Welcome

OVIC session being recorded

Please note the first part of today's presentation is being RECORDED

OVIC will advise you when recording ceases.

OVIC
Office of the Victorian Information Commissioner

Incident Insights

Victorian Information Security Network (VISN)

November 2022

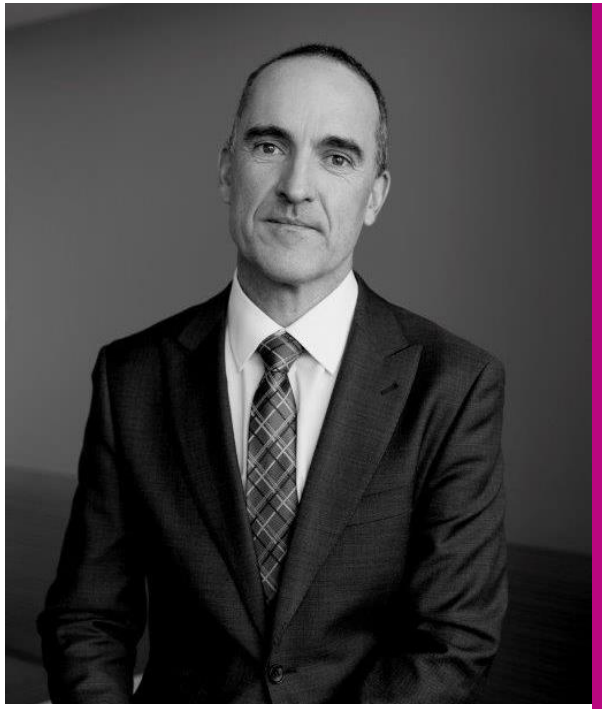
OVIC
Office of the Victorian Information Commissioner

We acknowledge the Wurundjeri people of the Kulin Nation as the Traditional Owners of the land from which we are presenting today.

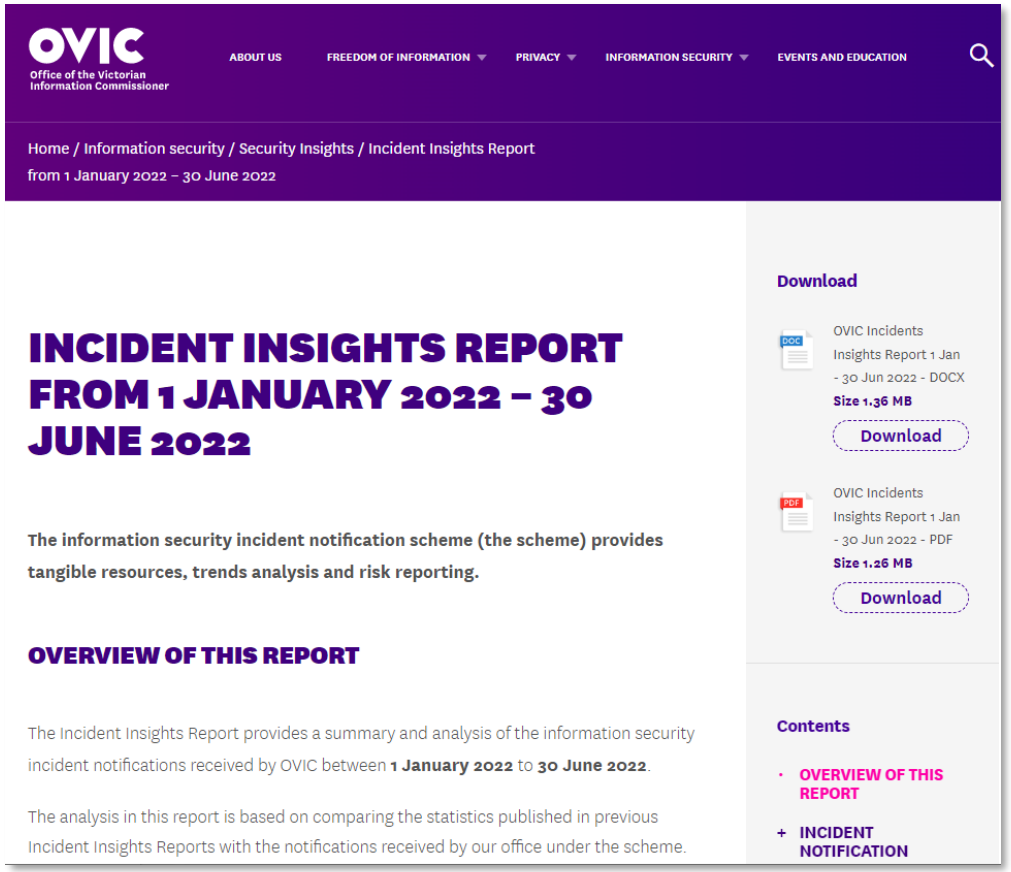
We pay our respects to their Elders, past and present, and Aboriginal Elders of other communities who may be with us today.

OVIC
Office of the Victorian Information Commissioner

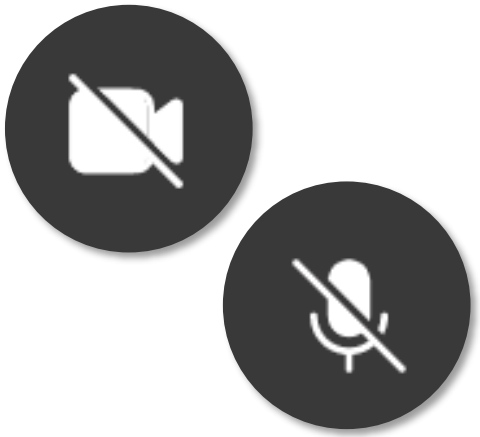
Commissioner's Welcome



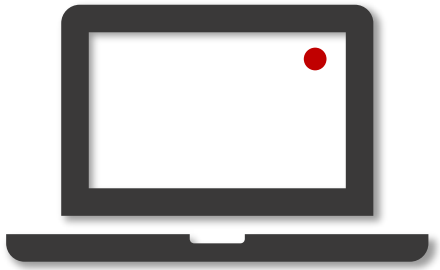
Sven Bluemmel
Information Commissioner



Housekeeping



Cameras and mics are muted.
If your Teams is running slow, try disconnecting from your VPN.



The first half the session will **be recorded.** Following the Insights from OVIC, the recording will stop.

slido

Join the conversation using **#NovVISN** at **slido.com** or using the chat feature in **MS Teams**.

What we'll explore today

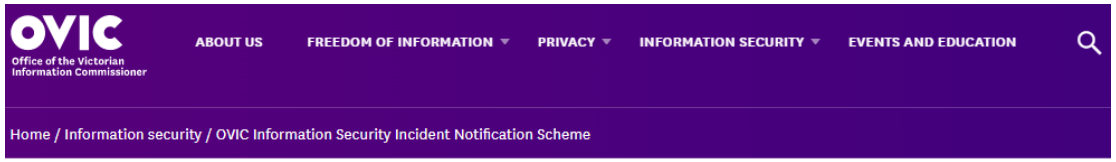
- What is the Incident Notification Scheme?
- The latest Incident Insights Report – themes and trends
- TAC incident reporting to OVIC
- Privacy insights – lessons from recent breaches
- Session close

What is the Incident Notification Scheme?

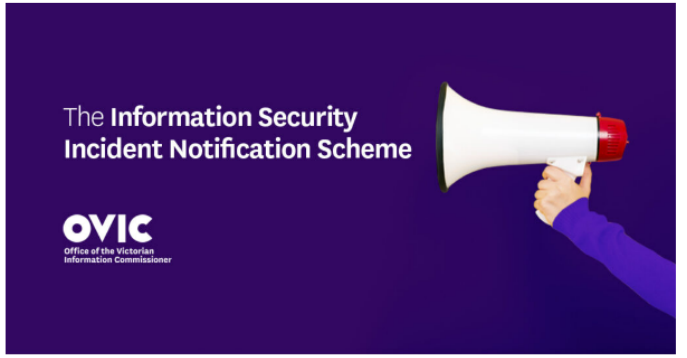
Office of the Victorian Information Commissioner

What is the scheme?

Victorian government agencies or bodies are required to notify OVIC of incidents that compromise the **confidentiality**, **integrity**, or **availability** of public sector information in all forms.



OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME



What sort of incidents need to be notified to OVIC?

Incidents that reach the threshold of a business impact level (**BIL**) of 2 (limited) or higher.

The Latest Incident Insights Report Themes and Trends

Anna Harris
Principal Advisor, Information Security - OVIC

OVIC
Office of the Victorian Information Commissioner

Themes and Trends

Volume

Information format

Information type

Security attributes

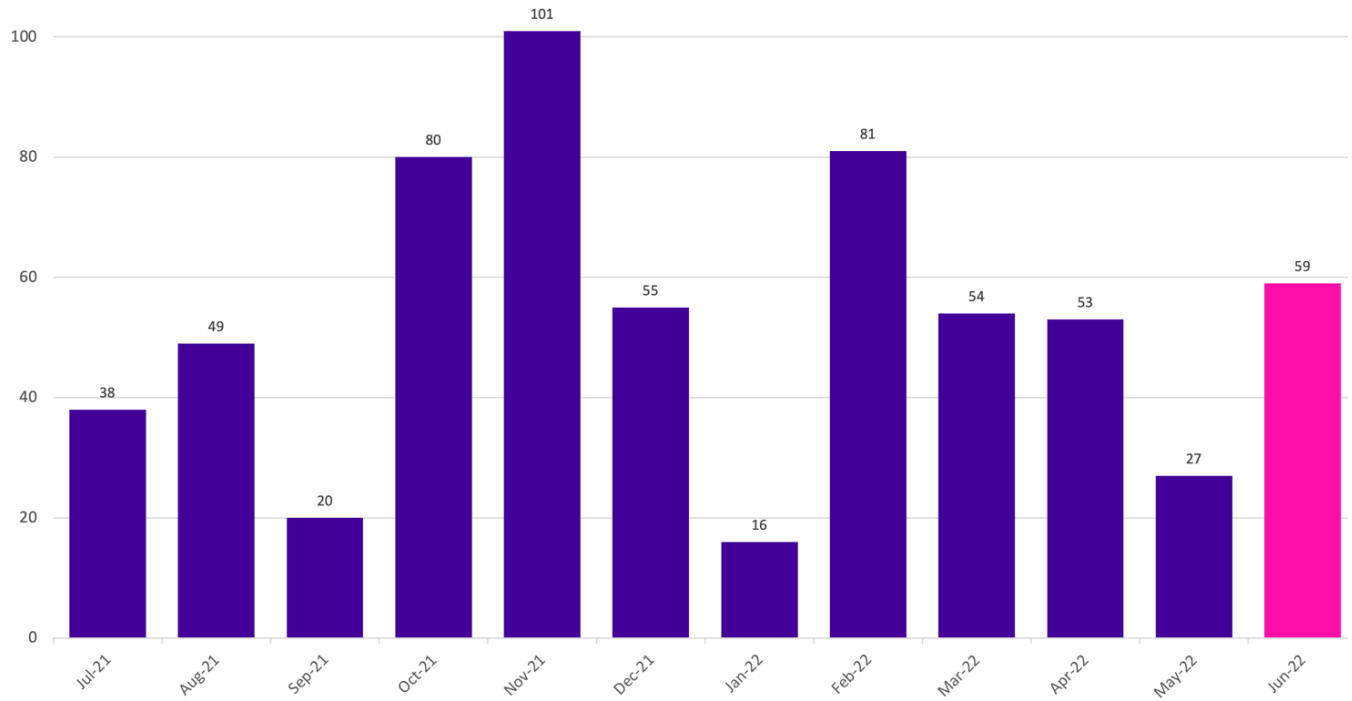
Control areas

Threat types

Threat actors

Volume - 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.

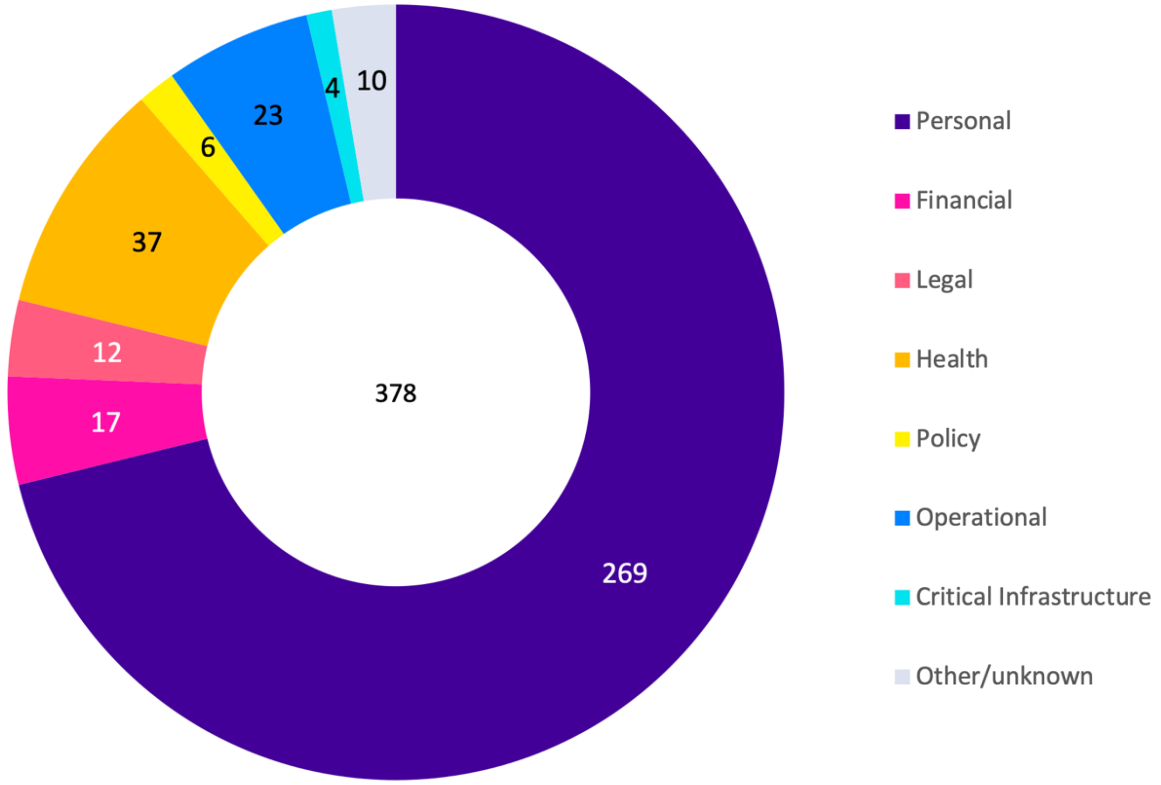


Information format

- **221** notifications indicate compromises of **electronic information**.
- Half of the incidents affecting electronic information related to emails - predominantly **sending emails to the incorrect recipient**.
- **74%** incidents involving hard copy information were related to **mail**.

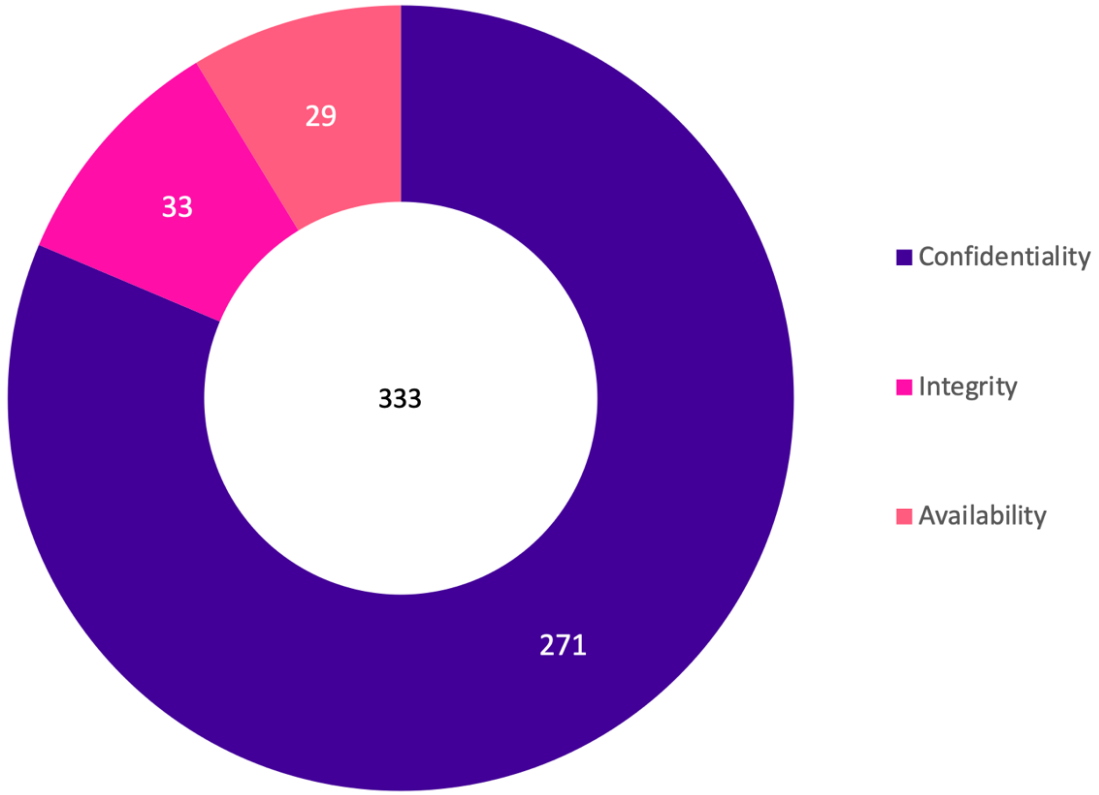
Information type

- **93%** incident notifications indicate compromises of **personal** information.
- Most **(33 out of 37)** notifications that nominated health information also selected personal information.
- **3** incident notifications where the type of information involved was **Unknown**.



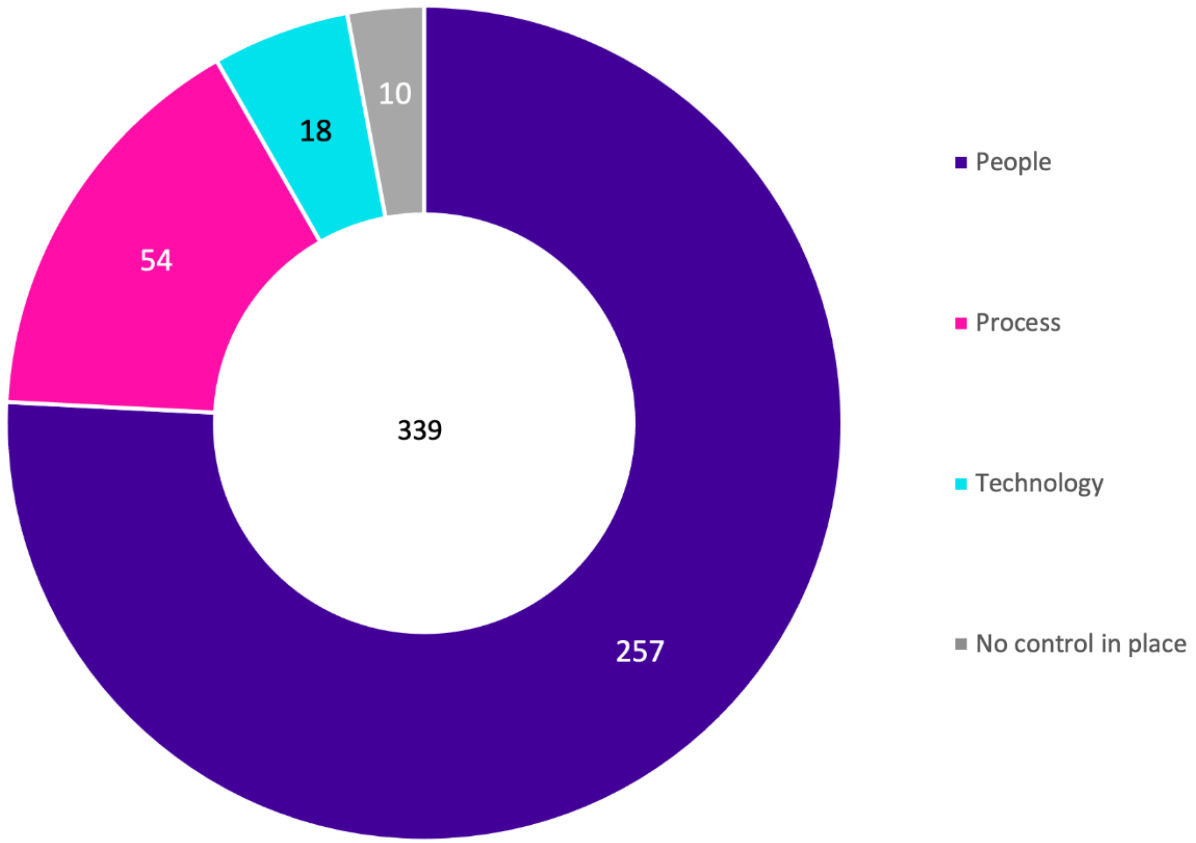
Security attributes

- **93%** of incident notifications indicate compromises of the **confidentiality** of information.
- **12%** of notifications selected more than one option for this field.



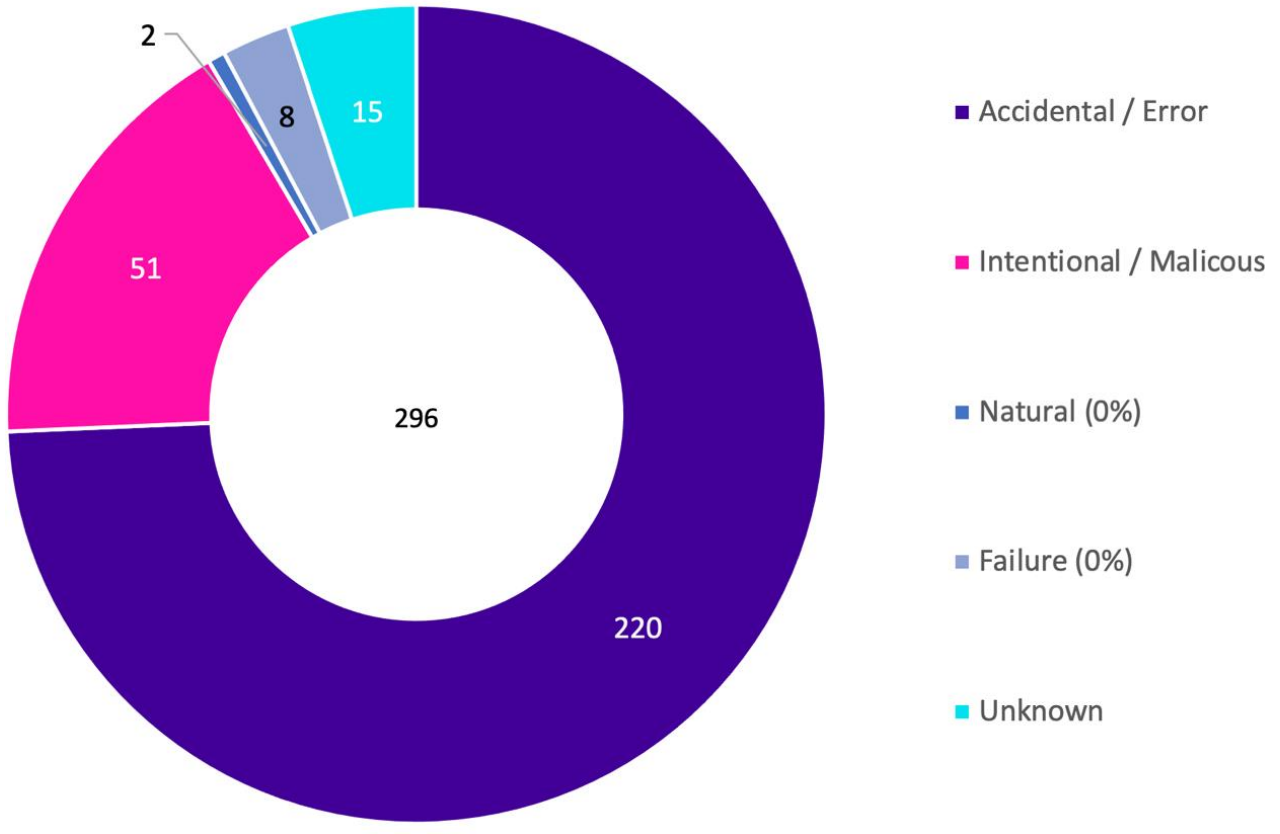
Control areas

- **89%** of notifications related to **people** (including internal staff, authorised third-party personnel or malicious external actors).
- **83%** of notifications where **process** was selected, also selected **people**.
- **10** notifications (**3%**) where the incident occurred due to a **missing control(s).**



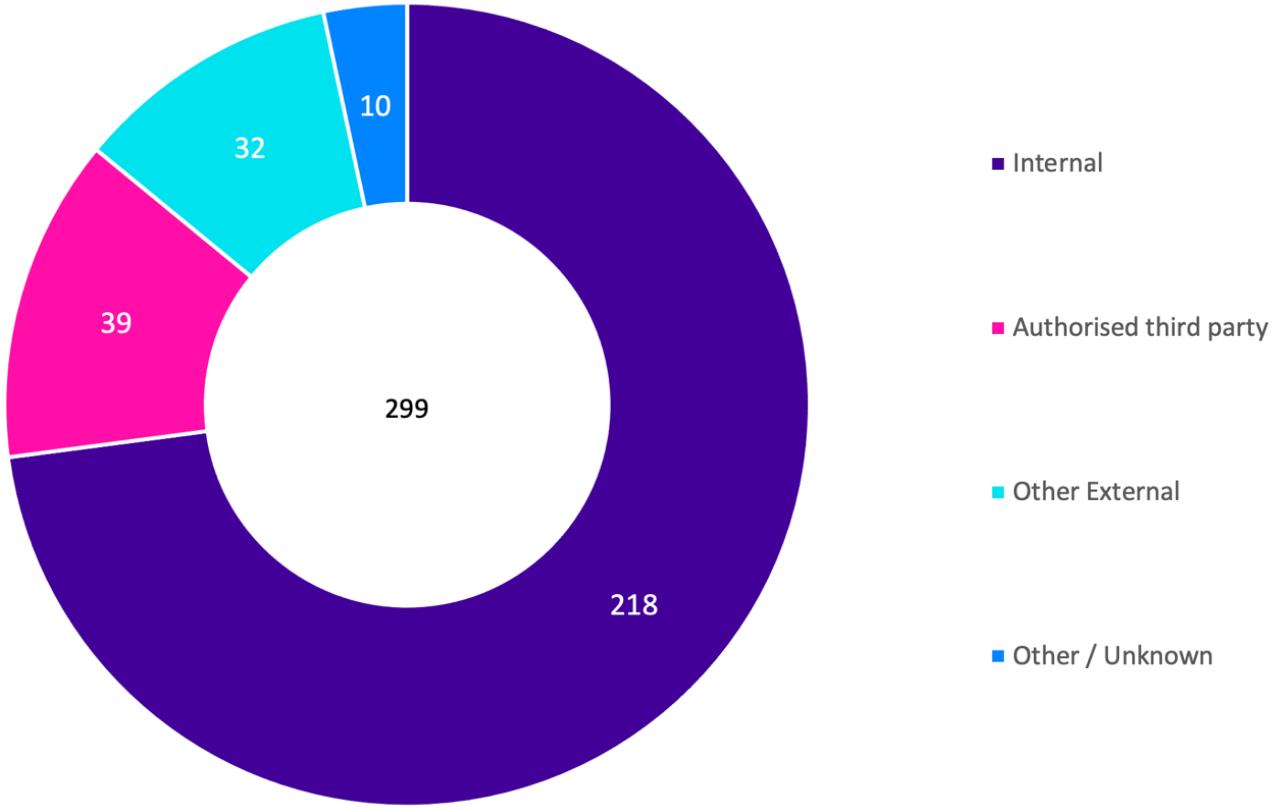
Threat types

- **76%** of notifications related to **accidental actions**
- **18%** of notifications related to **intentional/ malicious actions** by threat actors



Threat actors

- **75%** of notifications related to **internal staff**.
- **13%** of notifications related to **authorised third parties** such as contracted service providers.
- **11%** of notifications indicating that **external threat actors** were involved.



Risk statements

The risk of…	caused by…	resulting in…	
financial fraud	malicious threat actors conducting a business email compromise (BEC) and intercepting communications	impact on organisation's finances	I
unauthorised access to sensitive information after purchasing a secondhand computer	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	C
unauthorised access to hard copy documents containing personal information	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	C A

Questions?

Contact the Information Security Unit
security@ovic.vic.gov.au

OVIC
Office of the Victorian Information Commissioner

Recording to cease

Jacinta Rawkins

Privacy Coordinator – External Affairs
Transport Accident Commission (TAC)

OVIC
Office of the Victorian Information Commissioner

TAC incident reporting to OVIC

22 November 2022

About the TAC

The TAC is a Victorian Government-owned organisation (Statutory Authority).

We promote road safety and manage the claims of people who are injured in transport accidents

We collect, use and disclose personal, health and sensitive information for:

- Managing TAC claims
- Road Safety research
- Defending legal proceedings.

Information and Privacy team – what we do

Privacy – Jacinta, Felicity and Delilah

- Provide privacy training and support to the business
- Handle breaches and complaints
- Manage security incidents – work closely with IT
- Delete documents from electronic claims management system
- Owns the risk for cyber security awareness
- Privacy Impact Assessments and advice
- Provide guidance for the informal release of information (ROI)
- Manage relationships with privacy regulators, e.g. OVIC, OAIC and HCC

How we got here

- Privacy awareness program began in 2015
- Developed into a mature privacy and security culture over time
- Established culture of reporting – no fear of reporting
- Operational staff understand how security and privacy breaches affect client experience and trust

- **Note -** Mature privacy program explains our incident numbers.

Reporting to OVIC

- TAC is required to report Business Impact Level (BIL) 2 incidents and above to OVIC under the information security incident notification scheme
- Started reporting in August 2021
- Prepared the business with 12 months notice that reporting will begin
- Worked with OVIC about how to report – we don't use OVIC's notification form

Reporting to OVIC

- We report:
  - Security incidents
  - Privacy incidents – where information has been lost
  - Deletion of documents from systems
  - Where we have paid the wrong person/organisation

- Every month I send:
  - New month's data
  - Previous 2 months data – helps OVIC track incidents through their lifecycle (3 months in total)

- OVIC send back OVIC reference numbers, which helps with ongoing tracking

Reporting security incidents

- We don’t use the Business Impact Level (BIL) definition of a security incident – we report **all** incidents, including privacy breaches
- Examples from the last 6 months:
  - Medibank, Optus and PNORS – TAC disclosed information to these entities directly or via third party contracts
  - Emails sent to the wrong address / wrong attachment in the email
  - Reports of suspicious emails / phishing emails from clients and staff
  - Folder in shared drive contains client sensitive information and has no permission restrictions
  - Payment made to scammer – Business Email Compromise
  - Stolen work iPhone
  - Bulk emails from the TAC sent from an unrecognizable address – resulted in reports of phishing / scams

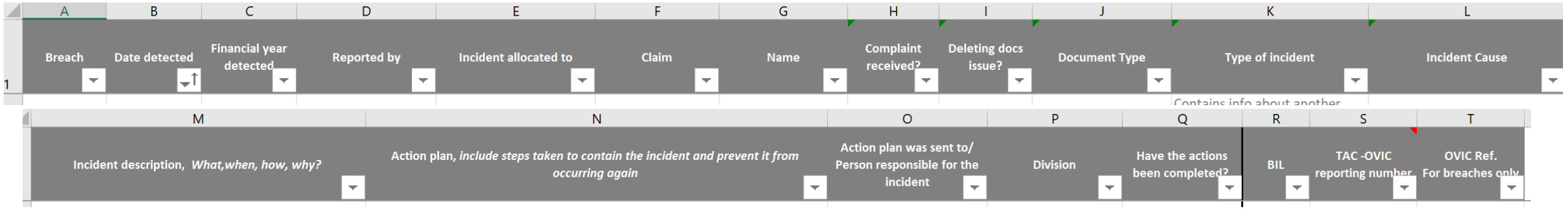
Reporting security incidents

- Excel spreadsheet
- All client identifiable information removed

Financial Year	Date	Name of staff member	Incident description	Incident type	Action taken	Attachments	OVIC reference number
					Email from Adam in ITSS advising of the cyber		

Reporting Privacy incidents

- Excel spreadsheet – all client identifiable information removed
- Designed for:
  - Handling privacy incidents
  - Managing and tracking trends
  - Replicates fields in the OVIC notification form



	A	B	C	D	E	F	G	H	I	J	K	L
1	Breach	Date detected	Financial year detected	Reported by	Incident allocated to	Claim	Name	Complaint received?	Deleting docs issue?	Document Type	Type of incident	Incident Cause

	M	N	O	P	Q	R	S	T
	Incident description, *What,when, how, why?*	Action plan, *include steps taken to contain the incident and prevent it from occurring again*	Action plan was sent to/ Person responsible for the incident	Division	Have the actions been completed?	BIL	TAC -OVIC reporting number	OVIC Ref. For breaches only

Reporting Privacy incidents

- Excel is not designed for this kind of data collection and analysis
- Growing privacy awareness means more data than a spreadsheet can handle
- Exploring use of reporting software to better track and manage incidents
- Reporting to OVIC has assisted with the business case for purchasing incident management software

Notification

We notify affected people whenever their information has been:

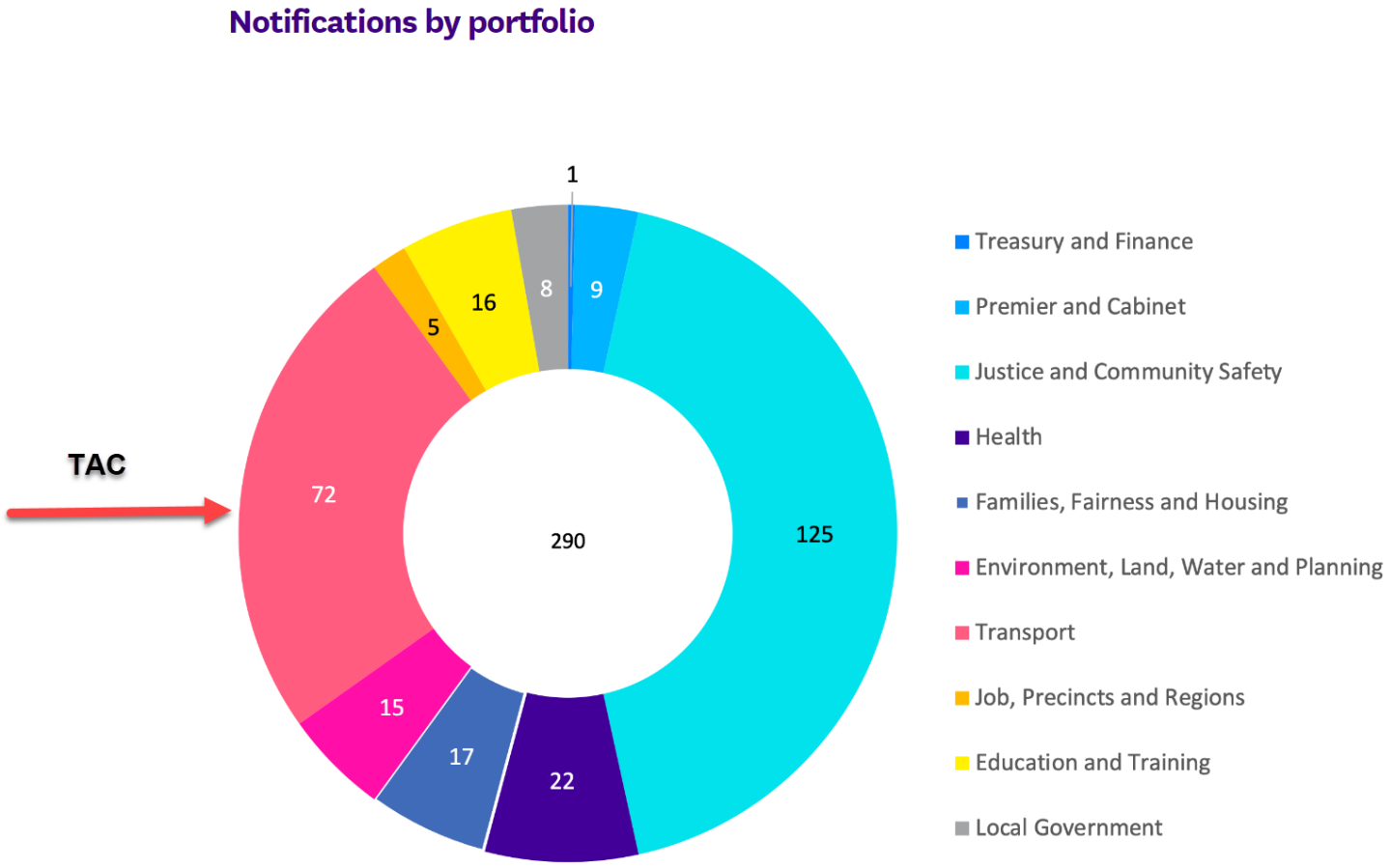
- Lost
- Compromised

- We don’t know what harm could have been caused
- People have a right to know when their privacy has been breached
- Notification allows people to take steps to protect themselves, e.g. changing passwords, notifying their bank, being aware of phishing emails and texts, etc.
- We have refined how we notify – we only notify when we can tell people specifically what information has been lost or compromised.

Benefits of reporting to OVIC

- Drives an increased focus on causes of security incidents and privacy breaches
- Provides support for changes to processes
- Benchmarking against other, bigger agencies puts our issues in perspective
- Gives OVIC oversight of the security threats landscape
- OVIC can provide advice and support

Benefits of reporting to OVIC



https://ovic.vic.gov.au/information-security/security-insights/

Benefits of reporting to OVIC

When OVIC ask for more information about an incident – this can assist to get the problem resolved

Dialog/Whispr example

- MyTAC app – Dialog are the TAC's contracted service provider for the app

- Emails notifying clients that they have a message from the TAC in the TAC app were coming from a strange email address: Matthew.Gale@dialog.com
- Clients were reporting these emails – results in decreased trust in Government agencies
- Reported multiple times to our IT teams – no fix after at least 5 years
- Reported to OVIC – OVIC asked why the incident had not been resolved
- Notified IT of OVIC's interest - Immediate fix

Wrapping up

- OVIC are easy to work with
- Healthy relationship with OVIC means better privacy and security outcomes generally

Questions?

Dermot Dignam

Manager, Privacy Guidance and Dispute Resolution
Office of the Victorian Information Commissioner

OVIC
Office of the Victorian Information Commissioner

Privacy insights

Lessons from recent breaches

Dermot Dignam

Manager, Privacy Guidance and Dispute Resolution
Office of the Victorian Information Commissioner

OVIC
Office of the Victorian Information Commissioner

Incidents & Privacy

- **93%** incident notifications involve compromises of **personal** information.

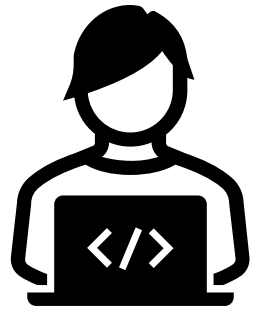
- OVIC triage and privacy follow-up:
  - Clarify or obtain more information;
  - Guidance on notifying individuals; and
  - Discussions on remediation

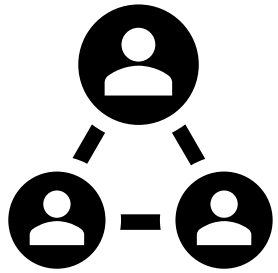
Privacy insights – recent developments

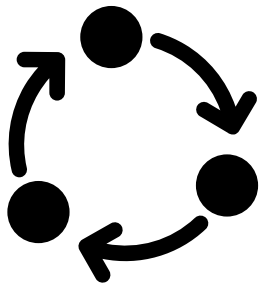
Increased cyber attacks by external threat actors.

Human error.

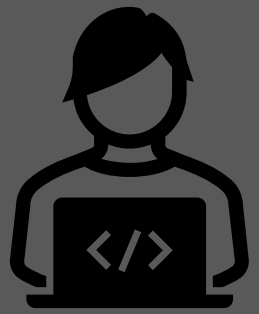
Internal processes, technology and access controls.





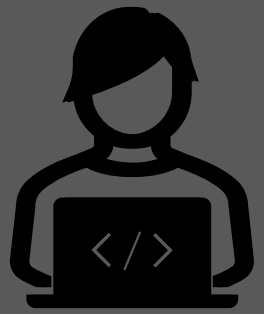


Privacy insights – Cyber attacks



- Minimising risk of them happening
- Importance of being prepared
- Notifying affected individuals

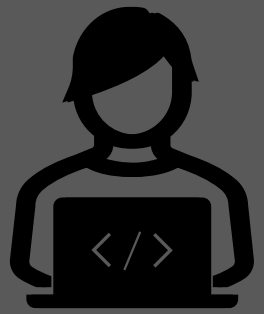
Cyber attacks – notifying individuals



- Do you notify?
  - What are the risks to individuals?
- When?
  - Do you have enough information?
  - Is there an immediate risk?
  - Could premature or over-notifying cause undue distress?
- How?
  - Is there a need for ongoing communications?

Key consideration – reducing risk of harm to individuals

Cyber attacks – notifying individuals



Scenario

It's Wednesday afternoon and you are informed of a cyber incident at your organisation. A staff member has clicked on a link in an email that turned out to be a phishing attack. You believe there may be suspicious activity across your network.

Extent of the compromise:

- Access to certain parts of the network?
- Access to the entire network?
- Who is impacted? What if it's unclear?

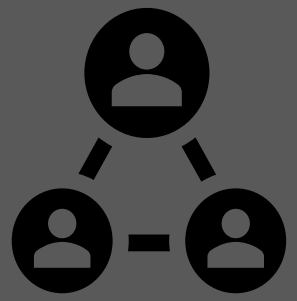
Nature of the information

- Is it sensitive or delicate?
- Does it carry a risk of harm?

Considerations for notifying?

- Notifying in stages?
- Timing – immediate risk? Could premature or over-notifying cause undue distress?

Privacy Insights – Human error



It can’t be eliminated, but can the risk be reduced?

Did any other factor facilitate the human error?

Scenario:

Information disclosed via telephone

John calls up a local council. He explains to a customer service officer, Andrew, that his sister is getting married, but that he is not able to get in contact with his lost family friend. John asks if Andrew could give him a residential address so he can send her an invitation?

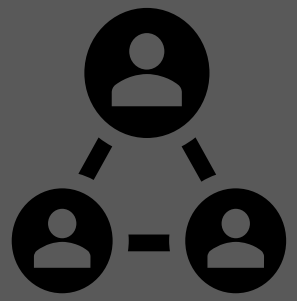
Andrew has been taking calls all afternoon, and there are four callers waiting in the queue. All Council staff have access to Council's database, so Andrew can easily access Janine's details. Andrew knows the basics of privacy, but he thinks "well, what harm could come from this Janine receiving a wedding invitation, I'll just give him the address."

After hanging up the phone, Andrew feels that something doesn't feel right. He speaks to his manager.

"Hmmm, call up Janine" his manager says. "Just give her a heads up that you've given out her address to this John fellow. Hopefully she says it's fine."

Andrew dials Janine's number. Janine answers the phone but sounds panicked. She is at the local police station making a statement. John is her former partner, and had arrived on her doorstep, in breach of a family violence intervention order in place to protect Janine and her children. Janine had relocated for her safety; now John tracked down Janine using the address Andrew provided.

Privacy Insights – Human error

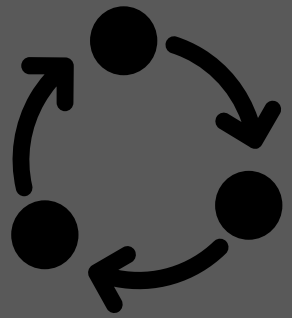


Could the human error have been avoided?

- Access controls?
- Policies and procedures – relevant to the role
- Job-specific training – focusing on role of staff handling large volume of personal information & highlighting specific risks.

Privacy Insights –

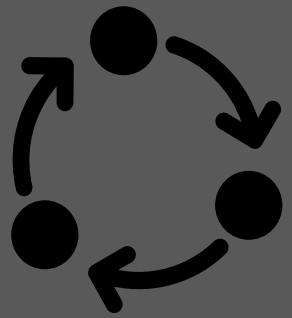
Internal processes, technology and access controls.



Collaborative platforms	Internal processes	Technology
SharePoint	Verification	Automation
OneNote	Online portals	Access controls
Trello	Off-boarding	Codebase bugs

Privacy Insights –

Internal processes, technology and access controls.



What to consider when your internal processes result in a data breach?

- What training do you have, how often it is provided and is it targeted?
- What resources does your organisation rely on, are they effective?
- What system configurations can you change or enhance?
- How often do you conduct an audit?
- Are authorised third parties aware of their obligations?

Deputy Commissioner's Final Thoughts

Rachel Dixon
Deputy Commissioner
Privacy and Data Protection

The key causal factors for security incidents are people, internal, and accidental.

Find out more

Visit the OVIC website to download our guidance material, read our examination reports, and find out more!

ovic.vic.gov.au

Contact the Information Security Unit

security@ovic.vic.gov.au