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.

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 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:

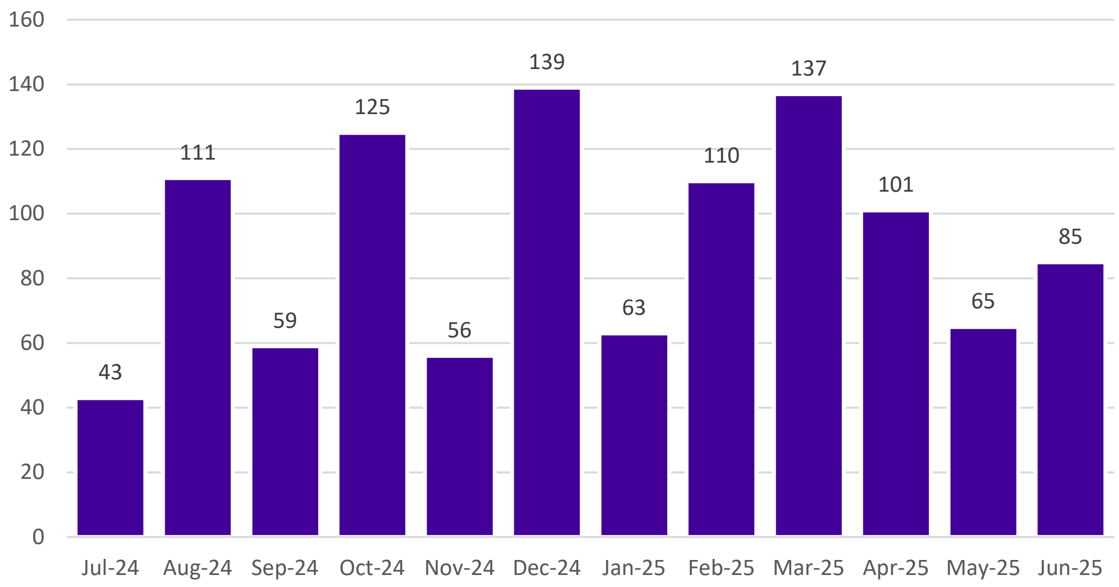
- information format
- type of information
- security attributes
- control area
- threat actor
- threat type

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.

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

Information security incident notification insights from January – June 2025

Notifications by month



Insights:

OVIC received **561** notifications between **1 January** to **30 June 2025** (inclusive). There was a **5%** increase in notifications compared to the previous notification period July to December 2024 (**533 notifications**). This is the highest number of notifications that OVIC has received for any period since the establishment of the information security incident notification scheme.

OVIC received the highest number of notifications in March (**137**) and February (**110**) which is a large increase from March 2024 (**55**) and February 2024 (**47**), and higher than March and February in any previous year since the scheme began.

The higher numbers in March mostly came from organisations who sent through multiple months' worth of notifications.

The lowest number of notifications were received in January (**63**). This is generally a quieter time of the working year; however, this number is still higher than some other months in the previous notification period such as July 2024 (43), and November 2024 (56).

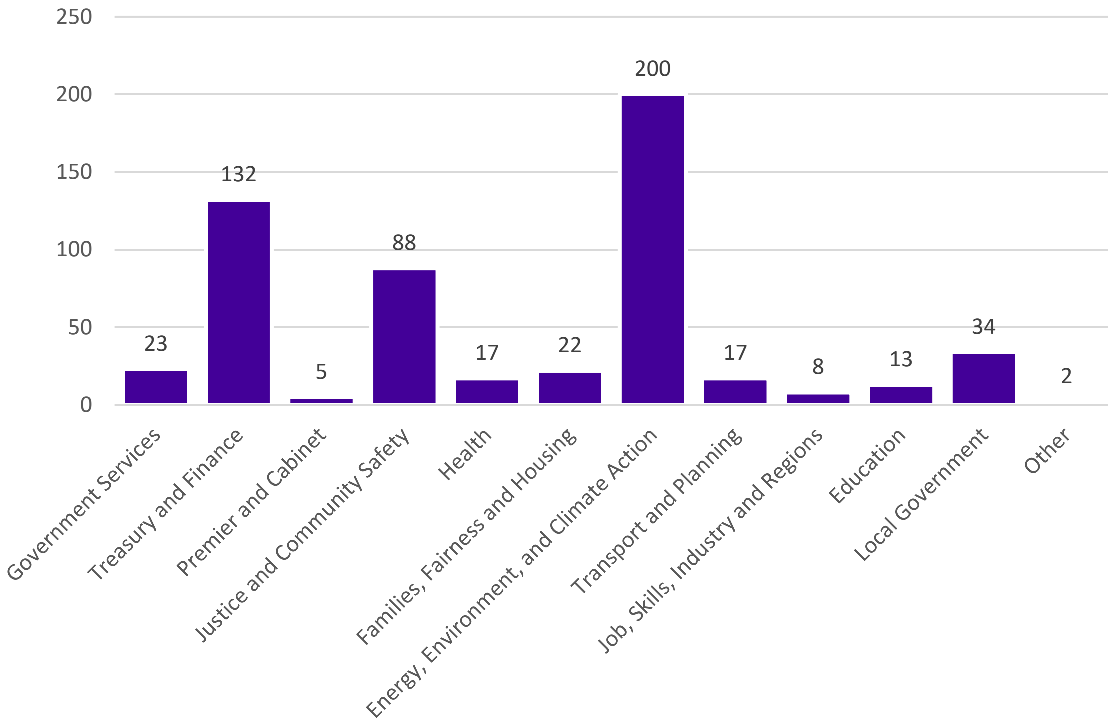
Disclaimer
The information in this document is general in nature and does not constitute legal advice.

Note:

- The date of notification does not necessarily reflect when an incident occurred but rather reflects when a notification was made to OVIC.
- The higher number of notifications from these organisations does not necessarily reflect that they have more incidents but may mean they have established or improved incident management and reporting processes.
- The lower number of notifications from organisations does not necessarily reflect that they have less incidents but may mean they have less mature incident management and reporting processes.

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

Notifications by portfolio



Insights:

Similar to the previous notification period, most of the **561** notifications received by OVIC came from the energy, environment, and climate action portfolio (**200**) followed by the treasury and finance portfolio (**132**). These were mostly from Greater Western Water (**GWW**) and the Transport Accident Commission.

There was an increase in the number of notifications provided by the Department of Government Services from one notification to **23** in this period as the department implements its incident management processes. These 23 notifications included 16 incidents that occurred during 2024.

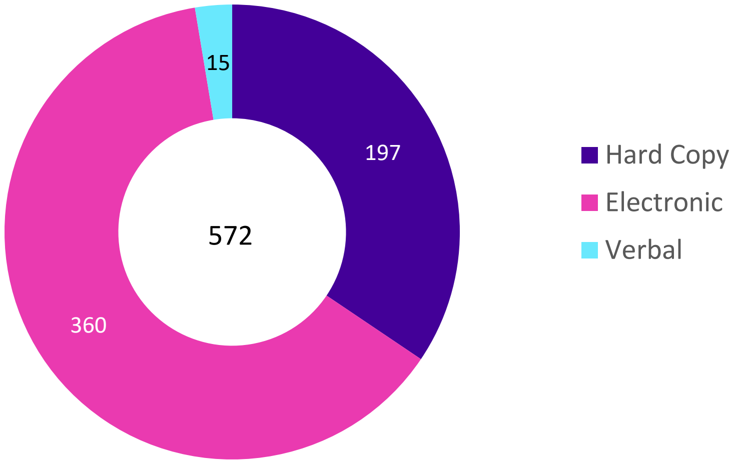
There was also an increase in notifications across most of the portfolios including: Premier and Cabinet (**5**), Families, Fairness and Housing (**22**), and Local Government (**34**) compared to the last notification period which were 3, 13, and 31 respectively.

This notification period had a decrease in notifications received from the Transport and Planning (**17**) and Education (**13**) portfolios compared to the previous notification period which were 38 and 28 respectively.

There was also another decrease in **Other** portfolio notifications with **2** compared to 6 in the previous notification period.

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

Information format (Multiple options can be selected)



Insights:

Most incidents related to compromises of **electronic** information (**360**), followed by **hard copy** information (**197**). These numbers are very similar to the previous notification period which were 353 and 192 respectively.

The number of incidents involving **verbal** information (**15**) were consistent with the previous notification periods July to December 2024 (18), January to June 2024 (16) and July to December 2023 (17). All of these relate to unauthorised disclosure/oversharing of public sector information which have been reported in previous Incident Insights Reports. Some examples of verbal disclosures include disclosing information to a caller without checking the caller's identity first, and unauthorised disclosure of information to a caller who didn't have formal authority to receive the information.

With the advancement of generative artificial intelligence (**AI**) in the workplace, there was an incident where AI technology (Otter AI) which was installed on a staff member's computer attended a virtual meeting, even though that staff member was absent from the meeting.

64% of the incidents affecting electronic information related to emails, which is similar to the same time last year (January to June 2024) with 66%. Incidents involving hard copy information that related to mail (**79%**) were also similar to the previous notification period (July to December 2024) with 78%.

Most (**91%**) of incidents had an element of unauthorised release/disclosure of information, regardless of information format. This is an increase from the previous notification period which was 85%. Apart from the usual examples of unauthorised release/disclosure of information caused by misdirected emails and mail, other examples include:

- paperwork having another person's completed form in the pile of documents

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

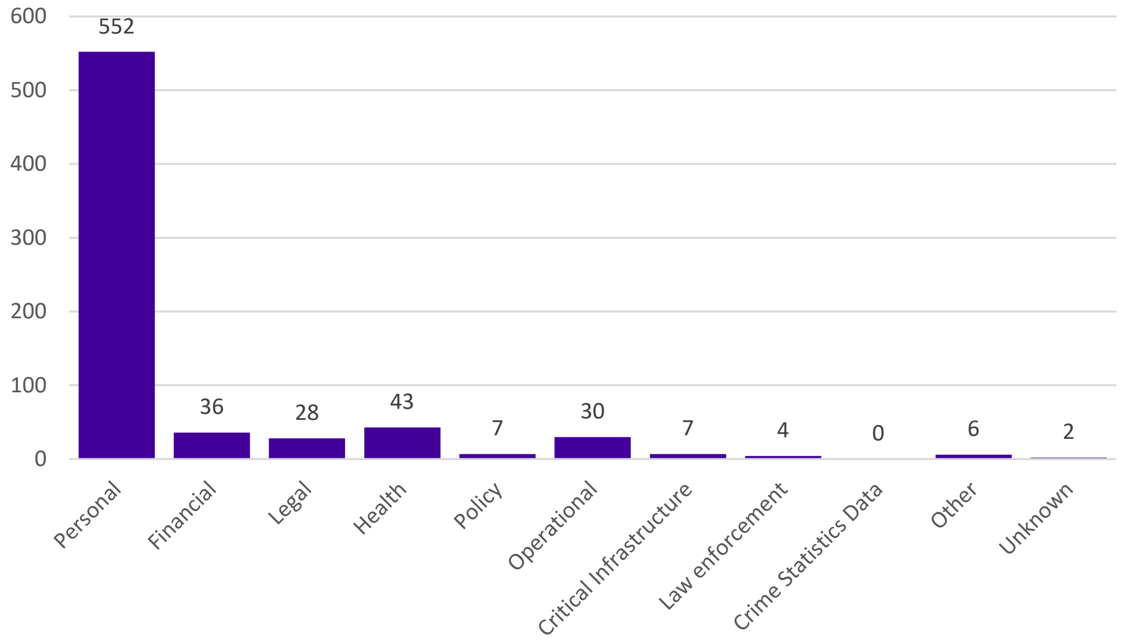
- client files stolen during a break-in
- printouts left in printer tray for others to see
- information shared without redacting personal details first
- eight (**8**) misdirected SMS/text messages.

Although it is uncommon for multiple information formats to be affected in the same incident, multiple options can be selected for this field. There were **11** incidents that affected two information format attributes compared to the previous notification period (30).

Some examples of incidents involving two information formats include:

- call recordings (**verbal and electronic**) on test system weren't paused leading to overcollection of personal financial information
- incorrect documents scanned and emailed (**hard copy and electronic**) because the documents were mixed into the client's hardcopy file at the storage facility
- driver's licence (physical and digital) with incorrect details.

Type of information impacted (multiple options can be selected)



Insights:

Similar to the previous notification period, most (**98%**) incidents related to compromises of **personal** information, that is, **552** out of the 561 notifications.

Taking into consideration the correction from the last reporting period, the numbers for most of the information types are either the same as the previous reporting period e.g. legal (**28**), operational (**30**), law enforcement (**4**), and crime statistics data (**0**), or otherwise similar to, the previous notification period.

This notification period saw a rise in incidents affecting **policy** information from 3 in the previous notification period to **7**. In all these instances, policy information was affected along with other information types.

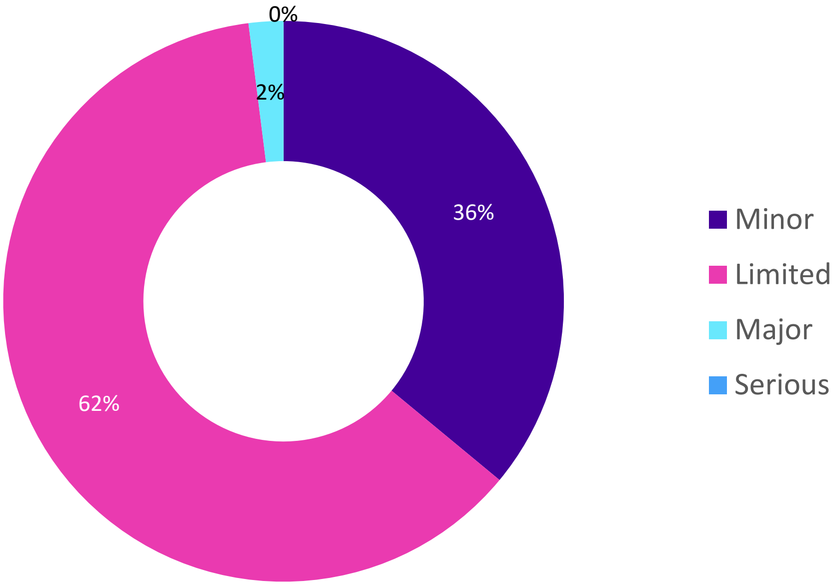
There were **6** incidents affecting the **other** information type. Examples include incidents affecting credentials, system-related metadata, and a certificate book.

There were **2** incidents where the type of information involved was **unknown** due to the organisation not knowing exactly what information was incorrectly disposed and what information was contained in stolen laptops after a break-in.

Multiple options can be selected for this field. In all instances where health information was affected in an incident (**43**), personal information was also selected. There were **21** incidents where three or more information types were affected in a single incident, for example:

- **personal, financial, health, operational, and critical infrastructure** information was affected when a disgruntled employee accessed a system without legitimate business need
- **personal, health, policy, operational, critical infrastructure and other** information was affected by a ransomware incident
- **personal, health, financial, legal, policy, operational and law enforcement** information was affected in an incident related to multiple compromised M365 service accounts.

Information Business Impact Level (BIL)[1]



Insights:

The Business Impact Level (**BIL**) statistics for this notification period are similar to the previous period due to GWW once again submitting notifications related to utility bill incidents affecting contact and billing information at BIL 1 with no sensitive information. The number of incidents affecting information assessed as having a **limited** impact or **BIL 2** is **347** or **62%** compared with 68% in the last period and **minor** impact or **BIL 1** is **203** or **36%** compared with 31% in the last period.

Two per cent of incidents affected **BIL 3** information. In terms of numbers, incidents affecting BIL 3 information was double the previous notification period from 5 to **11** incidents this period. Some examples of incidents affecting BIL 3 information include:

- incorrect permissions on a data warehouse system
- disclosure of a customer's new address details to an ex-partner
- cabinet submission sent to a personal email account.

Like the previous notification period, there were no notifications received for incidents affecting business impact level **BIL 4** information.

Note: The BIL field, in the incident notification form, relates to the information (e.g., BIL 2 / Limited / OFFICIAL: Sensitive) affected in the incident and does not relate to the severity of the incident itself.

For example, an incident relating to inadvertently sending an email attachment containing sensitive personal information to the incorrect recipient should be notified under the scheme, because it impacts BIL 2 information. This is true even though

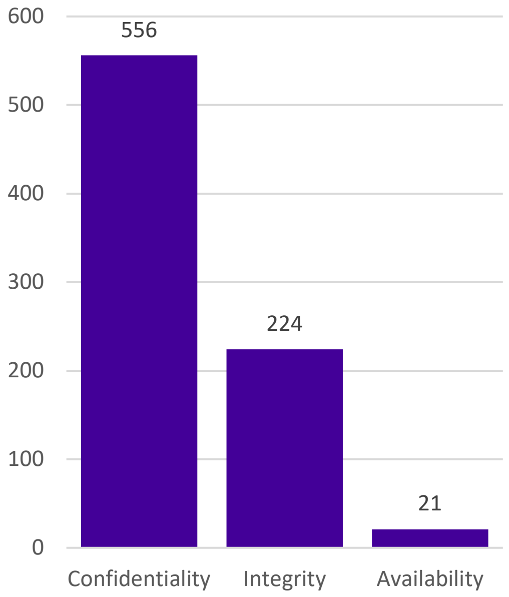
[1] Refer to https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-framework-business-impact-level-table-v2-1/

the severity of the incident itself may be assessed as LOW because it was managed locally with minimal adverse impact e.g., incident was contained quickly, swiftly acted upon, deleted, affected person notified.

Disclaimer

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

Security attributes impacted (multiple options can be selected)



Insights:

Like the previous notification period where 98% of incident notifications indicated compromises of the **confidentiality** of information, there were **99%** in this notification period (**556**). There was a similar number of incidents affecting the **integrity** (**224**) of information compared to the previous period (200). A good portion of these were related to GWW's data quality issues they are experiencing during their billing system upgrade project.

As a result of the ongoing incidents related to GWW, OVIC published a Report on the privacy impacts of Greater Western Water's migration to a new billing and payment system with a high-level overview of OVIC's findings to provide lessons for other agencies when undertaking data migration or integration activities as part of system upgrades or other significant operational changes.

Incidents affecting the **availability** of information are similar with **21** this notification period compared to 16 and 17 in the previous two periods.

Unauthorised disclosure (**confidentiality**) of public sector information regardless of information format (hard copy, electronic, verbal) continues to dominate the incidents for this period accounting for **91%**.

There were **3** incidents affecting the **availability** of information without any other security attribute, for example stolen devices.

There were **2** incidents affecting the **integrity** of information without any other security attribute, for example Business Email Compromise (**BEC**) and incorrect details on a letter.

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

Multiple options can be selected for this field. While 196 incidents affected both the **confidentiality** and **integrity** of the information, there were **8** incidents affecting the **confidentiality** and **availability** of the information for example:

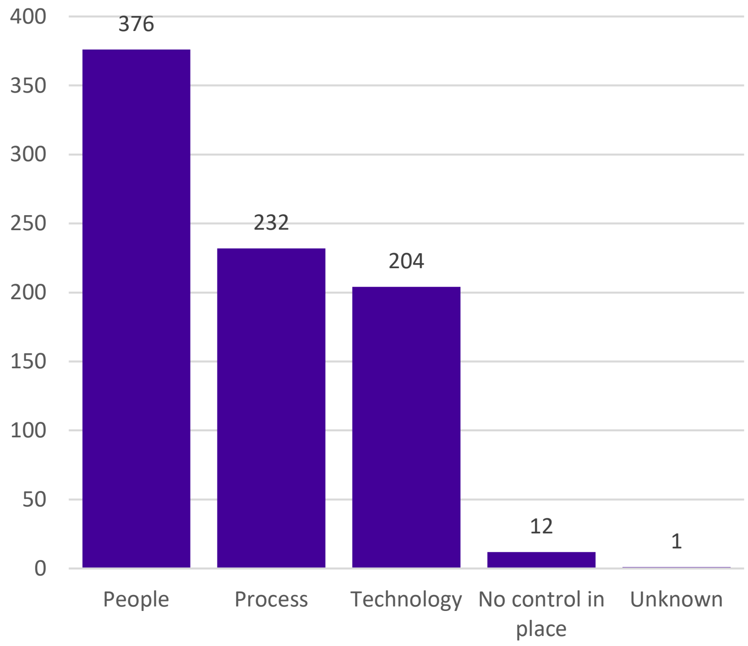
- malware attack on a fourth-party supplier leading to data being published on the dark web
- a function within a new system enabled users to see other users' data (so the information was available to those without a need-to-know)
- stolen mail from a letterbox.

There were **9** incidents affecting all three security attributes (**confidentiality, integrity** and **availability**) of information. For example:

- unauthorised access to a customer portal account by an external threat actor locking out the legitimate account holder
- unauthorised disclosure due to an incorrect workorder request processed
- unauthorised access to another customer's account due to incorrect account configuration.

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

Control area(s) affected (multiple options can be selected)



Insights:

This notification period saw another decrease in the percentage of incidents caused by **people** (**67%**) compared with the previous two notification periods (72% and 96%). This is because there was an increase in **process** and **technology** incidents.

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

Mail mis-delivery whether it is postal mail or email accounted for **65%** of incidents received this notification period. This includes **people** sending mail to the wrong recipient, as well as mail mis-delivery caused by **process** and **technology** errors (**38%**) by the GWW billing system upgrade project also discussed in the previous report.

There was another increase in **process** (**232**) related incidents compared to the last notification period (199) as well as **technology** (**204**) related incidents compared to the last notification period (160).

Multiple options can be selected for this field. Like the previous notification period, there were **12** notifications where **no control(s) in place** was selected, in addition to other control area(s) being involved. For example:

- **process and no control(s) in place:** overshare of information in email
- **people, technology and no control(s) in place:** threatening emails sent from a compromised M365 account

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

- **people, process and no control(s) in place:** Business Email Compromise (**BEC**).

There was **1** incident regarding a compromised server where the control area affected was **unknown**.

There were **5** incidents related to **process** only and **12** incidents related to **technology** only as the cause of the incident. Examples of process-related incidents include:

- staff member continued working before re-doing their annual police check which was overdue
- process not followed when linking accounts leading to unauthorised disclosure

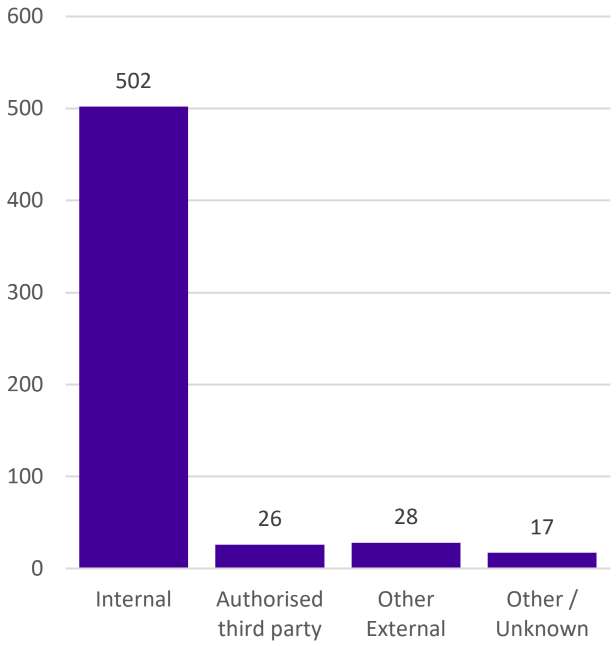
Examples of technology-related incidents include:

- generative AI technology attended a virtual meeting even though that staff member was absent from the meeting
- two people were matched by the customer matching system, and their accounts were linked in error
- unauthorised access to a customer account due to automated processing adding the email address of another customer to their record.

There were **6** incidents related to all control areas: **people**, **process**, **technology** and **no control(s) in place**. For example:

- compromised account(s)
- incorrect folder permissions
- ransomware.

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, **89%** of incidents were caused by **internal** staff (**502**) compared to 90% (481).

Incidents caused by **authorised third parties** remain at similar numbers, with **26** this period compared to 29 in the July to December 2024 period, 21 in the January to June 2024 period, and 30 in the July to December 2023 period. For example:

- third party provider granted system access without following correct approval process
- service provider misconfigured system leading to inadvertent publishing of call records
- contractor sent documents to personal email account.

There were **28** incidents caused by **other external** threat actors, compared to 19 in the previous notification period. These incidents are usually always coupled with an intentional/malicious intent rather than accidental. Examples of incidents caused by **other external** include:

- threatening emails sent from compromised M365 accounts
- stolen documents from vehicle
- stolen laptops from office break-in
- fourth party malware attack.

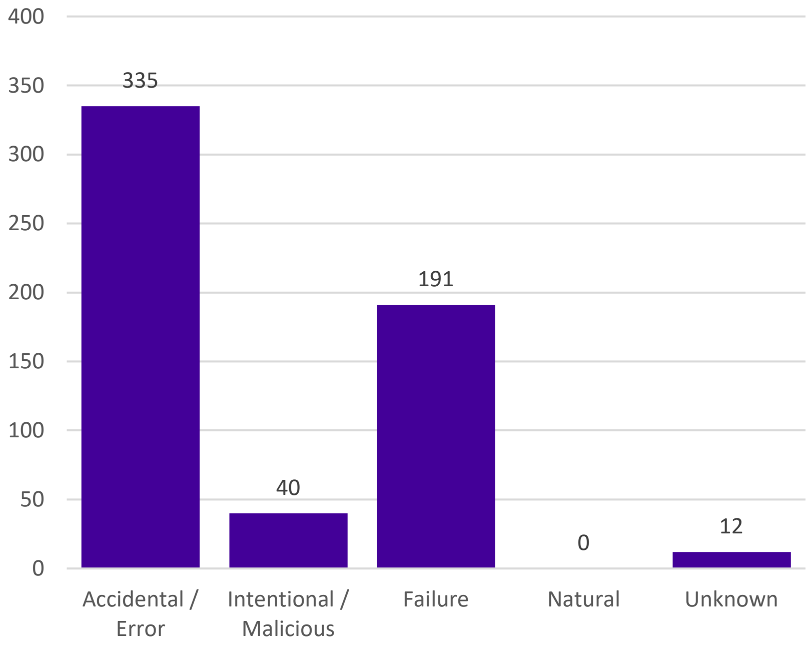
Disclaimer
The information in this document is general in nature and does not constitute legal advice.

There were **17** incidents where the threat actor was **other / unknown** compared to the previous notification period (9). For example, it was unclear who was behind an incident related to an unredacted document being published on a website and, another example was trying to ascertain who was behind an auto-forward all emails rule being set up on an email mailbox. Where there are third party arrangements in place and inadequate logging, it is sometimes difficult to ascertain the cause of incidents to assist with remediation.

Although it is uncommon for more than one threat actor to be involved in an incident, there were **12** incidents caused by multiple threat actors. For example, both **internal** and **authorised third party** representatives caused an incident related to overcollection of personal financial information in call recordings on a test system. Another example was where **internal** and **other / unknown** threat actors caused an incident when a staff member accessed and shared information about a client with an ex-partner who then relayed this information back to the client.

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

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



Insights:

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

Incidents caused by **accidental** actions (**335**) were the same as the previous notification period. There was a decrease in incidents caused by **intentional** actions (**40**) compared to the previous notification period (50).

Like the previous notification period, incidents caused by **failure** (**191**) continued to increase compared to 153. Most of these incidents came from GWW. Other examples include:

- two people were matched by the customer matching system, and their accounts were linked in error
- staff not following mail sorting and dissemination process
- messaging service sent SMS to incorrect number.

Half of the **intentional/malicious** incidents were caused by internal staff. There has been an upward trend in staff accessing systems without a legitimate reason and data exfiltration by staff sending public sector information to personal email accounts, for example:

- inappropriate system access without business need
- disgruntled employee accessing other staff files on the electronic document management system unrelated to their role

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

- corporate documents sent to/from personal email address
- copying recruitment information onto personal USB storage device.

Once again, there were no incidents in this notification period that were due to **natural** causes.

There were **12** incidents where the threat type was **unknown**. For example, in half of these instances, the organisation was unable to determine if access to the system information without a business need was intentional or accidental.

Although multiple options can be selected for this field, there is usually one threat type associated with each incident. There were **17** incidents caused by more than one threat type. Most of these incidents included both **accidental** and **failure** (where failure related to a failure of process as opposed to a system failure). For example, a document was uploaded into the incorrect client record and then released to the incorrect person and another example was an unredacted report published on the organisation's website.

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

Victoria Police Statistics

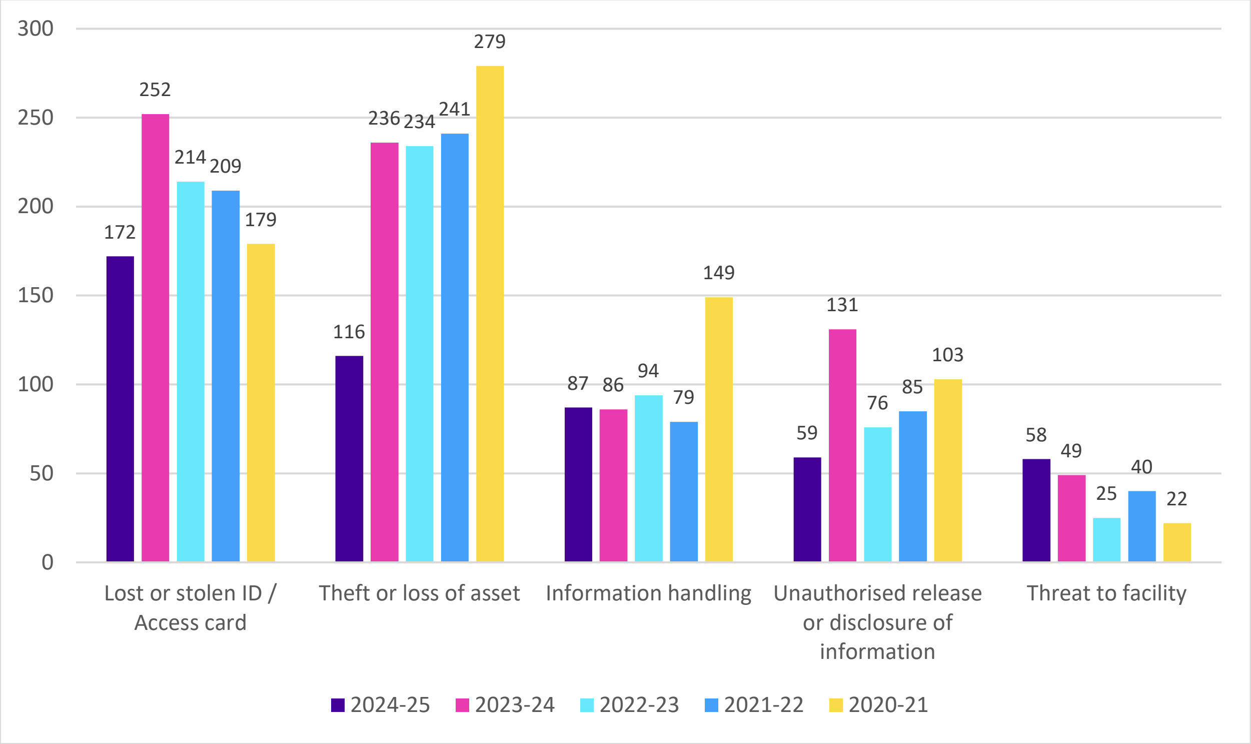
OVIC receives incident notifications from the Victoria Police Security Incident Registry team.

During the period 5 September 2024 – 30 January 2025, OVIC received no notifications from Victoria Police due to industrial action occurring, so any incidents completed during this time have been excluded. Therefore, incident numbers for 2024-25 differ from previous years so comparisons are only made regarding incident categories as opposed to the incident numbers themselves.

Comparison between the last five financial year periods shows four of the top five 'completed' incident categories remain the same with **Lost or stolen ID / Access card**, **Theft or loss of asset**, **Information handling** and **Unauthorised release or disclosure of information**.

To complete the top 5 categories for the 2024/25 reporting period, the Communications Faults category was replaced with **Threat to Facility** which had high numbers compared to any previous reporting period even with only partial reporting numbers.

Note: OVIC reports on 'completed' Victoria Police incidents. The statistics are based on the number of 'completed' incidents, meaning they were investigated by Victoria Police and confirmed incidents where any follow-up actions have been completed. OVIC does not report on both 'open' and 'completed' incidents because there is a percentage that are categorised as 'no incidents' once they have been investigated and found not to be an incident, but OVIC will sometimes follow up on items categorised as no incident to confirm Victoria Police's assessment.



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

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…**[2]
Unauthorised transfer/release of information including cabinet, intellectual property and personal information about other staff *(Compromise of confidentiality)*	Disgruntled staff member sending information to/from their own personal email account	Impact to individuals whose personal information was affected Impact on public services (reputation of, and confidence in, the organisation)
Disclosure of personal information published on website *(Compromise of confidentiality and availability)*	Misconfiguration of platform by third party not selecting the correct fields to redact before displaying information	Impact to individuals whose personal information was affected Impact on public services (reputation of, and confidence in, the organisation)
Incorrect customer records leading to unauthorised disclosure of address details to ex-partner *(Compromise of confidentiality and integrity)*	Incorrect data matching and linking of accounts during system migration	Impact to service delivery Impact to individuals whose personal information was affected 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/data-protection/agency-reporting-obligations/incident-notification/

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

[2] 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.