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 January 2021** to **30 June 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.

Victoria Police incident statistics are reported on an annual basis consistent with existing reporting commitments. These have been included towards the end of this report with comparisons made from our [Incident Insights Report for 29 October 2019 – 30 June 2020](https://ovic.vic.gov.au/data-protection/security-insights/incident-insights-report29-october-2019-30-june-2020/).

Information security incident notification insights from January 2021 – June 2021

Notifications by month

Chart

Description automatically generated

OVIC received 218 notifications between **1 January 2021** to **30 June 2021** (inclusive). This is a steady increase in the number of notifications compared to the last reporting period (155 notifications). This represents a 40% increase.

We received the highest number of notifications in January (53) and April (51) 2021.

**Take-out:**   
*As predicted, notifications have steadily increased as awareness of the scheme increases across the Victorian public sector (****VPS****). We received 78 notifications in the first reporting period and 155 in the last reporting period, compared to 218 notifications this reporting period.*

*The increase in notifications in January and April may reflect organisations catching up on paperwork or administrative tasks after the Christmas and Easter festivities and holiday periods 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

Chart, sunburst chart

Description automatically generated

Of the 218 notifications received by OVIC, the majority come from the justice sector, specifically from the Department of Justice and Community Safety (**DJCS**).

DJCS participated in a panel discussion at the March 2021 Victorian Information Security Network (**VISN**) Incident Insights forum to explain how they have implemented a supporting internal process to meet their notification obligations.

Although the health and human services sector was split on 1 February 2021 into separate sectors, their incident notifications are represented as a single sector in this report. This is due to some incidents occurring prior to 1 February and administrative reporting processes still being developed.

**Take-out:**During this reporting period, OVIC met with some organisations for their Protective Data Security Plan (**PDSP**) insights sessions. During discussions related to Victorian Protective Data Security Standards (**VPDSS**) Element 9.010, it became clear that some organisations:

* did not know the incident notification scheme exists;
* experienced incidents that did not reach the Business Impact Level (**BIL**) 2 threshold; or
* were in the process of setting up their incident management policy and procedures including defining the term ‘incident’.

Following these discussions with OVIC, organisations reported a better understanding of their obligations and the types of incidents that should be notified to OVIC.

Information format

A picture containing graphical user interface

Description automatically generated

Like previous reporting periods, most incident notifications related to compromises of electronic information followed by hard copy information.

Most of the incidents involving hard copy information were related to mail and included lost mail, incorrect addressee, or incorrect document/s. This is like trends observed in incidents involving the electronic version of mail i.e., email.

Of the notifications relating to information in electronic format, approximately 50% of incidents related to emails. These incidents were either related to phishing, incorrect recipients, or incorrect attachments.

**Take-out:** *Following an email incident such as sending to the incorrect recipient, attaching the wrong document, or inserting an incorrect protective marking, organisations are increasingly implementing mitigation strategies such as adding a minor time delay when sending emails. This involves implementing a delay of 2-3 minutes after sending, to minimise incidents given the majority are detected by the sender within moments of clicking send.*

*We encourage organisations to refer to our privacy guidance on* [*Tips to reduce data breaches when sending emails*](https://ovic.vic.gov.au/resource/tips-to-reduce-data-breaches-when-sending-emails/) *on our website.*

Type of information impacted

Chart, sunburst chart

Description automatically generated

Like previous reporting periods, most notifications received by OVIC related to compromises of personal information, followed by health information. Although the percentage of incidents related to personal information decreased from 81% to 70%. This perceived drop gave an overall increase in all other information types affected by an incident, for example an increase in notifications regarding compromises of ‘legal’, ‘policy’ and ‘operational’ related information.

**Take-out:**   
*We published guidance on the types of information impacted field in our* [*January 2021 newsletter*](https://mailchi.mp/f81a1d6d1dca/ovic-newsletter-january21?e=%5bUNIQID%5d) *to spotlight the types of information OVIC accepts notifications for under the scheme. It is encouraging to see incidents related to other information types being identified and notified in this period.*

*Organisations can select multiple options when filling in this field. 3% of notifications mentioned compromised staff account(s) so in these cases, almost all options may be selected depending on what information the staff member had access to, or the content of emails contained in their compromised mailbox.*

Information Business Impact Level (BIL)

Shape

Description automatically generated

The number of notifications affecting information assessed as BIL 2, or ‘Limited’, increased from 66% in the last reporting period to 87% this period. Like the last reporting period, there was an even spread of incident notifications affecting information assessed as minor and major business impact level.

Some incident notifications (12%) were received through OVIC’s privacy data breach reporting form which does not have a field to indicate the BIL. In these instances, subjective assessments were made by OVIC practitioners using the information provided in the notifications to nominate a corresponding BIL.

**Take-out:**   
*As maturity in assessing the security value (BIL) of public sector information improves, these fields will be more widely understood and more accurately reported on.*

*OVIC recently conducted a review into how Standard 2 of the VPDSS is implemented in four VPS organisations. The review looked at policies and procedures on how these organisations assess the security value of public sector information. OVIC will publish a report on the review later in 2021.*

Potential business impact category affected

Chart, sunburst chart

Description automatically generated

Given most notifications related to personal information, the most selected BIL category was ‘personal*’,* as the compromise was assessed to have the potential to cause harm to an individual. This is consistent with the previous reporting periods.

**Take-out:**   
*In OVIC’s* [*March newsletter*](https://mailchi.mp/056a87a43886/ovic-newsletter-feb-19503697#incidentreport) *we published guidance on how to fill in this field.*

*After a year of operation to see where improvements can be made to the incident notification scheme, we have consolidated the privacy breach and security incident forms into a single form which removes this field.*

*Given this field was related to the ‘potential’ impact of the affected information and not directly related to the ‘actual’ impacts as a result of the incident, it was deemed unnecessary to collect this data.*

Security attributes impacted

Chart, sunburst chart

Description automatically generated

While the actual number of notifications received relating to compromises of the confidentiality of public sector information doubled, the percentage compared to other security attributes remained the same as the last reporting period at 82%.

**Take-out:**   
*More than 85% of incidents affecting the confidentiality of public sector information were related to email/mail disclosures. The second highest observed confidentiality related incidents were due to incorrect access permissions applied to systems including shared drives, MS Teams, Google drive, HR systems and other business systems.*

*There was an increase in notifications related to third parties e.g. Allens, Law In Order, after publishing guidance in our* [*January 2021 newsletter*](https://mailchi.mp/f81a1d6d1dca/ovic-newsletter-january21?e=%5bUNIQID%5d)*. The guidance* *highlighted that when public sector information is handled by a third party that has suffered an incident, OVIC should still be notified under the scheme.*

Security areas affected

Shape, rectangle

Description automatically generated

There was an increase in incidents related to a failure in the personnel security area from 6% to 13%. e.g., user error. Similarly, there was an increase in incidents related to a failure in the physical security area from 1% to 5% e.g., inadequate physical security controls in a foyer.

Some (12%) notifications were received through the privacy data breach reporting form which does not have a field to select the ‘security area’. In these instances, OVIC practitioners used the information provided in the notifications to nominate a corresponding security area. This explains the increase in the selection of ‘personnel’ and ‘physical’, given our understanding of the intent of this field.

**Take-out:**   
*After a year of operation to see where improvements can be made to the incident notification scheme, we consolidated the privacy breach and security incident forms into a single form which removes this field.*

*There was confusion around the intent of this field as ‘information’ is listed as both a security area as well as a type of incident. The new form replaces this field with new fields that collect details about the control area(s) that caused the incident e.g., people, process, technology, and the threat type e.g., accidental, failure, malicious or natural.*

VICTORIA POLICE STATISTICS

Chart, bar chart

Description automatically generated

OVIC receives incident notifications from the Victoria Police Security Incident Registry (**SIR**) team.

Comparison between the 2018-19, 2019-20 and 2020-21 financial year periods shows the top five closed incident categories are the same.

However, the numbers for 2020-21 show a considerable increase in the number of closed ‘information handling’ incidents. This is because Victoria Police have prioritised this category and implemented proactive monitoring to detect the unauthorised movement of law enforcement data including information saved in an incorrect folder, or an email sent to external personal email account. There was also an increase in closed ‘other event’ incidents due to more regular reporting of communications outages at Victoria Police facilities across the state.

On 1 March 2021, Victoria Police modified the level of detail that is provided to OVIC for incidents recorded as ‘Minor’ or ‘Insignificant’. This change was initiated by Victoria Police to enable the SIR to focus efforts on isolation, containment, and remediation for all ‘Moderate’ and above security incidents.

While the SIR continues to notify OVIC of ‘Minor’ and ‘Insignificant’ incidents, the level of detail for these incidents is not as descriptive as more significant incidents. The statistics of incidents gathered from Victoria Police by OVIC to allow for regular reporting such as this insights report are not affected by the change in process.

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) | |
| --- | --- | --- | --- | --- | --- |
| Unauthorised disclosure of employee information  (Compromise of confidentiality) | | Incorrect permissions set on shared drive / MS Teams / line of business system / Google drive | | Impact to individuals whose personal information was affected | |
| Inappropriate handling of investigations information  (Compromise of confidentiality) | | Employee using unauthorised third-party software not approved by the organisation | | Impact on public services (reputation of, and confidence in, the organisation) | |
| Inappropriate handling of identity information  (Compromise of confidentiality and integrity) | | Employees failing to follow the identity checking process and being helpful to callers probing for information over the phone to change other customer records | | Impact to individuals whose personal information was affected | |
| Loss of client files  (Compromise of availability) | | Third party suffering a ransomware attack | | Impact to service delivery | |
| Customers not receiving their documents (letters/bills) in a timely manner  (Compromise of availability) | | Physical mail missing and not reaching intended mailing address | | Impact to individuals | |

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](mailto: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)