The information security incident notification scheme (**the scheme**) provides tangible 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 2021** to **31 December 2021**.

Our observations and take-outs in this report are 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 an annual basis consistent with existing reporting commitments. For their latest incident statistics refer to OVIC’s [Incident Insights Report for 1 January – 30 June 2021](https://ovic.vic.gov.au/data-protection/incident-insights-report-from-january-2021-june-2021/#victoria-police-statistics).

Information security incident notification insights from July – December 2021

Notifications by month



OVIC received **343** notifications between **1 July** to **31 December 2021** (inclusive). This is a 57% increase in the number of notifications compared to the last (January - June 2021) reporting period (**218 notifications**).

We received the highest number of notifications in October (**80**) and November (**101**).

**Take-out:**
Notifications continue to steadily increase as awareness of the scheme increases across the Victorian public sector. We received **78** notifications in the first reporting period, **155** in the second reporting period, **218** in the third reporting period and **343** notifications in this reporting period.

Between 2020 and 2021 monthly notifications doubled, except for September 2021 (see Table 1).

During May to July 2021, OVIC met with some organisations for their Protective Data Security Plan (**PDSP**) insights sessions. During these sessions, the requirements of Element 9.010 were discussed which provided organisations with a better understanding of their obligations. This may be another factor in the increase in notifications for this reporting period.

|  |  |  |
| --- | --- | --- |
| ***Month*** | ***2020 notification #*** | ***2021 notification #*** |
| ***July*** | *12* | *38* |
| ***August*** | *21* | *49* |
| ***September*** | *33* | *20* |
| ***October*** | *26* | *80* |
| ***November*** | *50* | *101* |
| ***December*** | *13* | *55* |

 *Table 1. Comparison between 2020 and 2021 monthly notification figures*

The increase in notifications in October and November may reflect organisations undertaking increasing administration activities before the end of year and does not necessarily reflect more incidents occurring. For this reason, caution should be observed drawing conclusions from month-to-month comparisons.

Notifications by portfolio



Of the **343** notifications received by OVIC, the majority come from the justice sector, specifically from the Department of Justice and Community Safety (**DJCS**), and the transport sector, specifically from the Transport Accident Commission (**TAC**).

This reporting period saw the health and human services sectors notify separately under the health portfolio or the families, fairness, and housing portfolio.

Notifications from local government increased from three (**3**) to **12** as awareness of the scheme grows within that sector for any Committee of Management information they handle or where they require privacy assistance for incidents related to personal information.

The three notifications categorised as **Other** either related to incidents that affected multiple Victorian government organisations or came from a non-Victorian government organisation.

**Take-out:**The increase of notifications from the transport sector from eight (**8**) in the last reporting period to **81** this period is a result of TAC notifying OVIC rather than more incidents occurring*.* As more organisations establish their incident management frameworks which includes notification protocols, we expect to see similar increases in notifications to our office across the Victorian public sector.

Most notifications from the families, fairness and housing portfolio came from the department itself, and were received by OVIC’s privacy team. This is a good demonstration of whereorganisations can report to OVIC once rather than needing to notify security and privacy areas separately and can utilise existing relationships with our office to fulfil their reporting obligations.

Information format



Once again, most incident notifications related to compromises of electronic information followed by hard copy information.

Like previous reporting periods, approximately **55%** of incidents affecting electronic information related to emails. These incidents predominantly involved sending emails to the incorrect recipient.

Most of the incidents involving hard copy information were related to mail including delivery to wrong person or incorrect labelling.

There were two (**2**) notifications that affected both hard copy and electronic information. One of these related to stolen information (hard copy files and an electronic device) and the other one was an incident affecting both digital and hard copy letter mailout.

**Take-out:**Incidents involving phishing and ransomware are published daily in the news and are some of the top sources in the current threat environment. The Office of the Australian Information Commissioner's (**OAIC**) [Notifiable Data Breaches Report: January – June 2021](https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021) noted **54%** of cyber incidents were from phishing and ransomware.

In contrast, **0.6%** of notifications under our scheme were a result of phishing and **1.5%** were ransomware. This discrepancy is due to various factors including differing scopes, jurisdictions, thresholds, information types, and data points e.g., confirmed data breach versus security incident.

Type of information impacted



Incidents involving personal information continue to exceed incidents affecting other types of information. This period saw a slight increase in incidents involving personal information (**78%**) compared to the last reporting period (**70%**).

There were four (**4**) incident notifications where **Other** information type was selected relating to administrative information, investigation information, draft internal notes, and cabinet information.

There were two incident notifications where the type of information involved could not be ascertained. For example, the incident related to a weather event which damaged a building, and it isn’t known what, if any, public sector information was impacted.

**Take-out:**
OVIC accepts notifications in differing forms and the security team fills in any blank fields from information provided in the notification. Sometimes there isn’t enough information provided in notifications to determine some fields.

Three per cent (**3%**) of notifications related to incidents involving Covid-19 related information such as vaccination status, test results or border permits.

Analysing the data for the notifications which identified critical infrastructure information involved in the incident has highlighted the need for OVIC to define what is meant by critical infrastructure information (**CII**). There appears to be a misunderstanding of what is meant by this term and these incidents that identified CII was affected may not be accurate. Industrial Control and Automation Systems (**IACS**) is a specialised field with only a few organisations operating these types of systems and associated data, primarily used in operational sectors such as water and transport. The updated [VPDSS Glossary](https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-standards-glossary-v2-1/) published on the OVIC website includes definitions for CII and IACS.

Information Business Impact Level (**BIL**)



The number of notifications affecting information assessed as BIL 2, or **Limited**, slightly increased from **87%** in the last reporting period to **90%** this period.

Although the percentage of incidents related to BIL 3 / PROTECTED information dropped from **6%** last reporting period to **3%** this reporting period, the actual number of notifications affecting BIL 3 information (**11**) is the same.

Ten per cent (**10%**) of incident notifications were received through OVIC’s privacy team and utilise differing forms depending on individual organisation’s privacy unit. In instances where the BIL is not provided, subjective assessments were made by OVIC practitioners using the information provided in the notifications to nominate a corresponding BIL.

**Take-out:**
Looking at the affected information in the incident notifications indicates a growing understanding of the threshold for notifying OVIC of incidents related to BIL 2 or higher information. Some organisations notify OVIC of incidents related to lower-level information either because they aren’t confident with their BIL assessment or require privacy assistance from OVIC. We accept all notifications and encourage organisations to notify even if in doubt.

Analysis of the notifications affecting BIL 3 information indicates that half of the notifications do not appear to relate to the business impact of the information itself but perhaps were chosen to reflect the severity of the incident or the priority that the organisation placed on the incident.

Standard 2 of the Victorian Protective Data Security Standards (**VPDSS**) requires organisations to identify and assess the security value of public sector information. OVIC undertook an audit on Standard 2 in 2021. The audit report has been published and is available on [OVIC’s website](https://ovic.vic.gov.au/audit-report-standard-2-of-the-victorian-protective-data-security-standards/). It covers the application of Standard 2 broadly across four organisations and focusses on the implementation of each element under Standard 2 including element 2.040 which covers assessing the security value of public sector information. Using the outcomes from this security value assessment allows organisations to identify incidents related to public sector information assessed as BIL 2.

Security attributes impacted

**

The percentages of security attributes were similar to previous reporting periods with incidents affecting the confidentiality of information still the most common.

There was an increase in incidents affecting the integrity of information from **9%** to **12%** this reporting period. Although this is a slight increase in percentage, the actual number has doubled from **24** to **49** incidents.

**Take-out:**
Previously, most confidentiality related incidents were from email disclosures (**85%**). In this period **45%** of incidents affecting the confidentiality of public sector information were related to email/mail disclosures.

Other confidentiality related incidents were due to:

* incorrect access permissions applied to folders;
* misconfiguration of systems;
* oversharing information in meetings or over the phone;
* inappropriate access to systems for personal use;
* not checking redacted documents before releasing;
* sharing filled in templates instead of blank forms; and
* applying workarounds e.g., using personal email accounts when work supplied systems do not work.

Most of the incidents affecting the integrity of information were due to incorrect linking of records in databases or input of wrong data e.g., wrong suburb in an address field.

There were occasions where multiple attributes were selected. For example, the reason for the disclosure of the information (confidentiality) was due to incorrect data on the record or file (integrity) or the information being sent to the incorrect recipient (confidentiality) meant that the right recipient didn’t receive their information in a timely manner (availability).

Introduction of three new fields

We introduced three new fields in this reporting period:

* **controls area(s);**
* **threat actor(s);** and
* **threat type(s).**

We included these new fields as part of the release of the refreshed [notification form](https://ovic.vic.gov.au/information-security-and-privacy-incident-notification-form/) which incorporates previously separate privacy breach and security incident forms. These forms have been consolidated to enable organisations to report once to OVIC and report consistently.

The introduction of the three new fields provide an at-a-glance view of key causal factors of security incidents.

Control area(s) affected



This is a new field introduced during this reporting period.

Most(**80%**) incident notifications related to **people**. This is not surprising as people are behind almost all interactions with information whether it is misdirecting information, misconfiguring permissions or system settings, inputting wrong data or oversharing.

Fifteen per cent(**15%**) of incident notifications indicated process failures and **6%** indicated failures in technology.

**Take-out:**
The key causal factors of security incidents are people; internal; and accidental. For example, staff accidentally sending emails to incorrect recipients.

There were occasions where multiple control areas were selected. For example, a staff member (**people**) sent information to the incorrect customer because the accounts matching process was set to match two pieces of information instead of three or more (**process**).

The introduction of this field enables organisations to identify where current controls are not operating effectively and where attention is required. These learnings can be fed into the post incident review or risk monitoring and review cycle to ensure gaps are actioned and risk treatments are adequate and prioritised. For example, where incidents related to **people** continue to occur, an organisation may prioritise staff training or review of the process over technology investment.

Threat actor(s)



This is a new field introduced during this reporting period.

The majority(**77%**) of incident notifications related to internal staff and **13%** related to authorised third parties such as contracted service providers. A smaller percentage (**7%**) account for external threat actors e.g., scammers, hackers, who are outside the control of the organisation.

There were **4%** of notifications where the threat actor could not be ascertained.

**Take-out:**
The key causal factors of security incidents are people; internal; and accidental.

Since the majority (**90%**) of incidents are caused by threat actors within the organisation’s closer control e.g., internal staff or authorised third parties, organisations have an opportunity to improve their controls to minimise these exposures either through stronger personnel security practices, better training and awareness, updated policies and procedures, or revised third party arrangements.

Threat type(s)



This is a new field introduced during this reporting period.

Most(**84%**) incident notifications related to accidental actions with **12%** accounting for intentional / malicious actions by threat actors.

There was one notification related to a weather event (natural).

The threat type of **3%** of notifications could not be ascertained.

**Take-out:**
The key causal factors of security incidents are people; internal; and accidental.

Where incident notifications related to malicious actions as opposed to intentional actions, these were mostly carried out by external threat actors rather than internal staff.

Where internal staff were involved and the intentional / malicious field was selected, these involved intentional actions rather than malicious reasons e.g., staff knowingly going against policy to access systems to gather information for personal gain to check a customer record without legitimate business reason.

The OAIC’s [Notifiable Data Breaches Report: January – June 2021](https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-january-june-2021) identified **65%** of breach sources were malicious and **30%** human error. This contrasts with notifications OVIC received where **12%** are malicious and **84%** are errors. This discrepancy is due to various factors including differing scopes, jurisdictions, thresholds, information types, and data points e.g., confirmed data breach versus security incident.

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…[[1]](#footnote-1) |
| --- | --- | --- |
| Misuse of customer information for personal gain(Compromise of confidentiality) | Employees looking up customers records without legitimate business reason | Impact to individuals whose personal information was affected Impact on public services (reputation of, and confidence in, the organisation) |
| Accidental access to client information (Compromise of confidentiality) | Third parties not following the labelling requirements of the organisation | Impact to individuals whose personal information was affected  |
| Customers not receiving their letters in a timely manner(Compromise of integrity and availability) | Employees not paying attention and inputting incorrect data into customer database | Impact to individuals whose personal information was affected |
| Unauthorised access to systems and data(Compromise of confidentiality and availability) | Malicious threat actors stealing government devices and poor password practices by employees (password stuck on stolen device) | Impact on service deliveryImpact 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 if you would like to discuss this report any further.

1. 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-1)