Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Incident Insights Report

1 July 2025 – 31 December 2025

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

Overview of this report

The Incident Insights Report provides a summary and analysis of the information security incident notifications OVIC received between **1 July 2025** and **31 December 2025**.

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

Victoria Police incident statistics are reported annually, consistent with existing reporting commitments. For the latest incident statistics from Victoria Police refer to OVIC's Incident Insights Report for 1 January – 30 June 2025.

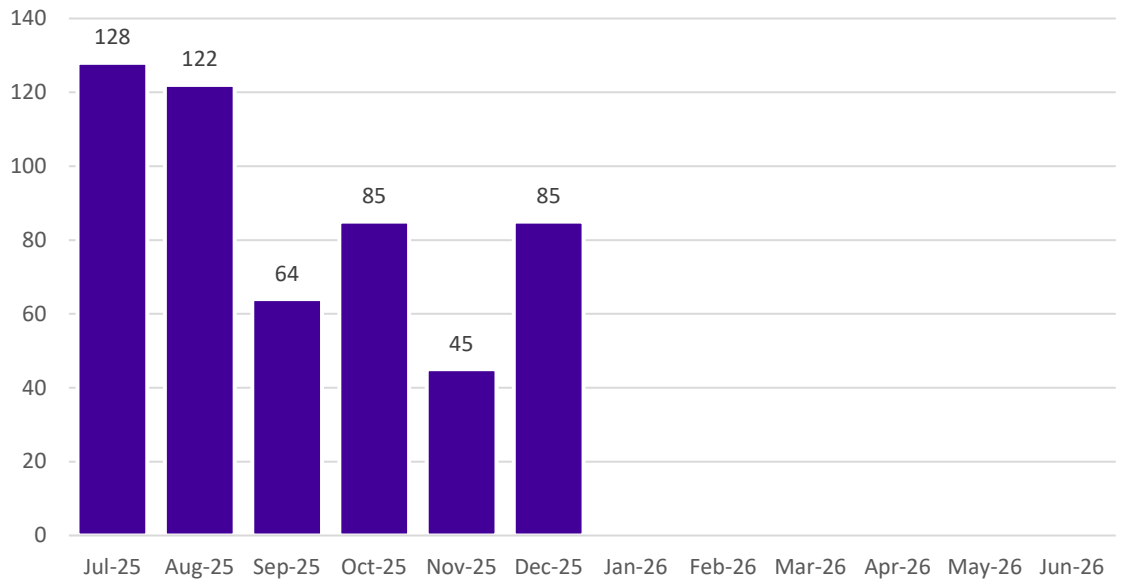
Note: The incident notification form allows for **more than one response** to be selected for the following fields:

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

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

Information security incident notification insights from July – December 2025

Notifications by month



Insights:

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

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

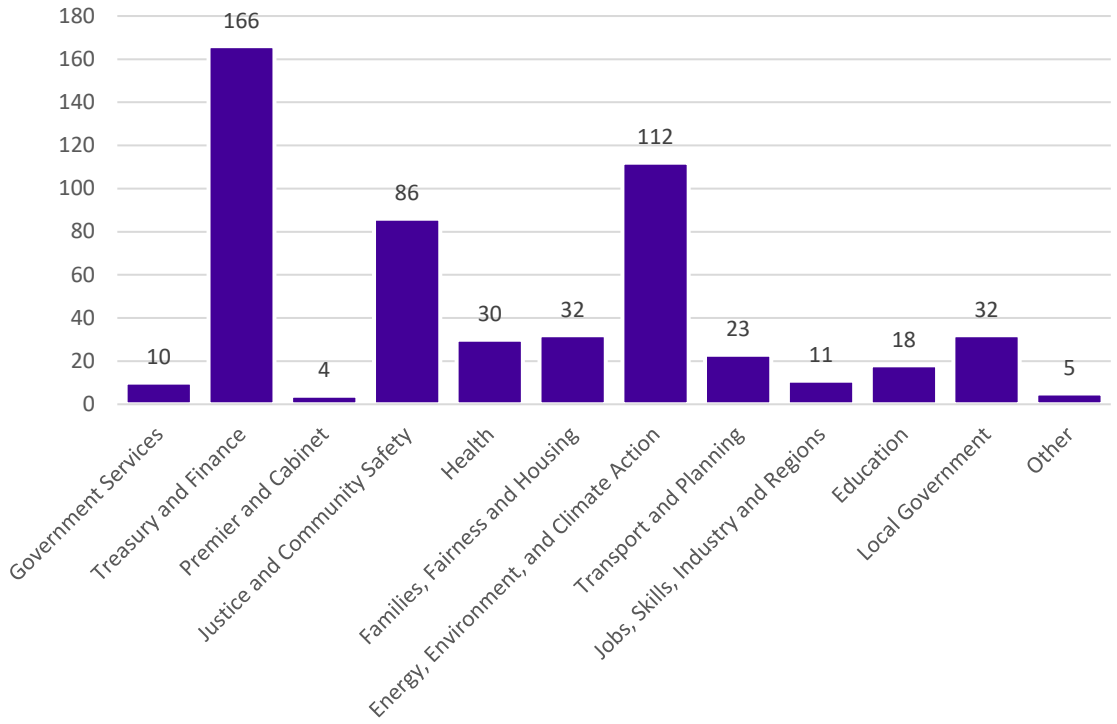
The higher numbers in July mostly came from the water sector.

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

Note:

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

Notifications by portfolio



Insights:

Similar to the previous notification period, most of the **529** notifications received by OVIC came from the Treasury and Finance portfolio (**166**) followed by the Energy, Environment, and Climate Action portfolio (**112**).

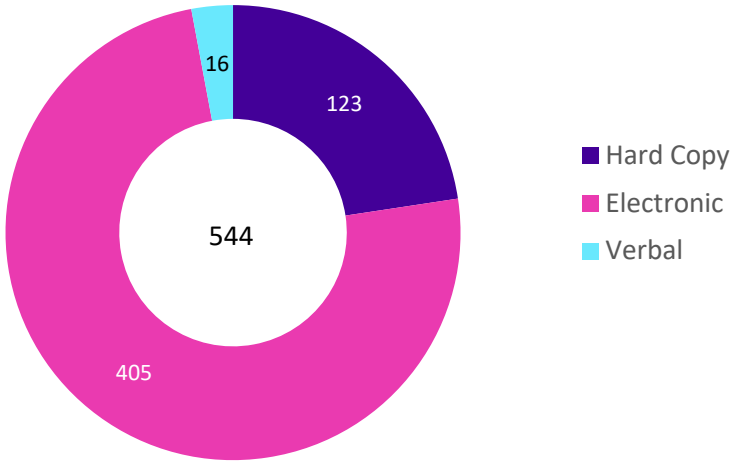
Notification numbers across several portfolios appear consistent, for example Premier and Cabinet (**4**), Justice and Community Safety (**86**), Jobs, Skills, Industry and Regions (**11**), and Local Government (**32**) compared to the previous notification period which were 5, 88, 8 and 34 respectively.

There was an increase in notifications received from Health (**30**), Families, Fairness and Housing (**32**), Transport and Planning (**23**) and Education (**18**) portfolios compared to the previous notification period which were 17, 22, 17, and 13 respectively.

There was a decrease in notifications from the Government Services (**10**) portfolio compared to the previous notification period (23).

Five notifications were received from organisations categorised under the portfolio '**other**'. These organisations are either Victorian Government organisations but do not reside under a portfolio or are out of jurisdiction for Part 4 of the *Privacy and Data Protection Act 2014* (Vic).

Information format (multiple options can be selected)



Insights:

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

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

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

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

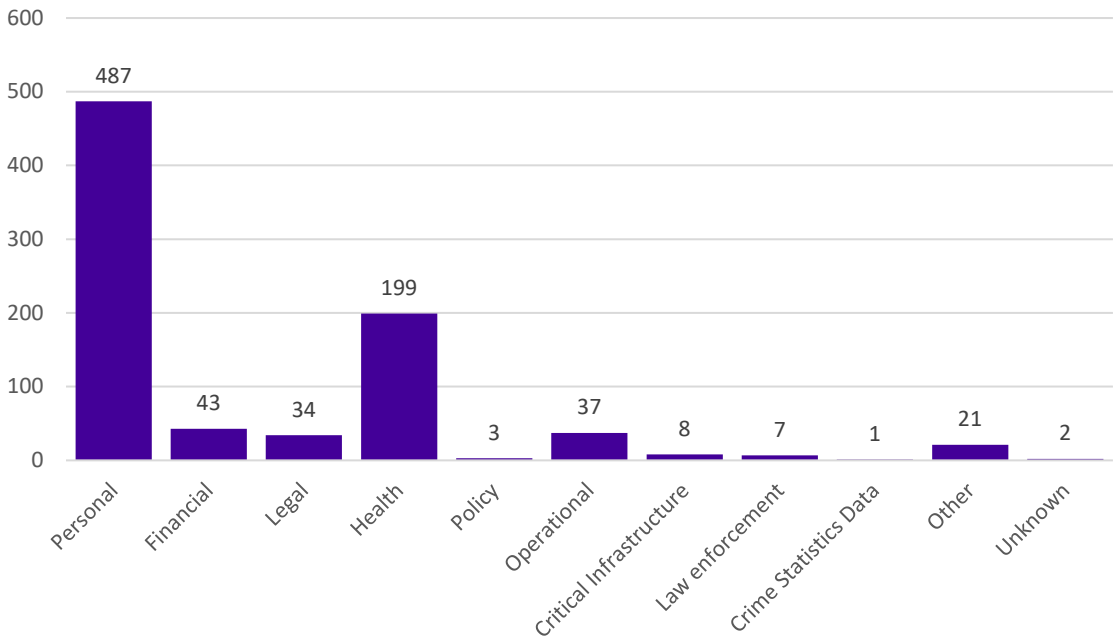
- visitor slips falling out of an unsecured rubbish truck
- hard copy paper that already had information on it was re-used to print a new document
- paperwork lost when left on top of a vehicle
- documents printed to another agency's printer
- mail merge error with infringement notices printed double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

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

Some examples of incidents involving 2 information formats include:

- tender documents emailed to Officeworks to print (**electronic and hard copy**)
- inappropriate system access by employee and subsequent sharing of information to a third party (**electronic and verbal**)
- mental health session automatically recorded leading to overcollection of information (**verbal and electronic**)
- licence (**physical and digital**) with incorrect details.

Type of information impacted (multiple options can be selected)



Insights:

Most (92%) incidents related to compromises of **personal** information, that is, **487** out of the 529 notifications.

There was a large increase in the number of incidents affecting health information (**199**) compared to the previous notification period (43) and any other periods. This increase reflects process improvement changes by some organisations rather than an increase in health-related incidents, where this information type has now been included in notifications going forward. All but 3 of the 199 health-related notifications also involved personal information.

This notification period saw an increase in all information types except for **policy** information which decreased from 7 in the previous notification period to **3**. In all these instances, policy information was affected along with other information types.

There were **7** incidents affecting law enforcement information compared to 4 in the previous notification period. These were not Victoria Police incidents and include infringement notices, an accident report, and a GenAI meeting recording that captured a conversation discussing law enforcement matters.

There were **21** incidents affecting the **other** information type compared to 6 in the previous notification period. Examples include:

- cabinet information
- credentials for a test mailbox
- hacked website

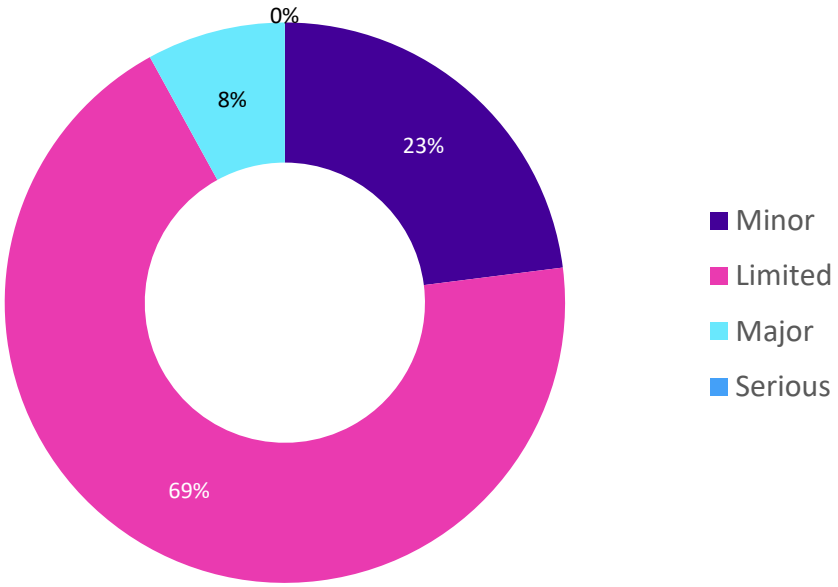
- API keys

There were 2 incidents where the type of information involved was **unknown** due to the organisation not knowing exactly what information was stolen after the Australia Post break-in.

Multiple options can be selected for this field. There were 25 incidents where 3 or more information types were affected in a single incident, for example:

- **Personal, health, other** information was affected when an online complaint form was misconfigured.
- **Personal, health, legal** information was affected when client case information was sent to a personal email address.
- **Personal, financial, operational** information was affected in the disclosure of an internal audit report.
- **Personal, health, financial, legal, policy, operational** information was stored in a backup offshore without gaining consent from the organisation.

Information Business Impact Level (BIL)[1]



Insights:

The Business Impact Level (BIL) statistics for this notification period are similar to the previous notification period. The number of incidents affecting information assessed as having a **limited** impact or **BIL 2** is **365** or **69%** compared with 347 or 62% in the previous notification period.

There was a large decrease in incidents affecting information assessed as having a **minor** impact or **BIL 1** **23%** (**120**) compared with 36% (203) in the previous notification period. This is because GWW stopped their regular monthly reporting to OVIC in October regarding their 2024 migration to a new billing and payment system as they resumed normal operations. OVIC expects incident notifications related to BIL 1 information to restore to similar numbers that were reported prior to the GWW billing and payment system migration incident.

Eight per cent of incidents affected **BIL 3** information. In terms of numbers, incidents affecting BIL 3 information continues to increase with **43** incidents in this notification period compared to the previous 2 notification periods having 11 and 5 incidents. Some examples of incidents affecting BIL 3 information include:

- critical infrastructure information sent to personal account
- insecure disposal of financial documents
- confidential information input into Notion AI software without authorisation.

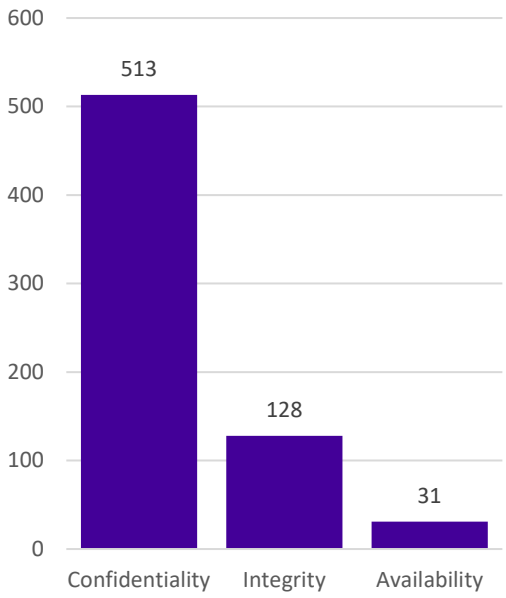
There was **one** incident affecting **BIL 4** information related to an outage affecting financial systems that had the ability to have state-wide impact if secondary systems did not work.

[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:

Similar to the previous notification period where 99% of incident notifications indicated compromises of information **confidentiality**, there were **97%** in this notification period (**513**).

There was a decrease in the number of incidents affecting information **integrity** (**128**) compared to the previous notification period (224). This is because most of the integrity incidents from the last few notification periods have come from GWW that related to the data quality issues they experienced during their billing system upgrade project. GWW stopped their regular monthly reporting to OVIC in October as they resumed normal operations. OVIC expects incidents related to information integrity to restore to similar numbers that were reported prior to the GWW billing and payment system migration incident. Some examples of other incidents affecting information integrity include:

- using an incorrect distribution list
- changing account details without receiving formal consent first
- tampering of laptop settings without permission
- incorrect name used when speaking on the phone.

There was an increase in incidents affecting information **availability** (**31**) compared with 21 in the previous notification period. For example:

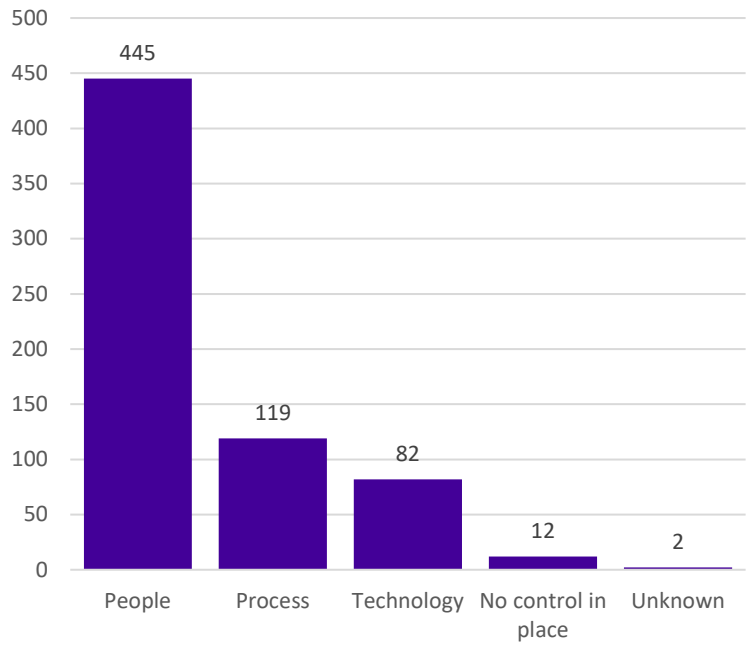
- inadvertent deletion of emails in system
- lost book
- Westpac financial services outage
- Australia Post mail break-in.

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 **92%**.

There were **14** incidents affecting all 3 security attributes (**confidentiality, integrity** and **availability**) of information compared to 9 in the previous notification period. For example:

- employee provided with their personnel file which contained documents relating to someone else
- personal email address of committee members published in error
- malfunctioning system workflow sent client referrals to incorrect third party.

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



Insights:

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

This notification period saw an increase in the percentage of incidents caused by **people** (**84%**) compared with the previous notification period (67%).

Mail errors, whether it is postal mail or email, accounted for **68%** of incidents received this notification period. There were **11** incidents related to SMS errors (incorrect recipient or incorrect information) compared with the previous notification period (9).

There was a decrease in **process**-related incidents (**119**) compared to the previous notification period (232) as well as **technology**-related incidents (**82**) compared to the previous notification period (204). This is because most of the process and technology incidents from the last few notification periods have come from GWW's data quality issues they experienced during their billing system upgrade project. GWW stopped their regular monthly reporting to OVIC in October as they resumed normal operations. OVIC expects process and technology incidents to restore to similar numbers that were reported prior to the GWW billing and payment system migration incident.

There were **13** incidents related to **process** only and **9** incidents related to **technology** only as the cause of the incident without other controls areas being involved. Examples of process-related incidents include:

- process not followed when publishing website content leading to unauthorised disclosure of email addresses

- process not followed when granting permissions to a mailbox
- verification process not followed leading to disclosure of information to the incorrect person.

Examples of technology-related incidents include:

- unauthorised disclosure of complaint information on online form due to caching
- supply chain attack using compromised Salesloft OAuth tokens to access and exfiltrate data from Drift/Salesforce tenant(s)
- sensitive information ended up in a public SharePoint site due to an IT syncing error.

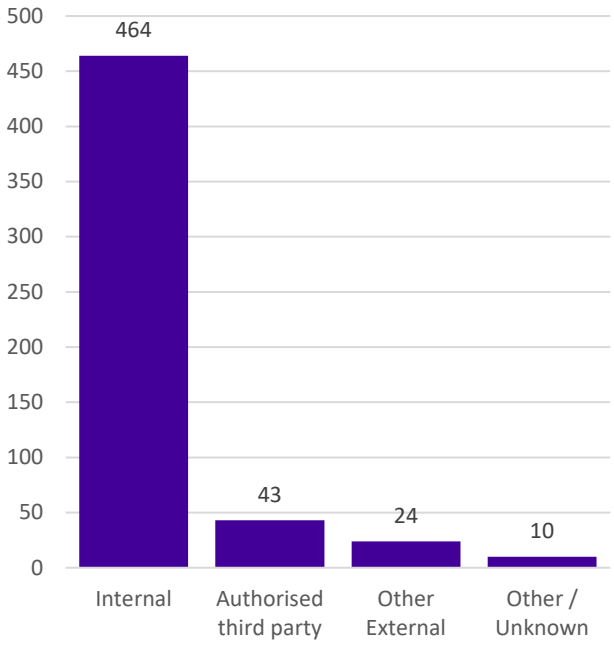
Like the previous notification period, there were 12 notifications where no control(s) in place was the cause of the incident. There were 2 incidents where the control area affected was unknown.

Multiple options can be selected for this field. There were 56 incidents related to process and technology control areas, for example a system with an incorrectly saved email address was then prefilled into an email which was sent in error and another example is a customer account mapping error in a database that led to the distribution of incorrect notices.

There were 5 incidents related to people and no control(s) in place, for example information input into ChatGPT. There were 2 incidents related to people, technology and no control(s) in place for example a GenAI application recorded a meeting.

There was one incident regarding incorrect folder permissions which related to all control areas, people, process, technology and no control(s) in place.

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



Insights:

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

Similar to the previous notification period, **88%** of incidents in this notification period were caused by **internal** staff (**464**) compared to 89% (502).

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

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

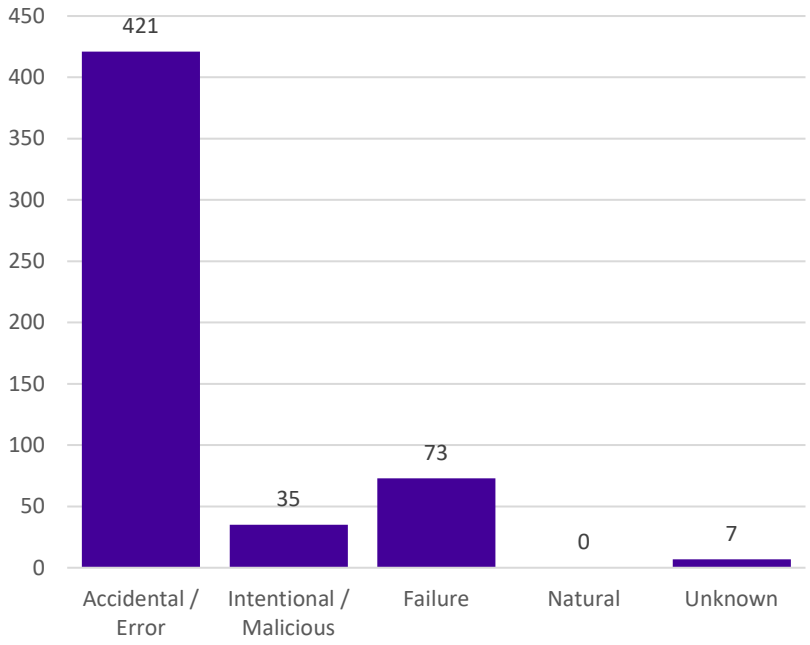
There were **24** incidents caused by **other external** threat actors, compared to 28 in the previous notification period. Examples of incidents caused by other external threat actors include:

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

There were **10** incidents where the threat actor was **other / unknown** compared to the previous notification period (17). For example, it was unclear who was behind an incident related to insecure disposal of financial records, and, in another example, a lost USB storage device in the mail.

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 which is the same as the previous notification period. For example, an **external** threat actor impersonated someone, leading to an **internal** staff member disclosing information when they should not have. Another example was where an **authorised third party** uploaded documents to the incorrect file and then an **internal** staff member did not check the contents of the file before disclosing the contents.

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



Insights:

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

There was an increase in incidents caused by **accidental/ error** actions (**421**) compared with the previous notification period (335).

There was a decrease in incidents caused by **intentional/ malicious** actions (**35**) compared with the previous notification period (40). Similar to the previous notification period, almost half of these incidents were caused by intentional actions of internal staff with a common theme of unauthorised access to information and systems. For example:

- inappropriate access to client records by a staff member without legitimate business need
- unauthorised access to SharePoint and OneDrive
- tampering of laptop settings without permission
- input confidential information into ChatGPT to produce content for report.

Incidents due to **failure** decreased from 191 in the previous notification period to **73** in this notification period. This is because most of the failure incidents from the last few notification periods have come from GWW that related to the data quality issues they experienced during their billing system upgrade project. GWW stopped their regular monthly reporting to OVIC in October as they resumed normal operations. OVIC expects incidents caused by failure to restore to similar numbers that were reported prior to the GWW billing and payment system migration incident.

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

There were 7 incidents where the threat type was **unknown**. For example, the organisation was unable to determine the threat type behind a lost USB storage device in the mail or the motivation behind the alleged unauthorised release of documents under a Freedom of Information request.

Although multiple options can be selected for this field, there is usually one threat type associated with each incident. There were 7 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 staff member went to email themselves to work around an issue but accidentally emailed someone else.

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

More information

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

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

[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.