Information for agencies

Incident Insights Report

1 July 2022 – 31 December 2022

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 2022** to **31 December 2022**.

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 its latest incident statistics refer to OVIC’s [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 July – December 2022

### Notifications by month



OVIC received **387** notifications between **1 July** to **31 December 2022** (inclusive). This is a 12% increase compared to July to December 2021 (**343 notifications**) and an even larger increase (33%) from the previous reporting period January to June 2022 (**290 notifications**).

We received the highest number of notifications (**91**) in November which is consistent with 2021.

Notifications received in December 2022 (**86**) were higher than December in any previous year since the establishment of the information security incident notification scheme.

**Take-out:**

The higher numbers in November and December mostly came from the Department of Justice and Community Safety (**DJCS**) and Transport Accident Commission (**TAC**). This was due to DJCS and TAC finalising and sending through their notifications before the end of 2022.

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



Of the **387** notifications received by OVIC, most came from the justice and transport sectors. These were mostly from DJCS, and TAC due to its established incident notification protocols.

There was a large increase in the number of notifications received from the Department of Education and Training during this period (**43**) compared to the previous reporting period (**16**) January - June 2022. In addition, notifications from local government organisations almost doubled in this period (**15**) compared to the previous reporting period (**8**).

This reporting period saw a decrease in the number of notifications from the premier and cabinet (**22%**); health (**31%**); and families, fairness, and housing (**58%**) sectors. The reasons for the decrease in notifications for these portfolios has not been identified.

Note: the portfolios used for this reporting period to group organisations were current up to 31 December 2022 prior to name changes and machinery of government changes.

**Take-out:**

This reporting period saw five **Other** notifications received from:

* other jurisdictions;
* third parties who suffered an incident such as the [Optus](file:///C%3A%5CUsers%5Caharris%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CINetCache%5CContent.Outlook%5C0Z9TRRHN%5COptus) data breach and the [Medibank Private](https://www.medibank.com.au/livebetter/newsroom/post/medibank-cyber-incident-response) data breach where Victorian public sector information was affected; and
* multiple Victorian public sector organisations across multiple portfolios who were affected by the same incident for example the [PNORS Technology group incident](https://www.pnors.com/page/cyber-event-updates).

There will be a shift in portfolio numbers in the next reporting period as a result of machinery of government changes effective 1 January 2023.

Under the information security incident notification scheme, OVIC has established a memorandum of understanding (**MOU**) with the Cyber Intelligence and Response Service (**CIRS**) which enables the sharing of incident information to minimise the reporting burden on organisations. As such, CIRS continued to keep OVIC up to date with relevant situational reports (**SITREP**s) for incidents, without each affected Victorian government organisation needing to notify OVIC separately.

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



Notifications regarding information format were consistent with previous reporting periods. Most incident notifications (**309**) indicated compromises of **electronic** information followed by **hard copy** information (**71**). Incidents involving **verbal** information remained the same (**10**).

Once again, **half** of the incidents affecting electronic information related to emails. Most (**70%**) of these emails related to incidents involved sending emails to the incorrect recipient.

**Half** of the incidents involving hard copy information were related to mail. This is a decrease from the previous reporting period where most incidents involving hard copy information were related to mail (**74%**).

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 three (**3**) notifications that selected more than one information format attribute.

For example, one of these incidents related to a victim providing verbal information on a phone call to a threat actor masquerading as NBN support while the threat actor had remote access to their laptop to assist them. Another incident was related to stolen documents and a laptop which had been left in an employee’s car overnight.

**Take-out:**

Consistent with previous notification periods, **64%** 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.

With the increase in digitisation of information, compromise of electronic information format continues to account for the most incidents. However, organisations should be mindful that other information types (hard copy and verbal) are still at risk of compromise and should be equally considered in any risk assessments.

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



Notifications regarding the type of information involved in incidents were consistent with previous reporting periods. Once again, most (**92%**) incident notifications indicated compromises of personal information followed by health information.

There were nine (**9**) incident notifications where the **Other** information type was selected.

Examples of when Other was selected include incidents related to:

* cabinet information;
* access to a wide range of public sector information which continued after personnel left the organisation due to poor offboarding practices; and
* verbal threats to staff.

There were **15** incident notifications where the type of information involved was **Unknown**.

Some examples of incidents where the information type affected could not be ascertained include:

* ransomware;
* stolen/lost phone;
* lost backup tape(s);
* stolen credentials; and
* use of an unapproved cloud application.

A recent update to the notification form added two new information types to the current list, including **law enforcement** and **crime statistics** information. These were added because OVIC has specific oversight of these two information types under Part 5 of the *Privacy and Data Protection Act* (**PDP Act**). In this reporting period there were two (**2**) incidents that affected law enforcement data handled by organisations other than Victoria Police (Victoria Police incidents are captured separately).

**Take-out:**

Of the **387** incident notifications, there were **64** notifications where more than one information type option was selected for this field.

There was one (**1**) notification where four (**4**) or more options were selected, and one (**1**) where six (**6**) or seven (**7**) information types were selected. These included an incident where a large amount of a public sector information was copied from an internal system to a secondary storage device and an employee continuing to access internal systems while being on a long period of leave.

There were nine (**9**) notifications related to ransomware incidents, which is almost double compared to the last reporting period. Some of these ransomware incidents affected third parties with access to Victorian public sector information.

Examples of some publicised ransomware incidents affecting Victorian government during the July to December period include:

* [PNORS Technology group](https://thecyberexpress.com/australia-pnors-cyberattack/)
* [G4S](https://www.itnews.com.au/news/g4s-australia-confirms-staff-data-leaked-following-july-breach-586113)
* [Fire Rescue Victoria](https://australiancybersecuritymagazine.com.au/data-stolen-in-fire-rescue-victoria-cyber-attack-now-on-dark-web/) (**FRV**)
* [Dialog](https://itwire.com/business-it-news/security/singtel-owned-it-services-provider-dialog-hit-by-windows-ransomware.html)
* [Wordfly](https://cybernews.com/news/attackers-shut-down-wordfly-siphon-arts-institutions-data/)

In these notifications, sometimes **Other** was selected, sometimes **Unknown** was selected and sometimes organisations knew what information was affected so they selected specific information types like **personal** information.

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



The number of notifications identifying incidents affecting information assessed as having a Limited impact or Business Impact Level (**BIL**) 2 is consistent with the previous reporting period at **92%**.

Around **37%** of notifications did not identify the BIL of the information affected at the time of notification, either because the field was left blank, or a different form was used (e.g., an organisation-specific privacy form). 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.

**Take-out:**

There were **11** notifications nominating **BIL 3** which is consistent with the same time last year. Looking at these notifications, it appears BIL 3 was correctly chosen for most of these e.g., where it affected law enforcement, critical infrastructure, cabinet or security classified information.

It is encouraging to continue seeing organisations notify OVIC of incidents regardless of threshold, for example notifying of incidents affecting **BIL 1** information, to enable us to not only look at trends and themes but also provide privacy assistance where required for incidents affecting personal information.

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



All except for **10** incident notifications (**98%**) indicated compromises of the confidentiality of information followed by integrity and availability. Even with the **33%** increase in notifications this reporting period compared to the previous reporting period, the percentage of incidents affecting the integrity or availability of information did not increase and was either the same (**10% integrity**) or less (**6% availability**).

**Take-out:**

Identical to the last reporting period, **12%** of incident notifications related to more than one option for this field. Where more than one option was selected, the majority of these selected both **confidentiality** and **integrity**.

For example, an internal fraud incident can not only affect the **confidentiality** of customer’s bank accounts, but also the **integrity** of the system with incorrect data. An example of where **confidentiality** and **availability** were both selected included a lost device such as a phone or backup tape.

There were only a couple occurrences where **availability** was selected on its own. An example of this included a configuration change to block a legitimate email address without consulting the business.

Even though most incidents affect the confidentiality of information, organisations should be mindful that other security attributes (integrity and availability) are still at risk of compromise and should be equally considered in any risk assessments.

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



This reporting period saw a slight increase in the incident notifications related to **people** (**92%**) followed by **process** issues. Although there was an increase in the total number of incident notifications for this reporting period, the number of incidents caused by deficiencies in **process** decreased from **19%** in the previous reporting period to **10%** of the total notifications received in this reporting period.

Multiple options can be selected for this field. Like the last reporting period, in most (**83%**) occurrences where **process** was selected, **people** was also selected. There were only six (**6**) notifications where **process** was selected on its own and **14** notifications where **technology** was selected on its own as a cause of an incident.

There were four (**4**) notifications (**1%**) where the incident occurred due to a missing control(s) and there were **ten** notifications where the control area affected could not be determined.

**Take-out:**
The key causal factors for security incidents remain as **people**, **internal**, and **accidental** (for example, staff accidentally sending emails to incorrect recipients).

It comes as no surprise that **people** are constantly reported as the number one cause of information security incidents under the scheme. Whilst this might seem alarming, the positive news is that with increased training and awareness, organisations can address more foundational issues and hopefully see a decrease in incidents cause by people.

There were five (**5**) notifications that nominated all three control areas: **people**, **process**, and **technology**.

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

* Superannuation accounts being inadvertently created for employees by a payroll system;
* Employees continuing to have active credentials and access to an organisation’s systems after leaving the organisation; and
* Incorrect access permissions to files in SharePoint.

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



This reporting period saw an increase in the number of incidents relating to internal staff. The majority(**82%**) of incident notifications selected **internal** as the cause of the incident.

There was a slight decrease in the number of notifications identifying authorised third parties as the cause of the incident (**24**) compared to the last reporting period (**39**).

Although not common, multiple options can be selected for this field.

There were **17** notifications where the threat actor could not be ascertained.

**Take-out:**

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

Even though there were some incidents affecting approved third parties providing services to Victorian government organisations in this reporting period, such as PNORS, G4S, Dialog, and Wordfly, these incidents were not caused by the third party itself.

Rather, these incidents were caused by **other external** threat actors exploiting vulnerable systems, persons or processes of these third parties and in turn affecting public sector information. This highlights the need for strong supply chain controls.

Although it’s not common for more than one threat actor to be involved in an incident, there were four (**4**) occasions where both **internal** and **authorised third-party** were selected.

For example, one incident identified two errors that had occurred on a single account whereby an authorised third party provided an incorrect property address and in addition an internal employee added an incorrect email address to the account.

In another example, an employee had provided a list containing contact details to an authorised third party which it shouldn’t have, and the third party then used this to contact individuals on the list that it shouldn’t have.

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



In this reporting period, **79%** of incident notifications related to accidental actions and **16%** intentional actions.

There was one (**1**) notification where **natural** was selected, however this appears to have been selected incorrectly.

The threat type of **10** notifications could not be ascertained.

**Take-out:**

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

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

There were less than a handful of occurrences where more than one threat type was selected.

For example, the incorrect disposal of hard copy documents (**accidental**) that subsequently identified a wider systemic problem with the secure disposal of hard copy information (**failure**).

Another example is the allocation of incorrect permissions in SharePoint (**accidental**) that subsequently identified other incorrectly assigned permissions (**failure**).

Although the threat type **failure** is generally associated with a technology e.g., hard drive or power supply failure, these incidents demonstrate failures of process.

There were **14** notifications related to unauthorised / inappropriate access.

Of these 14 notifications, most (**11**) were **intentional** unauthorised access to public sector information and seven (**7**) were caused by internal staff.

For example, copying information to secondary storage or changing bank details for personal gain or searching the system with no legitimate business need.

## 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…[[2]](#footnote-2) |
| Financial fraud **(Compromise of confidentiality and integrity)** | Internal staff intentionally accessing customer accounts and changing bank details | Impact on organisation’s finances Impact to individuals whose personal information was affected |
| Unauthorised access to sensitive information**(Compromise of confidentiality)** | Malicious threat actor launching a cyber-attack on an authorised third-party who retained public sector information longer than the required timeframe | 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)** | Lost back up tapes during transit from authorised third party to public sector organisation  | Impact to individuals whose personal information was affectedImpact on service delivery |

## 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)