Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Incident Insights Report

1 January 2024 – 30 June 2024

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 2024** to **30 June 2024**.

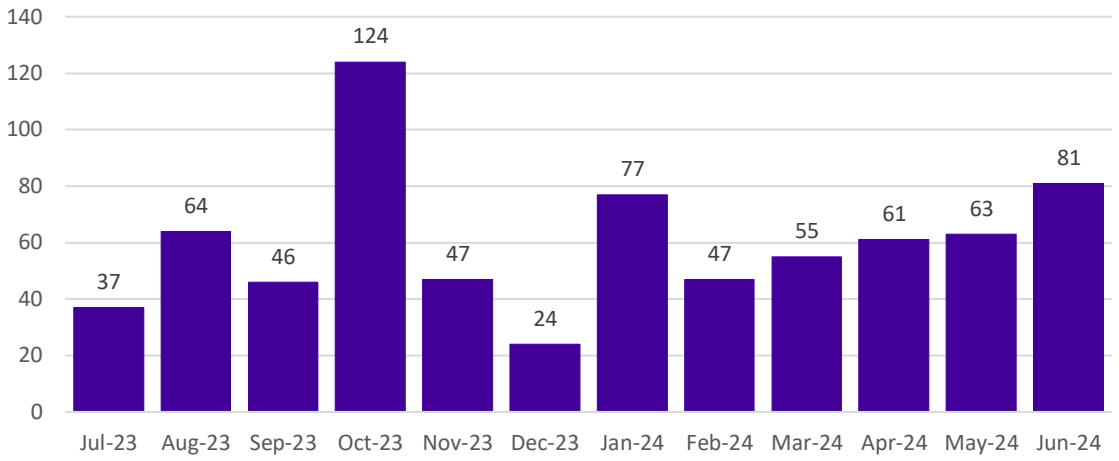
The analysis in this report is based on comparing the statistics published in previous Incident Insights Reports with the notifications received by our office under the scheme.

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 2023 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**, and **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.

Information security incident notification insights from January – June 2024

Notifications by month



Insights:

OVIC received **384** notifications between **1 January** to **30 June 2024** (inclusive). There was a **12%** increase in notifications compared to the previous notification period July to December 2023 (**342 notifications**). This is the highest number of notifications that we have received for the Jan-Jun notification period since the establishment of the information security incident notification scheme.

OVIC received the highest number of notifications (**81**) in June which is an increase from June 2023 (**49**) and higher than June in any previous year since the scheme began.

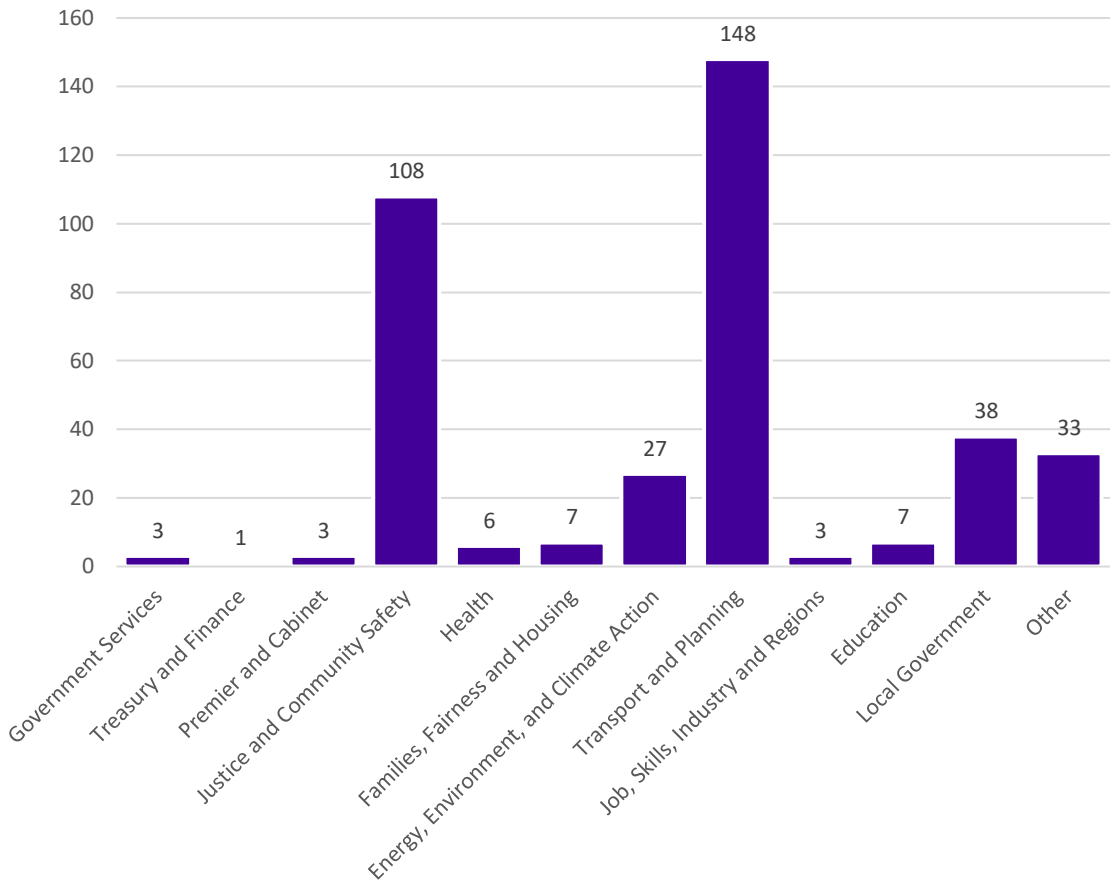
The higher numbers in June mostly came from the Department of Justice and Community Safety (**DJCS**) and the Transport Accident Commission (**TAC**). This was due to DJCS and TAC sending through the notifications from multiple months before the end of the notification period.

It is interesting to see the high number of notifications in January (**77**) which has traditionally been a quiet time of the year to receive notifications. This is based on previous notification periods such as January 2023 with **35** notifications and January 2022 with **16** notifications.

Note:

- the date of notification does not necessarily reflect when an incident occurred, but rather reflects when a notification was made to OVIC; and
- the higher number of notifications from these organisations does not necessarily reflect that they have more incidents but rather that they have established incident management and reporting processes.

Notifications by portfolio



Insights:

Most of the 384 notifications received by OVIC came from the justice and transport sectors. These were mostly from DJCS, and TAC due to their established incident notification protocols.

This notification period saw a decrease in notifications received from health (six (6)) and families, fairness and housing (seven (7)) portfolios compared to the last notification period which were 27 and 20 respectively.

There was an increase in the number of notifications across half the portfolios such as energy, environment, and climate action (27) and education (seven (7)) compared to the last notification period which were 22 and two (2) respectively. Although most notifications from the transport and planning sector continue to come from TAC, there was an increased use of the scheme by Registration and Licencing Services (VicRoads) as they establish incident notification protocols.

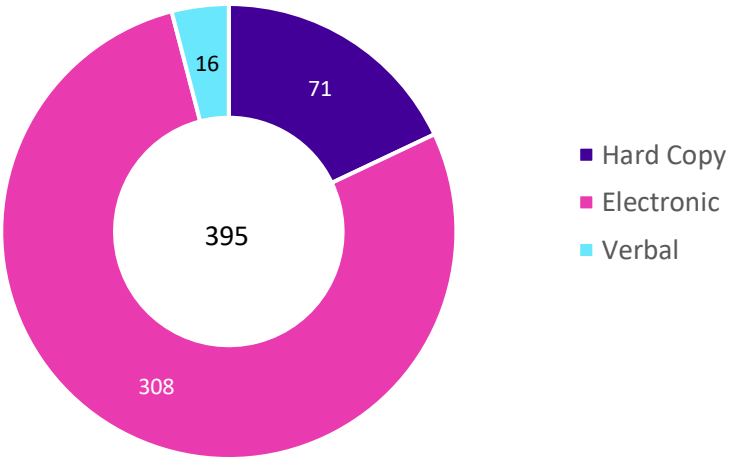
Notifications from local government continued to steadily rise this notification period (**38**) compared to the previous periods July to December 2023 with **30**, January to June 2023 with **26**, July to December 2022 with **15** and January to June 2022 with eight (**8**) notifications.

This notification period saw an increase in **Other** portfolio notifications with **33** instances from:

- organisations that do not reside under a portfolio (**28**) e.g., Victorian Ombudsman
- organisations out of jurisdiction for Part 4 of the Privacy and Data Protection Act (one (**1**)) e.g., universities
- multiple organisations for the same incident (four (**4**)) e.g., OVIC received 20 notifications for the OracleCMS incident which mostly impacted local government councils and water organisations.

Note: OVIC continues to conduct annual reviews of the scheme to identify areas for improvement. In the future, for incidents that affect multiple organisations, OVIC will register each notification with its own unique reference number even if it relates to the same incident to get a better indication of individual notification numbers rather than incident numbers.

Information format (Respondent percentage)



Insights:

Notifications affecting electronic information continues to be the most selected information format **(78%)**. Most notifications indicated compromises of **electronic** information (**308**) followed by **hard copy** information (**71**).

The number of incidents involving verbal information (**16**) were similar to the previous notification period (**17**). All of these relate to unauthorised disclosure / oversharing of public sector information. Some examples of verbal disclosures include:

- discussing intelligence information with unauthorised staff members
- disclosing another person's identity to an unverified caller
- discussing sensitive information with a person listed on a spreadsheet which was received by a staff member in error
- phone calls monitored and recorded in error

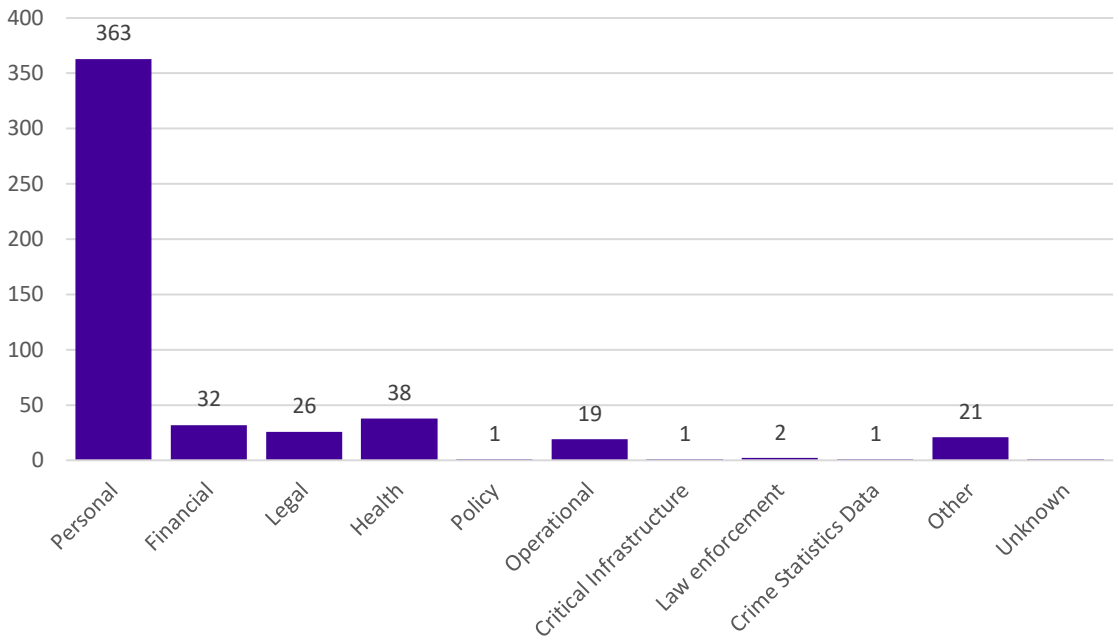
66% of the incidents affecting electronic information related to emails and similarly, 69% of the incidents involving hard copy information were related to mail. There was an increase in incident notifications, that involved unauthorised release/disclosure of information, regardless of information format, from 75% in the previous period to 82% this period. Examples of unauthorised release/disclosure, includes verbal disclosures; sending emails or mail to the incorrect recipient; or attaching incorrect information.

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 notifications that selected two (2) information format attributes.

Some examples of incidents involving two information formats includes:

- lost laptop and manila folder
- unauthorised recording and use of AI to summarise a staff team meeting (speech to text)
- incorrect address on system leading to document being sent to incorrect address

Type of information impacted (Multiple options can be selected)



Insights:

Notifications regarding the type of information involved in incidents were consistent with previous notification periods. Most (**95%**) notifications indicated compromises of **personal** information, followed by compromises of **health** information (a reminder that the scheme covers incidents related to all public sector information, not just personal information).

There were **21** notifications where the **other** information type was selected. Examples include incidents related to:

- claim numbers
- DNS records
- investigation reports

There was one (**1**) incident where the type of information involved was **unknown** where the incident related to leaked credentials, however there was no evidence of any subsequent unauthorised use of the credentials.

Multiple information types can be involved in a single incident. **18%** of notifications selected more than one information type.

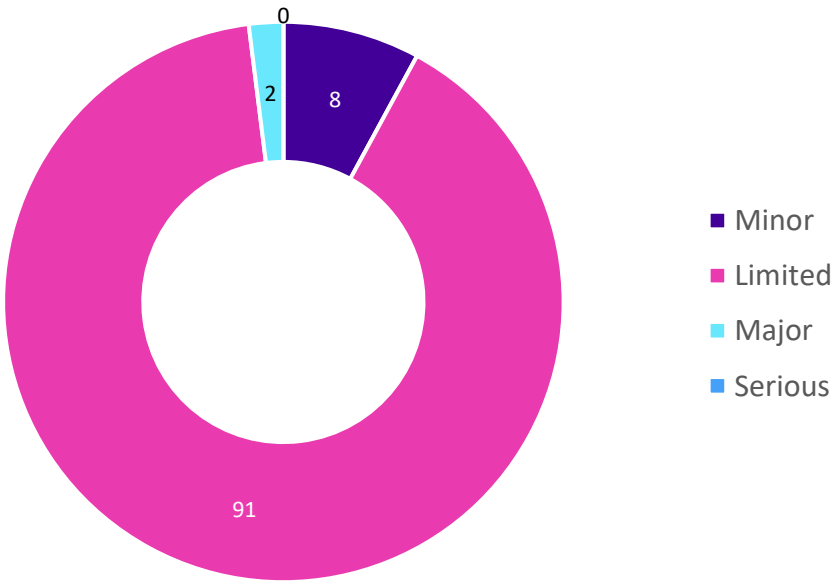
Like the previous period, all except two (**2**) notifications where health information was selected, personal information was also selected. Similarly, for notifications where more than one information type was selected, personal information was selected for all these instances.

There were four (**4**) notifications where four (**4**) or more options were selected. Examples include:

- **personal, financial, policy, operational,** and **other** information was contained on a stolen laptop
- **personal, health, operational, critical infrastructure** and **other** information was affected when a compromised account led to the organisation's systems being encrypted.

Information Business Impact Level (**BIL**)[1]

Highest BIL percentage (% rounded up)



Insights:

The Business Impact Level (**BIL**) statistics for this notification period are consistent with the previous period. The number of notifications identifying incidents affecting information assessed as having a **Limited** impact or **BIL 2** is **91%** and **Minor** impact or **BIL 1** is **8%**.

This period saw a rise in the number of notifications across all the business impact levels except for **BIL 4** with no notifications. **Two percent** of notifications indicated **BIL 3** information was affected. In terms of numbers, this is half the notifications, six (**6**), nominating **BIL 3** information compared to the last notification period (**12**). This decrease in notifications affecting high risk information such as BIL 3 or higher is positive. This may indicate better controls in place to protect high value information and the

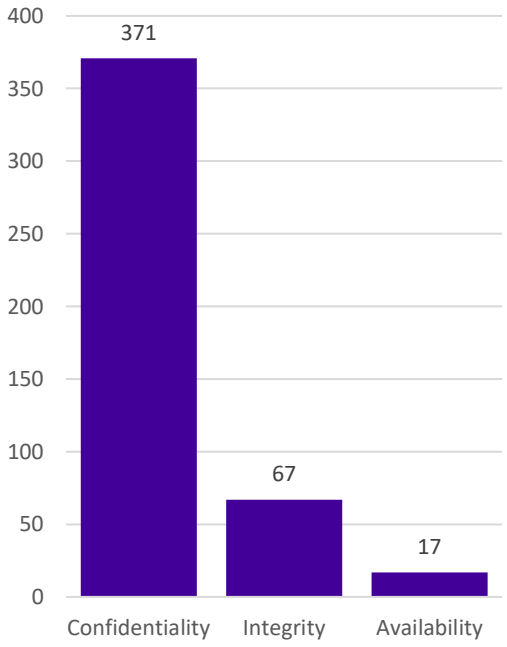
[1] Refer to https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-framework-business-impact-level-table-v2-1/

low volume of high value information in Victorian government. Some examples of incidents affecting BIL3 information include:

- the inadvertent release of commercial pricing information in tender documentation
- disclosure of a carer's address in a text message
- social engineering staff whereby an external threat actor impersonating as a contractor, obtained the access code to gain system access to the client database

Note: The BIL field 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 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.

Security attributes impacted (Multiple options can be selected)



Insights:

97% of incident notifications indicated compromises of the **confidentiality** (**371**) of information followed by **integrity** (**67**). Even with the increase in the number of notifications received this period, incidents affecting the **availability** of information decreased to **17** compared to **21** in the previous notification period.

This period saw the number of incidents affecting the **integrity** of information more than double from the previous period which was **30** to **67**.

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 **82%** of the notifications received.

17% of incident notifications selected more than one option for this field. In almost all instances where multiple options were selected, **confidentiality** was selected. There was only one (**1**) instance where the confidentiality security attribute was not selected where the incident affected multiple attributes. In this notification, the incident affected the integrity and availability of the information due to a defaced website where the content of the website had been altered and the correct information was not available.

There were four (**4**) notifications where the **availability** security attribute was selected on its own for example:

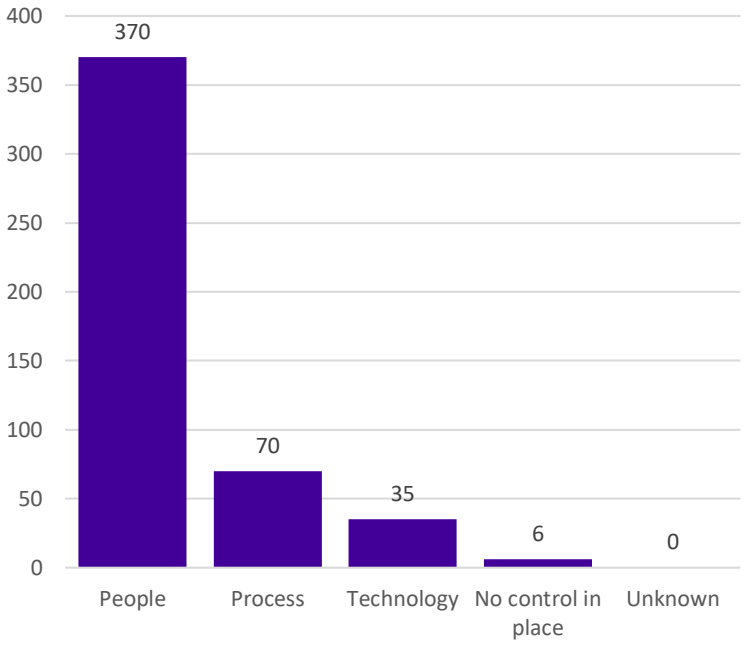
- lost mobile phone
- unavailability of phone service and electronic monitoring service due to telecommunications provider outage
- denial of service (**DoS**) attack on a DNS service

Like the last period, there were eight (**8**) notifications where the **integrity** security attribute was selected on its own for example:

- incorrect claim number, or email address added to a case file
- staff falsifying records on a system
- invoice saved to the wrong claim

Once again, there were six (**6**) notifications where all three security attributes were selected. For example, an incorrect mobile number was recorded during the lodgement of an application resulting in another nonrelated person receiving text messages rather than the correct person. Another example is an incident whereby an existing staff member's account was cloned to create a new user account resulting in incorrect permissions being granted to new user.

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



Insights:

This notification period saw a small rise in the percentage of incidents caused by **people** (**96%**) from the previous notification period (**92%**). Of the 384 notifications received, only 14 notifications didn't select people being involved in the incident.

The key causal factors for security incidents remain as people, internal, and accidental, for example, mail misdelivery whether it is postal mail or email (**58%**).

There was a decrease in the number of notifications selecting **process** (**70**) compared to the last notification period (**86**) and the numbers for **technology** (**35**) related incidents slightly increased compared to the previous period (**27**).

There were six (**6**) notifications where **no control(s)** was selected, and all these notifications selected **people** as well. Examples include an incorrect entry on a system leading to an email being sent to the incorrect recipient and pre-filled in forms being published instead of blank forms. This indicates that all these examples relate to people, process or technology issues. As part of continuous improvement, OVIC will review the need for **no control(s)**.

There were no notifications in this notification period, where the control area affected was **unknown**.

Where multiple control areas are part of the incident, most of the time, the **people** field is selected in addition to other causal factors. Like the previous notification period, there were two (**2**) notifications

where process and technology were selected without people as one of the causal factors. However, looking at the detail of these incidents, it appears that malicious threat actors were responsible for both of these incidents which would indicate people are a control area affected.

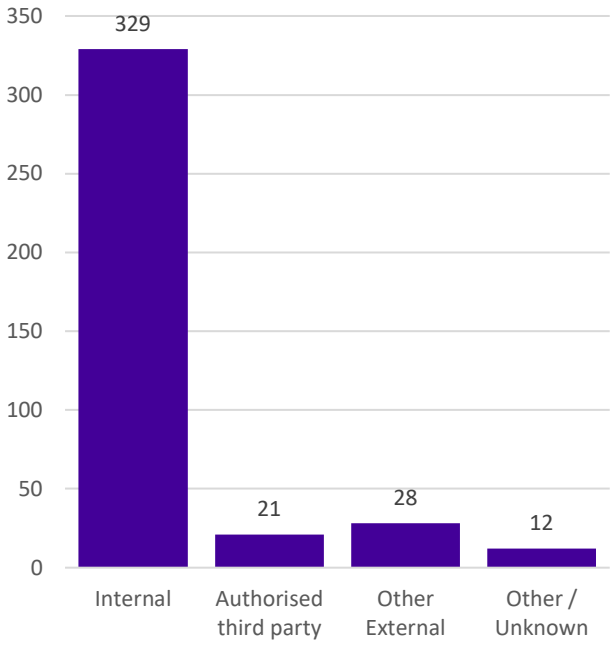
There were two (2) notifications where process was selected on its own and 10 notifications where technology was selected on its own as the cause of the incident. Examples of technology related incidents include:

- unavailability of phone service and electronic monitoring service due to telecommunications provider outage
- system functionality issue where the front-end portal did not update the back end of the system leading to incorrect data
- technical problems with the temp file path during payroll processing caused the run to fail part way leading to some pay advice being uploaded to the incorrect self-service account

There were 10 notifications that nominated all three control areas: people, process, and technology. Examples of instances when these three control areas were selected include:

- letters sent to residents with the incorrect details because staff didn't follow the process to cross check the extracted data set before the mailout
- a system feature was altered (people) after system acceptance testing had occurred (process) and automatic reminder emails (technology) were sent to applicants with incorrect attachments

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 (**84%**), **86%** of incidents in this notification period were caused by **internal** staff.

The number of notifications selecting **authorised third parties** as the cause of the incident (**21**) decreased compared to the last period (**30**), but this was similar (**18**) to the same time last year. Incidents affecting third parties providing services to multiple Victorian government organisations include:

- OracleCMS phone call service provider.
- ZircoDATA records and information management service.
- Herron Todd White property valuation service.

This period also saw incidents affecting organisations due to a fourth-party instead of third-party compromise. For example, an organisation's authorised third party had their managed service provider compromised (e.g. Ticketek), and an organisation's contracted service provider had their subcontractor become victim of a ransomware.

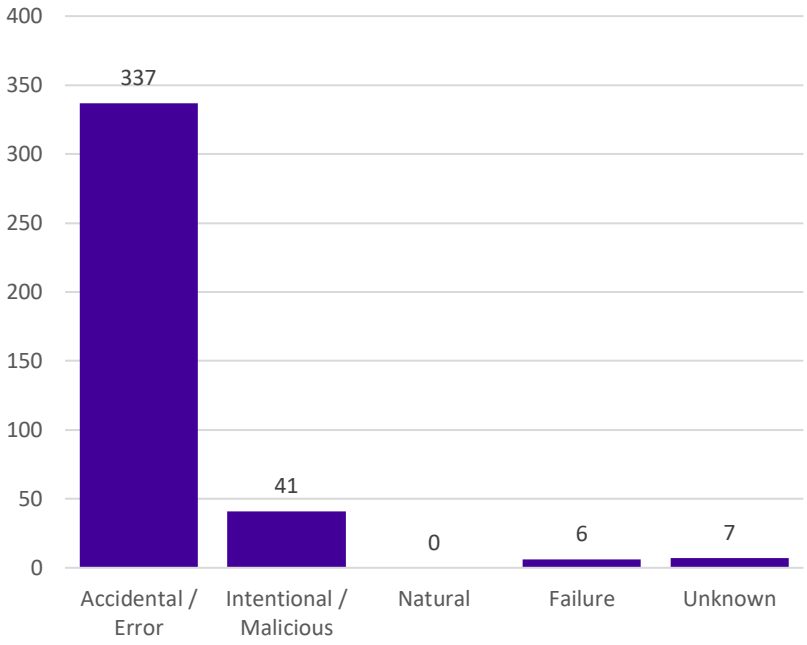
There was a slight increase in notifications selecting **other external** threat actors **28,** compared to **20** in the previous notification period. Examples of incidents include:

- hackers installing ransomware to encrypt systems
- thief stealing a laptop
- an ex-employee using personal information they gained during the course of their employment to contact residents after they left

There were **12** notifications where the threat actor could not be ascertained.

Although it is uncommon for more than one threat actor to be involved in an incident, there were five (**5**) notifications where multiple threat actors were selected. For example, both **internal** and **other external** were selected when an external threat actor used social engineering to get a staff member to change the contact details on another customer's account so the threat actor could gain access. Another example is where an organisation was affected by the OracleCMS incident and has subsequently had a secondary incident during the mailout to notify affected individuals.

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



Insights:

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

Like previous notification periods, most notifications (**88%**) related to **accidental** actions (**337**) and **11% intentional** actions (**41**).

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

In terms of the spread of notifications selecting **intentional/malicious**, half of them were caused by external threat actors and the other half were internal staff. Although these incidents caused by internal staff were intentional actions, they were not always malicious and most of the time were either due to not knowing the correct process or negligence. For example:

- sending public sector information to a personal email address to work on from home computer
- sending public sector information to a personal email address for recordkeeping
- inappropriate system access without legitimate business need to improve skills in using the system
- disclosure of public sector information to partner in social setting
- inappropriate system access to gain personal information of customer to request connection on social media

There was a decrease in the number of notifications where the threat type was **unknown** (**7**) compared to the last notification period of **13**. An example relates to being unable to ascertain if it was accidental, malicious or natural events that led to a telecommunication's provider outage where phone and electronic monitoring services were unavailable.

Although multiple options can be selected for this field, there is usually one threat type associated with each incident.

There were seven (**7**) occurrences where more than one threat type was selected. For example, **malicious** and **failure** was selected when staff made changes to customer records failing to follow the evidence of identity process leading to the threat actor gaining access to customer accounts. In another example, **intentional** and **failure** were selected when an organisation was manually processing payments and storing credit card information incorrectly in unredacted form.

Victoria Police Statistics

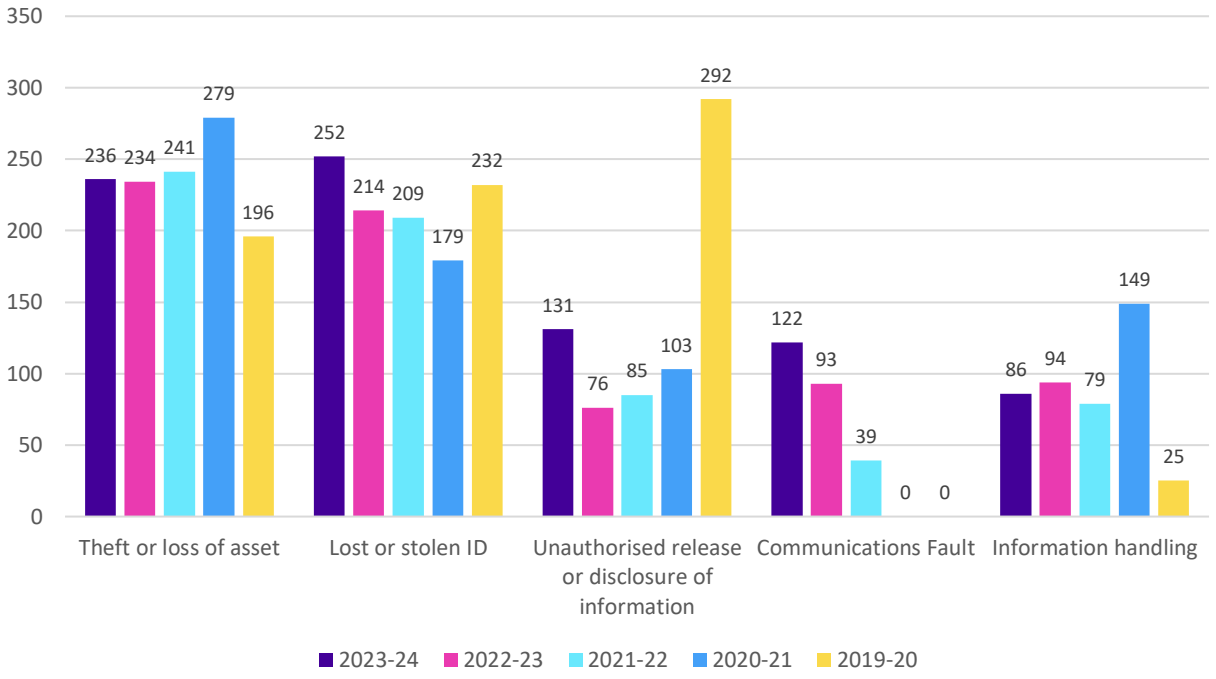
OVIC receives security incident notifications from the Victoria Police Security Incident Registry (**SIR**) team.

Comparison between the last five financial year periods shows four of the top five 'completed' incident categories remain the same.

The numbers for 2023-24 **lost or stolen assets** and **IDs** as well as **information handling** incidents are consistent with the last reporting period. There has been an increase in the number of incidents completed relating to **unauthorised release or disclosure of information** and **communications faults**.

The communications faults category was a new entry into the top five last financial year 22/23 and continues to be in the top five this reporting period as the streamlined process between the SIR team and the Victoria Police Security Control Room, who monitor and manage communications faults, continues to improve. Communication faults was a new category developed in 2021-22.

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.



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

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.