Information for agencies

Incident Insights Report

1 July 2023 – 31 December 2023

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 2023** to **31 December 2023**.

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 2023](https://ovic.vic.gov.au/information-security/security-insights/incident-insights-report-1-january-2023-30-june-2023/).

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 July – December 2023

## Notifications by month

### Insights:

OVIC received **342** notifications between **1 July** to **31 December 2023** (inclusive). This period saw a **20%** increase in notifications compared to the previous notification period January to June 2023 (**283 notifications**) and an **11%** decrease from the previous period July to December 2022 (**387 notifications**).

OVIC received the highest number of notifications (**124**) in October, which is a largest monthly number received since the establishment of the information security incident notification scheme.

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

It is interesting to note the lower figures for November (**47**) and December (**24**). In previous years these have been higher (for example 91 in November 2022 and 86 in December 2022) as organisations tend to complete administrative activities before the end of the year.

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:

Of the **342** notifications received by OVIC, most came from the justice and transport sectors. These were mostly from DJCS, and the Transport Accident Commission (**TAC**) due to their established incident notification protocols.

This notification period saw an increase in the number of notifications across all the portfolios except two. Notifications from the education (**2**) and energy, environment, and climate action (**22**) portfolios fell compared to the last reporting period which were 20 and 27 respectively. Notifications from the transport and planning sector remain the same at **123** as well as government services, (**1**) and treasury and finance (**2**) portfolios, which also have the same number of notifications compared to the last period.

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

This reporting period saw eight (**8**) **Other** notifications received from:

* organisations that do not reside under a portfolio e.g., Independent Broad-based Anti-corruption Commission (**IBAC**);
* organisations not in OVIC’s jurisdiction;
* citizens observing inappropriate information handling.

## Information format (Multiple options can be selected)

### Information format respondent percentage

### Insights:

Notifications affecting electronic information continues to be the most selected information format **(80%)**. Most notifications indicated compromises of **electronic** information (**273**) followed by **hard copy** information (**57**). Incidents involving verbal information (**5%**) tripled from four (**4**) in the previous notification period to **17** this period. All of these relate to unauthorised disclosure / oversharing of public sector information. Some examples of verbal disclosures include:

* failing to identify the identity of a caller before providing personal information;
* reading an email in an open meeting before checking the contents of the email first; and
* attending a social event on a weekend and hearing discussions about work related topics.

**53%** of the incidents affecting electronic information related to emails and similarly, **56%** of the incidents involving hard copy information were related to mail. Consistent with previous notification periods, **75%** of the incident notifications, regardless of information format, involved unauthorised release/disclosure of information including 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 five (**5**) notifications that selected more than one information format attribute.

For example, one incident related to a staff member taking photos of the contents displayed on their computer screen (electronic) and then printing the photos (hard copy) to take off site. Another incident was related a citizen observing the contents displayed on computer screen (electronic) as well as viewing the contents of a hard copy file of a staff member on an aeroplane.

## 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 (**94%**) notifications indicated compromises of **personal** information, followed by compromises of **health** information. Just a reminder, the scheme covers incidents related to all public sector information, not just personal information.

There were **11** notifications where the **other** information type was selected. Examples include incidents related to:

* claim numbers;
* credentials (username and password);
* application vulnerability details;
* project and committee documents.

There were three (**3**) incidents where the type of information involved was **unknown** because the organisation could not ascertain with any certainty what information was locally saved on a stolen laptop; the incident was so long ago that the emails in question had since been deleted; and, the extent of the incident could not be ascertained (i.e., how far the threat actor got) to enable the organisation to determine what information was affected.

As in the last notification period, there were three (**3**) incidents that affected **law enforcement data** handled by organisations other than Victoria Police (Victoria Police incident notifications are captured separately), e.g., the [Court Services Victoria incident](https://courts.vic.gov.au/news/court-services-victoria-cyber-incident). There were two (**2**) notifications where **critical infrastructure** (**CI**) was selected. Although one of these appears to have selected CI incorrectly, the other notification is about information related to a CI asset.

Multiple information types can be involved in a single incident. **19%** of notifications selected more than one information type.

There were two (**2**) notifications where four (**4**) or more options were selected including an incident where **personal, operational, critical infrastructure,** and **law enforcement information** was published on an uncontrolled website and an incident where a SharePoint site storing a range of information had incorrect permissions.

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 but four (**4**) of these instances.

There were no notifications that selected incidents relating to **policy** information or **crime statistics data**.

## Information Business Impact Level (**BIL**)[[1]](#footnote-1)

### Highest BIL percentage

### 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 **89%** and **Minor** impact or **BIL 1** is **7%**.

This period saw a rise in the number of notifications across all the business impacts levels. This includes double the notifications (**12**) nominating **BIL 3** information was affected compared to the last notification period. Some examples include:

* the release of unredacted subpoenaed material;
* the sharing of committee documents containing sensitive commercial negotiations to attendees with conflict of interest issues; and
* leaving a sensitive voicemail message which could put a domestic violence client at high risk.

There were two (**2**) notifications that nominated **BIL 4** information was affected. An example of one of these incidents was the loss of availability of a critical system needed to provide real-time funds to clients to meet strict payment obligations, rather than an incident involving a compromise to the confidentiality of information.

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:

All except for **16** incident notifications indicated compromises of the **confidentiality** (**326**) of information followed by **integrity** (**30**) and **availability** (**21**). Incidents affecting the **availability** of information remained the same at **6%** for the third consecutive notification period.

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 **75%** of the notifications received.

Ninepercent (**9%**) of incident notifications selected more than one option for this field. In almost all instances where multiple security attributes 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 staff member either not entering the required information into the organisation’s case management system or only partially entering the information meaning records weren’t complete and up to date.

There were seven (**7**) notifications where the **availability** security attribute was selected on its own for example;

* stolen laptop;
* critical system crash; and
* an email add-on application stopping emails coming into shared mailboxes.

This period also saw a different trend with the **availability** security attribute where it was selected not because the information was not available to those who need to access the public sector information, but because the information was available to everyone including those who do not have a need-to-know.

There were eight (**8**) notifications where the **integrity** security attribute was selected on its own for example:

* the wrong claim number, address or contact number being added to a case file;
* linking two cases incorrectly; and
* saving one client’s email to another client’s file.

There were six (**6**) notifications where all three security attributes were selected. For example, a client’s email address was registered incorrectly so they never received email correspondence from the organisation but someone else did. Another example is related to incorrect SharePoint permissions and a misconfigured system allowing access to all users including those who do not have a need-to-know.

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

### Insights:

This notification period saw the same percentage of incidents caused by **people** (**92%**) as in the previous two notification periods.

The key causal factors for security incidents remain: people, internal, and accidental, for example, mail misdelivery whether it is postal mail or email (**47%**).

There was a large increase in the number of notifications selecting **process** (**86**)compared to the last notification period (**39**) and the numbers for **technology** (**27**) related incidents remained the same as the previous period.

Where multiple control areas are part of the incident, most of the time, the **people** field is selected in addition to other causal factors. There were only two (**2**) notifications where **process** and **technology** were selected without people as one of the causal factors, for example a system automatically sending a completed form to an incorrectly linked email address.

There were seven (**7**) notifications where **process** was selected on its own and **10** notifications where **technology** was selected on its own as the cause of the incident.

There were six (**6**) notifications that nominated all three control areas: **people**, **process**, and **technology**. Some examples of when these three control areas were selected include:

* inadvertent release of unredacted sensitive documents;
* release of arrears notices to incorrect parties via email due to the incorrect merging of two files into a system and not cross checking before sending; and
* public sector information published on an uncontrolled website.

There were five (**5**) notifications where **no control(s)** was selected for example, an organisation caught up in the [Pareto data breach](https://www.abc.net.au/news/2023-08-23/qld-charity-donors-dark-web-cyber-criminals-pareto-phone/102757194) where their information had been retained for longer than required past their engagement with the third party.

There were three (**3**) notifications where the control area affected could not be determined.

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

### Insights:

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

This notification period saw the spread of threat actor percentages selected in the notifications similar to the previous notification period, including **84%** caused by **internal** staff, **9%** caused by **authorised third parties** and **6%** caused by **other external** threat actors.

The number of notifications selecting **authorised third parties** as the cause of the incident (**30**) increased compared to the last period **18**,highlighting the ongoing risks around information sharing between organisations.

There were **11** notifications where the threat actor could not be ascertained, for example when the incident was still under investigation.

Although it’s not common 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 **authorised third-party** were selected where one organisation sent a USB drive to another and it was delivered to the front desk, rather than the registry, at which point it was passed onto facilities who screen all packages for dangerous items, and then was lost within a secure area. Another example is where an authorised third party input an incorrect wrong phone number onto a client’s file, so the public sector organisation sent text and calls to the incorrect recipient.

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

### Insights:

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

As in previous notification periods, most notifications (**84%**) related to **accidental** actions (**288**) and **11%** **intentional** actions (**36**).

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

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

There were five (**5**) occurrences where more than one threat type was selected. For example, **accidental** and **failure** was selected for a system crash following a staff member rebooting one network device after a configuration change, which caused a chain reaction on the rest of the network, leading to connectivity issues.

**61%** of notifications that relate to **intentional** actions were conducted by external threat actors such as hacking groups or opportunistic thieves, and **39%** were caused by internal staff. This was the first notification period to receive a notification related to the use of the generative artificial intelligence (**AI**) application ChatGPT by a staff member to write a report (internal and intentional).

There was an increase in the number of notifications where the threat actor was **unknown** (**13**) compared to the last notification period of two (**2**). Some examples of incidents where the threat actor was unknown include:

* an authorised third-party vacating premises in a rush and the premises remaining abandoned for a lengthy period until the public sector organisation attended the premises to find unsecured scattered documents
* a complaint form published on a website displayed data from previous visitor’s entries
* a misdelivery of a box of files by an authorised third party provider to the wrong public sector organisation after they sat unclaimed in the authorised third party’s office for a few months

## 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]](#footnote-2) |
| Employee payroll information shared without employee consent with a superannuation fund **(Compromise of confidentiality, integrity)** | System change triggering an override function and subsequently incorrectly processing data reverting employees to the default fund and informing the fund  | Impact on public services (reputation of, and confidence in, the organisation)Impact to individuals whose personal information was affected |
| Inability to access public sector information **(Compromise of availability)** | System crash following a staff member rebooting one network device after a configuration change which caused a chain reaction on the rest of the network leading to connectivity issues | Impact on service deliveryImpact on public services (reputation of, and confidence in, the organisation) |
| Inadvertent release of client information **(Compromise of confidentiality)** | Public sector organisation not redacting documents | 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.

1. Refer to <https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-framework-business-impact-level-table-v2-1/> [↑](#footnote-ref-1)
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. [↑](#footnote-ref-2)