Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Incident Insights Report

1 July 2024 – 31 December 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 July 2024** to **31 December 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. For the latest incident statistics from Victoria Police refer to OVIC's Incident Insights Report for 1 January – 30 June 2024.

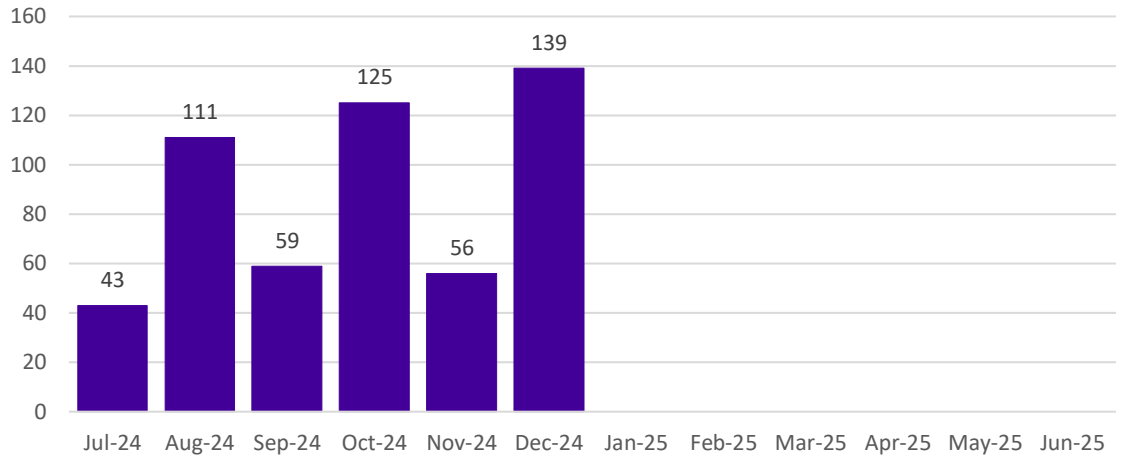
Note: The incident notification form allows for **more than one response** to be selected for the fields:

- 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.

Information security incident notification insights from July – December 2024

Notifications by month



Insights:

OVIC received **533** notifications between **1 July** to **31 December 2024** (inclusive). There was a **39%** increase in notifications compared to the previous notification period January to June 2024 (**384 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 (**139**) in December which is a large increase from December 2023 (**24**) and higher than December in any previous year since the scheme began.

The higher numbers in December mostly came from the Transport Accident Commission (**TAC**) and Greater Western Water (**GWW**). This was due to TAC sending through the notifications from multiple months before the end of the notification period and GWW working through significant technical issues arising from an upgrade to their billing system.

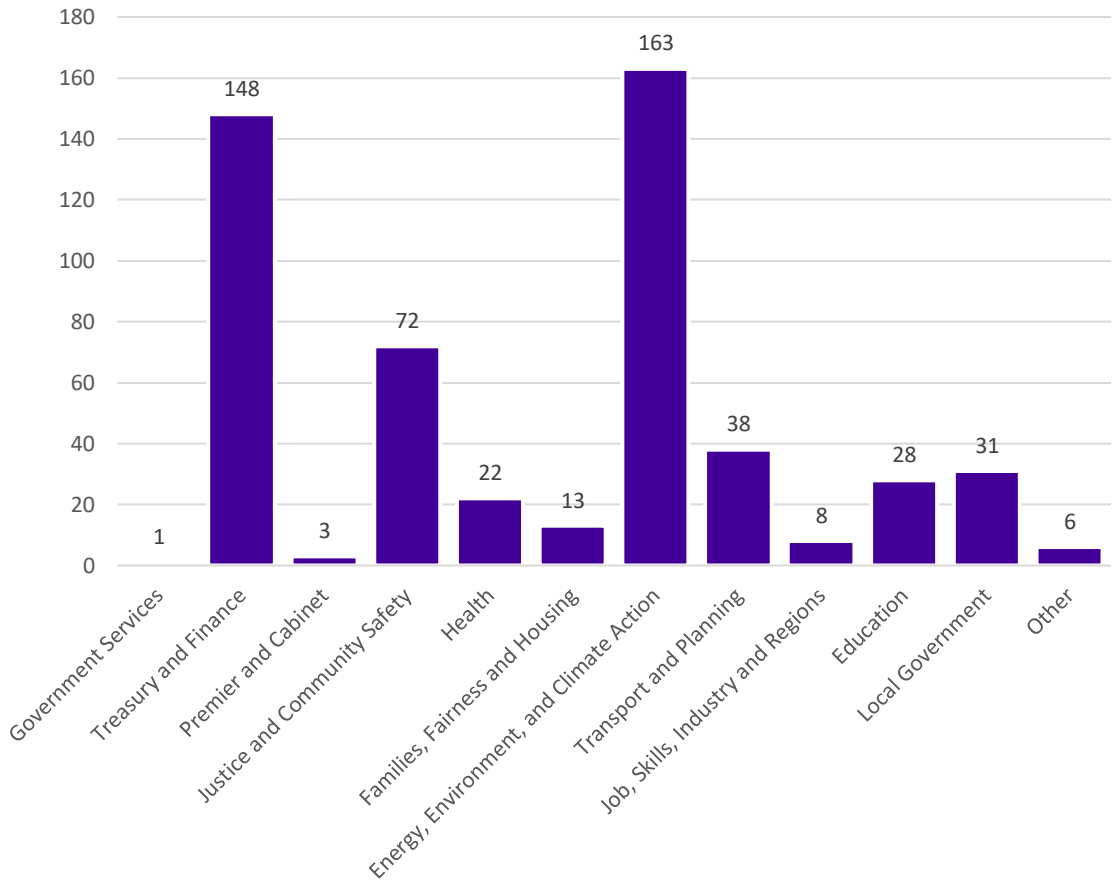
High notification numbers were also observed for August (**111**) which is a large increase from August 2023 (64) and higher than August in any previous year since the scheme began. The high numbers for October (**125**) were similar to the same time last year (124).

Although Victoria Police numbers are captured separately to the notification numbers above, industrial action at Victoria Police from September 2024 onwards will mean that for part of this period, OVIC received no notifications from Victoria Police.

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.

Notifications by portfolio



Insights:

For the first time, most of the **533** notifications received by OVIC came from the energy, environment, and climate action sector (**163**) followed by the treasury and finance sector (**148**). These were mostly from GWW and TAC.

This notification period had a decrease in notifications received from the justice and community safety (72) and local government (31) portfolios compared to the last notification period which were 108 and 38 respectively.

This decrease in notifications from local government is the first for some time, following steady rises during the previous periods:

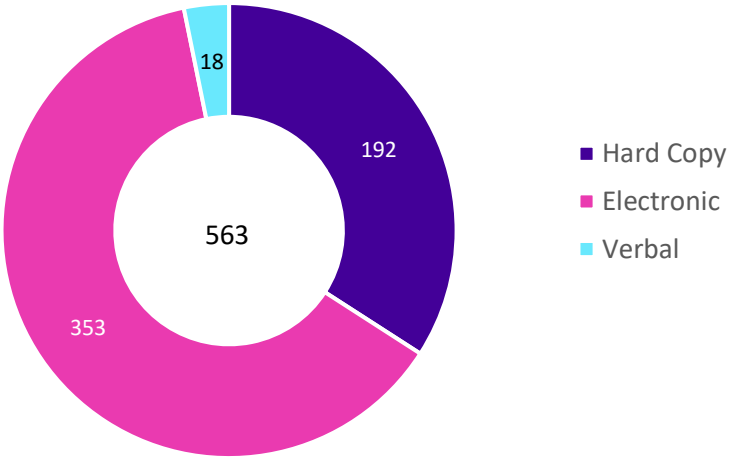
- January to June 2024 (38 notifications)
- July to December 2023 (30 notifications)
- January to June 2023 (26 notifications)
- July to December 2022 (15 notifications)
- January to June 2022 (eight notifications).

There was an increase in the number of notifications across most of the portfolios including: education (28), health (22), and families, fairness and housing (13) compared to the last notification period which were seven (7), six (6) and seven (7) respectively. With the TAC moving under the treasury and finance portfolio, most notifications from the transport and planning sector now come from Registration and Licencing Services (VicRoads).

This notification period saw a decrease in Other portfolio notifications with six (6) compared to 33 last notification period.

Correction: The two 2023 incident insights reports, and previous Jan-Jun 2024 incident insights reports, incorrectly reported TAC under the transport and planning sector instead of the treasury and finance sector post their machinery of government change on 1 January 2023. This means the treasury and finance sector incident notification numbers should have been reported higher in the previous three incident insights reports instead of the transport and planning portfolio.

Information format (Multiple options can be selected)



Insights:

Most incidents related to compromises of **electronic** information (**353**), followed by **hard copy** information (**192**).

However, with the high number of notifications from GWW related to water billing issues in both hard copy and electronic formats, the percentage of incidents affecting electronic information (**66%**) decreased from the previous notification period (78%) with an increase in the percentage of incidents affecting hard copy information from 18% in the previous period to **36%** this period.

The number of incidents involving **verbal** information (**18**) were consistent with the previous notification periods January to June 2024 (16) and July to December 2023 (17). All of these relate to unauthorised disclosure / oversharing of public sector information. Some examples of verbal disclosures include:

- inadvertent sharing of information due to misunderstood instructions
- disclosing another person's identity and services received to a caller without consent
- overshare of information by practitioner to client
- unauthorised disclosure of recruitment information to a staff member due to having privileged access to another person's mailbox

With the notifications received from GWW, there was a change in the incident numbers related to mail (email and postal mail). Over half (**54%**) of the incidents affecting electronic information related to emails, which is a decrease from the previous period 66%, and there was an increase in the incidents involving hard copy information that related to mail, from 69% in the previous period to **78%** this period.

There was an increase in incidents involving unauthorised release/disclosure of information, regardless of information format, from 82% in the previous period to **85%** this period. Examples of unauthorised release/disclosure, include:

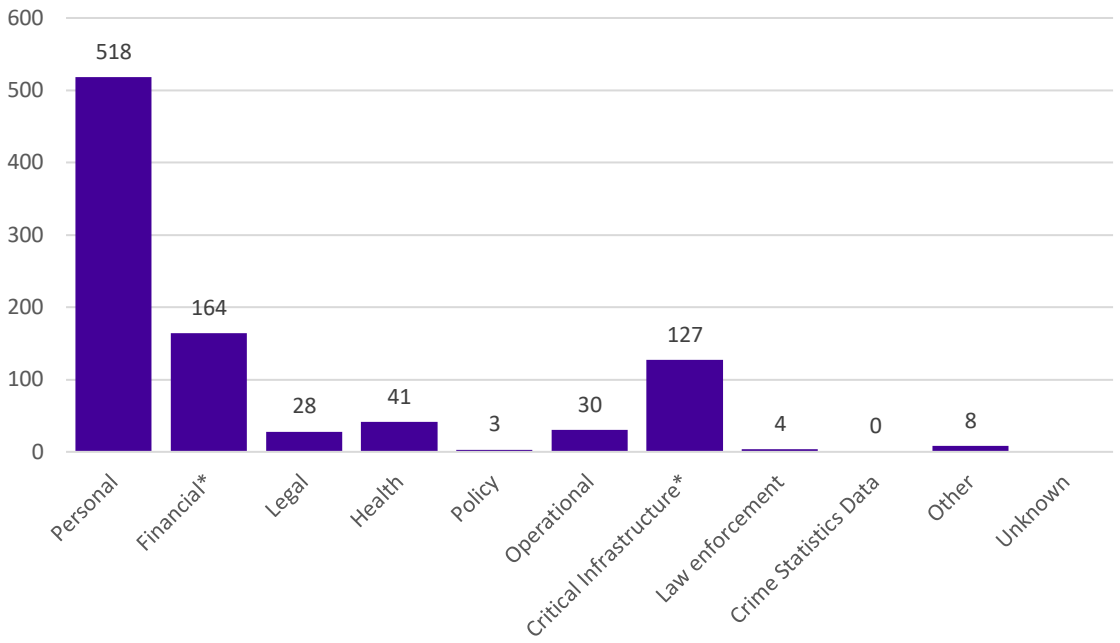
- verbal disclosures
- sending emails or mail to the incorrect recipient
- attaching incorrect information.

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 **30** incidents that affected two (**2**) information format attributes compared to the previous period (11).

Some examples of incidents involving two information formats include:

- incorrect account updated on system leading to incorrect identity document being issued
- unauthorised use of GenAI tool during MS Teams presentation (speech to text)
- incorrect customer account details on system so utility bills went to wrong postal address
- mobile, laptop, access cards and pages from notebook stolen from vehicle

Type of information impacted (Multiple options can be selected)



Insights:

While the majority of notifications regarding the type of information involved in incidents were consistent with previous notification periods, there were some big differences regarding financial and critical infrastructure information.

Most (97%) incidents related to compromises of **personal** information, that is, **518** out of the 533 notifications. However, because multiple options can be selected for this field, many incidents involved other information types. For example, the incidents encountered by GWW during their billing system upgrade project, affected **financial** and **critical infrastructure** information in addition to personal information. This translates to financial information increasing from 32 last period to **164** in this period and critical infrastructure increasing from one (1) last period to **127** in this period.

***Correction**. The GWW incidents relate to customer billing information rather than the organisation's finances or critical infrastructure information so the numbers related to financial information and critical infrastructure information should be disregarded and will be updated in any subsequent incident notifications related to the same billing system project. Discounting the GWW incidents, incidents affecting financial information should be **38** and incidents affecting CI information should be one (**1**) which are consistent with the numbers in the previous notification period.

This notification period saw a rise in incidents affecting **operational** information from 19 to **30** this period. Examples include incidents related to line of business and administration systems.

There were eight (**8**) incidents affecting the **other** information type. Examples include incidents related to:

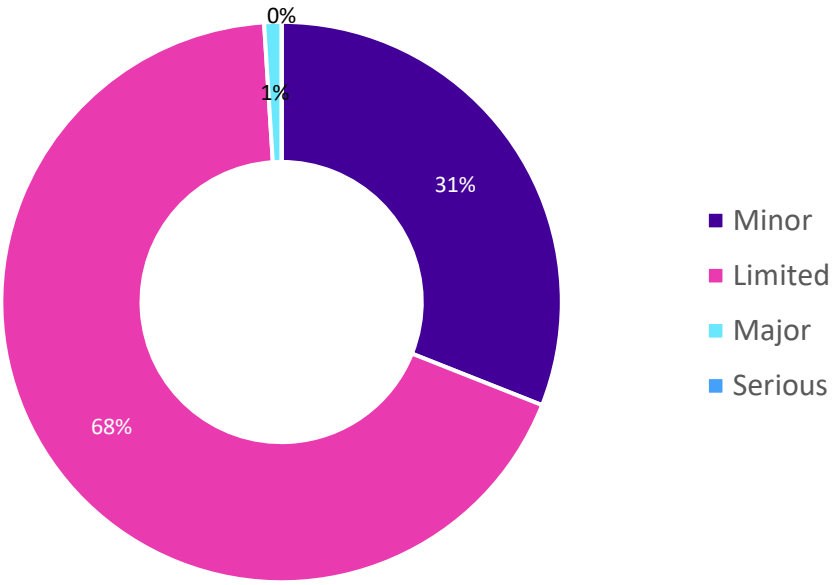
- commercially sensitive information
- safety and wellbeing reports
- incident trends and theme analysis.

There was one (**1**) incident where the type of information involved was **unknown** due to the organisation not knowing exactly what information was on a mobile phone that was stolen while travelling overseas.

There were **15** incidents (excluding GWW) where three or more information types were affected including one incident where six (**6**) information types were affected. For example, **personal, health, financial, legal, operational and law enforcement** information were affected in an incident related to a detailed investigations report being printed and left on the printer tray and then consequently being disposed of in a recycling bin near the printer instead of following the secure disposal process.

Information Business Impact Level (BIL)[1]

Highest BIL percentage (% rounded up)



Insights:

The Business Impact Level (BIL) statistics for this notification period are different when compared with the previous period due to GWW 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 365 or 68% compared with 91% in the last notification period and Minor impact or BIL 1 is 163 or 31% compared with 8% in the last notification period.

One per cent of incidents affected BIL 3 information. In terms of numbers, incidents affecting BIL 3 information was similar with five (5), compared to the last notification period six (6). Some examples of incidents affecting BIL 3 information include:

- sensitive data from cabinet briefings, containing financial and other sensitive details pertaining to a major project published by the media without knowledge or consent
- disclosure of law enforcement information to unintended person when a second screen with a sensitive document was displayed while the practitioner worked on the first screen
- inadvertent release of unredacted court reports emailed to several recipients.

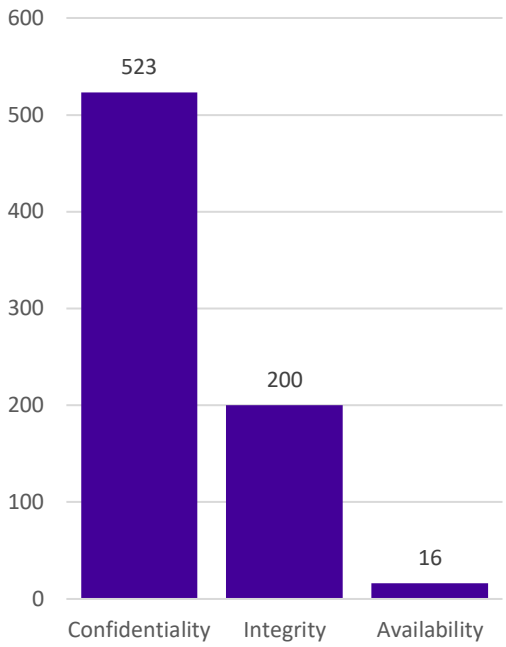
Like the previous period, there were no notifications received for incidents affecting business impact level BIL 4 information.

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

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 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:

Like the previous notification period where 97% of incident notifications indicated compromises of the **confidentiality** of information, there were **98%** in this notification period (**523**). With the increase in the number of notifications received this notification period, there was a large increase in the number of incidents affecting the **integrity** (**200**) of information compared to the previous two notification periods which were 67 in January to June 2024 and 30 in July to December 2023. The main reason for the increase in integrity incidents is because of the data quality issues that GWW was experiencing during their billing system upgrade project that affected not only the confidentiality but also the integrity of the data.

Even with the increase in the number of notifications received this period, incidents affecting the **availability** of information decreased again to **16** compared to 17 and 21 in the previous two notification 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 **85%** of the notifications received.

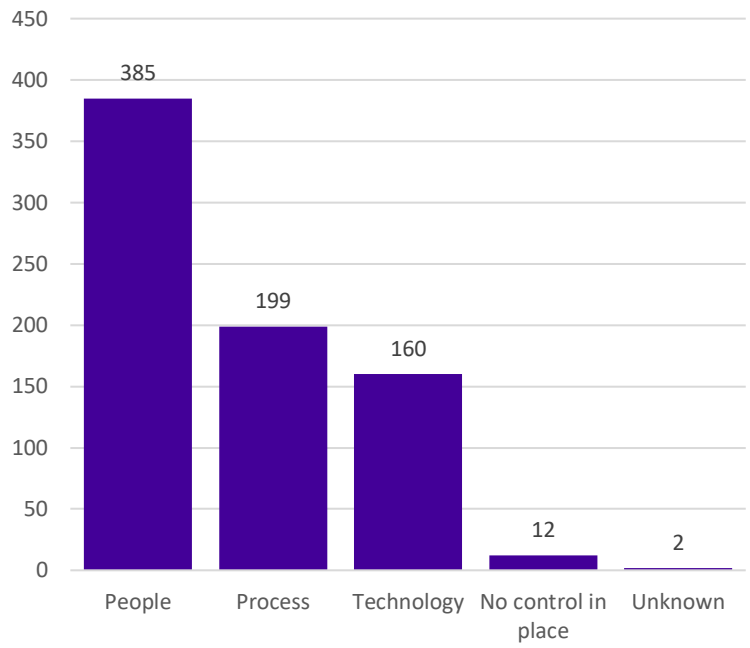
There were only two (**2**) incidents affecting the **availability** of information without any other security attribute, for example, lost account access and stolen device.

There were seven (**7**) incidents affecting the **integrity** of information without any other security attribute, for example:

- Business Email Compromise (**BEC**) accounted for three notifications
- indexing error
- misspelt email address

Multiple options can be selected for this field. There were four (**4**) incidents affecting all three security attributes (**confidentiality, integrity** and **availability**) of information and these all related to compromised application accounts.

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



Insights:

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

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

In previous incident insights reports, these causal factors related to mail mis-delivery whether it is postal mail or email. In this notification period, even though mail mis-delivery still accounted for **58%,** a high number of these incident notifications were process and technology related incidents instead of people.

There was an increase in **process** (**199**) related incidents compared to the last notification period (70) and the numbers for **technology** (**160**) related incidents continued to increase compared to the previous period (35). These large differences in the process and technology numbers compared to any previous notification period are due to GWW. For example, process was selected because of failures to follow data quality processes before rolling out the new system and technology was selected because the rollout of the new system didn't operate as expected.

There were **12** notifications where **no control(s) in place** was selected, in addition to the incident being caused by **people** as well. Examples include three BEC incidents and the publishing of organisation information on external website(s) outside of the organisation's control.

There were two (**2**) notifications where the control area affected was **unknown**. For example, legacy data from one Victorian government organisation found in another Victorian government organisation's system and the loss of access to a third-party online platform.

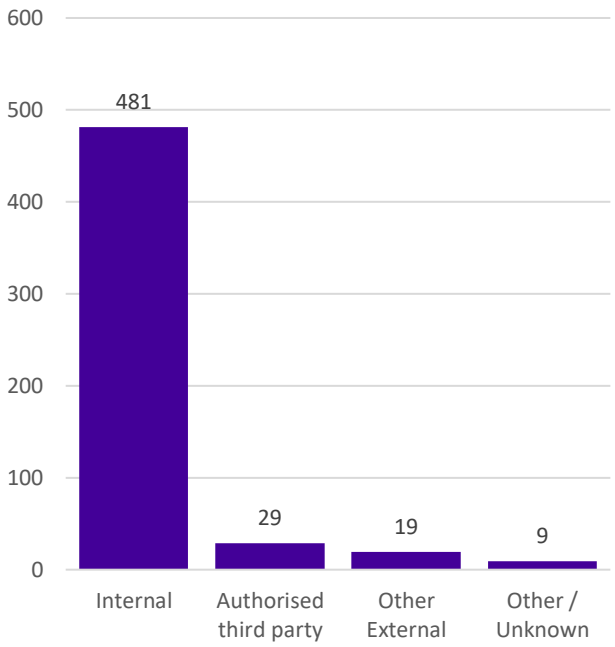
There were six (**6**) incidents related to **process** only and **10** incidents related to **technology** only as the cause of the incident. Examples of technology-related incidents include:

- software change gone wrong leading to employees being able to view the payslips of others
- incorrect system code used in a system update resulting in documents being incorrectly attached to some client records
- network design fault resulting in users being able to view information they weren't supposed to.

Where multiple control areas are part of the incident, in most cases the incident relates to people in addition to other causal factors.

There were five (**5**) incidents related to all control areas: **people**, **process**, **technology** and **no control(s) in place**. For example, compromised application accounts.

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



Insights:

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

90% of incidents in this notification period were caused by **internal** staff.

Similar to previous notification periods, there were 29 notifications of incidents caused by **authorised third parties**, compared with 21 in the January to June 2024 period, and 30 in the July to December 2023 period. For example:

- third party contracted debt collector issued debt collection notices with incorrect customer details
- third party services provider had their data, including public sector information, exfiltrated by a previous employee
- third party mail house did a bulk mailout where notices were sent to incorrect recipients
- work experience student took a photo of the workplace and then shared it on a social media platform without consent.

There were **19** incidents caused by **other external** threat actors, compared to 28 in the previous notification period. Examples of incidents include:

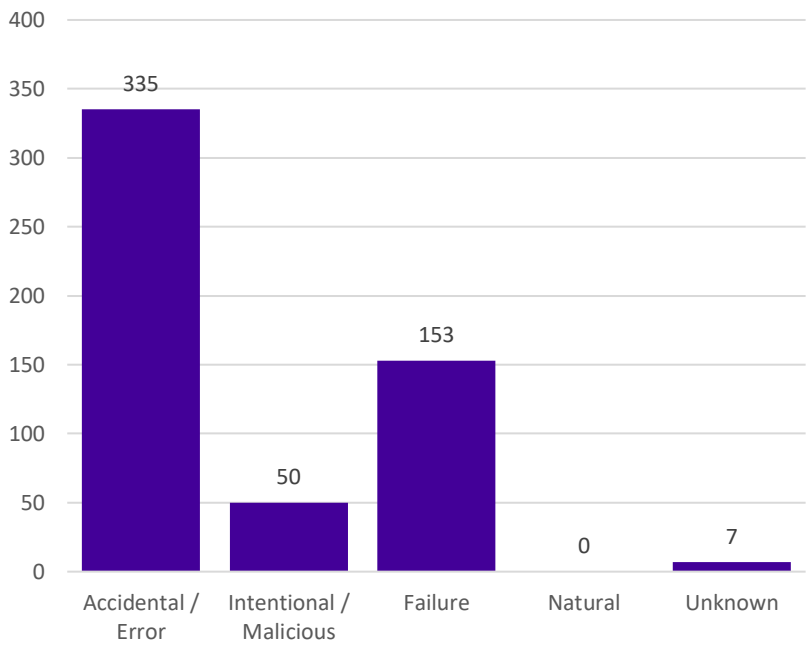
- hackers installing ransomware to encrypt systems
- compromised Drop Box account that included research data

- Business Email Compromise (**BEC**)
- stolen mobile while travelling overseas.

There were nine (**9**) incidents where the threat actor was **unknown**. For example, it was unclear who was behind an unsolicited email sent to a group of students and, another example was an incident where data was leaked to the media, but the threat actor could not be ascertained.

Although it is uncommon for more than one threat actor to be involved in an incident, like the previous notification period, there were five (**5**) incidents caused by multiple threat actors. For example, when a staff member clicked on a phishing email and the user credentials were subsequently compromised, **internal** and **other external** threat actors were the cause. An example of where both **internal** and **authorised third party** threat actors caused an incident was when a staff member sent information to an independent investigator which contained information from a previous case and this incorrect information was subsequently used by the independent investigator to contact an incorrect party.

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



Insights:

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

Due to the increase in incidents caused by **failure** as the threat type, the percentage of **accidental** incidents decreased compared to the previous period. Even though the actual numbers of incidents

related to both **accidental** actions (**335**) and **intentional** actions (**50**) were similar to the previous period which reported 337 and 41 respectively, the overall percentages decreased.

This change in percentages is attributed to the increase in incidents caused by **failure** (**29%**). The majority of the **153** incidents caused by failure were mostly from GWW. Other examples include:

- network services system bug
- defective function within online portal
- photo taken and posted online without consent
- hard copy information found during office re-location.

In terms of the spread of **intentional/malicious** threat types, half of the incidents were caused by internal staff. For example:

- taking a photo of home workspace with work information captured and posted online
- unauthorised access of family member's client file
- inappropriate access to system by terminated employee
- unauthorised use of recorded footage.

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

The number of notifications where the threat type was **unknown** (**7**) was the same as the previous notification period. For example, a fraudulent email sent to multiple recipients of a particular cohort and a loss of access to a third-party online platform.

Although multiple options can be selected for this field, there is usually one threat type associated with each incident. There were **10** 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, offboarding process not completed leading to ex-staff member having system access longer than required and another example was information related to a freedom of information request released without following the approved process.

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 disclosure of personal information or incorrect details due to utility bills being sent to incorrect recipient(s) and not the correct recipient ***(Compromise of confidentiality, integrity and availability)***	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)
Unauthorised disclosure of identity documentation ***(Compromise of confidentiality)***	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)
Inability to access an online Workplace Health and Safety Management platform to undertake normal operational duties ***(Compromise of availability)***	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)

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.