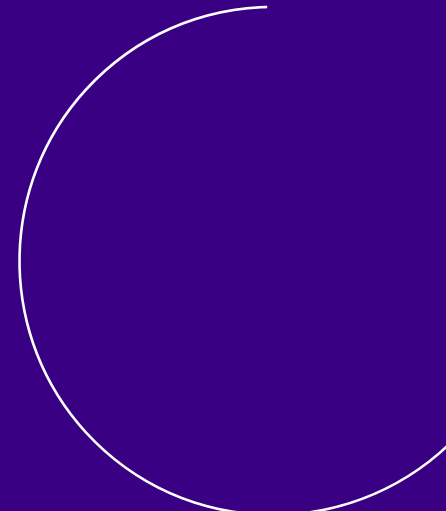
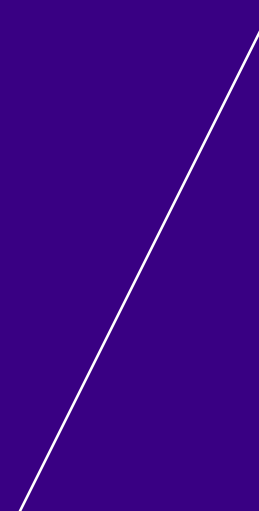
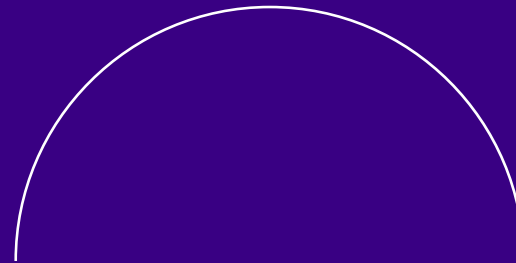


# *Information Security Incident Insights Forum*

Victorian Information Security Network (VISN)  
March 2025



A reminder – Today's session  
is being recorded.



# Acknowledgment of Country

## Anthony Corso

Assistant Commissioner –  
Information Security

*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.*

# Assistant Commissioner's welcome

## Incident Insights Reports

2024

Download the [Incidents Insights report for 1 July to 31 December 2024 as a Word file \(.docx\)](#) or download the [Incidents Insights report for 1 July to 31 December 2024 as a PDF file](#)

Download the [Incidents Insights report for 1 January to 30 June 2024 as a Word file \(.docx\)](#) or download the [Incidents Insights report for 1 January to 30 June 2024 as a PDF file](#)

2023

[Download the Incidents Insights report for 1 July 2023 to 31 December 2023 \(.docx\)](#)

[Download the Incidents Insights report for 1 January to 30 June 2023 \(.docx\)](#)

2022

[Download the Incidents Insights report for 1 July to 31 December 2022 \(.docx\)](#)

[Download the Incidents Insights report for 1 January to 30 June 2022 \(.docx\)](#)

2021

[Download the Incidents Insights report for 1 July 2021 to 31 December 2021 \(.docx\)](#)

[Download the Incidents Insights report for 1 January 2021 to 30 June 2021 \(.docx\)](#)

2020

[Download the Incidents Insights report for 1 July 2020 to 31 December 2020 \(.docx\)](#)

[Download the Incidents Insights report for 29 October 2019 to 30 June 2020 \(.docx\)](#)



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

**Anthony Corso**  
Assistant Commissioner –  
Information Security

# *Housekeeping*

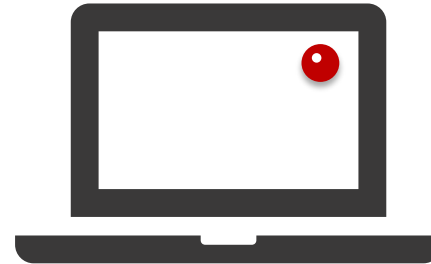
**Anthony Corso**

*Assistant Commissioner – Information Security (OVIC)*

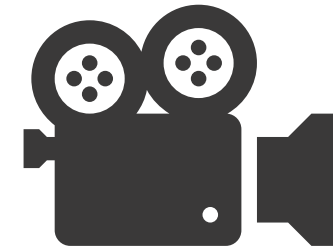
# Housekeeping



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

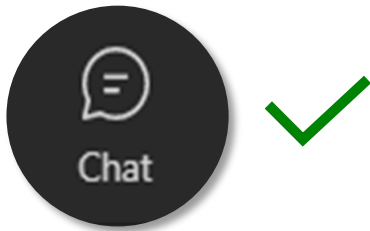
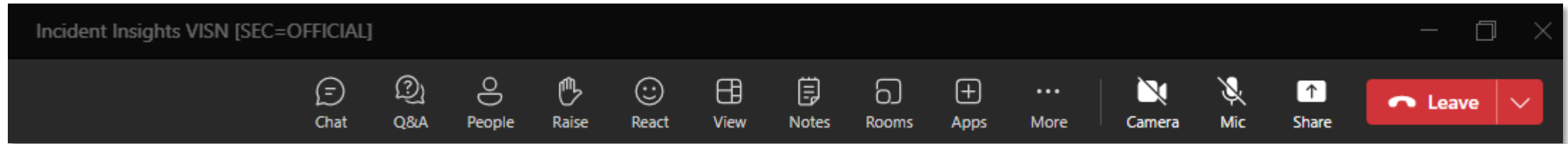


Today's session is being recorded.



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 speakers from VMIA
- Session close

OFFICIAL

# *Information Security Incident Notification Scheme*

OFFICIAL



# 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 should 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.

# 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

The screenshot shows the 'Incidents Notification Form' interface. At the top, a purple header contains the title and a progress bar with five steps: 1. Introduction, 2. Information about the incident, 3. Privacy incidents, 4. Incident notification scheme, and 5. Thank you. Below the header, the main content area is split into two sections. The left section has a white background and contains the text 'Information security and privacy incident notification form'. The right section has a light grey background and features a 'Start the form' button, followed by the text: 'This form will take 15 - 30 minutes to complete.' and 'You will be emailed a copy of your submission.'

## Option 2: Downloadable Incident Notification form

The screenshot shows a downloadable form titled 'Information Security and Privacy Incident Notification Form'. At the top, it says '[CHOOSE A PROTECTIVE MARKING]' in red. Below this is the OVIC logo and the text 'Office of the Victorian Information Commissioner'. The form includes a paragraph explaining that organisations subject to the Victorian Protective Data Security Standards (VPDSS) must notify OVIC of certain information security incidents, and that organisations 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. It states that any organisation subject to the PDP Act can use this form to report incidents to OVIC, whether voluntarily or by obligation. The form provides contact information: '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' with a table of fields for completion:

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?	

At the bottom of the form, it says 'www.ovic.vic.gov.au OVIC ref: 022/21438' and '[CHOOSE A PROTECTIVE MARKING]' in red.



## Option 3: Email to [incidents@ovic.vic.gov.au](mailto:incidents@ovic.vic.gov.au)

*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

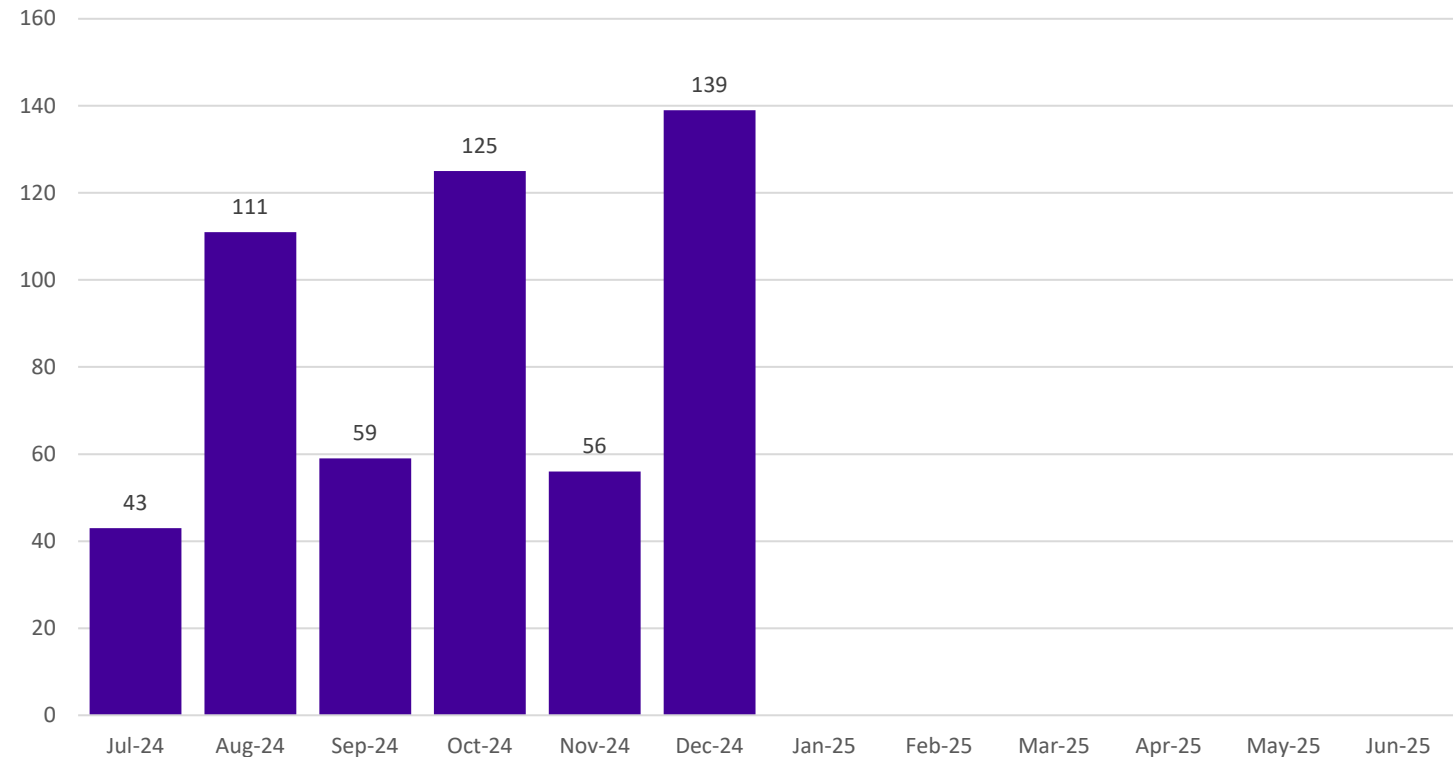


Threat  
types



# Volume – Notifications by month

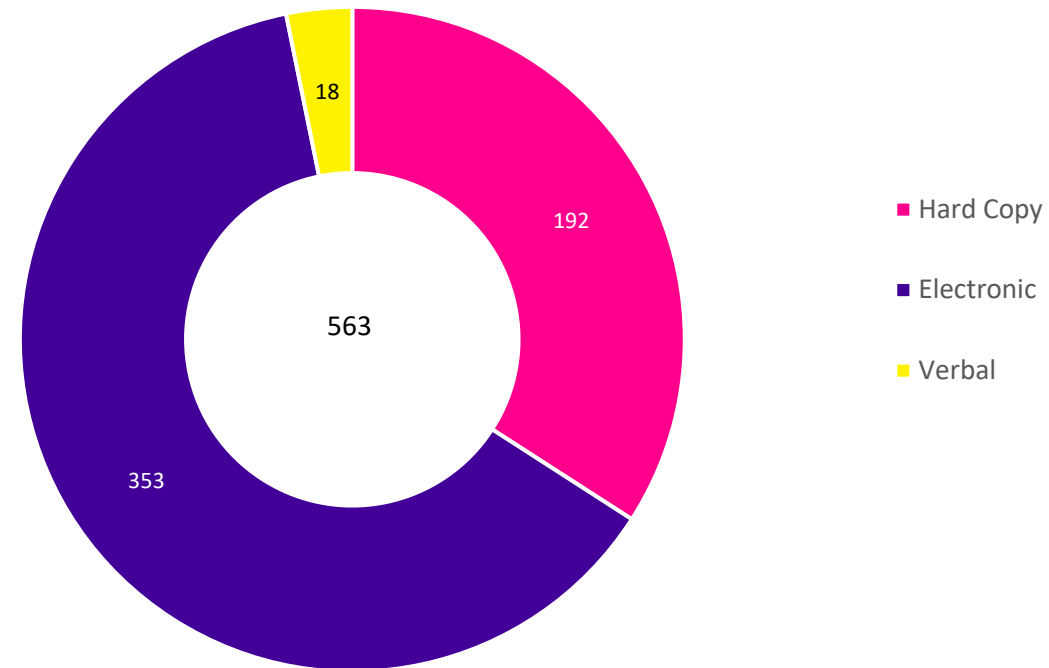
- OVIC received **533** notifications between **1 July** to **31 December 2024**.
- This is a **39%** increase compared to the previous notification period.





# Information format

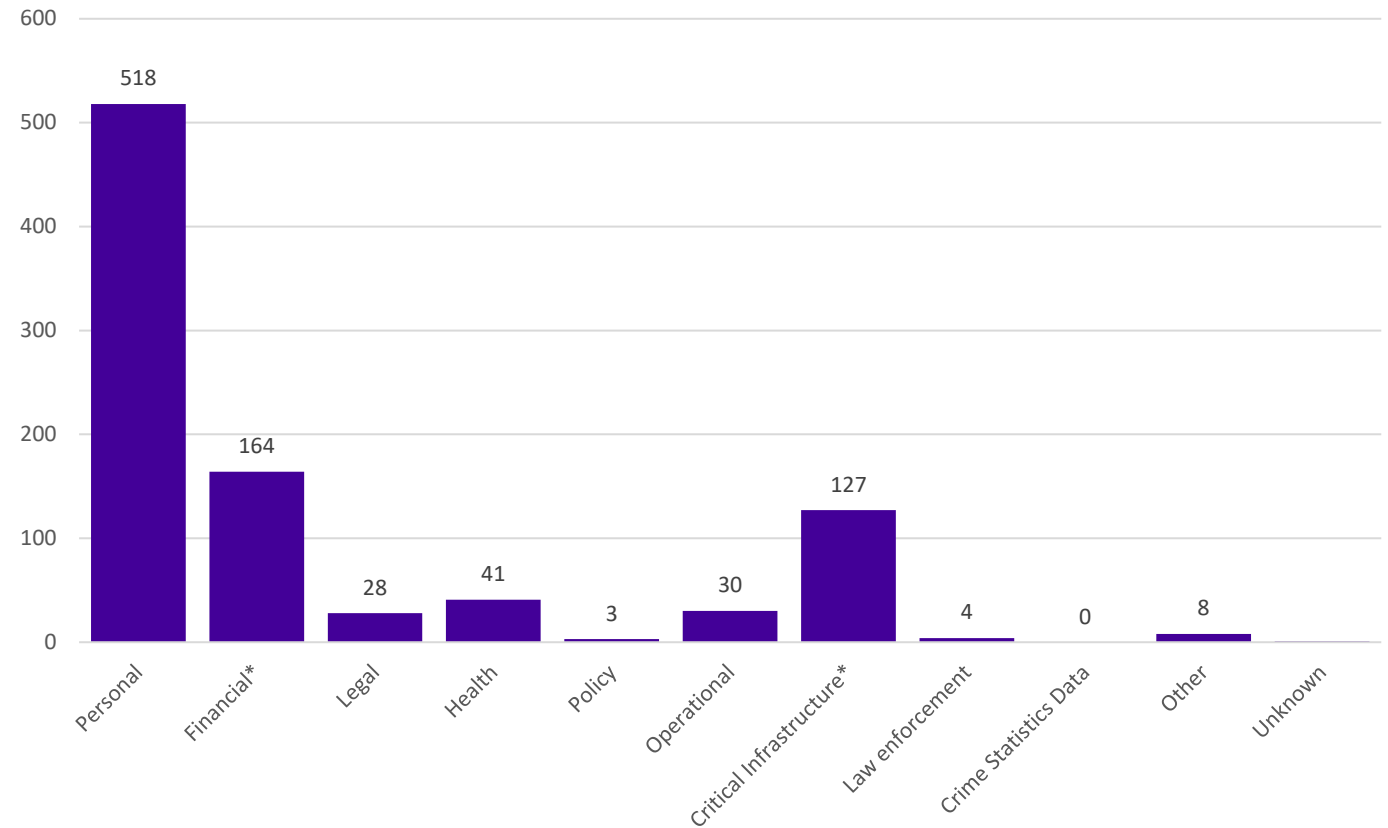
- 353 notifications indicate compromises of **electronic information**.
- Half of the incidents affecting electronic information related to emails (54%) - predominantly **sending emails to the incorrect recipient**.
- 78% of incidents involving hard copy information were related to **mail**.





# Information type

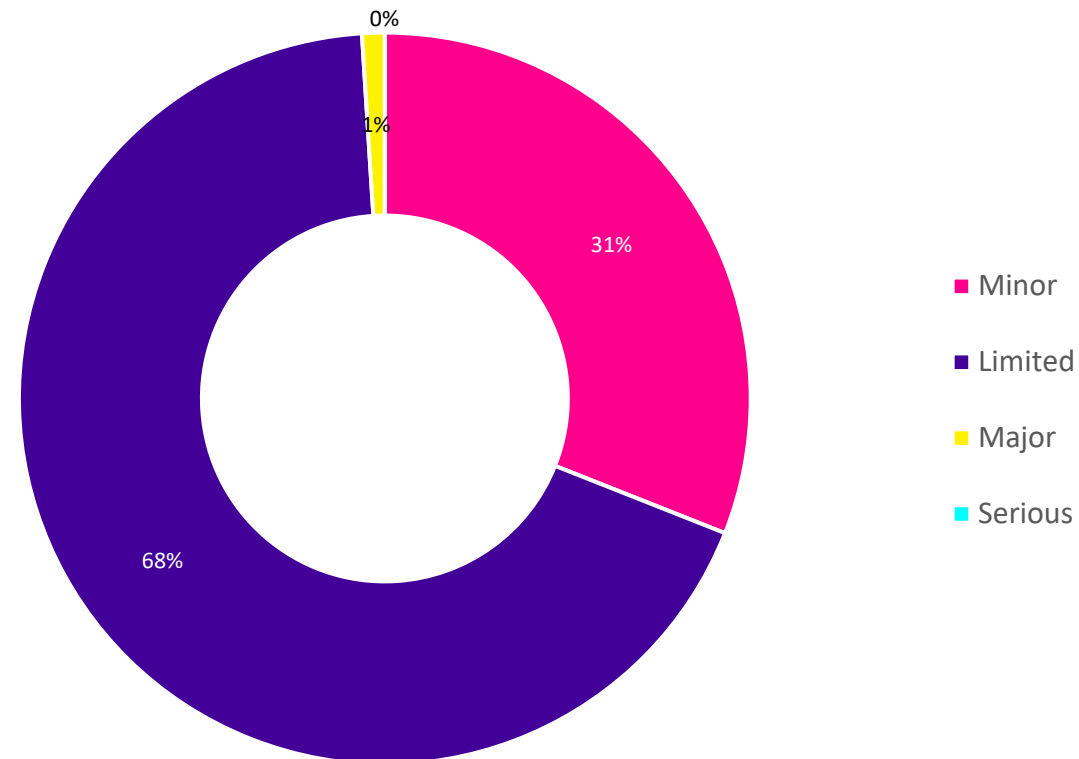
- **97%** incidents indicate compromises of **personal** information.
- **15** incidents involved three or more information types.
- There were **8** incidents that selected **Other** e.g., commercially sensitive information, safety and wellbeing reports, incident trends and theme analysis.





# Business Impact Level (BIL)

- **68%** of incidents were assessed as impacting **BIL 2** information (Limited harm or damage).
- **5** incidents affected **BIL 3** information.
- If in doubt of the BIL just notify.

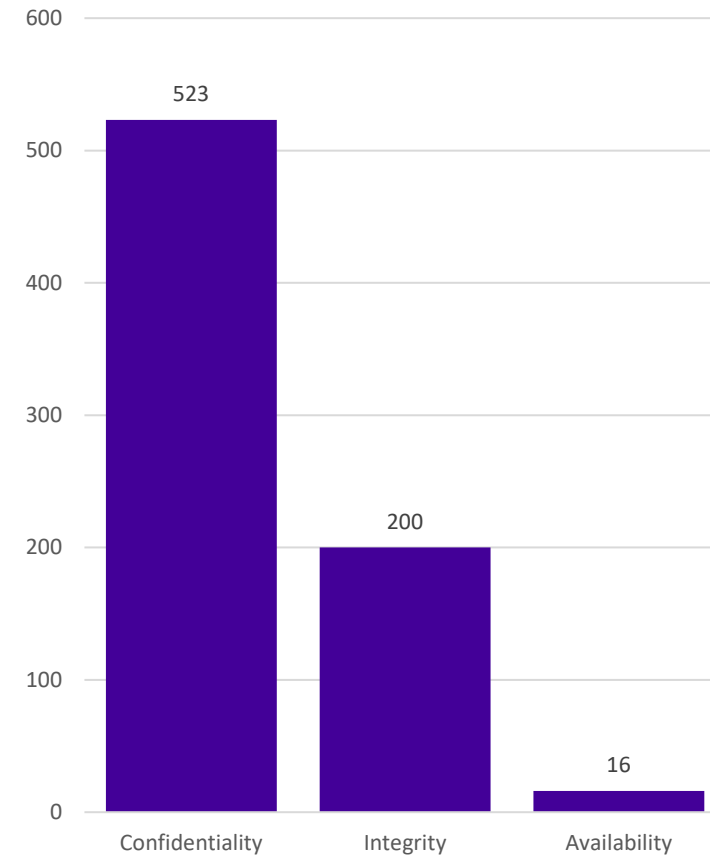






# Security attributes

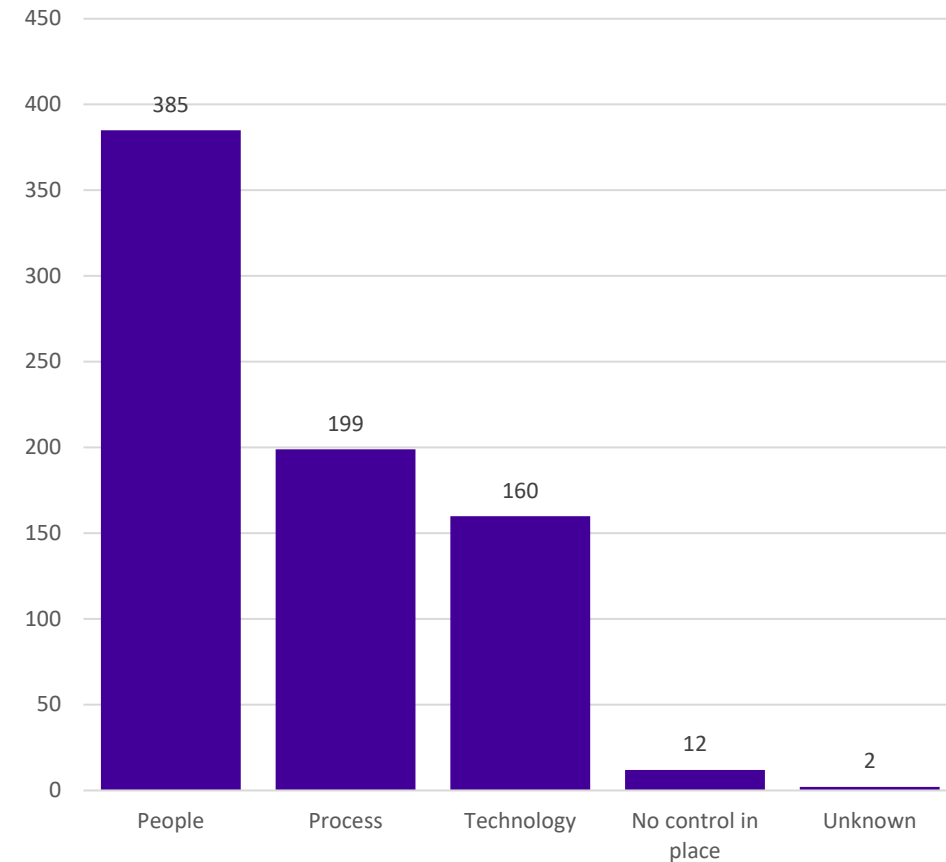
- **523** incidents were compromises of the **confidentiality** of information.
- **4** incidents affected all three security attributes (**confidentiality, integrity and availability**).





# Control areas

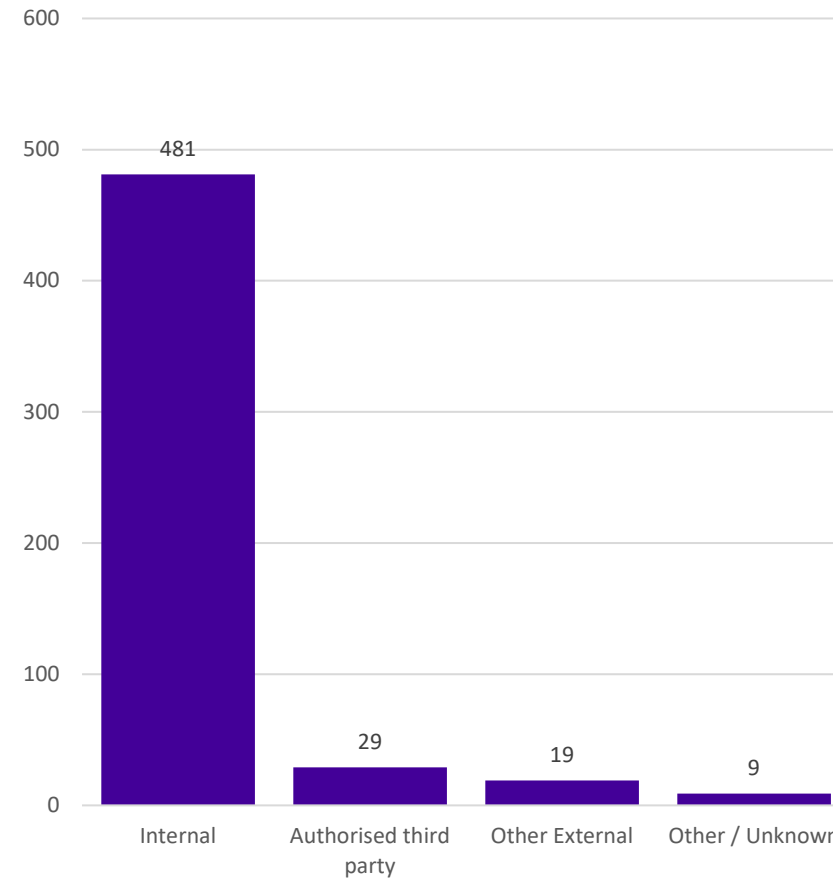
- 72% of incidents were caused by people.
- There was a large increase in incidents caused by **process** and **technology** issues.
- 5 incidents were caused by all three control areas.





# Threat actors

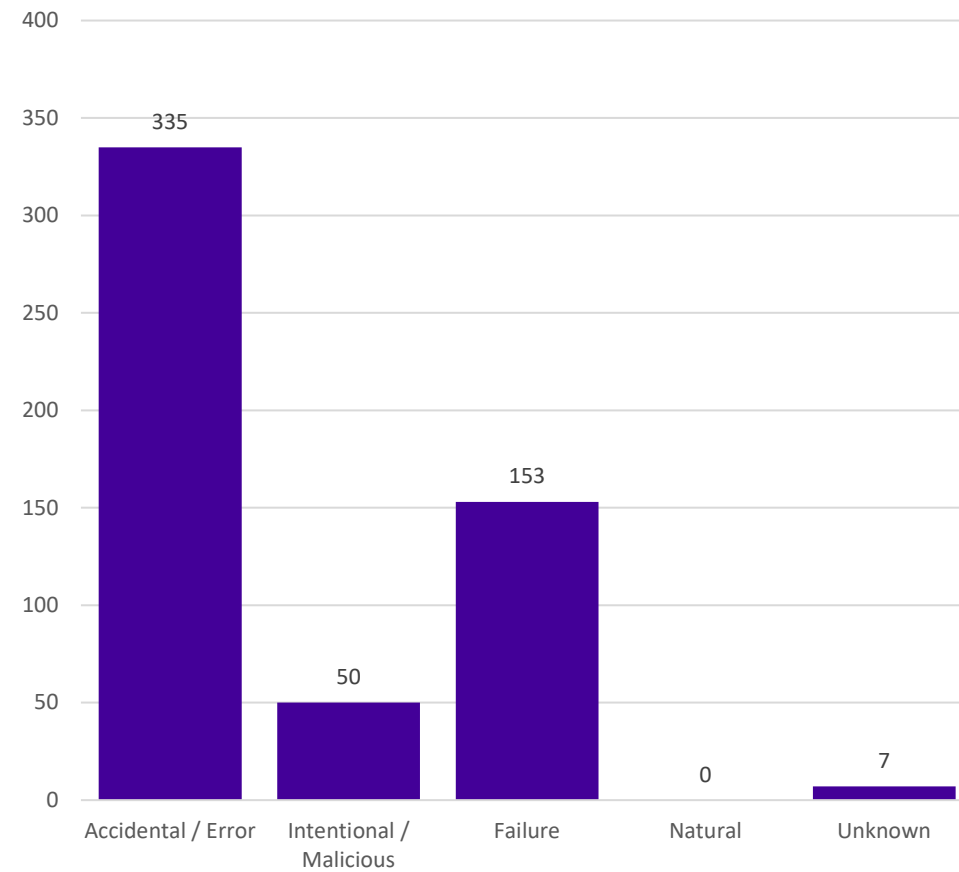
- **90%** of incidents were caused **internally**.
- **29** incidents were caused by **authorised third parties** such as contracted service providers.
- **5** incidents were caused by multiple threat actors.





# Threat types

- 63% of incidents were caused by **accidental actions**.
- 9% of 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...

caused by...

resulting in...

Unauthorised disclosure of personal information due to utility bills being sent to incorrect recipient(s)

System upgrade project with poor data quality

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

C  
IA

Unauthorised disclosure of identity documentation

Accidental errors by internal staff not paying attention to detail or applying due diligence

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

C

Inability to access an online Workplace Health and Safety Management platform to undertake normal operational duties

Reliance on authorised third party hosting the platform and being unavailable to answer/return any calls

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

A

## *Questions for OVIC?*

Contact the Information Security Unit  
[security@ovic.vic.gov.au](mailto:security@ovic.vic.gov.au)

# *Victorian Managed Insurance Authority (VMIA)*

**Gresa Halili**

*Client Capability Adviser (VMIA)*

**Nathan Lane**

*Senior Claims Specialist (VMIA)*



# Cyber Insurance and Risk Training

STANDARD







## Agenda

- About VMIA
- VMIA cyber insurance
- What happens when a claim or incident occurs
- Cyber claims – insights and learnings
- Cyber claim case study
- Risk resources and client learning



## About VMIA

VMIA is the Victorian Government's insurer and risk adviser, covering the people, places and projects that help Victorians thrive.

Our purpose is to support a confident, resilient Victoria through world-leading harm prevention and recovery.



Insurance



Harm prevention



Claims reduction



Risk advice



## What the policy covers

Your Expenses	Liability Cover
<ul style="list-style-type: none"><li>• Computer expert services</li><li>• Legal services</li><li>• Notification to affected persons and/or privacy regulators</li><li>• Call centre services</li><li>• Public relations and crisis management</li><li>• Credit monitoring or identity monitoring products</li><li>• Restoring or recreating impacted systems and data</li><li>• Business interruption loss.</li></ul>	<ul style="list-style-type: none"><li>• Defence of claims made by third parties due to a personal information data breach</li><li>• Legal liability to pay compensation</li><li>• Regulatory defence and penalties for a violation of a privacy law</li><li>• Failure to comply with a privacy policy</li><li>• Failure to prevent transmission of malicious code to outside parties</li><li>• Personal confidential information fines (theft/loss of payment card data).</li></ul>

## What the policy does not cover

- Security uplift of systems
- Contractual liability
- Bodily injury and property damage.

Depending on the facts and circumstances of a claim, other VMIA policies may respond to secondary Bodily Injury and/or Property Damage from a cyber event.

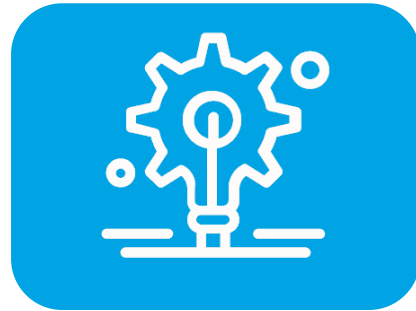
# What happens when a claim or incident occurs



## VMIA Claims Process



Contact the DGS Cyber Incident Response Service (CIRS)



Contact VMIA to lodge a claim and get immediate access to support services

- CIRS supports all Victorian Government organisations to respond to cyber security incidents.
- VMIA works collaboratively with CIRS following a client claim notification involving a major cyber incident to ensure that appropriate cyber vendor support services are provided to impacted clients through VMIA's panel of providers.
- VMIA can facilitate progress payments to your organisation to cover incurred costs and expenses that are verified and covered under the policy.

## VMIA Support Services

The VMIA has access to vendors that specialise in the following areas of cyber incident response:

- IT Forensic
- Legal advice (privacy breach)
- Data analysis
- Privacy impact assessments
- Notification
- Public relations and call centres
- Reducing harm of identity misuse
- Credit/Identity monitoring
- Dark web monitoring.

## Cyber Claims

### Key insights and learnings

A summary of the key IT forensic investigation recommendations post-incident:

### TOP 3

- Periodically resetting passwords and increasing password length and complexity. Consider privileged access management solutions to protect administrator, system and service accounts.
- Enforcing mandatory multi-factor authentication (MFA) requirement for every VPN session connection or re-design network and IDAM architecture to not use VPN.
- Implement geo-blocking and conditional access policies to restrict network access based on geographical location and other high-risk conditions.

### OTHER RECOMMENDATIONS

- Upgrade and/or replace unsupported systems and servers.
- Upgrade and/or replace existing firewalls and security monitoring tools.
- Network segmentation to prevent lateral movement for attackers.
- Keep operating systems and applications up to date with security patches.
- ICT Disaster Recovery plans and BCP plans stored offline and air gapped.
- Regular phishing simulation and user awareness training.
- Review data retention policies and ensure archived data is not stored on live servers.

## Cyber incident involving ransomware

Threat Actor has gained access to network using stolen credentials, encrypting network files and exfiltrating 100GB of data that is published on the Dark Web.

















### VMIA cyber insurance policy response

- > Specialist support services for breach response
- > Notification to affected individuals
- > System restoration and business interruption loss cover
- > Liability cover involving third-party claims



# Our training



 <p><b>April 8</b> Tuesday</p> <p> Risk Foundations</p> <p>VMIA clients only <b>Risk Foundations</b></p> <p> Online via TEAMS  08 Apr 2025, 10:00AM-12:30PM</p> <p>This session provides an introduction to the world of risk management.</p> <p><a href="#">Find out more &gt;</a></p>	 <p><b>April 11</b> Friday</p> <p> Cyber Risk Foundations</p> <p>VMIA clients only <b>Cyber Risk Foundations</b></p> <p> VMIA, Level 10 161 Collins St, Melbourne, 3000  11 Apr 2025, 10:00AM-2:00PM</p> <p>This workshop's designed to demystify cyber risk and provide risk practitioners with an overview of government's expectations, the Essential 8 mitigation strategies and how to use the popular bow tie tool to visualise these risks.</p> <p><a href="#">Find out more &gt;</a></p>	 <p><b>April 15</b> Tuesday</p> <p> Risk Culture Enabler</p> <p>VMIA clients only <b>Risk Culture Enabler</b></p> <p> VMIA, Level 10 161 Collins Street , Melbourne, 3001  15 Apr 2025, 10:00AM-3:00PM</p> <p>This session provides an overview of risk culture and how it impacts risk management.</p> <p><a href="#">Find out more &gt;</a></p>	 <p><b>May 1</b> Thursday</p> <p> Risk Appetite Foundations</p> <p>VMIA clients only <b>Risk Appetite Foundations</b></p> <p> VMIA, Level 10 South 161 Collins Street, Melbourne, 3000  01 May 2025, 10:00AM-3:00PM</p> <p>Defining and sharing your risk appetite statement informs decision makers how much risk your organisation will take and create. Find out more in this workshop.</p> <p><a href="#">Find out more &gt;</a></p>
---	---	---	--

# Practical guidance for managing risk

Risk thinking and management techniques can help you make better decisions everyday and into the future.



- Risk advice & support
- Risk management tools
- Risk Maturity Benchmark
- Cyber Maturity Benchmark

Search

I need to

Skill level

Risk Maturity Benchmark topic

Clear all

Our risk guidance materials are based on the updated [Victorian Government Risk Management Framework \(VGRMF\)](#) and [AS ISO 31000](#). If you have any questions or need some assistance, please reach out to [contact@vmia.vic.gov.au](mailto:contact@vmia.vic.gov.au).

Showing 8 out of 11 results



## Design, implement and evaluate your controls

Explore how effectively controlling a risk may reduce the likelihood of the event or the severity of its potential impact.



## What is risk?

To be able to assess risks, it's important to first understand what it is and how it can help you create and protect value for your organisation.



## Assure your responsible body

Assurance is about giving your responsible body confidence that decision-makers are exercising delegated power effectively, efficiently and ethically.



## Identifying, analysing and evaluating risks

Necessary steps to consider when assessing risks to your strategies, business plans and projects.





Thank you

[vmia.vic.gov.au](http://vmia.vic.gov.au)



**VICTORIA**  
State  
Government

## *Final thoughts*

**Rachel Dixon**

*Deputy Commissioner, Privacy and Data Protection (OVIC)*

# 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](https://ovic.vic.gov.au)

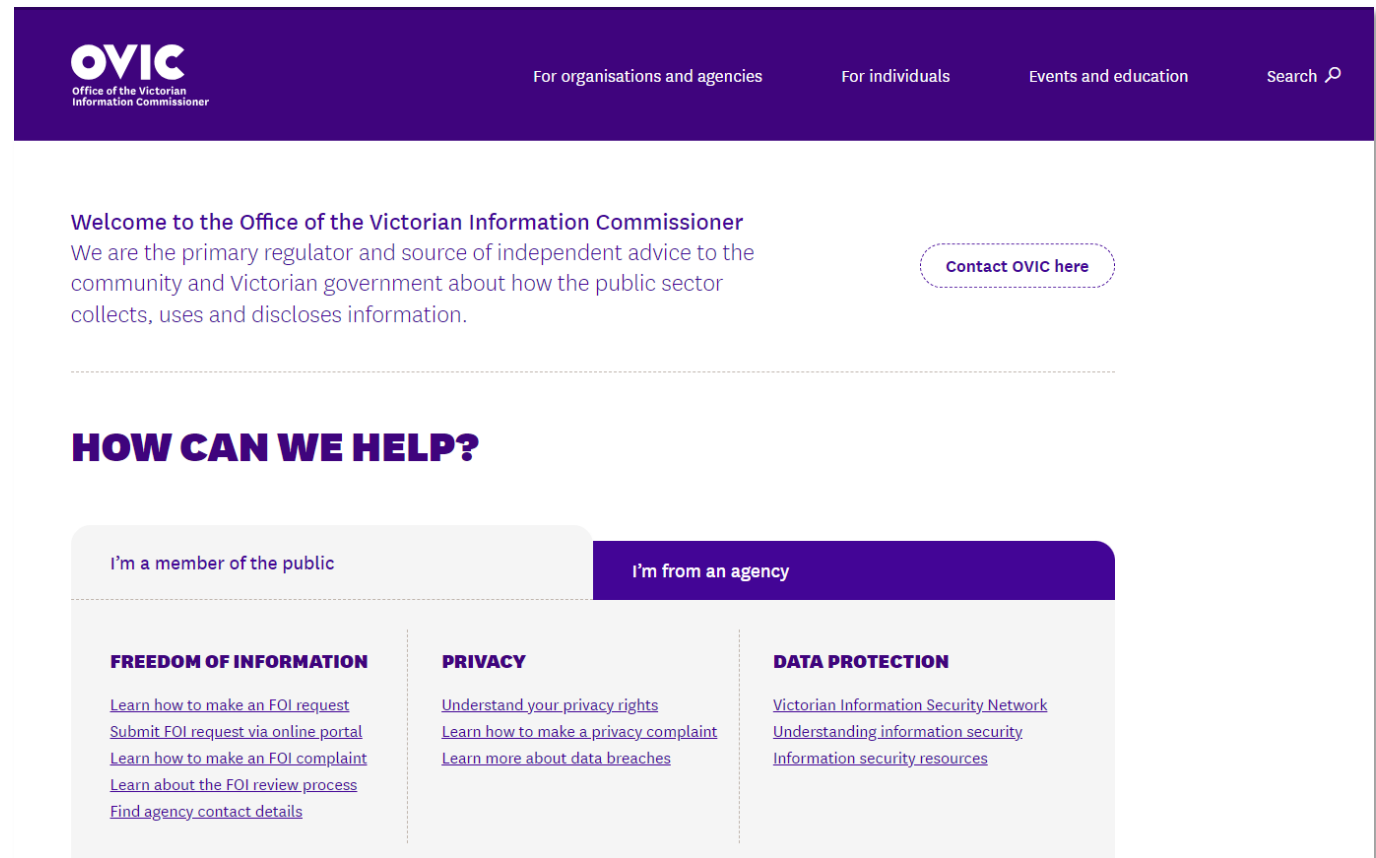
Contact the Information Security Unit by emailing

[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



**OVIC**  
[ovic.vic.gov.au](http://ovic.vic.gov.au)