Information for agencies

Incident Insights Report

1 January 2023 – 30 June 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 January 2023** to **30 June 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. These have been included towards the end of this report with comparisons made from our [Incident Insights Report for 1 January – 30 June 2022](https://ovic.vic.gov.au/information-security/security-insights/incident-insights-report-from-from-1-january-2022-30-june-2022-2/).

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 2023

### Notifications by month

A graph of a number of people

Description automatically generated with medium confidence

Insights:

OVIC received **283** notifications between **1 January** to **30 June 2023** (inclusive). This period saw a **27%** decrease in notifications compared to the previous reporting period July to December 2022 (**387 notifications**) and a slight decrease (**2%**) from the previous reporting period January to June 2022 (**290 notifications**).

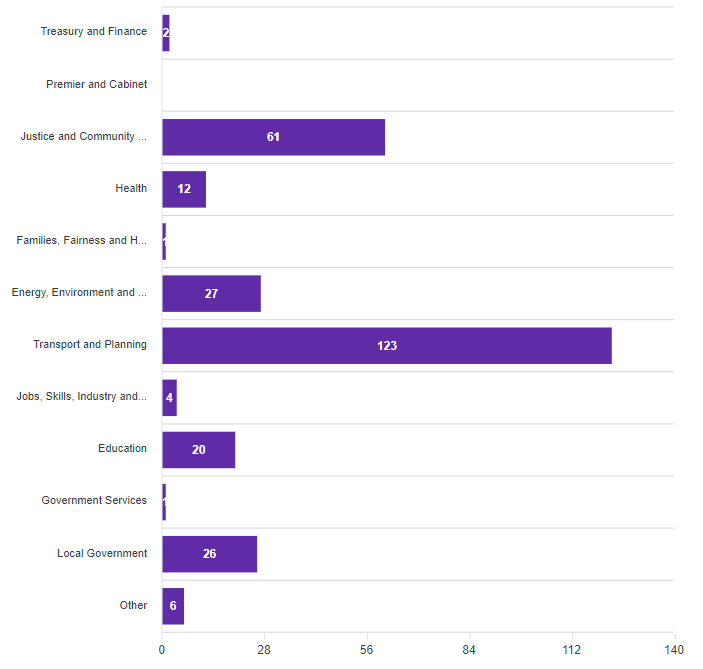
We received the highest number of notifications (**92**) in May which is a large increase from May 2022 (**27**) and higher than May in any previous year since the establishment of the information security incident notification scheme.

The higher numbers in May 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 reporting period. In addition, the lower notification numbers for this period are attributed to the delay in receiving DJCS notifications where the department is behind in their reporting to OVIC.

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 **283** 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 reporting period saw a decrease in the number of notifications across all the portfolios except for local government. For example, notifications from the justice (**61**) and education (**20**) portfolios almost halved compared to the last reporting period which were 139 and 43 respectively. Reasons provided by organisations for the decrease in notifications includes difficulties in filling vacancies, actioning and recording incidents to the required standard, as well as pressures of incident response for complex incidents which are prioritised and take up considerable time and resources.

A table of the portfolio notification numbers for this reporting period and last reporting period is provided below for comparison.

|  |  |  |
| --- | --- | --- |
| Portfolio | This reporting period (Jan-Jun 2023) | Previous reporting period (Jun-Dec 2022) |
| Premier and Cabinet | 0 | 7 |
| Justice and Community Safety | 61 | 139 |
| Families, Fairness and Housing | 1 | 7 |
| Education | 20 | 43 |

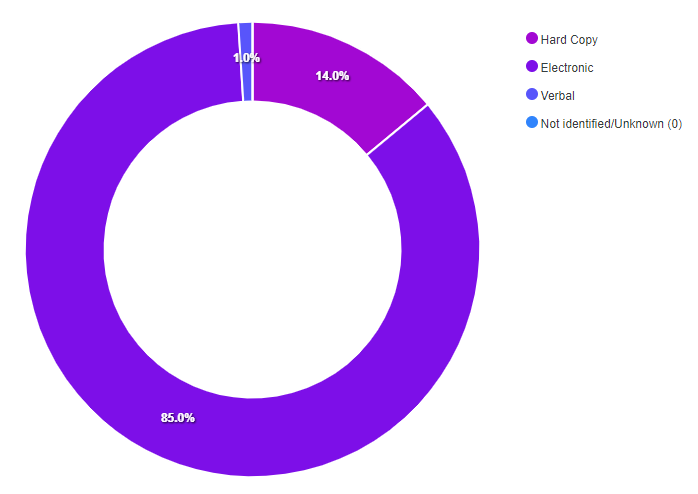
Notifications from local government organisations continue to almost double (**26**) compared to the previous reporting periods July to December 2022 with **15** and January to June 2022 with eight (**8**) notifications.

The portfolios used for this reporting period to group organisations include the name changes and machinery of government changes that came into effect 1 January 2023. There were no incidents received from the premier and cabinet portfolio.

This reporting period saw six (**6**) **Other** notifications received from:

* organisations who do not reside under a portfolio e.g., Victorian Ombudsman;
* other jurisdictions;
* third parties who suffered an incident such as the [Latitude](https://www.latitudefinancial.com.au/latitude-cyber-incident/) and [HWL Ebsworth](https://hwlebsworth.com.au/cyber-incident/) data breaches where Victorian public sector information was affected; and
* multiple Victorian public sector organisations across multiple portfolios who were affected by the same incident.

### Information format (Multiple options can be selected)



Insights:

Notifications affecting electronic information continues to be the most selected information format. Most notifications (**242**) indicated compromises of **electronic** information followed by **hard copy** information (**41**) and **verbal** information (**4**).

**60%** of the incidents affecting electronic information related to emails with almost **70%** of these email incidents involving sending emails to the incorrect recipient.

Similarly, **60%** of the incidents involving hard copy information were related to mail. Misdelivery (sending something to the wrong recipient) also tops the miscellaneous errors in the Verizon [2023 Data Breach Investigations Report](https://www.verizon.com/business/en-au/resources/reports/dbir/?cmp=paid_search:google:ves_international:gm:awareness&utm_medium=&utm_source=google&utm_campaign=GGL_BND_AU_Branded_Unlimited&utm_content=AU_Security_DBIR&utm_term=verizon%20data%20breach%20report&gclid=Cj0KCQjwrMKmBhCJARIsAHuEAPTZYN2jkzn-TbV8AfMlWjZvtP_6cHoD9T4kVN7Yc0M9OAy401WKzUEaAlJ0EALw_wcB&gclsrc=aw.ds) (**DBIR**) and accounts for 43% of breach-related errors.

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 four (**4**) notifications that selected more than one information format attribute.

For example, two of these incidents related to stolen ICT equipment and hard copy documents. Another incident was related to an employee having incorrect permissions and accessing sensitive information on a system followed by sharing it verbally with others in the team.

Consistent with previous notification periods, **63%** 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 the incorrect information.

### Type of information impacted (Multiple options can be selected)

A screenshot of a computer

Description automatically generated

Insights:

Notifications regarding the type of information involved in incidents were consistent with previous reporting periods. Once again, most (**95%**) notifications indicated compromises of **personal** information followed by **health** information.

There were five percent (**5%)** of notifications where the **Other** information type was selected.

Examples of when **Other** was selected include incidents related to:

* cabinet information;
* claim numbers;
* credentials (username and password);
* tax advice.

There was one (**1**) incident where the type of information involved was **unknown** because unauthorised access was detected on an organisation’s system, but it is unknown what information the malicious actor accessed.

Same as the last reporting period, there were two (**2**) incidents that affected **law enforcement data** handled by organisations other than Victoria Police (Victoria Police incident notifications are captured separately). 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.

Of the **283** incident notifications, there were **43** notifications where more than one information type option was selected for this field.

There were four (**4**) notifications where four (**4**) or more options were selected, and two (**2**) of these had six (**6**) information types selected. These included an incident where a large amount of a public sector information was copied from an organisation’s system to an unprotected and uncontrolled secondary storage device and an incident when a user’s mailbox was misconfigured to forward all emails to another person.

As expected, for all notifications where **health** information was selected, **personal** was also selected. Similarly, for notifications where more than one information type was selected, **personal** information was selected for all but one of these instances.

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

A purple circle with numbers and percentages

Description automatically generated

Insights:

The Business Impact Level (**BIL**) statistics for this reporting period are consistent with the previous reporting period. The number of notifications identifying incidents affecting information assessed as having a Limited impact or BIL 2 is **93%** and Minor impact or BIL 1 is **5%**.

Around **14%** of notifications did not identify the BIL of the information affected in the incident. This is a large decrease from the last reporting period where **37%** of notifications didn’t identify a BIL. In instances where the BIL is not provided, subjective assessments are made by OVIC practitioners using the information provided in the notifications to nominate a corresponding BIL.

It is encouraging to see an increase in the number of notifications which have the BIL field filled in. This may indicate a greater awareness of assessing the security value of public sector information and an understanding of what this field represents.

There were half the number of notifications (**six**) nominating BIL 3 information was affected compared to the last reporting period. Looking at these notifications, it appears BIL 3 was correctly chosen for most of these e.g., where it affected law enforcement, and cabinet information or legal professional privilege advice on major impact cases.

### Security attributes impacted (Multiple options can be selected)

A screenshot of a graph

Description automatically generated

Insights:

All except for six (**6**) incident notifications indicated compromises of the confidentiality of information followed by integrity and availability. Even though there were 100 notifications less this reporting period, the percentage of respondents that selected **confidentiality** were the same as the last reporting period (**98%**). Incidents affecting the **availability** of information also remained the same at **6%**.

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 **63%** of the notifications received.

Similar to the last reporting period, **16%** of incident notifications selected more than one option for this field. In almost all cases where multiple security attributes were selected, the **confidentiality** was selected. There was only **one** 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 some legacy email addresses being used to send SPAM emails.

Most notifications that affected the **availability** of the information were either loss of information by internal staff or theft of information or systems (laptops, hard drives) caused by external threat actors. There was one notification where the **availability** security attribute was selected on its own related to some files that were temporarily lost within the office and found.

There were four (**4**) notifications where the **integrity** of the information was only affected for example, the wrong claim number being added to a case file.

There were five (**5**) notifications where all three security attributes were selected. For example, a client’s postal address was registered incorrectly so they never received mail correspondence from the organisation but someone else did. Another example is where multiple reports had been inadvertently saved in the incorrect location so they couldn’t be found and staff without a need-to-know could access these reports.

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

A screenshot of a graph

Description automatically generated

Insights:

This reporting period saw the same percentage of incidents caused by **people** (**92%**) as the previous reporting period. The DBIR also mentions the big role people play in incidents with 74% of all breaches including the human element.

The key causal factors for security incidents remain as people, internal, and accidental (for example, staff sending emails to incorrect recipients or emailing incorrect attachments (47%)).

Although there were around 100 notifications less in this reporting period, the numbers for incidents relating to **process** (**39**)or **technology** (**27**) issues were similar to the previous reporting period which were 37 and 23 respectively.

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 multiple options were selected and people weren’t one of the causal factors, for example compromised legacy shared mailboxes where multi-factor authentication was not set up.

There were nine (**9**) notifications where **process** was selected on its own and eight (**8**) notifications where **technology** was selected on its own as the cause of the incident.

There were eight (**8**) notifications that nominated all three control areas: **people**, **process**, and **technology**.

Some examples of when these three control areas were selected include:

* The use of a mail merge function going wrong and subsequently sending emails to the incorrect recipients
* Staff enabling a threat actor masquerading as IT support to take remote control of computer
* Phishing email attack, and
* Ransomware attack.

There were three (**3**) notifications where the incident occurred due to a missing control(s) and there were three (**3**) notifications where the control area affected could not be determined.

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

A screenshot of a graph

Description automatically generated

Insights:

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

Even with around 100 fewer notifications, this reporting period saw the same spread of threat actor percentages selected in the notifications as the previous reporting period including **82%** caused by **internal** staff, **6%** caused by **authorised third parties** and **9%** caused by **other external** threat actors. Although this varies from the Verizon [DBIR](https://www.verizon.com/business/en-au/resources/reports/dbir/?cmp=paid_search:google:ves_international:gm:awareness&utm_medium=&utm_source=google&utm_campaign=GGL_BND_AU_Branded_Unlimited&utm_content=AU_Security_DBIR&utm_term=verizon%20data%20breach%20report&gclid=Cj0KCQjwrMKmBhCJARIsAHuEAPTZYN2jkzn-TbV8AfMlWjZvtP_6cHoD9T4kVN7Yc0M9OAy401WKzUEaAlJ0EALw_wcB&gclsrc=aw.ds) where external threat actors were responsible for 83% of breaches, the DBIR covers breaches[[2]](#footnote-2) as opposed to incidents.

In terms of respondent numbers, there was another decrease in the number of notifications identifying **authorised third parties** as the cause of the incident (**18**) compared to the last reporting periods **24** and **39**.

There were **10** notifications where the threat actor could not be ascertained.

Examples of **external** threat actor incidents affecting approved third parties providing services to Victorian government organisations include Latitude, and HWL Ebsworth. The data breach affecting [MOVEit](https://www.cshub.com/attacks/news/pwc-and-ey-impacted-by-moveit-cyber-attack) which is used by firms such as PricewaterhouseCoopers (PwC) and Ernst & Young (EY) had a flow on effect for Victorian government organisations who although may not have used MOVEit directly, had engaged third parties who used the data transfer service during the engagement with the Victorian government organisations. This is a good example of the need for strong supply chain controls where it’s not enough to secure the initial third-party engagement, but also subsequent parties involved in the engagement.

Eight (**8**) notifications related to compromised credentials that **external** threat actors either published on the dark web or used to gain access to systems e.g., conduct phishing attacks. Most notifications that involved theft of information or systems, six (**6**), were caused by **external** threat actors.

Although it’s not common for more than one threat actor to be involved in an incident, there were two (**2**) notifications where multiple threat actors were selected. For example, both **internal** and **authorised third party** were selected where two Victorian government organisations attempted to do a file transfer involving each of their respective contracted service providers and inadvertently shared incorrect information.

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

A screenshot of a graph

Description automatically generated

Insights:

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

Similar to previous reporting periods, most notifications (**82%**) related to **accidental** actions and **14%** **intentional** actions.

There were no notifications in this reporting period that were due to **natural** causes other than those reported separately by Victoria Police as highlighted in the Victoria Police Statistics section of this report.

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

There were four (**4**) occurrences where more than one threat type was selected. For example, staff had unknowingly navigated to a malicious website and downloaded a remote control application (**accidental**) that subsequently allowed an external threat actor to gain access to the computer (**intentional**).

**63%** of notifications that relate to **intentional** actions were conducted by external threat actors and **30%** were caused by internal staff. There were a few notifications that related to the intentional actions by external threat actors where [usernames and passwords had been collected from people who had used government logins to access websites around the internet](https://www.afr.com/technology/more-than-100-000-suspected-government-logins-found-in-massive-breach-20230106-p5cauf). For example, hackers may have stolen the credentials of a government employee who used their work email to log in to another service like Netflix or Twitter.

### 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’[[3]](#footnote-3) incident categories remain the same. The **Communications Fault** category is the new entry into the top five, replacing “**Other**” category. Communications Fault is a new category developed in 2021-22.

The numbers for 2022-23 are consistent with the last reporting period except for the number of completed Communications Fault incidents which has increased considerably. Victoria Police have advised this spike in 2022-23 can be attributed to an improved, streamlined process between the SIR team and the Victoria Police Security Control Room. The Security Control Room monitor and manage communications faults such as planned/unplanned network, power, or telecommunication outages, and communications equipment faults. Extreme weather events have also impacted on unplanned outages during this reporting period.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Category** | **22/23** | **21/22** | **20/21** | **19/20** | **18/19** |
| Theft or Loss of Asset | 234 | 241 | 279 | 196 | 67 |
| Lost or Stolen ID | 214 | 209 | 179 | 232 | 220 |
| Information Handling | 94 | 79 | 149 | 25 | 21 |
| Communications Fault | 93 | 39 | - | - | - |
| Unauthorised Release or Disclosure of Information | 76 | 85 | 103 | 292 | 74 |

## Risk statements

Based on the incident notifications received by OVIC, we developed the following risk statements for consideration by VPS organisations when reviewing their information security risks:

|  |  |  |
| --- | --- | --- |
| The risk of… | Caused by… | Resulting in…[[4]](#footnote-4) |
| Poor data quality  **(Compromise of integrity)** | Internal staff manually processing an application and inadvertently linking it to the wrong case | Impact on public services (reputation of, and confidence in, the organisation)  Impact to individuals whose personal information was affected |
| Unauthorised access to / inability to access public sector information  **(Compromise of confidentiality and availability)** | Thieves breaking into an authorised third-party premises and stealing a book / hard copy files and hard drive | Impact on service delivery  Impact on public services (reputation of, and confidence in, the organisation) |
| Unauthorised access to public sector information  **(Compromise of confidentiality, integrity, and availability)** | Malicious threat actor hacking third party application account credentials that are the same as credentials used on VPS systems to either access public sector systems or publish on dark web | Impact on public services (reputation of, and confidence in, the organisation)  Impact on service delivery  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/information-security/incident-notification/>

We welcome your feedback on this report. Contact OVIC at [security@ovic.vic.gov.au](mailto: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. Verizon definition of Breach: “An incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party.” [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)
4. 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-4)