Incident Insights Report

1 January 2022 – 30 June 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 January 2022** to **30 June 2022**.

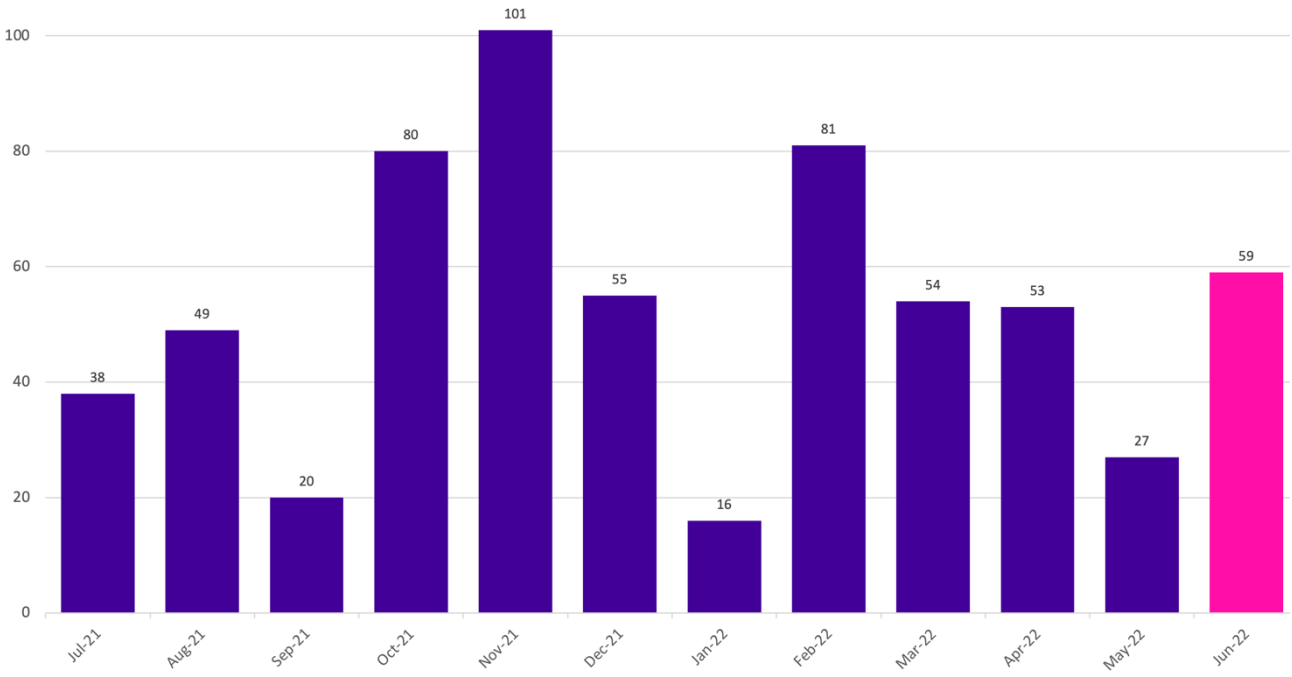
The analysis in this report is based on comparing the statistics published in previous Incident Insights Reports with the notifications received by our office under the scheme.

Victoria Police incident statistics are reported on annually, consistent with existing reporting commitments. These have been included towards the end of this report with comparisons made from our Incident Insights Report for 1 January – 30 June 2021.

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 with an asterisk* in this report.

Information security incident notification insights from January – June 2022

Notifications by month



OVIC received **290** notifications between **1 January** to **30 June 2022** (inclusive). This is a 33% increase compared to the same time last year (**218 notifications**).

We received the highest number of notifications (**81**) in February.

Take-out:
We received fewer notifications this year compared to the previous reporting period 1 July to 31 December 2021 (**343**). However, there was an increase in notifications when compared to the same time last year (1 January to 30 June 2021).

Between 2021 and 2022, monthly notifications increased except for in January 2022. February notifications were particularly high as the Department of Justice and Community Safety (**DJCS**) and Transport Accident Commission (**TAC**) each submitted two months' worth of notifications. This also accounts for the lower figure for January 2022 (see Table 1).

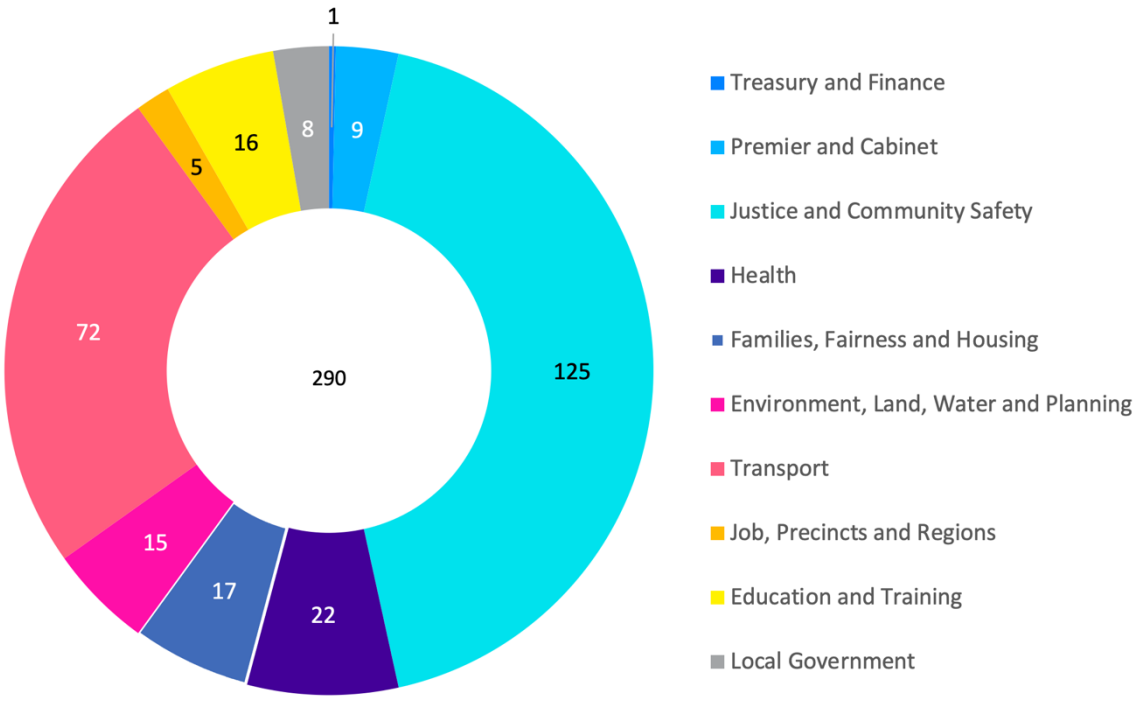
Month	2021 notification #	2022 notification #
January	53	16
February	25	81
March	39	54

April	51	53
May	10	27
June	40	59

Table 1. Comparison between 2021 and 2022 monthly notification figures

Caution should be observed drawing conclusions from month-to-month comparisons, as they do not necessarily reflect when an incident occurred, but rather reflect when a notification was made to OVIC.

Notifications by portfolio

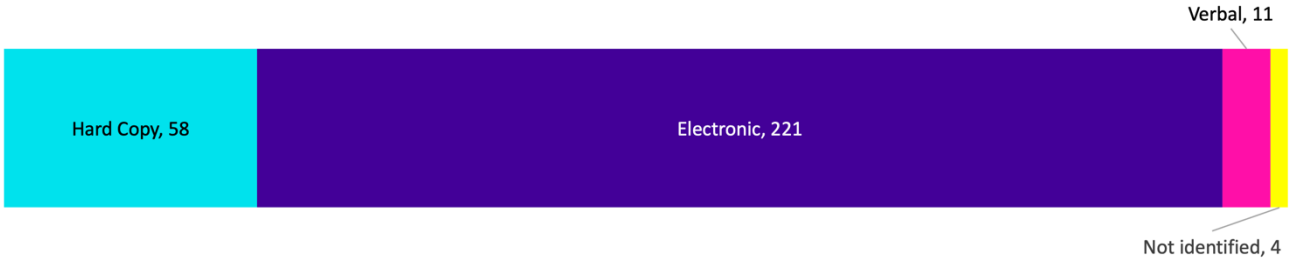


Of the **290** notifications received by OVIC, most come from the justice sector, specifically from the Department of Justice and Community Safety (**DJCS**), and the transport sector, specifically from the Transport Accident Commission (**TAC**). DJCS and TAC have both set up regular monthly incident reporting procedures which includes notification to OVIC.

In April, the Privacy and Data Protection Deputy Commissioner wrote to the department secretaries reminding them of their obligations to notify OVIC of information security incidents including requesting them to share a copy of the letter with their portfolio agencies.

Take-out:
There was a consistent number of notifications across all portfolios compared to the previous reporting period. However, there were increases in the Health (**27%**), Environment, Land, Water, and Planning (**13%**), and Premier and Cabinet (**66%**) sectors.

Information format*



Notifications regarding information format are like previous reporting periods. Most incident notifications (**221**) indicate compromises of **electronic** information followed by **hard copy** information (**58**).

Half of the incidents affecting electronic information related to emails. These incidents predominantly involved sending emails to the incorrect recipient.

Most incidents involving hard copy information were related to mail (**74%**).

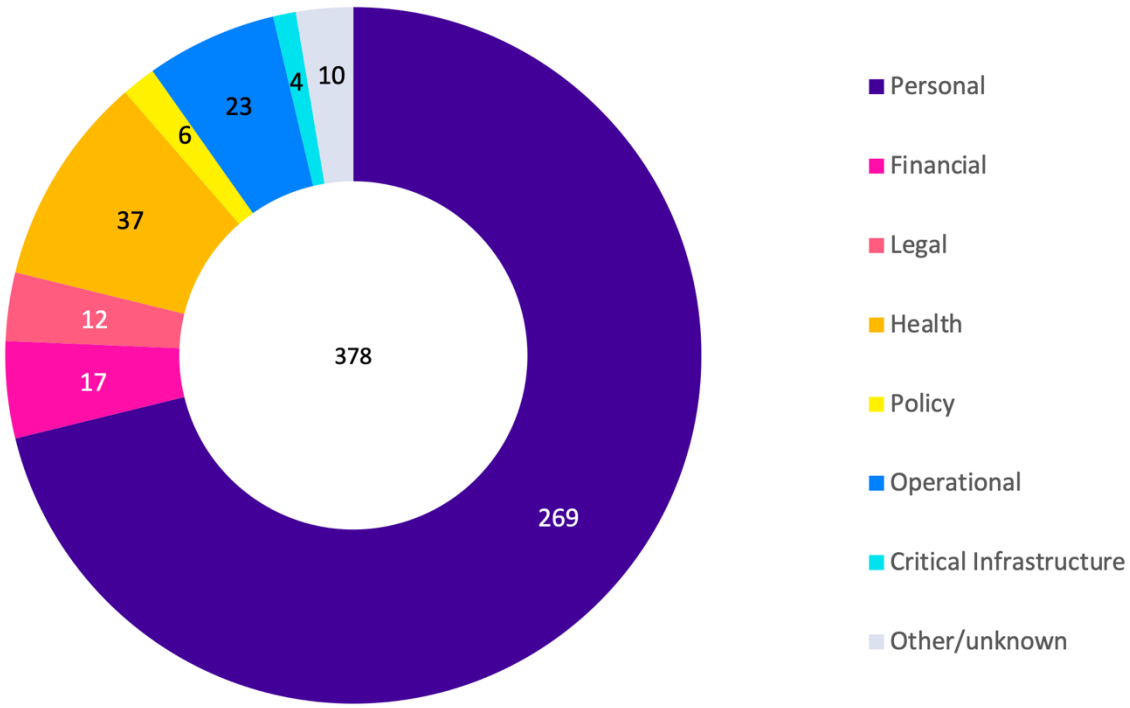
Since multiple options can be selected for this field, there were four (**4**) notifications that selected more than one information format attribute. For example, one of these incidents related to stolen information (hard copy book) where content from the book was then captured as screen shots on a device and shared.

There were four (**4**) notifications where the information format could not be ascertained. For example, one notification related to a caller who requested information, but this was not disclosed because the caller was not authorised to receive it (regardless of format).

Take-out:
In this period, OVIC received 11 notifications involving **verbal** information, which is the same amount as last reporting period. The majority of these related to unauthorised release/disclosure of information.

Half of the incident notifications involve unauthorised release/disclosure of information including verbal disclosures; sending emails or mail to the incorrect recipient; or attaching the incorrect information. This category is consistent with the trends seen with Victoria Police completed incidents where unauthorised release/disclosure of information features in the top five (5) incident categories (refer to the Victoria Police statistics section for further information on Victoria Police incidents).

Type of information impacted*



Notifications regarding the type of information involved in incidents are like previous reporting periods. Most (**93%**) incident notifications indicate compromises of personal information followed by health information.

Multiple options can be selected for this field. Most (**33**) notifications that nominated health information also selected personal information.

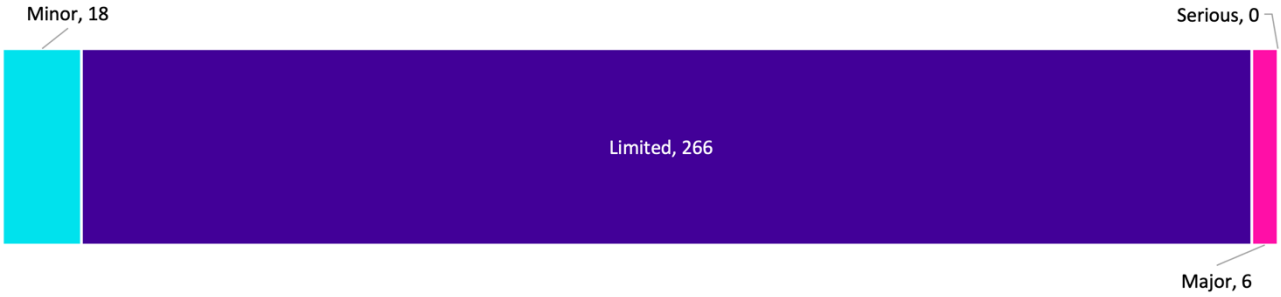
There were two (**2**) incident notifications where the **Other** information type was selected relating to law enforcement information. The next iteration of the notification form will add two new information types to the current list, including law enforcement and crime statistics information. These will be added because OVIC has oversight of these two information types under Part 5 of the *Privacy and Data Protection Act* (**PDP Act**).

There were three (**3**) incident notifications where the type of information involved was **Unknown**. One of these incidents related to a second-hand computer being purchased which still contained information from a Victorian government organisation but the specifics of what public sector information was impacted is unknown. The other two incidents related to compromise of a user's network account where it could not be ascertained exactly what information was impacted.

Take-out:
This field is a good example of a field where multiple options can be selected. Of the 290 incident notifications, there were **63** notifications where more than one option was selected for this field.

There were also four (**4**) notifications where four (**4**) or more options were selected, and some where all seven (**7**) were selected. These were all related to unauthorised access generally, due to compromised network accounts which reflects the range of different information types that accounts have access to.

Information Business Impact Level (**BIL**)[1]



The number of notifications identifying incidents affecting information assessed as having a Limited impact or Business Impact Level (**BIL**) 2 slightly increased from **90%** in the last reporting period to **92%** this period.

Around **36%** 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.

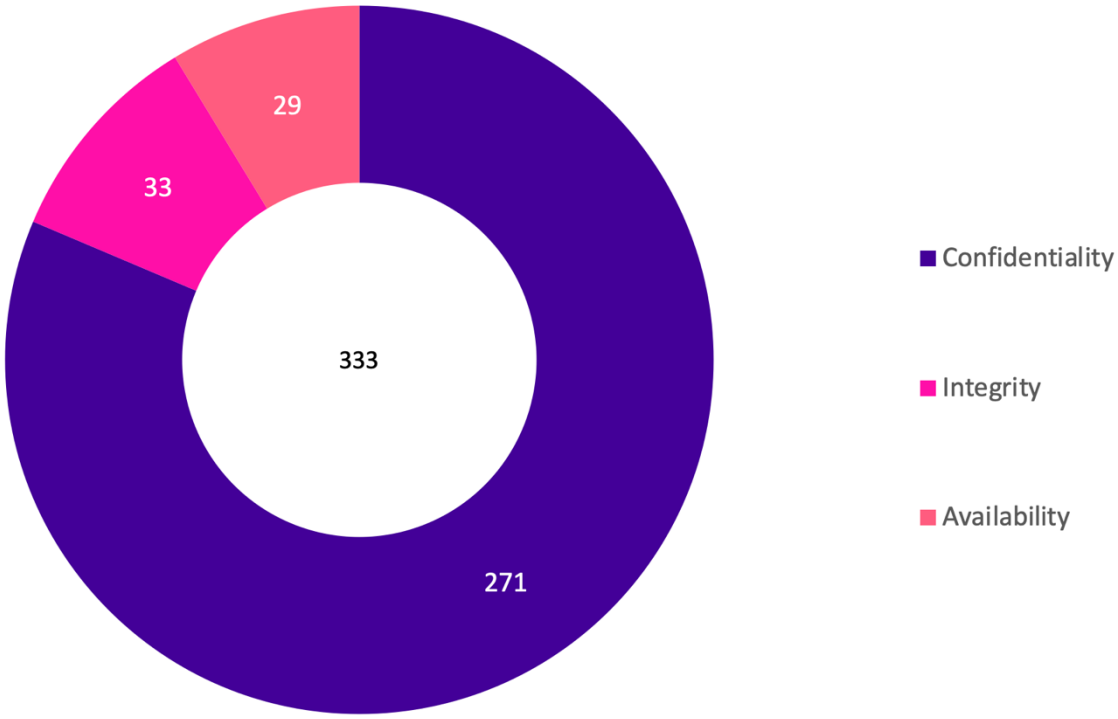
We accept all notifications and encourage organisations to notify if in doubt of the threshold reached.

Take-out:

Analysis of the BIL field indicates a growing understanding of this field, in that it relates to the business impact of the information impacted rather than the severity of the incident or the priority that the organisation placed on the incident. For example, there were only six (**6**) notifications nominating **BIL 3** in this reporting period as opposed to 11 in the previous two periods, and of these six notifications, most appear correct in selecting BIL 3.

[1] Refer to https://ovic.vic.gov.au/data-protection/victorian-protective-data-security-framework-business-impact-level-table-v2-1/

Security attributes impacted*



The percentages of security attributes are like previous reporting periods. Most (**93%**) incident notifications indicate compromises of the confidentiality of information followed by integrity and availability.

Multiple options can be selected for this field.

Take-out:
In this period, **57%** of incidents affecting the confidentiality of public sector information related to potential[2] email or mail disclosures.

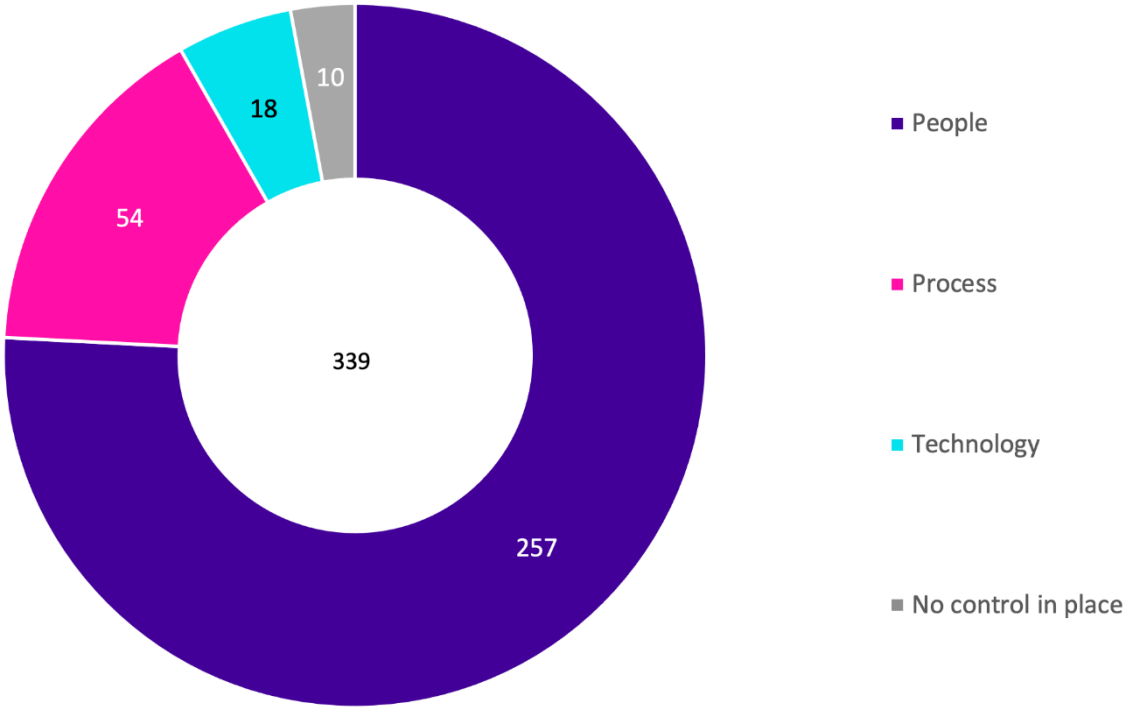
There was an increase in the number of notifications related to Business Email Compromise (**BEC**) compared to previous periods. In November 2021, OVIC held a Victorian Information Security Network (**VISN**) forum that included a presentation on a BEC case study which may have raised awareness of this type of incident.

Of the notifications received, **12%** selected more than one option for this field. For example, compromised accounts can affect the **confidentiality, integrity, and availability** of public sector information because the threat actor can disclose information they have access to (confidentiality), as well as manipulate information e.g. send emails on the account holders behalf (integrity), or delete information (availability).

Another example is information stolen from a facility (availability) may be subsequently disclosed (confidentiality).

[2] Potential disclosure because some email/ mail was reported as being deleted/ disposed of without reading the content.

Control area(s) affected*



Consistent with the previous reporting period, most (**89%**) incident notifications related to **people** (including internal staff, authorised third-party personnel or malicious external actors), followed by **process** issues.

Multiple options can be selected for this field. For example, in most (**83%**) occurrences where **process** was selected, **people** was also selected.

There were 10 notifications (**3%**) where the incident occurred due to a missing control(s).

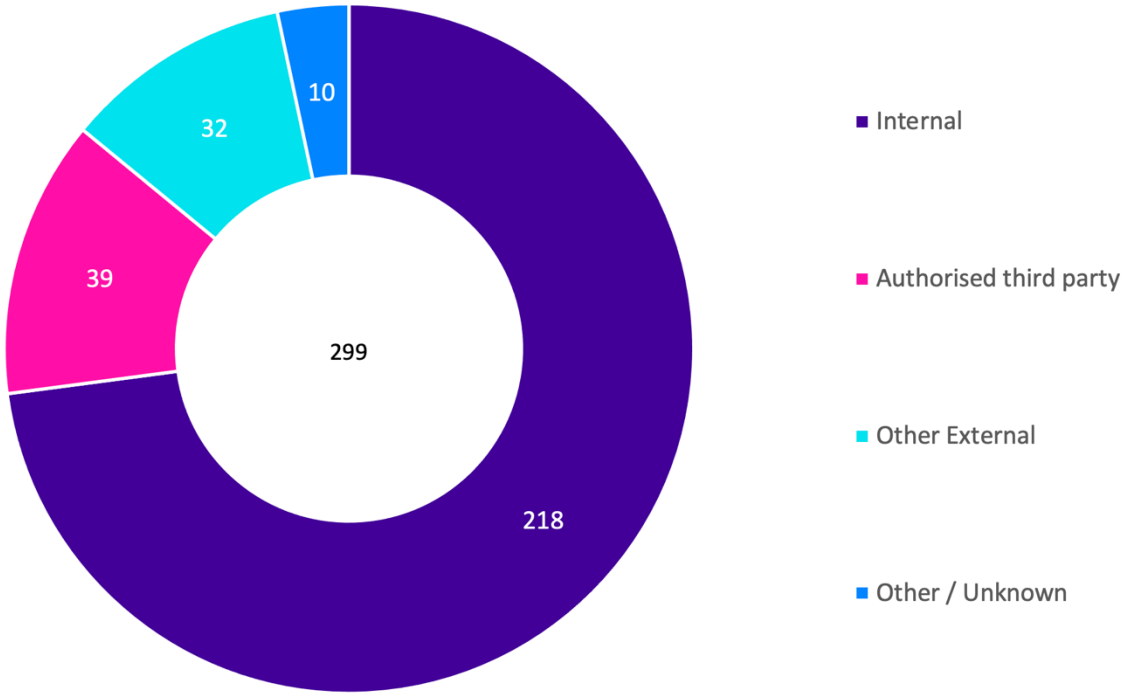
Take-out:
The key causal factors for security incidents are people, internal, and accidental (for example, staff accidentally sending emails to incorrect recipients). Of the 70 notifications that identified sending emails to the incorrect recipient, there were nine (**9**) notifications that identified the email recipient auto-populate function in the user's email program as a factor in the incident, but only two (**2**) of these notifications also selected **technology** as a control area.

Examples of when **technology** was selected as a cause of an incident include:

- Error in matching engine reconciliation;
- Codebase bug in online app;
- Backend misrouting of phone numbers;
- Log4J vulnerability;
- Internet bot creating thousands of online accounts from a Vic Gov website; and

- Cameras and telephony freezing intermittently.

Threat actor(s)*



Consistent with the previous reporting period, the majority (**75%**) of incident notifications related to internal staff and **13%** related to authorised third parties such as contracted service providers.

There was a slight increase (**11%**) of notifications indicating that external threat actors (e.g., scammers and hackers) were involved compared to the last reporting period (**7%**).

Multiple options can be selected for this field.

There were **3%** of notifications where the threat actor could not be ascertained.

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

Although multiple options can be selected for this field, most of the time (**97%**) only one option was selected because usually there is only one threat actor type per incident.

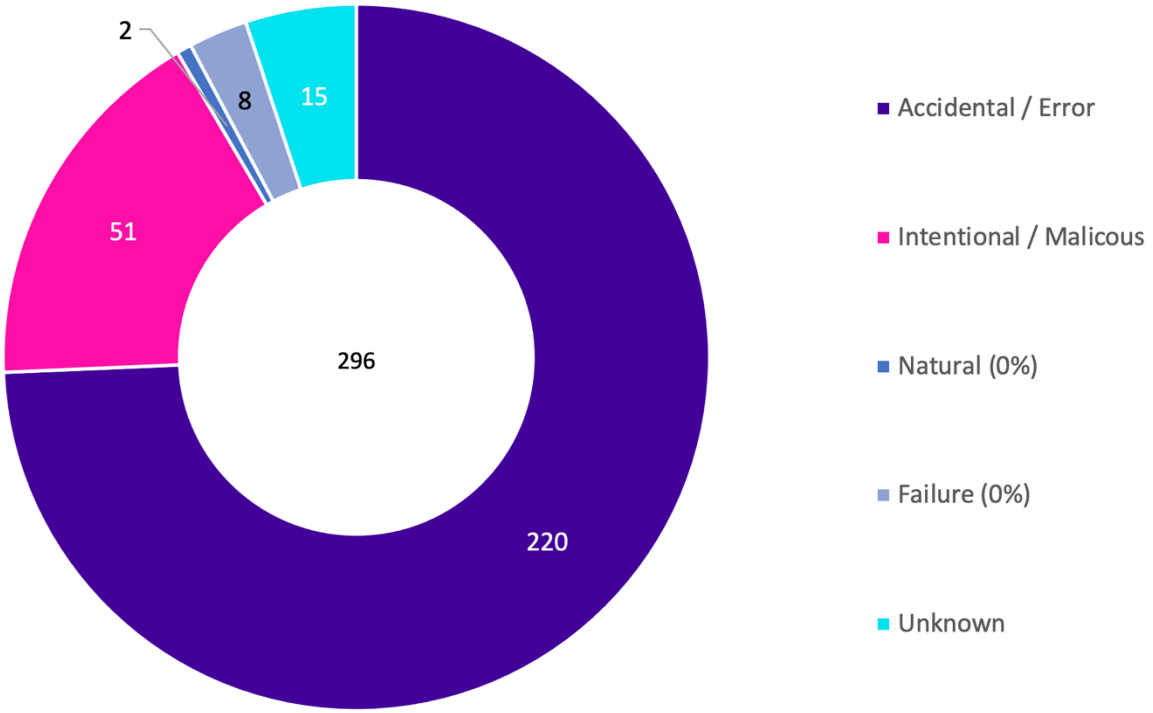
For the few notifications where more than one option was selected, most of these selected both **internal** and **authorised third-party**. For example, the incident related to an internal person opening mail, but it was due to the mail having incorrect labelling placed on the outside by the authorised third-party or it was related to a shared database that both parties use. This could involve mail being sent to an incorrect address but where the address was selected from a database that is maintained by an authorised third-party with incorrect data.

There was also an incident related to the supply chain, whereby both **internal** and **other external** was selected. This incident involved an organisation's web developers adding a third-party application to the website that wasn't tested by the organisation before being commissioned, and when a customer interacted with the website, data was sent to the third-party application vendor and not the organisation or

web developers.

There were 10 notifications where an authorised third-party had suffered an incident, usually a cyber-attack and in these scenarios, **other external** is selected because the incident was caused by a malicious external party and not the authorised third-party. See an example of a cyber incident involving the software company Frontier.

Threat type(s)*



Although most (**76%**) incident notifications related to accidental actions, there was a decrease from the previous reporting period (**85%**) and a subsequent increase in intentional/ malicious actions by threat actors (**18%**) compared to **12%** last reporting period.

Multiple options can be selected for this field.

There were two notifications related to natural causes. While one appears to have been selected in error, the other incident related to an intermittently operating electronic security management system due to malfunctioning machinery and plant for heating, cooling, radiation, electricity.

The threat type of **5%** of notifications could not be ascertained.

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

Given most incidents are accidental, there is an opportunity to implement human-centric controls including training and awareness to prevent incidents.

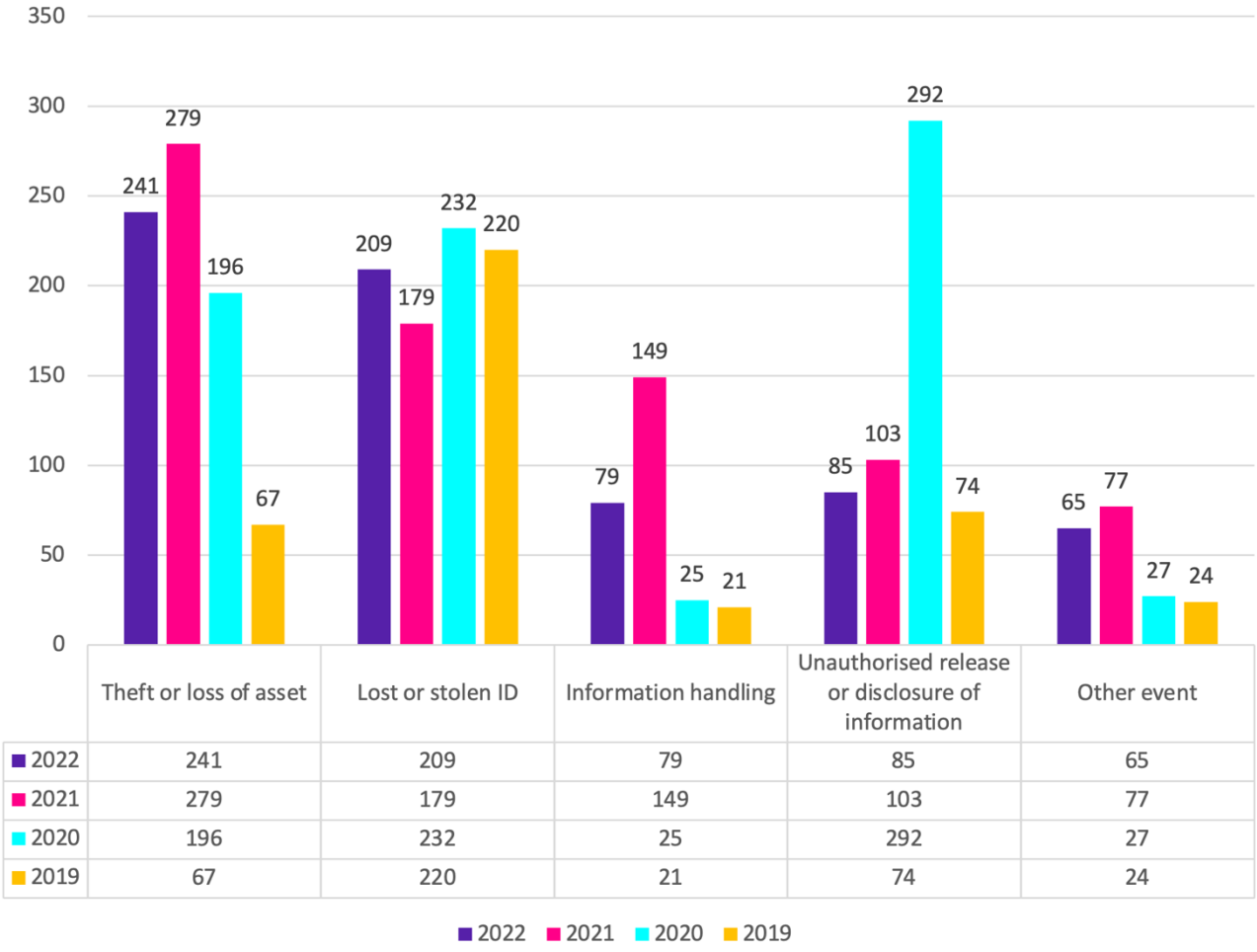
As many incidents relate to sending email/ mail to incorrect recipients, a good portion of incidents could be prevented by encouraging staff to double check the recipient list before they click send.

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

There were only a handful of occurrences where more than one threat type was selected. For example, the incorrect certificate was **accidentally** sent to a customer, but exact details of why this occurred could not

be ascertained (**unknown**) because the employee had since left the organisation. There was another example where technology failed (**failure**) but the cause of this failure could not be determined (**unknown**) including whether someone was involved or if it was natural causes.

Victoria Police statistics



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

Comparison between the last four financial year periods shows the top five '**completed'**[3] incident categories are the same.

Overall, there was a decline in 'completed' incidents across all five incident categories compared to the previous year, except for **Lost or Stolen IDs**, although this statistic remained consistent since 2019.

The numbers for 2021-22 are consistent with the last reporting period except for the number of completed **Information Handling** incidents which has decreased considerably. This spike in 2020-21 can be attributed to:

- the COVID-19 pandemic, resulting in an exponential increase of employees working from home (many at short notice and without appropriate guidelines or infrastructure)

[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.

- identification of this vulnerability which was the subsequent target of IT Security proactive monitoring

- IT Security proactive monitoring, at this time, had a dedicated resource for approximately six months for the sole purpose of detecting **Information Handling** incidents

- this dedicated resource also assisted in the co-ordination of the incidents being promptly addressed by local management, which assisted in the timely completion of the incidents

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]
Financial fraud **(Compromise of integrity)**	Malicious threat actors conducting a business email compromise (**BEC**) and intercepting communications	Impact on organisation's finances
Unauthorised access to sensitive information after purchasing a secondhand computer **(Compromise of confidentiality)**	Authorised third-party not sanitising computers prior to reselling	Impact on public services (reputation of, and confidence in, the organisation) Impact to individuals whose personal information was affected
Unauthorised access to hard copy documents containing personal information **(Compromise of confidentiality and availability)**	Threat actor accessing key-safe box mounted on the exterior of the building and gaining entry to steal assets	Impact to individuals whose personal information was affected Impact 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.

[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.