Office of the Victorian Information Commissioner

# *Information Security Incident Insights Forum*

Victorian Information Security Network (**VISN**)
March 2026

A reminder – Today's session
**is being recorded.**

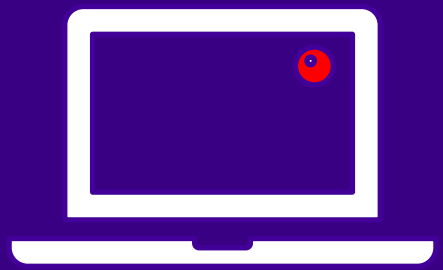
# Acknowledgement of Country

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

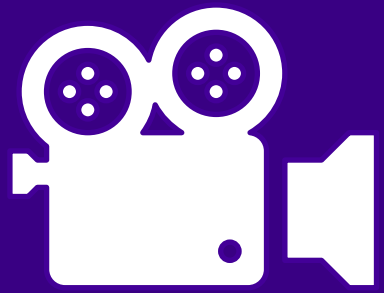
*We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.*

# Housekeeping - What to be aware of

**Cameras** and **mics** have been **muted** to minimise disruptions.

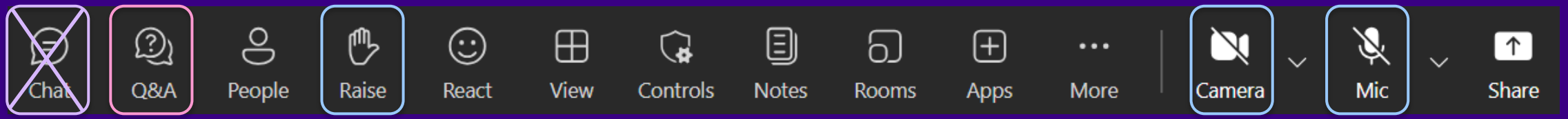


Today's session is **being recorded.**



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 has been **disabled** in this webinar.

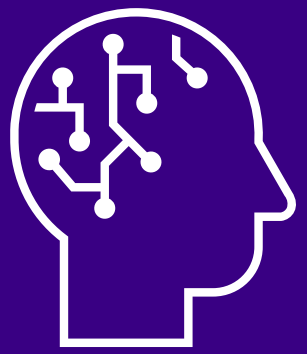
If you want to ask a **question**, type your question into the **Teams Q&A channel**. You select **anonymous** if you prefer to hide your name.

**Mics** and **cameras** will be **turned off** during the speakers' presentations.

Time permitting, mics and cameras will be **turned on** for verbal questions after each speaker.

Ask a question by **raising your hand** and **coming 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, Dr. Carl A. Gibson
- 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:

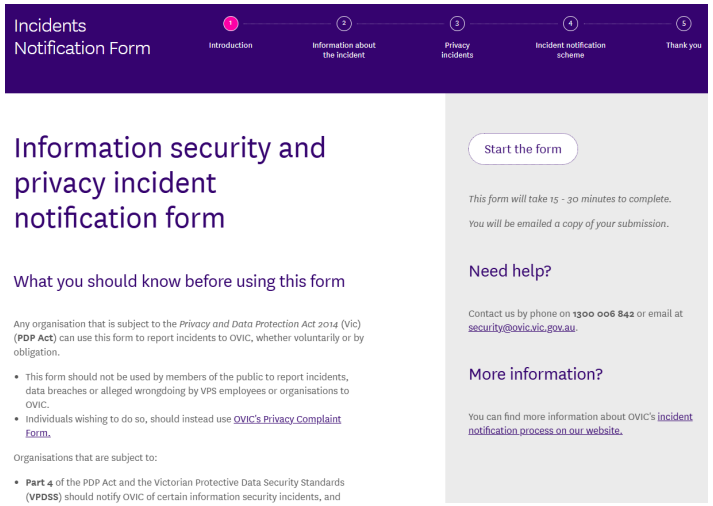
- OFFICIAL: Sensitive
- PROTECTED
- Cabinet-In-Confidence, or
- SECRET

# 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)


Incidents Notification Form

1 Introduction · 2 Information about the incident · 3 Privacy incidents · 4 Incident notification scheme · 5 Thank you

Information security and privacy incident notification form

What you should know before using this form

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.

- 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.
- Individuals wishing to do so, should instead use OVIC's Privacy Complaint Form.

Organisations that are subject to:

- **Part 4** of the PDP Act and the Victorian Protective Data Security Standards (**VPDSS**) should notify OVIC of certain information security incidents, and

Start the form

*This form will take 15 - 30 minutes to complete.*

*You will be emailed a copy of your submission.*

Need help?

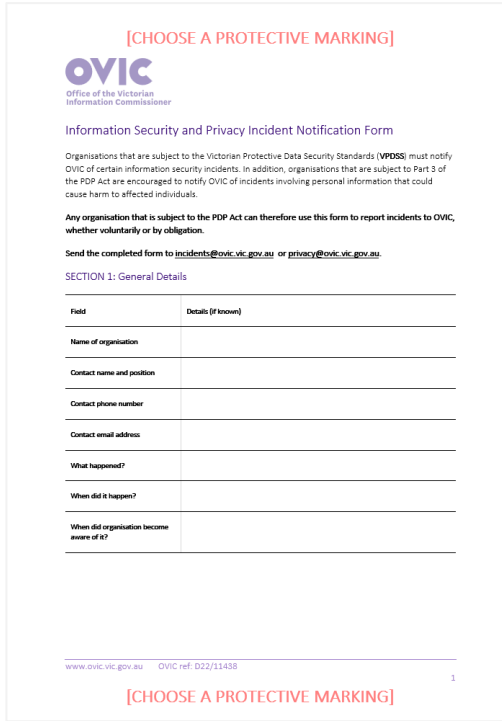
Contact us by phone on **1300 006 842** or email at security@ovic.vic.gov.au.

More information?

You can find more information about OVIC's incident notification process on our website.

## Option 2

### Downloadable Incident Notification form


[CHOOSE A PROTECTIVE MARKING]

OVIC Office of the Victorian Information Commissioner

Information Security and Privacy Incident Notification Form

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.

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

**Send the completed form to incidents@ovic.vic.gov.au or privacy@ovic.vic.gov.au.**

SECTION 1: General Details

| Field | Details (if known) |
|---|---|
| Name of organisation | |
| Contact name and position | |
| Contact phone number | |
| Contact email address | |
| What happened? | |
| When did it happen? | |
| When did organisation become aware of it? | |

www.ovic.vic.gov.au OVIC ref: D22/11438 1

[CHOOSE A PROTECTIVE MARKING]

## Option 3

**Send an email to incidents@ovic.vic.gov.au**

# Themes and trends from the latest Incident Insights Report

# Themes and trends


Volume

Information format

Information type

Business Impact Level (BIL)

Security attributes

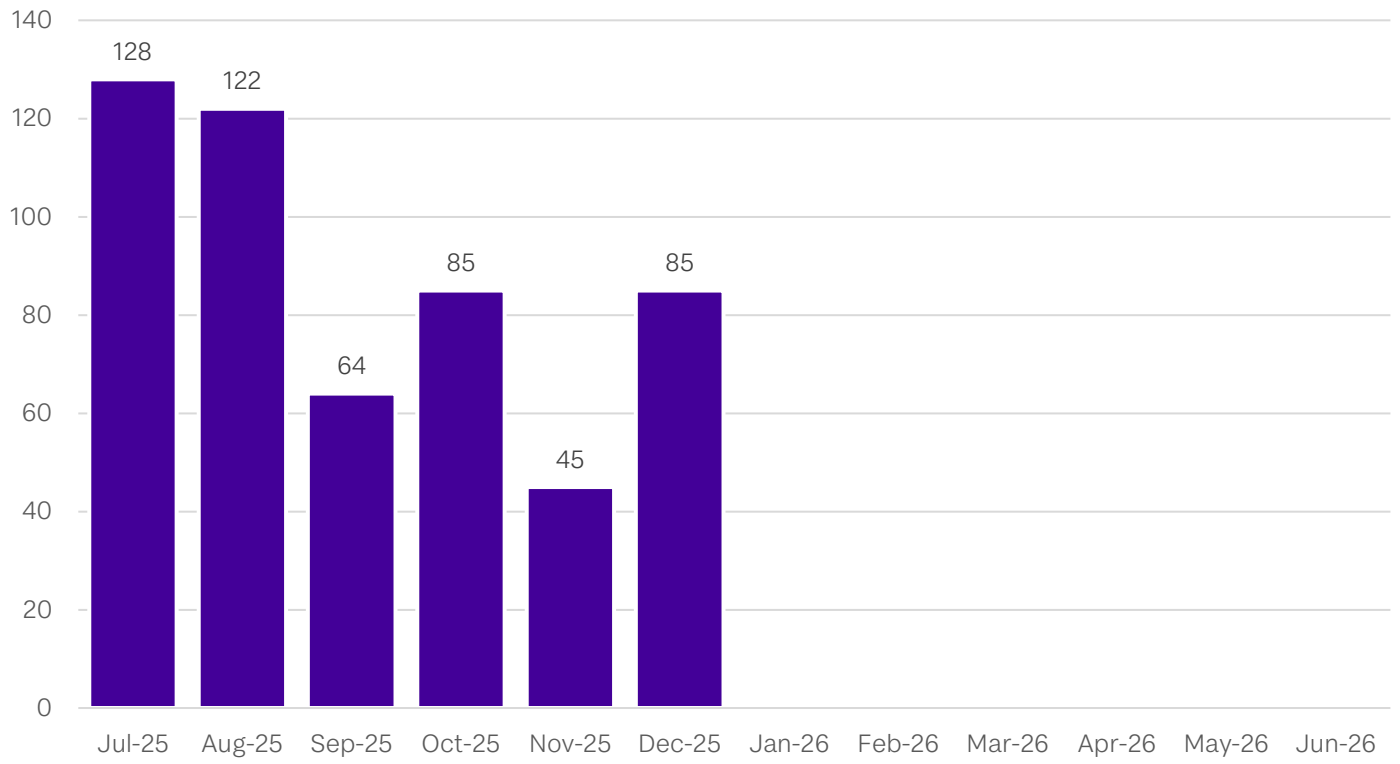
Control areas

Threat actors

Threat types

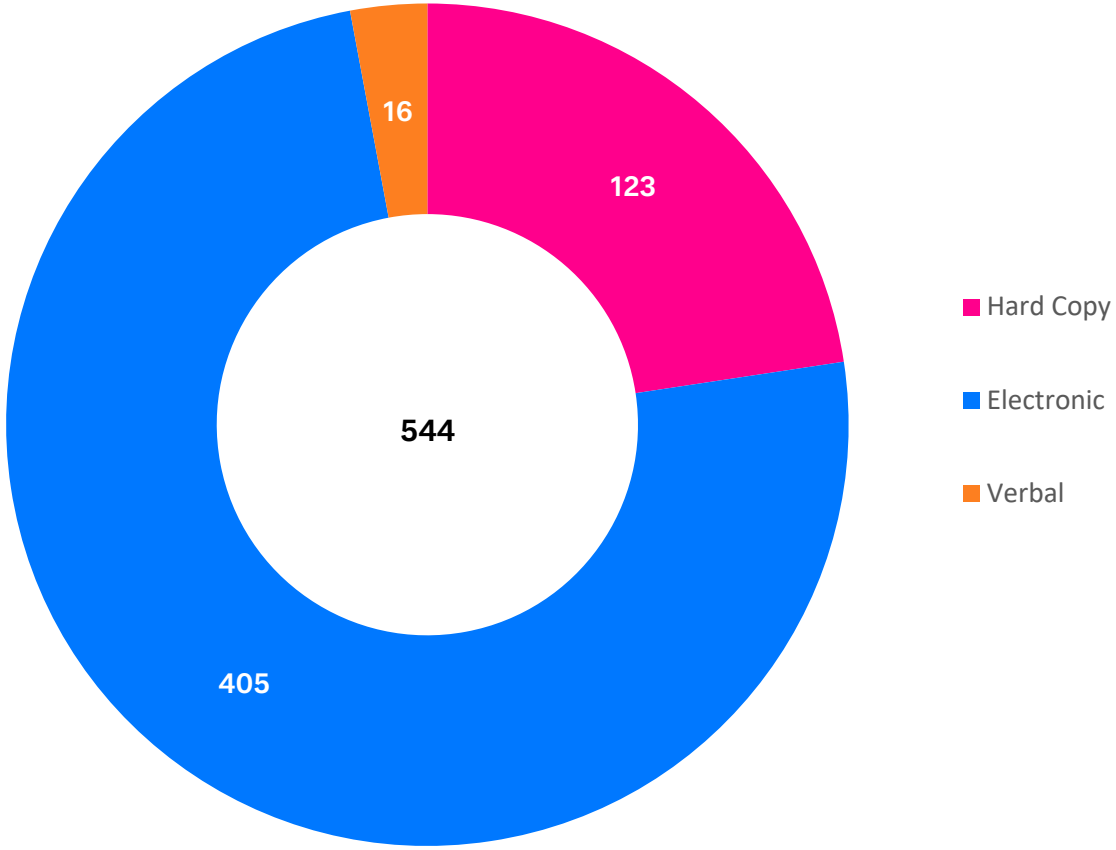
# Volume – Notifications by month

- OVIC received **529** notifications between **1 July to 31 December 2025.**
- This is a **5.7%** decrease compared to the previous notification period.



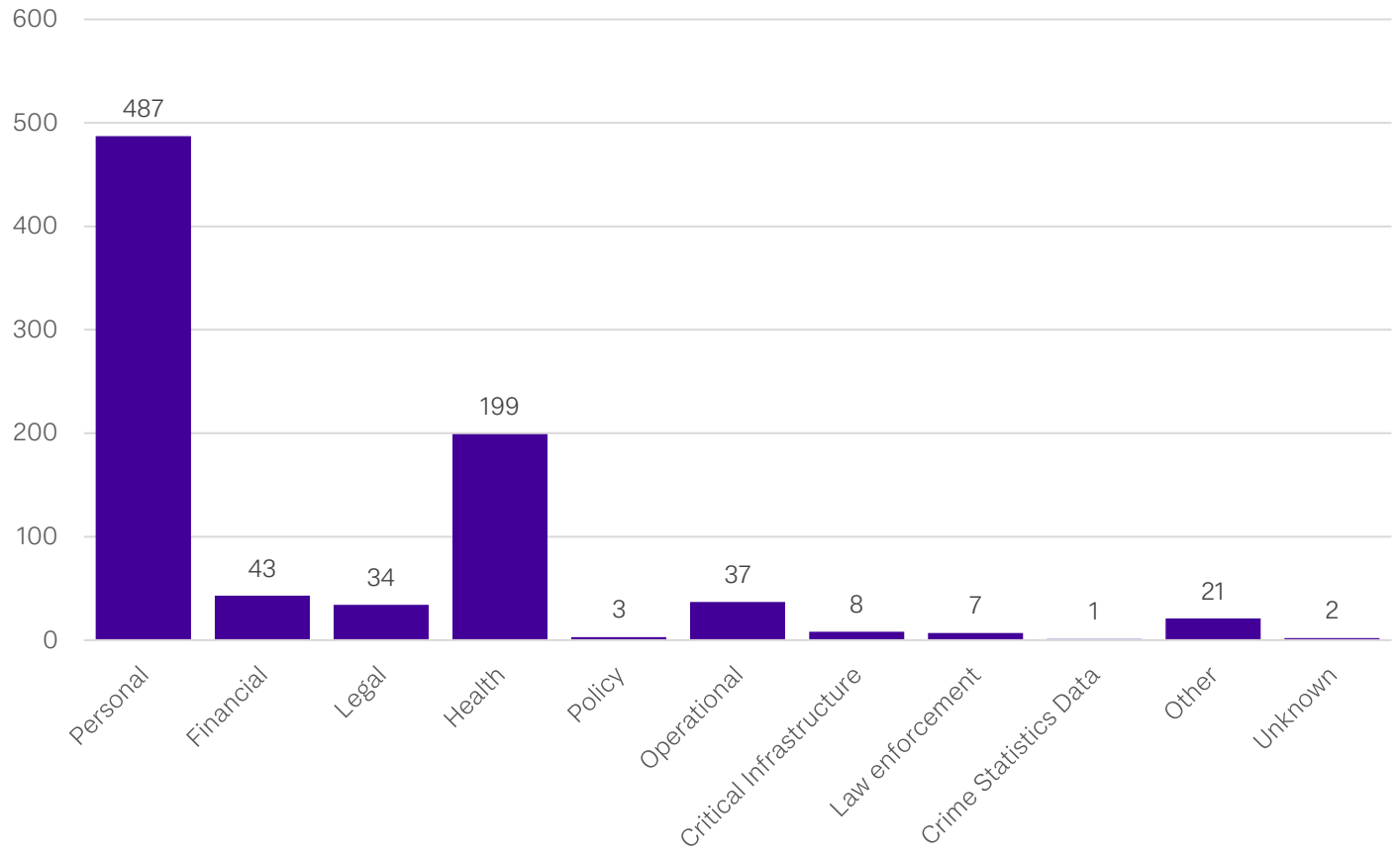
# Information format

- **405** incidents relate to compromises of **electronic information.**
- Over half of the incidents affecting electronic information related to email errors **(66%).**
- **73%** of incidents involving hard copy information were related to **mail.**



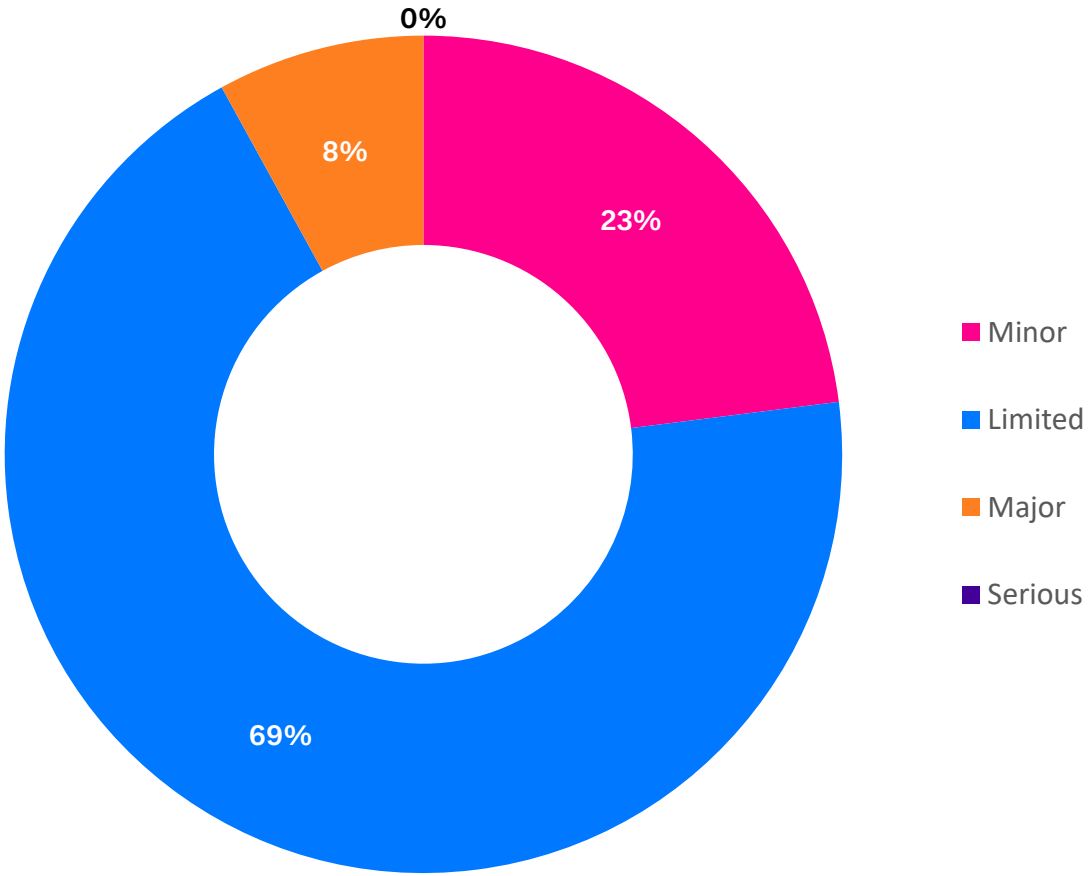
# Information type

- **92%** incidents indicate compromises of **personal** information.
- **25** incidents involved three or more information types.
- There were **21** incidents that selected **Other** e.g., cabinet information, credentials for a test mailbox, hacked website, API keys.



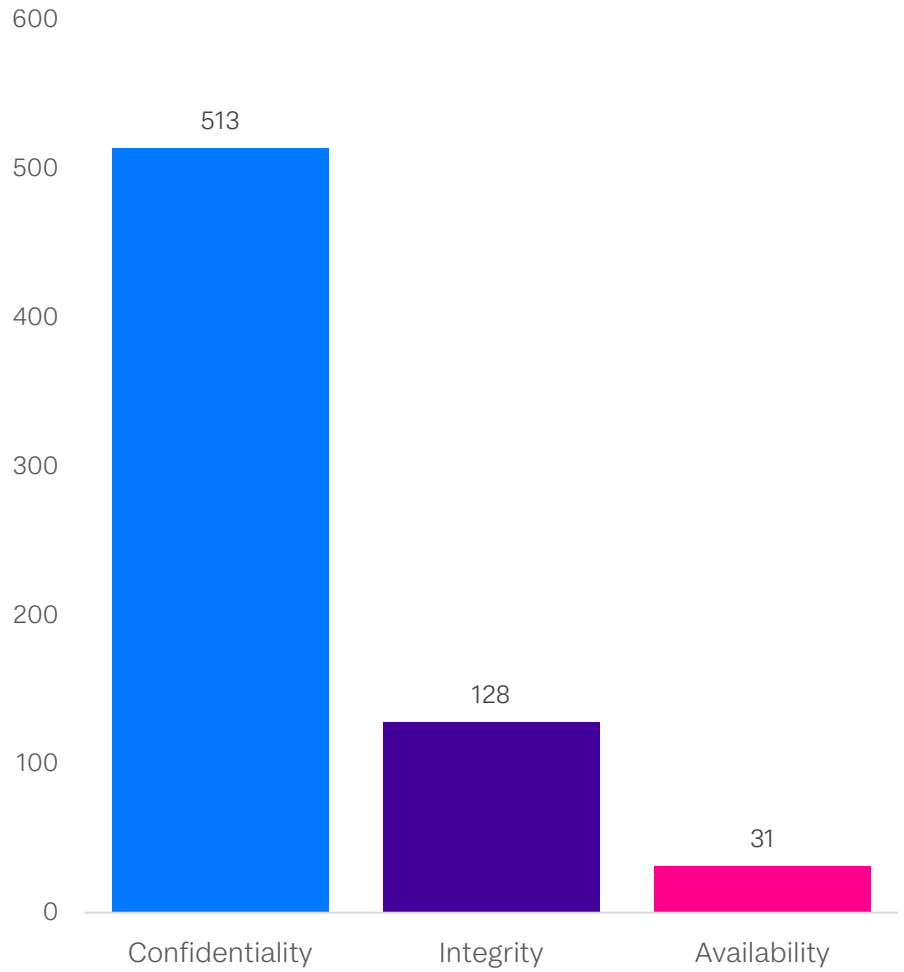
# Business Impact Level (BIL)

- **69%** of incidents were assessed as impacting **BIL 2** information (Limited harm or damage).
- **43** incidents affected **BIL 3** information.
- There was 1 notification related to BIL 4 information.
- If in doubt of the BIL, just notify.



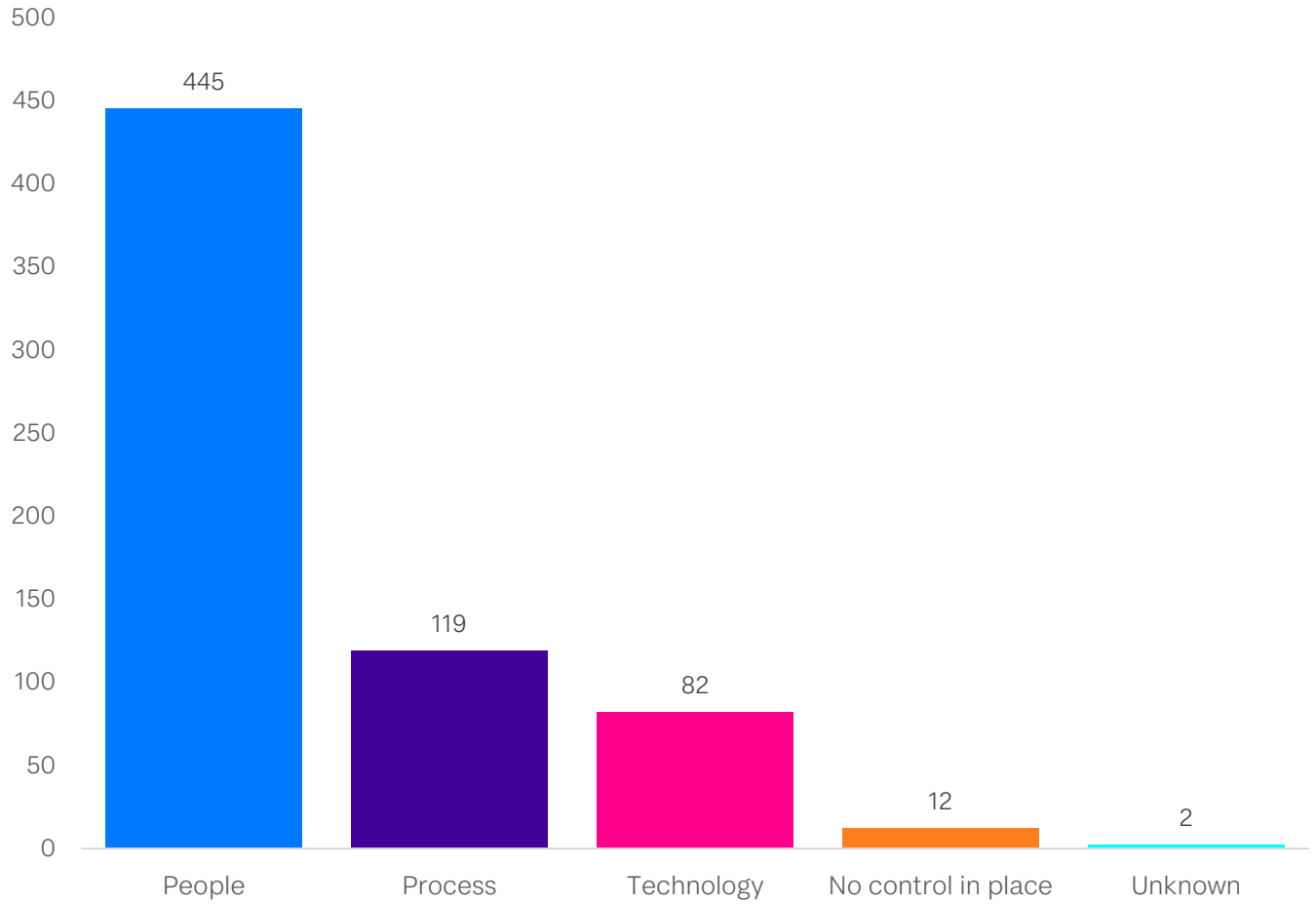
# Security attributes

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



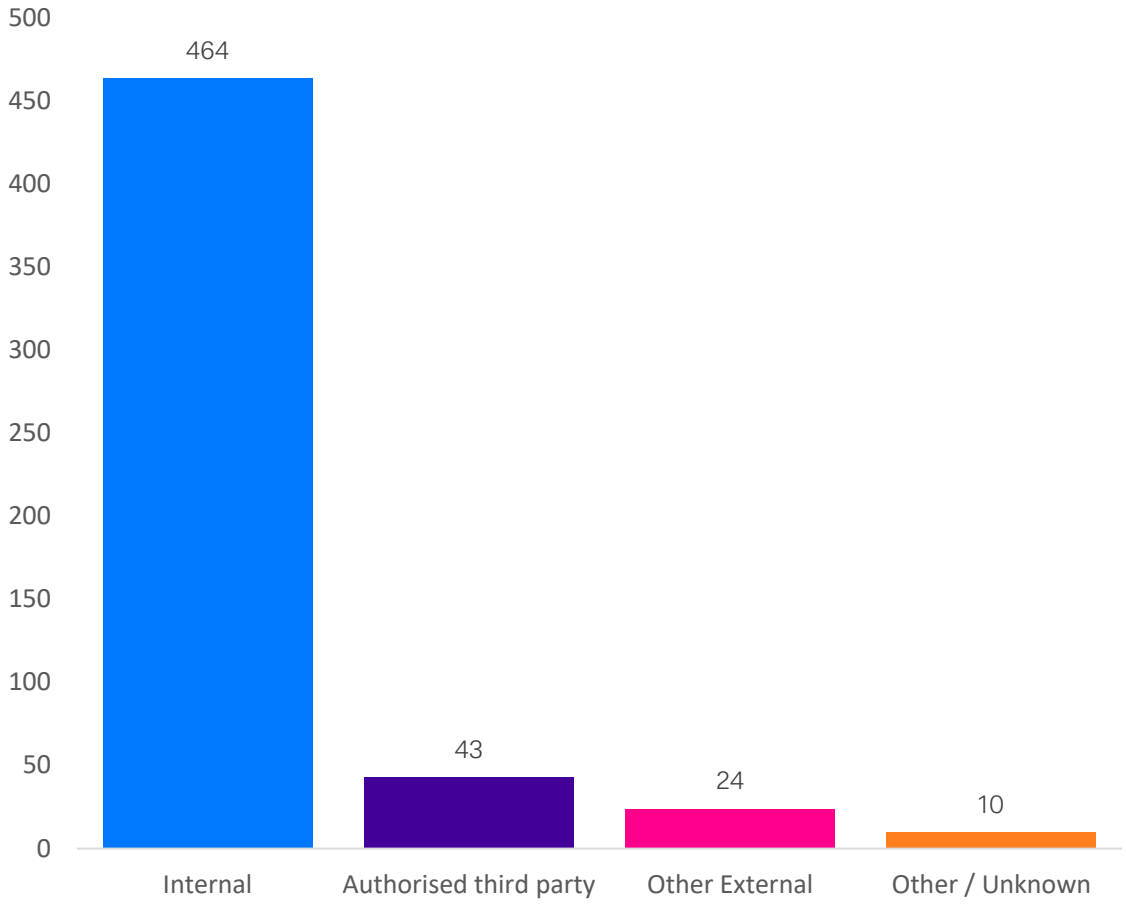
# Control areas

- **84%** of incidents were caused by **people**.
- There was a decrease in incidents caused by **process** and **technology** issues.
- 1 incident was caused by all control areas **(people, process, technology and no control(s) in place).**



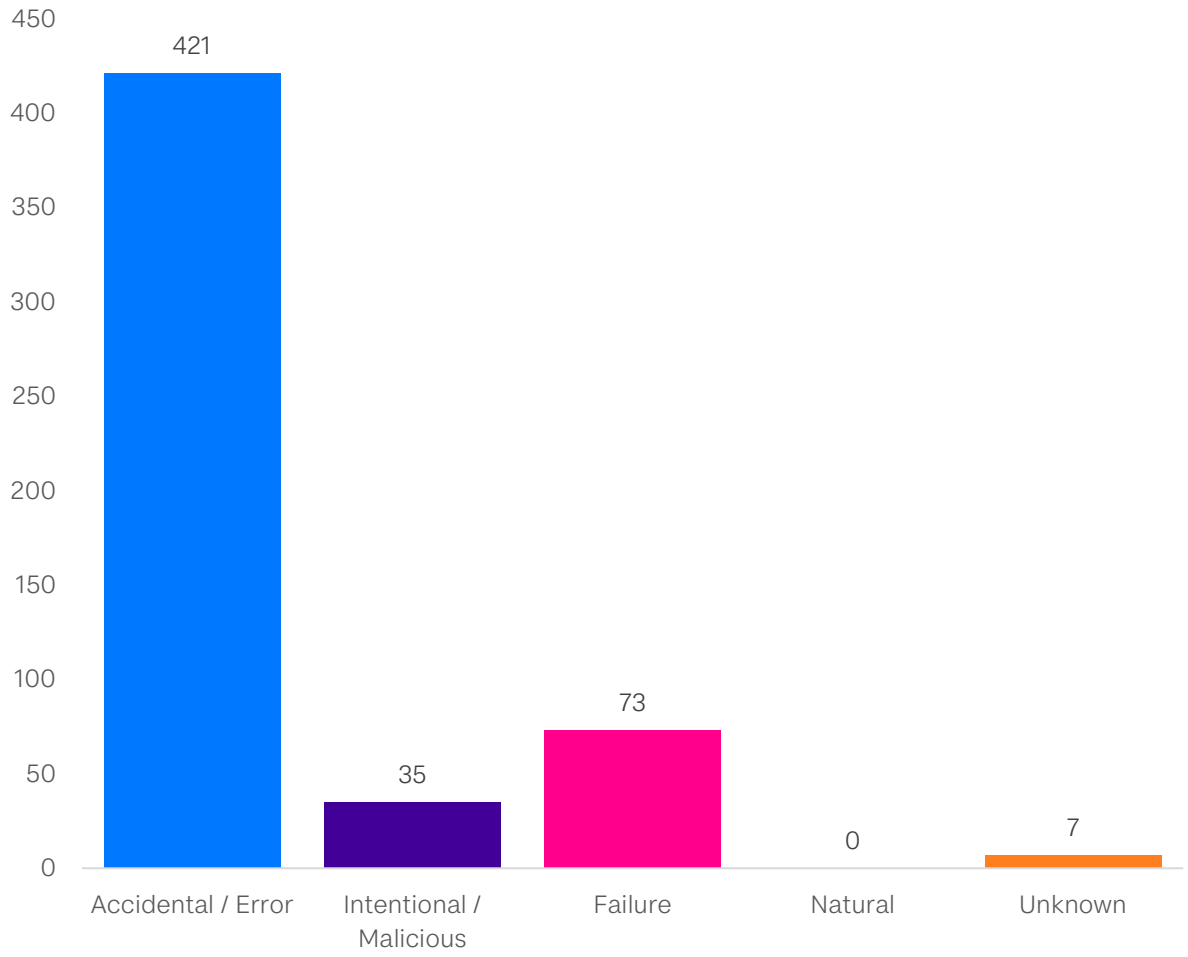
# Threat actors

- **88%** of incidents were caused **internally**.
- **43** incidents were caused by **authorised third parties** such as contracted service providers.
- **12** incidents were caused by multiple threat actors.



# Threat types

- **421** incidents were caused by **accidental actions.**
- **35** incidents were due to **intentional** actions of the threat actor.
- There were **7** incidents caused by more than one threat type.



# Risk statements

| The risk of... | caused by... | resulting in... | |
|---|---|---|---|
| Unauthorised use of corporate system(s) to evade detection of inappropriate actions | Intentional actions of a staff member installing unauthorised software and disabling multiple security controls on their computer | Impact on public services (reputation of, and confidence in, the organisation) | I |
| Defaced Victorian government website | Malicious external threat actor hacking a website and replacing Victorian government information with inappropriate content | Impact to service delivery<br>Impact on public services (reputation of, and confidence in, the organisation) | I A |
| Unauthorised access to and use of ChatGPT to produce reports | Staff member uploading confidential information onto commercial large language model and copying output into a new document | Impact to individuals whose personal information was affected<br>Impact on public services (reputation of, and confidence in, the organisation) | C |

# Questions for OVIC?

## Contact the Information Security Unit

security@ovic.vic.gov.au

Have your say on this VISN event -
https://forms.cloud.microsoft/r/GNGiUmRxdH

# Guest speaker

Dr. Carl Gibson

# Deputy Commissioner – closing remarks

**Anthony Corso**

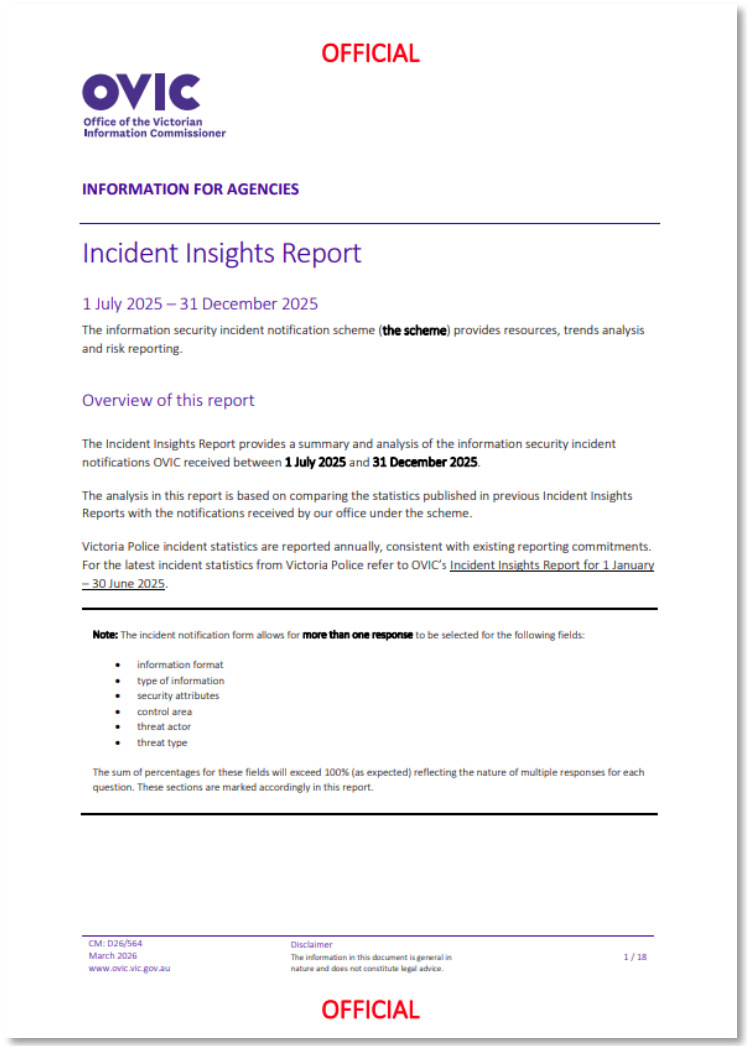
Acting Deputy Commissioner, Privacy and Data Protection

To read OVIC's Incident Insights reports visit:

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

To notify OVIC of an incident, visit:

https://incident-notifications.ovic.vic.gov.au/



OFFICIAL

OVIC Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Incident Insights Report

1 July 2025 – 31 December 2025

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

Overview of this report

The Incident Insights Report provides a summary and analysis of the information security incident notifications OVIC received between **1 July 2025** and **31 December 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 annually, consistent with existing reporting commitments. For the latest incident statistics from Victoria Police refer to OVIC's Incident Insights Report for 1 January – 30 June 2025.

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

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

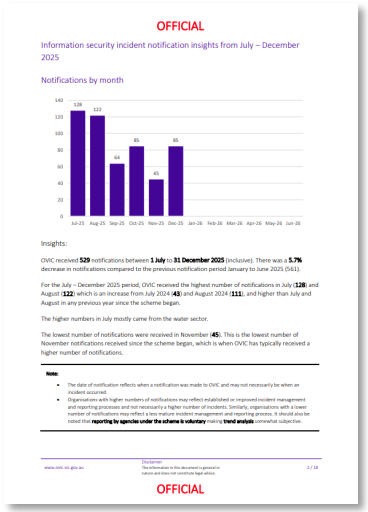
The sum of percentages for these fields will exceed 100% (as expected) reflecting the nature of multiple responses for each question. These sections are marked accordingly in this report.

CM: D26/564
March 2026
www.ovic.vic.gov.au

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

1 / 18

OFFICIAL



OFFICIAL

Information security incident notification insights from July – December 2025

Notifications by month



Insights:

OVIC received **529** notifications between **1 July** to **31 December 2025** (inclusive). There was a **5.7%** decrease in notifications compared to the previous notification period January to June 2025 (561).

For the July – December 2025 period, OVIC received the highest number of notifications in July (**128**) and August (**122**) which is an increase from July 2024 (**43**) and August 2024 (**111**), and higher than July and August in any previous year since the scheme began.

The higher numbers in July mostly came from the water sector.

The lowest number of notifications were received in November (**45**). This is the lowest number of November notifications received since the scheme began, which is when OVIC has typically received a higher number of notifications.

**Note:**

- The date of notification reflects when a notification was made to OVIC and may not necessarily be when an incident occurred.
- Organisations with higher numbers of notifications may reflect established or improved incident management and reporting processes and not necessarily a higher number of incidents. Similarly, organisations with a lower number of notifications may reflect a less mature incident management and reporting process. It should also be noted that **reporting by agencies under the scheme is voluntary** making **trend analysis** somewhat subjective.

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

OFFICIAL

OFFICIAL

Information format (multiple options can be selected)




Insights:

Most incidents related to compromises of **electronic** information (**405**), followed by **hard copy** information (**123**). These numbers differ compared to the previous notification period. This notification period saw an increase in electronic information incidents compared to the previous notification period of 360, and a decrease in hard copy incidents which was previously 197.

The number of incidents involving **verbal** information (**16**) was consistent with the previous notification periods January to July 2025 (15), July to December 2024 (18), January to June 2024 (16) and July to December 2023 (17). All of these incidents relate to unauthorised disclosure/oversharing of public sector information. Some examples of verbal disclosures include using an incorrect name when speaking on the phone and disclosing personal information to another person prior to consent being provided.

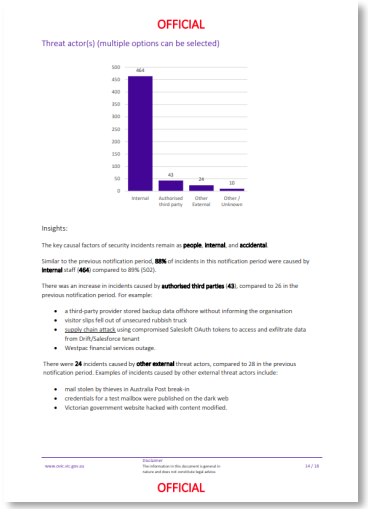
**66%** of the incidents affecting electronic information related to emails, which is similar to the previous notification period with 64%. There was a slight decrease in incidents involving hard copy mail with **73%** in this notification period compared with 79%.

Most (**92%**) of incidents had an element of unauthorised release/disclosure of information, regardless of information format. This is similar to the previous notification period which was 91%. Typical examples include misdirected emails and mail, however additional examples include:

- visitor slips falling out of an unsecured rubbish truck
- hard copy paper that already had information on it was re-used to print a new document
- paperwork lost when left on top of a vehicle
- documents printed to another agency's printer
- mail merge error with infringement notices printed double sided.

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

OFFICIAL



OFFICIAL

Threat actor(s) (multiple options can be selected)




Insights:

The key causal factors of security incidents remain as **people**, **internal**, and **accidental**.

Similar to the previous notification period, **88%** of incidents in this notification period were caused by **internal** staff (**404**) compared to 89% (502).

There was an increase in incidents caused by **authorised third parties** (**43**), compared to 26 in the previous notification period. For example:

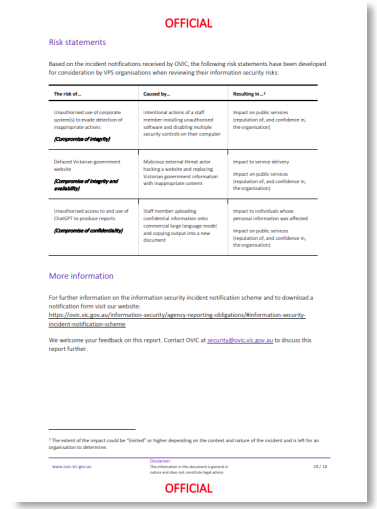
- a third-party provider stored backup data offshore without informing the organisation
- visitor slips fell out of unsecured rubbish truck
- supply chain attack using compromised Salesloft OAuth tokens to access and exfiltrate data from Drift/Salesforce tenant
- Westpac financial services outage.

There were **24** incidents caused by **other external** threat actors, compared to 28 in the previous notification period. Examples of incidents caused by other external threat actors include:

- mail stolen by thieves in Australia Post break-in
- credentials for a test mailbox were published on the dark web
- Victorian government website hacked with content modified.

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

OFFICIAL



OFFICIAL

Risk statements

Based on the incident notifications received by OVIC, the following risk statements have been developed for consideration by VPS organisations when reviewing their information security risks:

| The risk of... | Caused by... | Resulting in...* |
|---|---|---|
| Unauthorised use of corporate system(s) to evade detection of inappropriate actions<br>**(Compromise of integrity)** | Intentional actions of a staff member installing unauthorised software and disabling multiple security controls on their computer | Impact on public services (reputation of, and confidence in, the organisation) |
| Defaced Victorian government website<br>**(Compromise of integrity and availability)** | Malicious external threat actor hacking a website and replacing Victorian government information with inappropriate content | Impact to service delivery<br>Impact on public services (reputation of, and confidence in, the organisation) |
| Unauthorised access to and use of ChatGPT to produce reports<br>**(Compromise of confidentiality)** | Staff member uploading confidential information onto commercial large language model and copying output into a new document | Impact to individuals whose personal information was affected<br>Impact on public services (reputation of, and confidence in, the organisation) |

More information

For further information on the information security incident notification scheme and to download a notification form visit our website: https://ovic.vic.gov.au/information-security/agency-reporting-obligations/#information-security-incident-notification-scheme

We welcome your feedback on this report. Contact OVIC at security@ovic.vic.gov.au to discuss this report further.

* The extent of the impact could be "limited" or higher depending on the context and nature of the incident and is left for an organisation to determine.

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

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**

Contact the Information Security Unit by emailing:

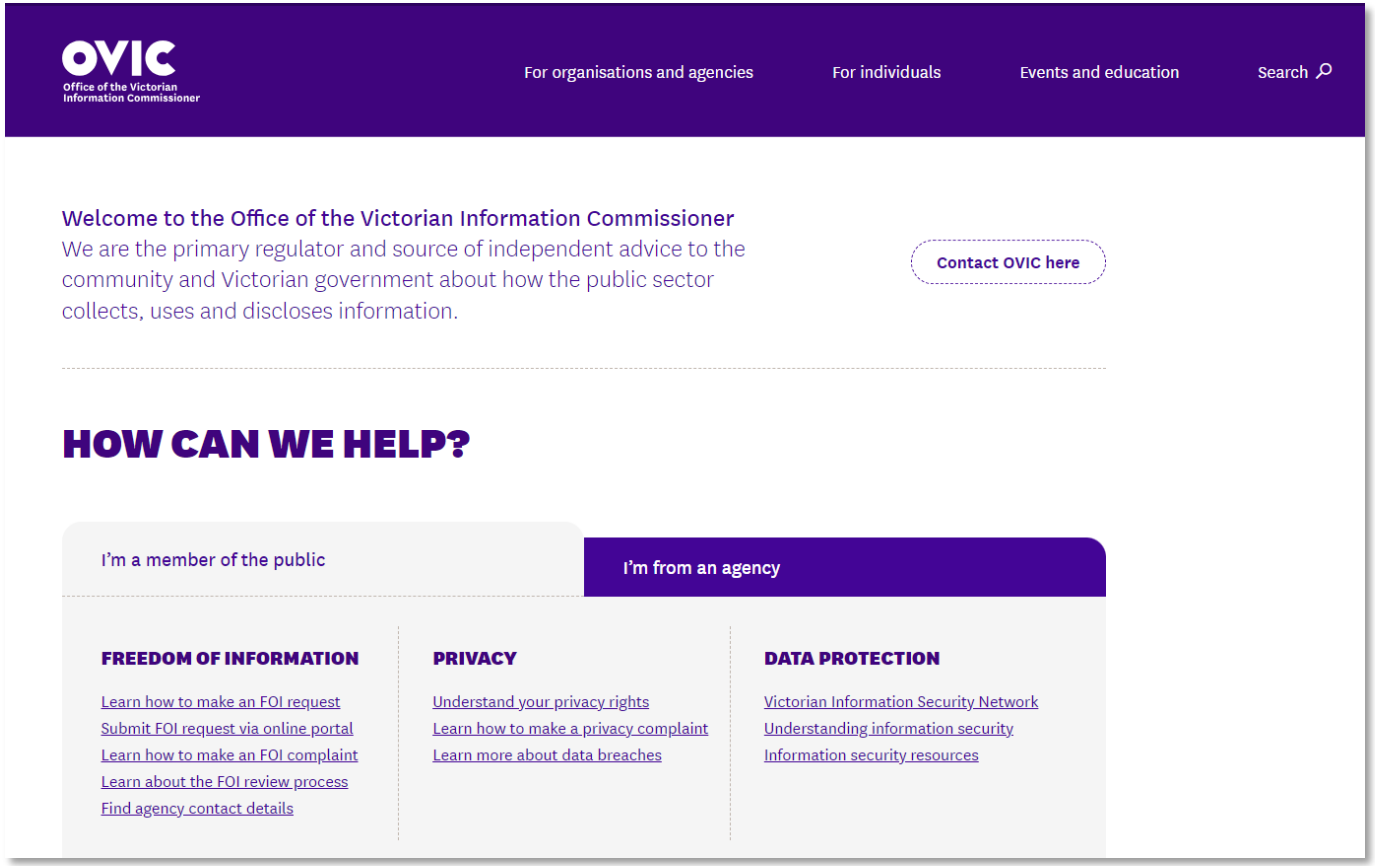
**security@ovic.vic.gov.au**

**incidents@ovic.vic.gov.au**

or call:

**1300 00 OVIC**

Have your say on this VISN event - https://forms.cloud.microsoft/r/GNGiUmRxdH



ovic.vic.gov.au