Incident Insights Report: 29 October 2019 - 30 June 2020

The information security incident notification scheme (**the scheme**) provides tangible resources, trends analysis and risk reporting.

Overview of this report

The Incidents Insight Report provides a summary and analysis of the information security incident notifications received by OVIC between **29 October 2019** to **30 June 2020**.

OVIC is publishing this report to enable Victorian public sector (**VPS**) organisations to use these insights to inform their own information security risk assessments.

This report covers key areas captured in incident notifications, including:

* information affected and format;
* Business Impact Level (**BIL**) and corresponding BIL categories; and
* security attributes and areas.

The report also includes the amount of notifications received and the portfolio in which agencies reside, and incidents submitted via OVIC’s voluntary privacy data breach reporting mechanism and the Department of Premier and Cabinet’s Cyber Incident Response Service (**CIRS**). Victoria Police incident statistics are captured separately and reported at the end of this report.

This report provides statistics on the total number of notifications received under the scheme regardless of whether they:

* meet the BIL 2 or above threshold; or
* relate to in scope agencies under Part 4 of the *Privacy and Data Protection Act 2014* (Vic).

This report will provide VPS organisations with greater insights into the whole of Victorian Government threat landscape.

What is the scheme about?

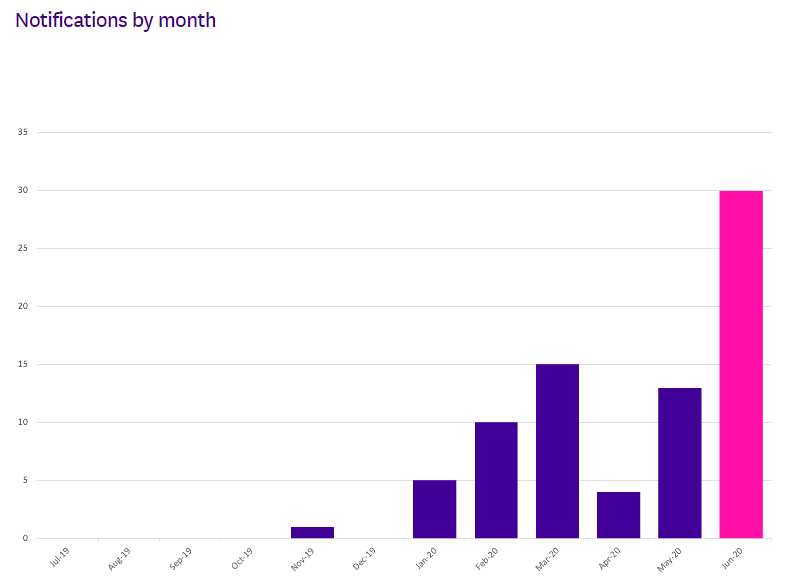
The scheme came into operation with the gazetting of the Victorian Protective Data Security Standards (**VPDSS**) V2.0 on 29 October 2019.

The scheme has been developed to centrally coordinate notification of information security incidents within Victorian government. It requires agencies or bodies to notify OVIC of incidents that compromise the confidentiality, integrity or availability of public sector information with a ‘limited’ business impact or higher[[1]](#footnote-1) on government operations, organisations or individuals. Element E9.010 within the VPDSS states:

*“The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity or availability of public sector information with a business impact level (****BIL****) of 2 (limited) or higher.”*

Incident notification assists OVIC with developing a comprehensive security risk profile of the Victorian government which can be used for trend analysis and understanding of the threat environment.

Notification insights from October 2019 – June 2020



OVIC received 78 notifications from October 2019 – June 2020. We received the highest number of notifications in June 2020.

Takeout: *This steady incline appears to correlate with increased awareness of the scheme, rather than a rise of actual incidents. We believe this trend will continue as awareness of the scheme increases across the VPS. This was evidenced with the increase in notifications received in March 2020, following OVIC’s February 2020 Victorian Information Security Network (****VISN****) event promoting the scheme. The decline in notifications in April 2020 could be a result of the mobilisation of VPS workforce and remote working arrangements due to COVID-19. OVIC has seen a steady incline in notifications since April 2020.*

A colorful circle with text

Description automatically generated

Of the 78 notifications received by OVIC, the majority came from two portfolios: Justice and Health and Human Services.

Takeout: *While these two portfolios had the greatest number of notifications, the statistic doesn’t necessarily mean that these portfolios have the most incidents. Instead, the number of notifications may indicate that these portfolios have greater awareness of the scheme, resources to identify and analyse incidents, and a willingness to report to OVIC.*

A blue rectangle with black text

Description automatically generated

Unsurprisingly, given the large number of digitisation projects currently underway across the State, less information is being generated in paper form. As such, most of the incidents reported related to compromises of electronic (soft copy) information.

Takeout: *Whilst there is a shift across the VPS to ‘digital first’ and an emphasis on soft copy information, organisations should remain mindful of potential compromises to hard copy information or unauthorised verbal disclosures.*

A colorful circle with text

Description automatically generated

Most notifications received by OVIC related to compromises of personal information. At this stage of the scheme, this is unsurprising, as this reflects the historic nature of reporting privacy breaches to OVIC, and familiarity with other privacy related notifiable data breach schemes[[2]](#footnote-2).

Takeout: *OVIC will continue to educate and advocate for the VPS to notify OVIC of incidents that impact all types of information (e.g. financial, legal, policy, projects etc).*

A screenshot of a computer screen

Description automatically generated

The majority of the notifications received by OVIC were for BIL 2 information. This aligns with existing data points that indicates there is only a small amount of higher sensitivity (BIL 3 and above) information handled by VPS organisations. Although the scheme has a notification threshold of incidents that meet BIL 2 or higher, OVIC did receive some notifications related to BIL 1 information. As OVIC accepts notifications in a variety of forms (e.g. referred notifications from OVIC’s privacy team and CIRS), not all notifications identify the BIL of the information affected.

Takeout: *While not an explicit requirement of the scheme, it is pleasing to see that organisations are providing incident notifications to OVIC regardless of impact level – this provides us with greater insights to share with the VPS.*

A pie chart with text

Description automatically generated

As the majority of the notifications related to personal information, the most commonly selected BIL category was ‘*personal’,* as the compromise was assessed to have the potential to cause harm to an individual.

Takeout: *It was surprising to see the category of ‘public services’ not being selected in every notification, as the compromise of public sector information has the potential to cause reputational harm to the organisation. This may reflect limited knowledge of the BIL categories and may be an opportunity for OVIC to develop more guidance in this area.*

A pie chart with numbers and text

Description automatically generated

The majority of the notifications received were related to compromises of the confidentiality of public sector information e.g. inappropriate disclosure, as opposed to compromises of the integrity or availability of information or ICT systems.

Takeout: *Inappropriate disclosure (such as accidentally sending an email to the wrong recipient) is also a key finding in the Verizon Data Breach Report[[3]](#footnote-3).*

A blue rectangle with black text

Description automatically generated

Even though the majority of the notifications nominated ‘information’ as the security area affected, the descriptions of most notifications related to control deficiencies around ‘ICT security’ practices given the format of the information was electronic (soft copy).

Takeout: *OVIC will provide further guidance on helping organisations understand what is meant by the security area ‘information’ e.g. inappropriate protective markings.*

Victoria Police statistics

OVIC receives notifications of incidents from the Victoria Police Security Incident Register team.

Comparison between the 2018-19 (depicted in orange) and 2019-20 (depicted in blue) period shows the top three closed incident categories are the same. However, the numbers for 2019-20 show a considerable increase in closed incidents related to these categories. This may not only be due to the increase in actual incidents but may also indicate improved processes and systems in detecting and handling incidents by Victoria Police.

A graph of different colored squares

Description automatically generated

Risk statements

Based on the incident notifications received by OVIC, we have 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) |
| --- | --- | --- |
| Unauthorised disclosure of personal information  *(Compromise of confidentiality)* | Employees accidentally sending emails to incorrect recipients | Impact to individuals whose personal information was affected |
| Unauthorised collection and use of client information  *(Compromise of confidentiality)* | Former employee extracting data from a system for their own personal gain | Financial impact to the organisation |
| Unauthorised handling of customer records  *(Compromise of confidentiality)* | Third party employees with inappropriate email settings | Impact to legal and regulatory compliance |
| Unauthorised access to health information  *(Compromise of the availability)* | Malicious external threat actor intercepting mobile communications | Impact to service delivery |
| Unauthorised modification of a database  *(Compromise of the integrity)* | Cybercriminal exploiting a vulnerability in a cloud hosted system | Impact to individuals whose personal information was affected |
| Unauthorised access to government information  *(Compromise of the confidentiality)* | Inappropriate disposal of hard copy records | Impact to reputation |

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. Refer to the current VPDSF BIL table on the OVIC website <https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/> for further information. [↑](#footnote-ref-1)
2. Other well-known schemes include the Office of the Australian Information Commissioner’s (OAIC) Notifiable data breaches <https://www.oaic.gov.au/privacy/notifiable-data-breaches/> [↑](#footnote-ref-2)
3. Refer to Verizon’s website for a copy of their report <https://enterprise.verizon.com/en-au/resources/reports/dbir/> [↑](#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)