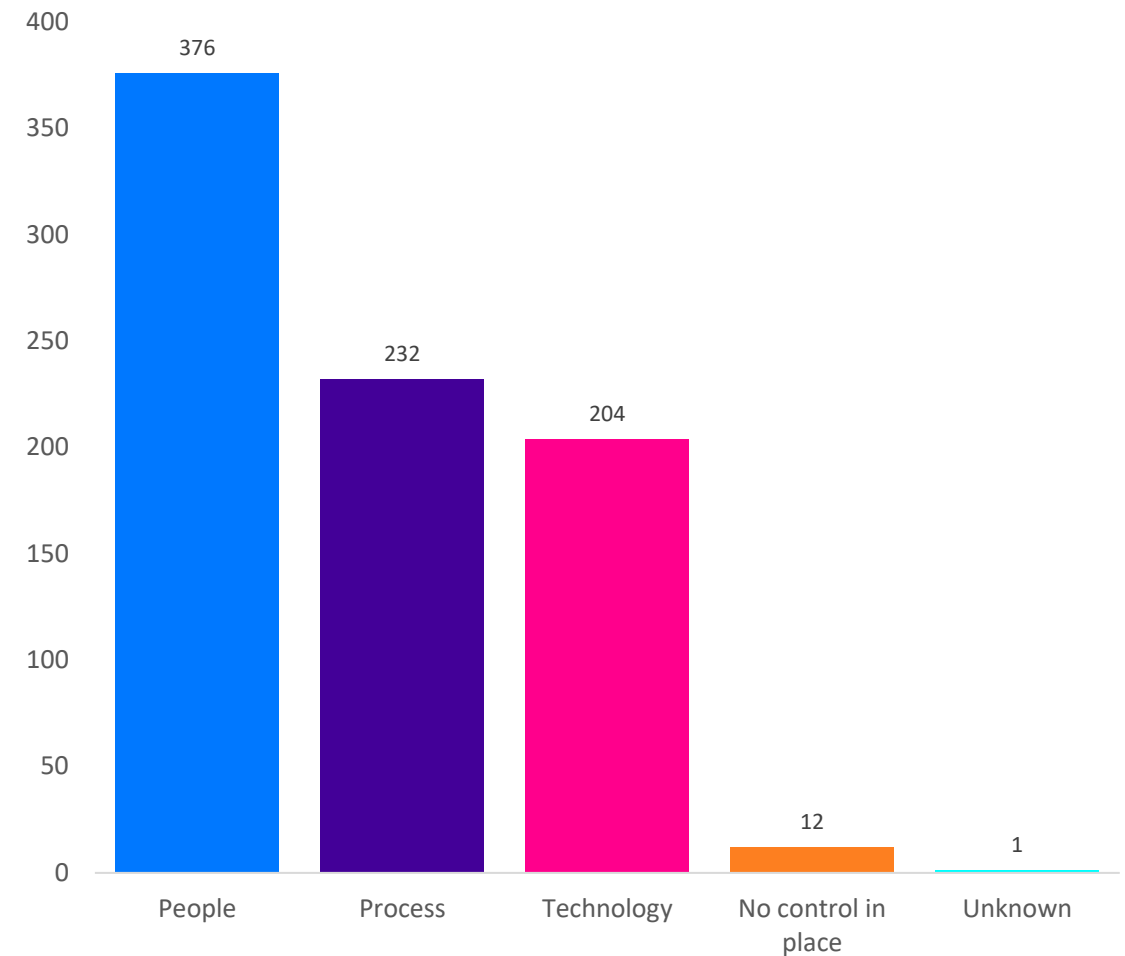
# Security attributes

- **556** incidents were compromises of the **confidentiality** of information.
- **9** incidents affected all three security attributes (confidentiality, integrity and availability).



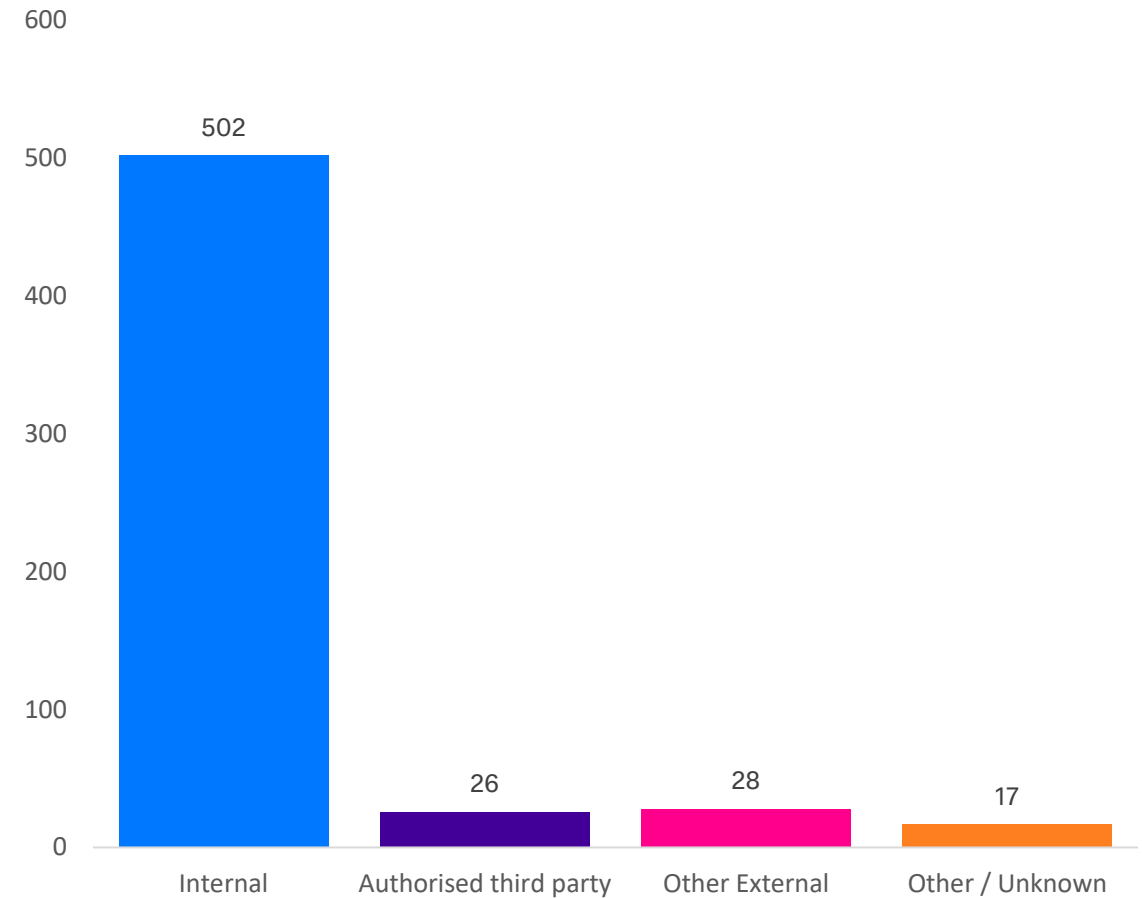
## Control areas

- 67% of incidents were caused by **people**.
- There was another increase in incidents caused by **process** and **technology** issues.
- 6 incidents were caused by all control areas (**people, process, technology** and no control(s) in place).



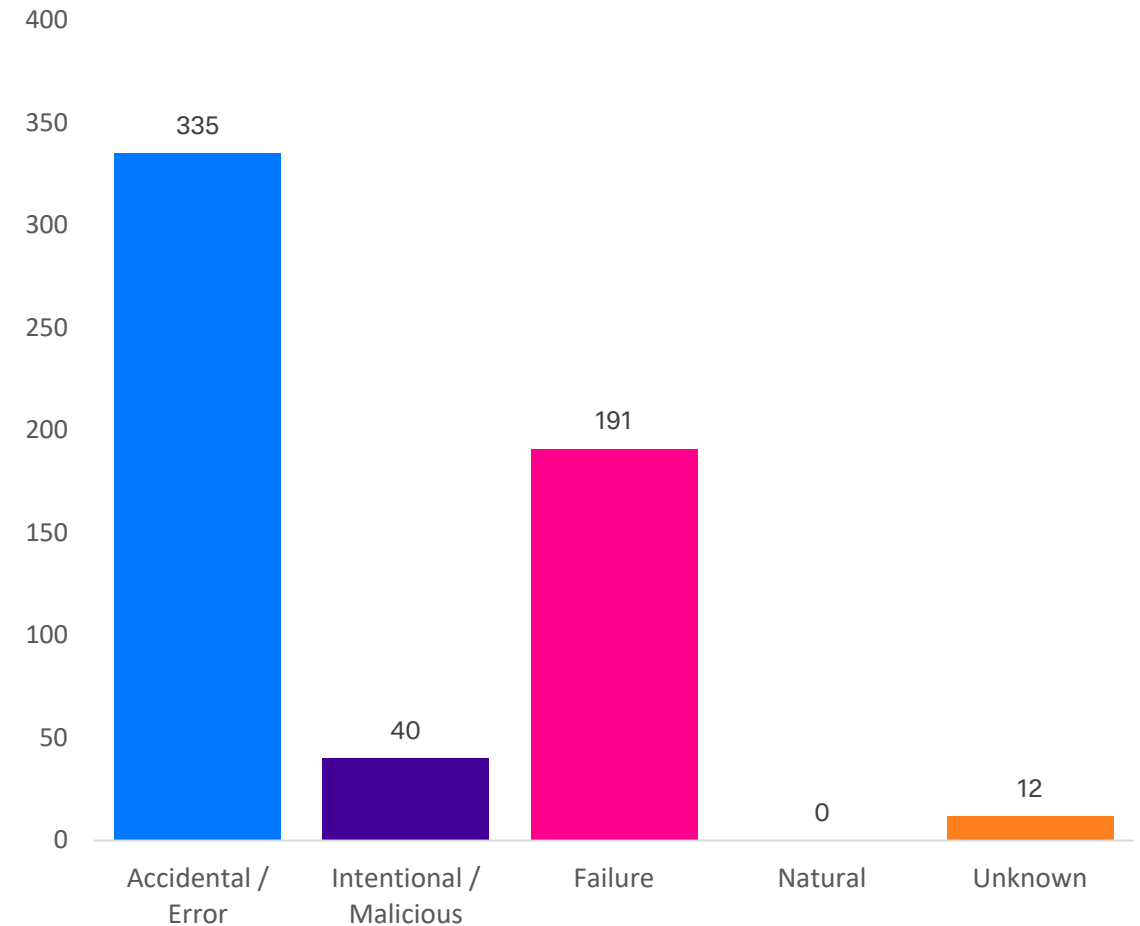
## Threat actors

- 89% of incidents were caused **internally**.
- 26 incidents were caused by **authorised third parties** such as contracted service providers.
- 12 incidents were caused by multiple threat actors.



## Threat types

- 335 incidents were caused by **accidental** actions.
- 40 incidents were due to **intentional** actions of the threat actor.
- There was an increase in incidents caused by a **failure** of systems and processes to operate as expected.



# Risk statements

## The risk of...

Unauthorised transfer/release of information including cabinet, intellectual property and personal information about other staff

Disclosure of personal information published on website

Incorrect customer records leading to unauthorised disclosure of address details to ex-partner

## caused by...

Disgruntled staff member sending information to/from their own personal email account

Misconfiguration of platform by third party not selecting the correct fields to redact before displaying information

Incorrect data matching and linking of accounts during system migration

## resulting in...

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

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

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

C

C  
AC  
I

## *Questions for OVIC?*

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



Have your say on this VISN event -  
<https://forms.office.com/r/LjZBwvMKt3>

# *Office of the Australian Information Commissioner*

**Warren Jacobs**  
*OAIC Director - Investigations*

# Information Commissioner's final thoughts

## Sean Morrison

### Information Commissioner

To read OVIC's Incident Insights report visit:  
<https://ovic.vic.gov.au/information-security/security-insights/#2025>

For more information on the OAIC's activities visit:

<https://www.oaic.gov.au/>

To read the Australian Signals Directorate's Annual Cyber Threat Report, visit:

<https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2024-2025>

**OFFICIAL**

**OVIC**  
Office of the Victorian Information Commissioner

### INFORMATION FOR AGENCIES

## Incident Insights Report

1 January 2025 – 30 June 2025

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

The incident insights Report provides a summary and analysis of the information security incident notifications received by OVIC between **1 January 2025 to 30 June 2025**.

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 2024 which can be found on our Security Insights webpage along with our other previous reports <https://ovic.vic.gov.au/information-security/security-insights/>.

Note: The incident notification form allows for more than one response to be selected for the fields:

- information format
- type of information
- security attributes
- control area
- threat actor
- threat type

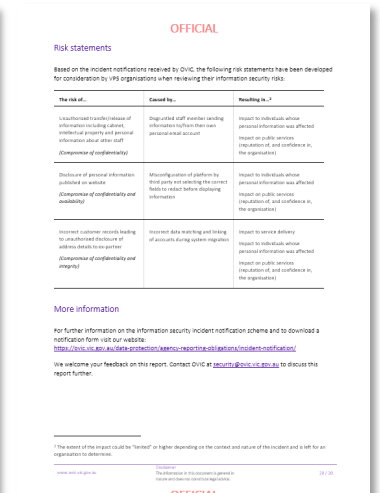
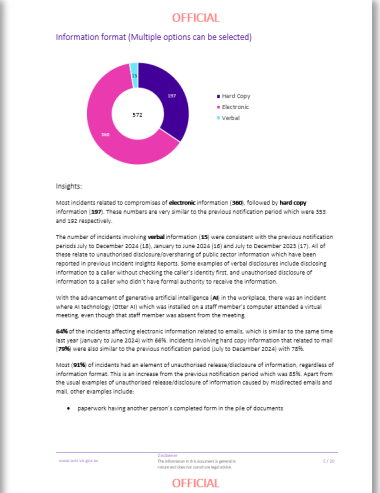
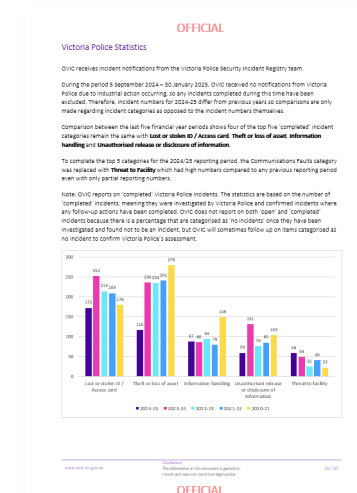
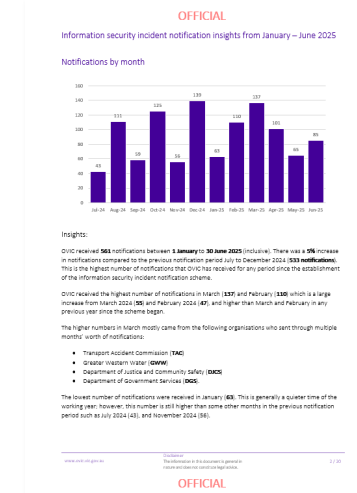
The sum of percentages for these fields will exceed 100% (as expected) reflecting the nature of multiple responses for each question. These sections are marked accordingly in this report.

OVIC 2025 View  
October 2025  
www.oaic.vic.gov.au

Disclaimer  
The information in this document is general in nature and does not constitute legal advice.

5 / 28

**OFFICIAL**



## 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 by emailing:

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

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

or call:

1300 00 OVIC



Have your say on this VISN event -  
<https://forms.office.com/r/LjZBwvMKt3>

The screenshot shows the OVIC website homepage. The header is purple with the OVIC logo and navigation links: 'For organisations and agencies', 'For individuals', 'Events and education', and a search icon. 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 present. 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 a request via an online portal, make an FOI complaint, learn about the FOI review process, and find agency contact details; 'PRIVACY' with links to understand privacy rights, 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](#)

