OVIC

Office of the Victorian Information Commissioner

Victorian Information Security Network

Information Security Incident Notification Scheme Insights

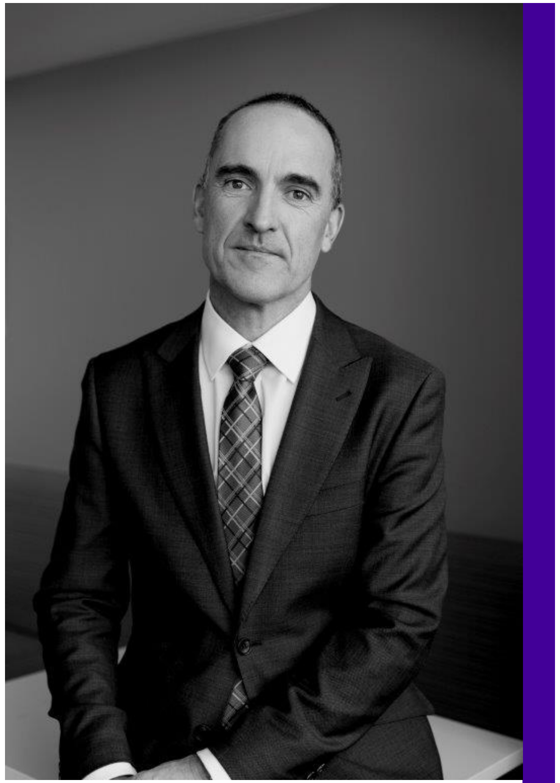
March 2022

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

Many of you will be joining from the traditional lands of other traditional owners.

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

Commissioner’s Welcome



Sven Bluemmel
Information Commissioner

Information Security is a risk management process designed to safeguard information assets and systems in a way that is proportionate to threats and supportive of business outcomes.

Victorian Protective Data Security Framework Glossary 2.1

Housekeeping

Office of the Victorian Information Commissioner

Housekeeping

Cameras and mics are muted.

The session is NOT being recorded, however the slides will be made available following the session.

join the conversation

SCAN ME

@slido.com

#MARCHVISN

Add your questions or comments in the Microsoft Teams Meeting chat

Agenda

01 Information Security Incident Notification Scheme
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC's Investigations and Assurance branch
Insights into the work of OVIC's Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Agenda

Anthony Corso

Assistant Commissioner

Information Security

Office of the Victorian Information Commissioner (OVIC)

01 **Information Security Incident Notification Scheme**
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC's Investigations and Assurance branch
Insights into the work of OVIC's Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Anna Harris

Principal Advisor

Information Security
Office of the Victorian Information Commissioner (OVIC)

Agenda

01 Information Security Incident Notification Scheme
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC's Investigations and Assurance branch
Insights into the work of OVIC's Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Agenda

Matthew Fiford

Manager

Investigations and Assurance
Office of the Victorian Information Commissioner (OVIC)

01 Information Security Incident Notification Scheme
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC’s Investigations and Assurance branch
Insights into the work of OVIC’s Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Agenda

Luke Johnson

Senior Manager

Cyber Intelligence and Response Operations

Digital Victoria

01 Information Security Incident Notification Scheme
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC's Investigations and Assurance branch
Insights into the work of OVIC's Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Agenda

Anthony Corso

Assistant Commissioner

Information Security

Office of the Victorian Information Commissioner (OVIC)

01 Information Security Incident Notification Scheme
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC's Investigations and Assurance branch
Insights into the work of OVIC's Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Agenda

Rachel Dixon

Deputy Commissioner

Privacy and Data Protection

Office of the Victorian Information Commissioner (OVIC)

01 Information Security Incident Notification Scheme
A brief overview of the scheme

02 Incident Insights
Emerging themes from the ISINS

03 OVIC's Investigations and Assurance branch
Insights into the work of OVIC's Investigations and Assurance branch

04 Cyber Intelligence and Response Operations
Further insights into emerging trends with a case study

05 Linking incidents, risks and controls
Why all these aspects are so closely linked

06 Wrap Up
A summary of the key discussion points

Information Security Incident Notification Scheme (ISINS)

A brief overview of the scheme

Anthony Corso

Office of the Victorian
Information Commissioner

ISINS – A brief overview of the scheme

Obligations

Key aspects

Contracted Service Providers

Benefits

Resources

ISINS – A brief overview of the scheme

Obligations

Key aspects

Contracted Service Providers

Benefits

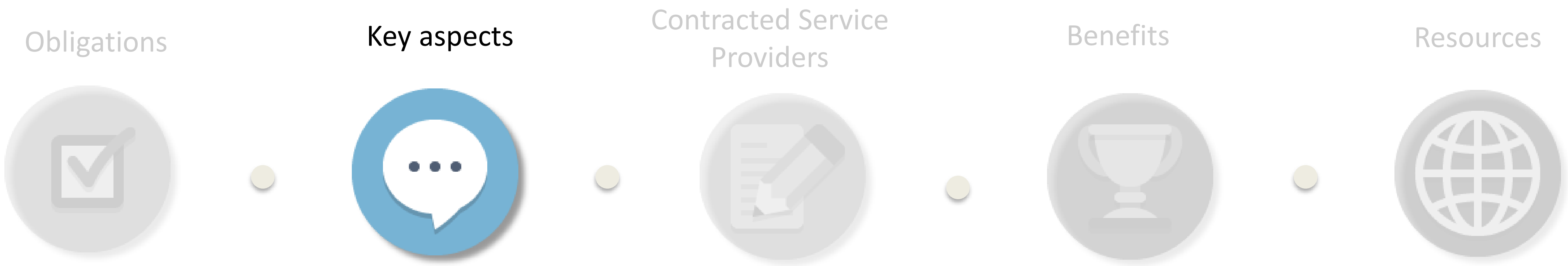
Resources

- VPDSS Implementation guidance 2.1 /**Element 9.010** for information security incident notifications

- Organisation's must notify OVIC of information security incidents that have an impact on the confidentiality, integrity or availability of public sector information with a **business impact level (BIL) of 2 (limited) or higher**

- Notification is **within 30 Days**

ISINS – A brief overview of the scheme



Obligations

Key aspects

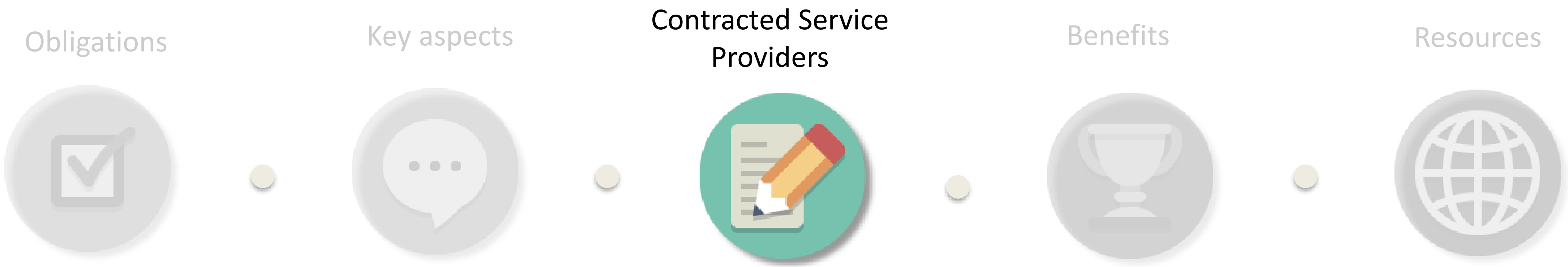
Contracted Service Providers

Benefits

Resources

- There is a distinct **difference between 'breach' vs. 'incident'.** Our scheme applies to **incidents**.
- The scheme applies to **all forms of public sector information** (soft copy / digital, hard copy and verbal)
- The scheme applies to information at a **BIL of 2 or higher**

ISINS – A brief overview of the scheme



- **S88.2** "A security risk profile assessment of an agency or body must include an assessment of any contracted service provider of the agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body."

- **S88.3** "A protective data security plan developed for an agency or body must address compliance by any contracted service provider of the agency or body with the protective data security standards applicable to that agency or body to the extent that the provider collects, holds, uses, manages, discloses or transfers public sector data for the agency or body."

ISINS – A brief overview of the scheme

Obligations

Key aspects

Contracted Service Providers

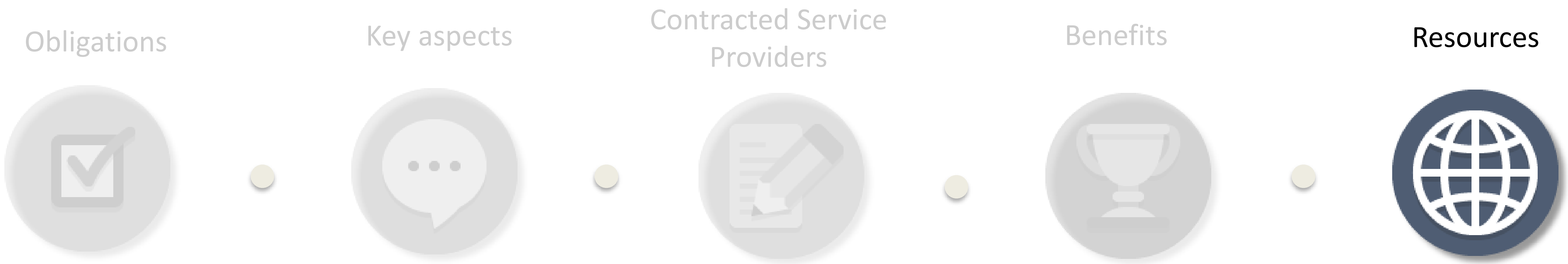
Benefits

Resources

- OVIC will, on a regular basis, provide assistance to all engaged organisations by **reporting on the current trends** using information from verified sources (i.e. industry reports, PDSPs and incident notifications).

- These reports will be **provided on a biannual basis** and should **assist with organisations' own risk reporting** forums and preparation of business cases for strategic security initiatives

ISINS – A brief overview of the scheme



Obligations

Key aspects

Contracted Service Providers

Benefits

Resources

- OVIC has produced an **information sheet** outlining the **information security incident notification scheme**.
- A copy of this can be found on the OVIC website. https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/
- For any other advice please **contact the Information Security Team** at security@ovic.vic.gov.au

The best vision is insight.

Malcolm Forbes, American Publisher

Incident Insights

Emerging themes from the ISINS

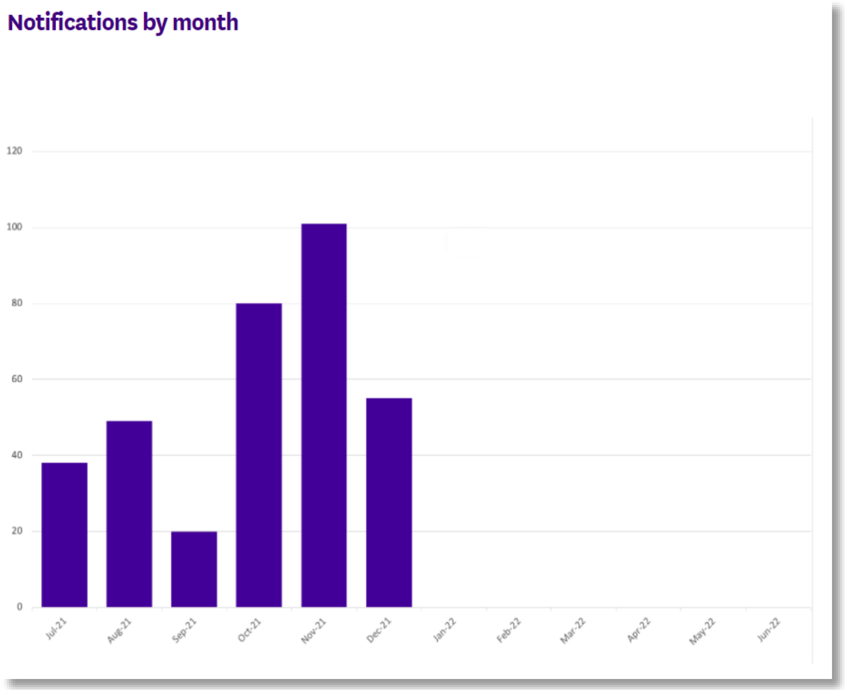
Anna Harris

Office of the Victorian Information Commissioner

Incident Insights – Emerging Themes

Volume | Information format | Information types | Security attributes | Business Impact Level | Control areas | Threat types | Threat actors

Incident Insights – Notifications by month



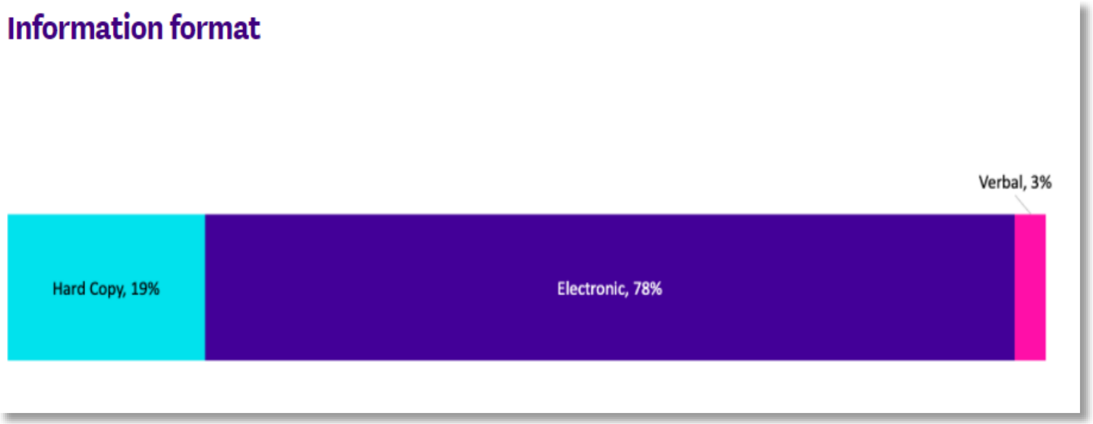
Notifications by month

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).

“Notifications continue to steadily increase as awareness of the scheme increases across the Victorian public sector.”

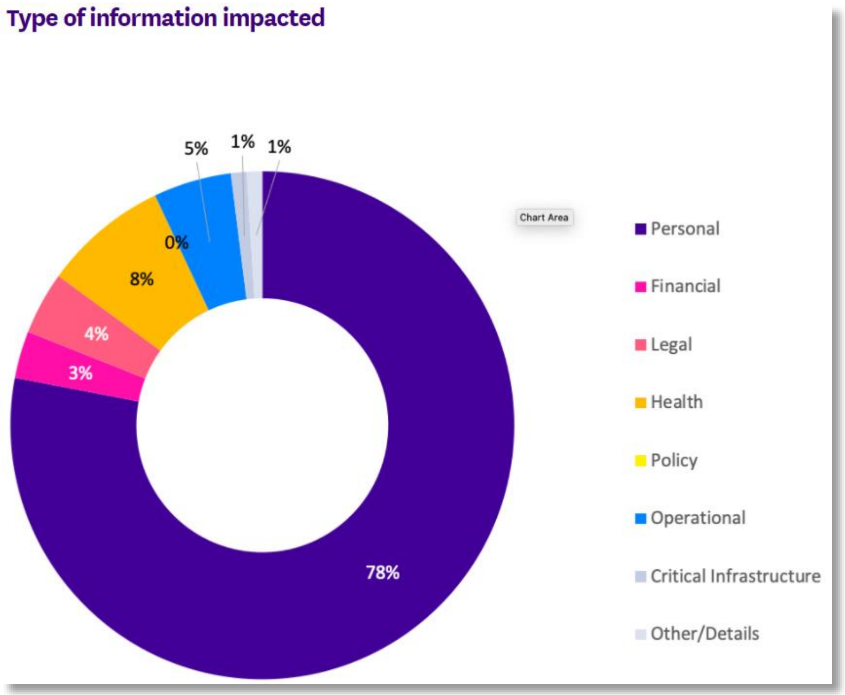
Incident Insights – Information format



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 including delivery to wrong person or incorrect labelling.”

Incident Insights – Types of information impacted

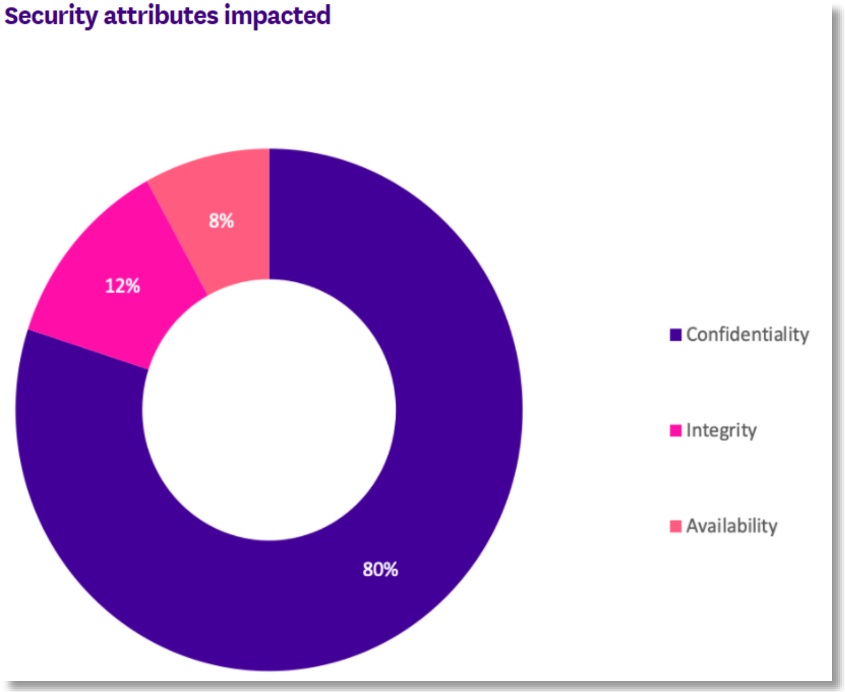


Incidents involving **personal information** continue to exceed incidents affecting other types of information.

This period saw a slight increase in incidents involving personal information (**78%**) compared to the last reporting period (**70%**).

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

Incident Insights – Security attributes impacted

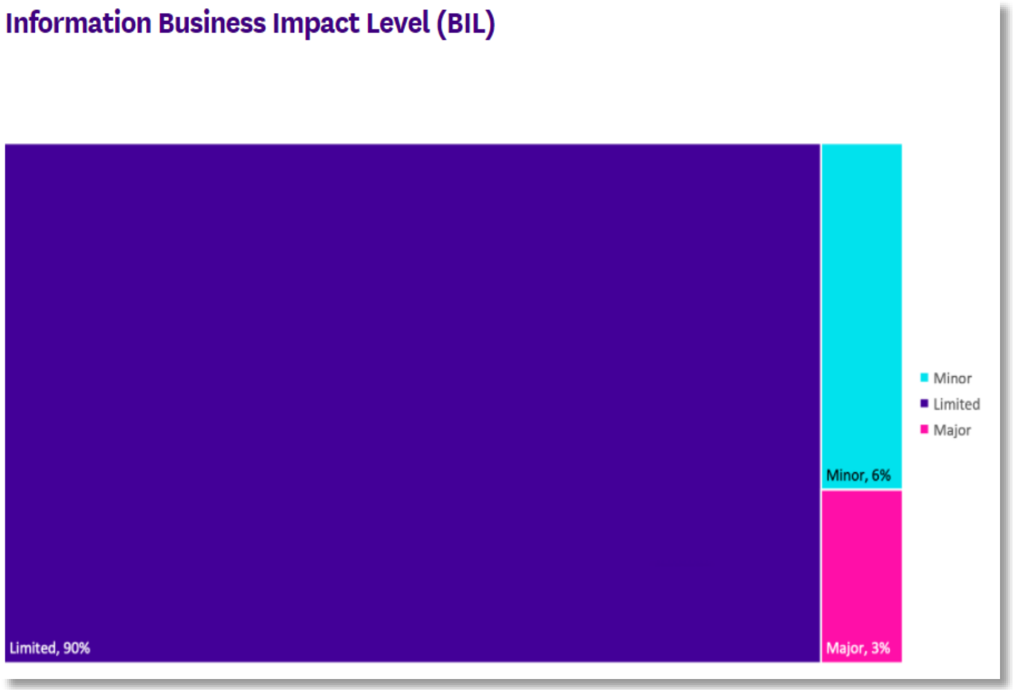


Previously, most confidentiality related incidents were from email disclosures (**85%**).

Ensuring the right people (**Confidentiality**) , have access to the right information (**Integrity**) at the right time (**Availability**) .

“In this period 45% of incidents affecting the confidentiality of public sector information were related to email/mail disclosures.“

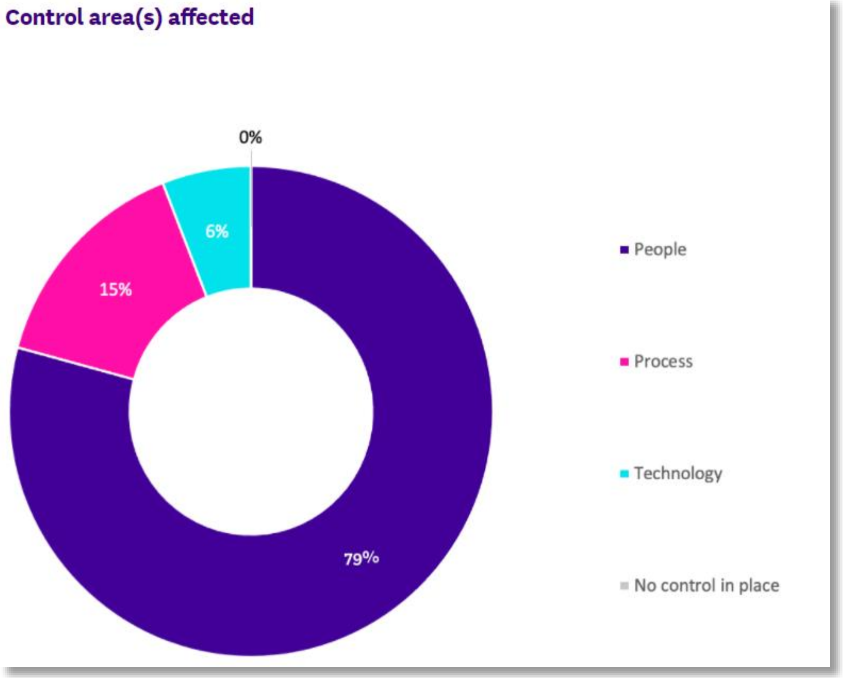
Incident Insights – Information Business Impact Level (BIL)



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.**

“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.”

Incident Insights – Control area(s) affected

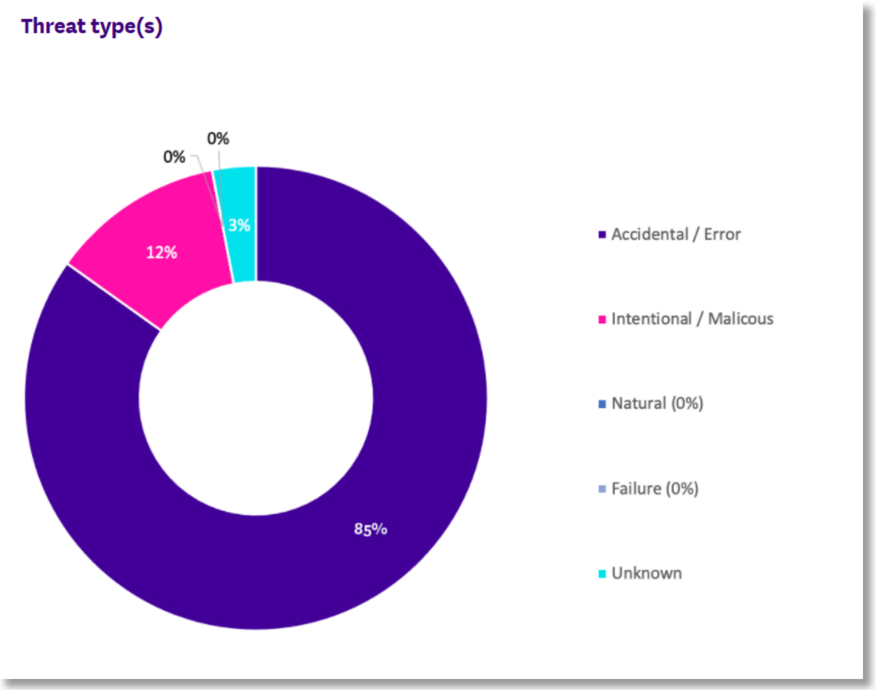


Most (**80%**) incident notifications **related to people**.

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.

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

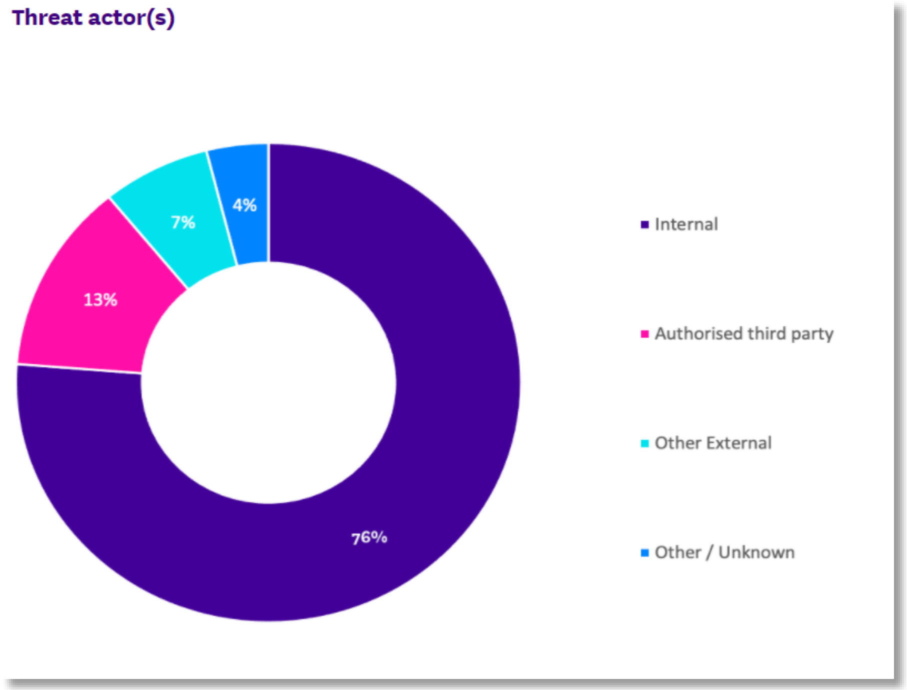
Incident Insights – Threat type



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

“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.“

Incident Insights – Threat actor(s)



The majority (**77%**) of incident notifications related to **internal staff** and **13%** related to **authorised third parties** such as contracted service providers.

“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”

OVIC Investigations Team

Matthew Fiford

Office of the Victorian Information Commissioner

Condemnation without investigation is the height of ignorance.

Albert Einstein

Who we are and what we do

- The investigations and Assurance team is responsible for developing and executing OVIC’s overall monitoring and assurance program of work.
- We **work with** the specialist teams across the office - privacy, freedom of information, and information security.
- We establish a **proactive** program of work.
- We undertake **reactive** work.
- We undertake regulatory action in accordance with the relevant **legislation** (our powers), and our **Regulatory Action Policy**.
- We establish **regulatory priorities** for OVIC.

(Some more of) what we do (under the PDP Act)

- *‘A risk-based, proportional, and targeted approach’*

- **Advice, education, and guidance** – encourage and support best practice
- **Preliminary inquiries** – gather information and resolve issues promptly by recommending improved practice or suggested actions to take.
- **Examinations** – the practices of an organisation
- **Audits –** the records of an organisation to assess compliance with the IPPs or Standards.
- **Investigations** – serious, flagrant or repeated breaches of the IPPs.

How do we identify issues that may require regulatory action?

- Media reporting
- Members of Parliament on behalf of their constituents.
- Privacy complaints and voluntary privacy breach reporting (members of public and VPS orgs).
- Public interest complaints (not disclosures).

AND

- **VPDSS incident notification reporting, including attendance at the weekly incident stand-up with ISU and executives.**

How do we initiate and conduct regulatory action?

- **Initial Assessment** phase
  - **Internal** – we consider the Act, RAP, open source, information and intelligence holdings. No engagement with the organisation at this stage.

- The focus here is facts ‘as at’ a point in time – the information known to date, the intelligence held to date. In effect a preliminary risk assessment is done to consider the benefit of taking action, and the risks of inaction.

Preliminary inquiries

- **Engage with the organisation** (collaboratively) to seek further information [for example, supporting documentation such as policy and process documentation, responses to questions, statements on the organisation's view of the breach or incident, or submissions on the breach or incident].

Examinations

Audits

Investigations

***Non of this is linear** – *where the risk associated with a privacy or information security breach or incident is high, or where a breach of the Act is flagrant, OVIC may take formal action immediately.*

Let’s get back to the theme of the VISN…

CSPs are a regulatory priority.

- We recognise the inherent privacy and information security risks involved in engagement CSPs.
- We have taken regulatory action on **several actual or potential** breaches involving third parties working with Victorian government organisations.
- And what is one outstanding point from all this work?

Organisations cannot ‘contract out’ **accountability** for privacy and information security

Let’s look at one example…

Investigation into the unauthorised access to client information held in a DHHS (now DFFH) database being accessed and used by a Departmental CSP.

*Overall, a failure in privacy and security governance – the failure to take reasonable steps to secure the personal information the Department held.**

Let’s focus on the CSP angle…

- The investigation identified that there was an **assumption** that the CSP would **meet their contractual obligations**.
- A comprehensive contractual framework existed – but it was too hard to piece together; it had been ‘added on to’ as time went by and the complexity of the relationship grew.
- The initial contract was signed in 2008…and no audit or other assurance activity had been undertaken by the Department to check the CSP was meeting its privacy and security obligations…
- until the breach.*

Take outs

- You can outsource the management of a program, but you cannot outsource **accountability**.
- Outsourcing cannot be ‘**set and forget**’.
- When building security and privacy protections, **assume things will go wrong**. Build your systems and processes to account for that.
    - Get the privacy and security basics right
    - Defense ‘in-depth’
    - Actively manage third party access to systems AND how privacy and security obligations are imposed (and assured and enforced).
- Your organisation retains both a **legal** and a **moral** duty to protect the information it holds.

Cyber Intelligence and Response Operations

Luke Johnson

Office of the Victorian Information Commissioner

Cyber Incident Response Service

Incident Response

Coordinate complex cyber incidents and advise WoVG on our collective risk

Works with federal and inter-jurisdictional partners

Support the Minister for Government Services and the Premier’s Office

Threat Intelligence

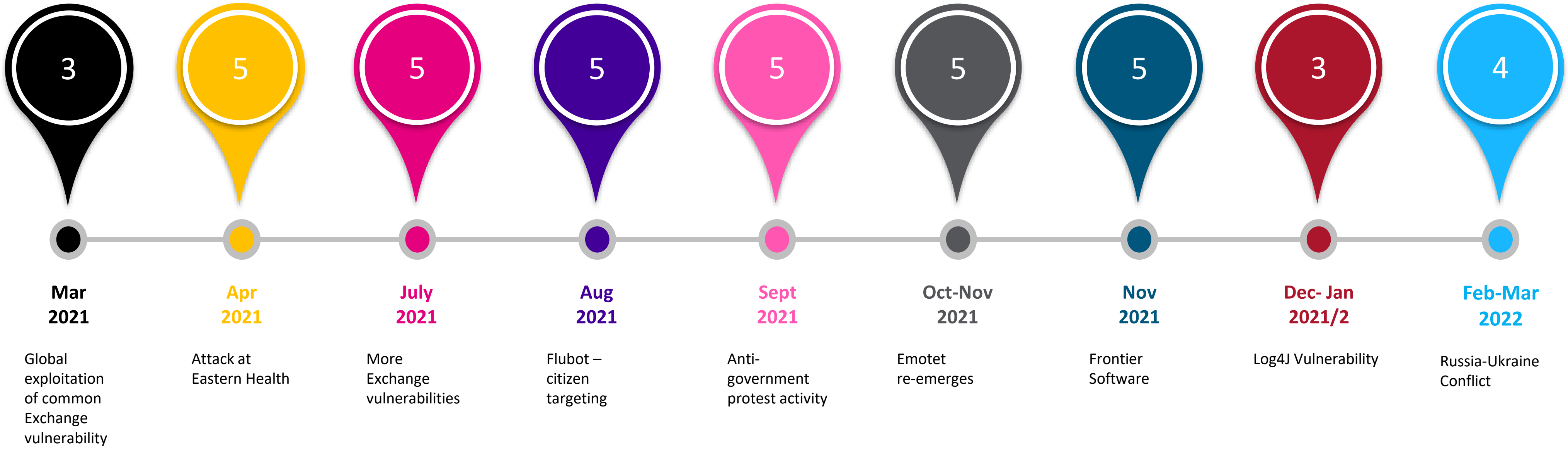
Threat alerting and intelligence products

Emergency Management

DPC is the control agency responsible for leading the operational response to cyber security emergencies in Victoria

The last twelve months have been threatening

- All jurisdictions, governments, industry and citizens are being targeted
- Victorian government organisations are targeted, specifically and opportunistically
- Our third parties are targeted in the same way as our organisations
- It is our responsibility to ensure we understand their cyber risk



3
Mar 2021
Global exploitation of common Exchange vulnerability

5
Apr 2021
Attack at Eastern Health

5
July 2021
More Exchange vulnerabilities

5
Aug 2021
Flubot – citizen targeting

5
Sept 2021
Anti-government protest activity

5
Oct-Nov 2021
Emotet re-emerges

5
Nov 2021
Frontier Software

3
Dec- Jan 2021/2
Log4J Vulnerability

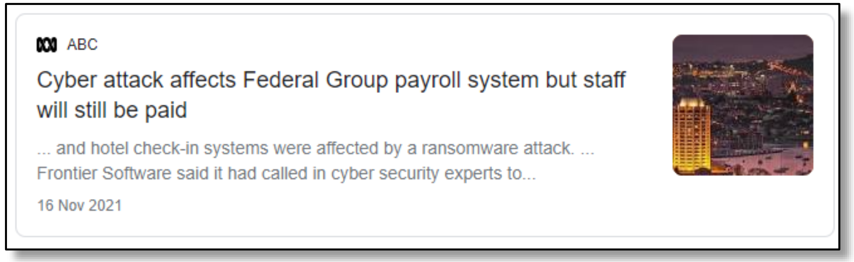
4
Feb-Mar 2022
Russia-Ukraine Conflict

Frontier case study

5

Nov 2021

Frontier Software

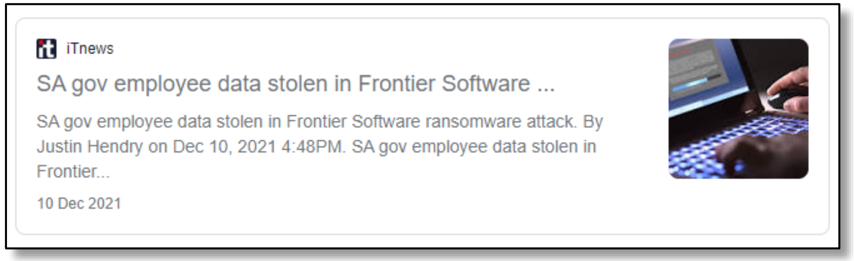


ABC

Cyber attack affects Federal Group payroll system but staff will still be paid

... and hotel check-in systems were affected by a ransomware attack. ... Frontier Software said it had called in cyber security experts to...

16 Nov 2021

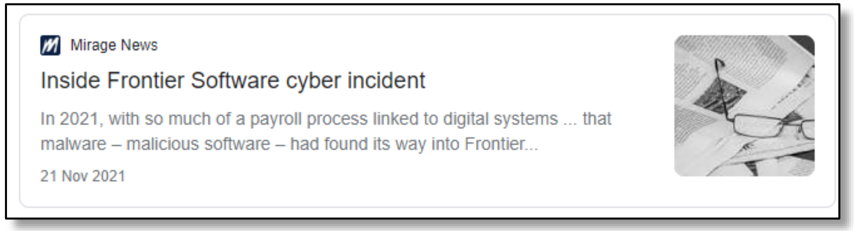


iTnews

SA gov employee data stolen in Frontier Software ...

SA gov employee data stolen in Frontier Software ransomware attack. By Justin Hendry on Dec 10, 2021 4:48PM. SA gov employee data stolen in Frontier...

10 Dec 2021

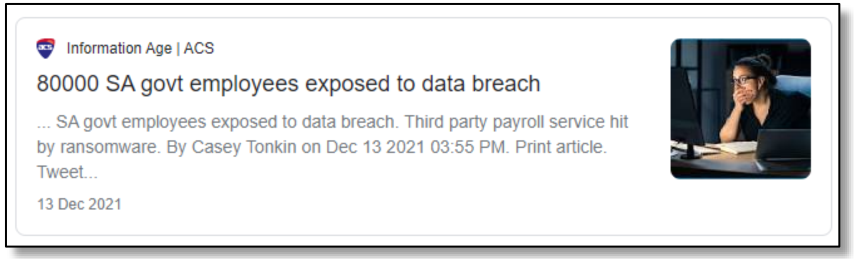


Mirage News

Inside Frontier Software cyber incident

In 2021, with so much of a payroll process linked to digital systems ... that malware – malicious software – had found its way into Frontier...

21 Nov 2021



Information Age | ACS

80000 SA govt employees exposed to data breach

... SA govt employees exposed to data breach. Third party payroll service hit by ransomware. By Casey Tonkin on Dec 13 2021 03:55 PM. Print article. Tweet...

13 Dec 2021

- Large, multi-national Human Resource and payroll provider
- Contractual arrangements with Australian government and industry
- Ransomware incident and lots of stolen data
- Some significant public exposure
- A risk assessment for organisations

What to do

Contracts
Find your third party contracts, read them, update them.

Data
What data do they hold, where is it and what are their obligations to protect it?

Technical diagrams
Understand how your organisation is connected to its suppliers.

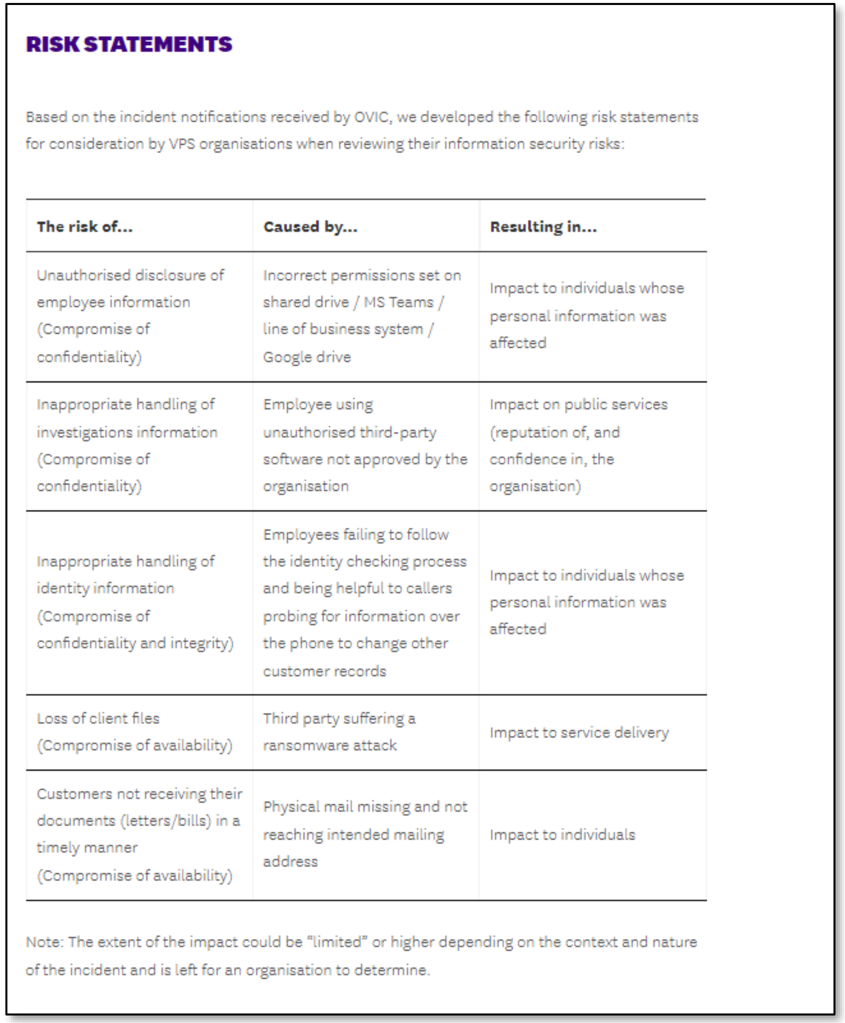
Assess
Seek assurance, do testing, ask for evidence.

Linking incidents, risks and controls

Anthony Corso

Office of the Victorian Information Commissioner

Risk Statements



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:

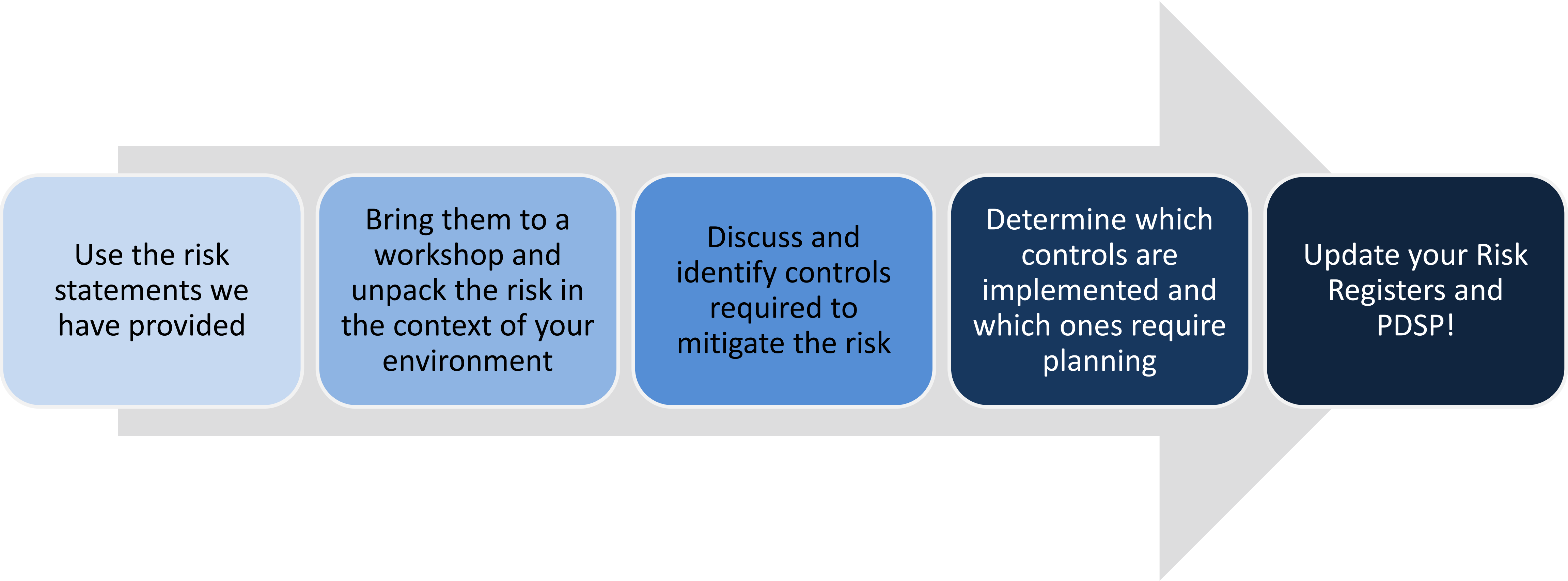
The risk of...	Caused by...	Resulting in...
Unauthorised disclosure of employee information (Compromise of confidentiality)	Incorrect permissions set on shared drive / MS Teams / line of business system / Google drive	Impact to individuals whose personal information was affected
Inappropriate handling 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

Note: 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.

With every insights publication, we include risk statements based on emerging trends.

- Did you know this?
- Do you use them?
- What do they mean?

A risk based approach to security



Use the risk statements we have provided

Bring them to a workshop and unpack the risk in the context of your environment

Discuss and identify controls required to mitigate the risk

Determine which controls are implemented and which ones require planning

Update your Risk Registers and PDSP!

Lets work through an example using a specific risk…

The risk of (event):	Loss of client files
Caused by:	Third party suffering a ransomware attack
Resulting in:	Impact to service delivery

Define the event ….

Event
Loss of client files

Identify the cause ….

Cause
Third party suffering a ransomware attack

Event
Loss of client files

⚠

Understand the impact ….

Cause
Third party suffering a ransomware attack

Event
Loss of client files

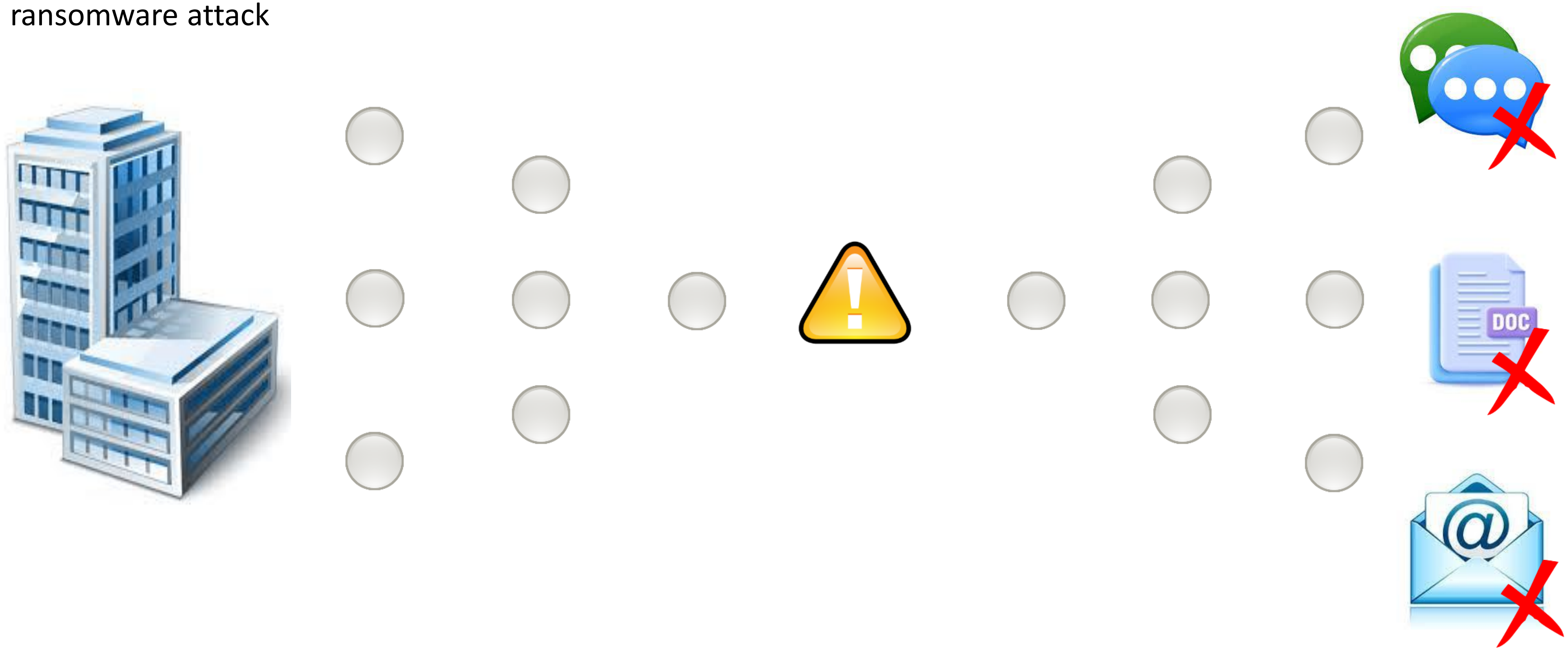
Resulting in
Impact to service delivery

Let’s talk controls….

Cause
Third party suffering a ransomware attack

Event
Loss of client files

Resulting in
Impact to service delivery

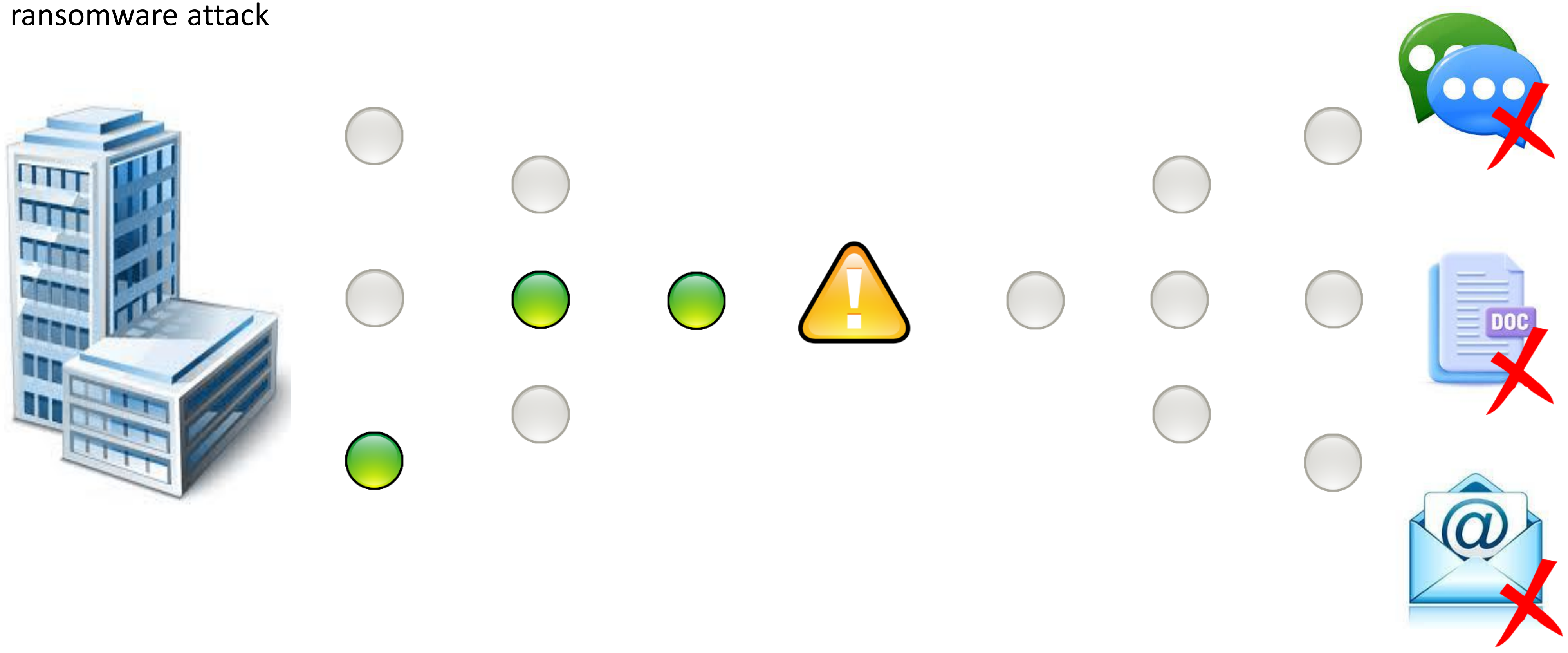


What controls may prevent ….

Cause
Third party suffering a ransomware attack

Event
Loss of client files

Resulting in
Impact to service delivery

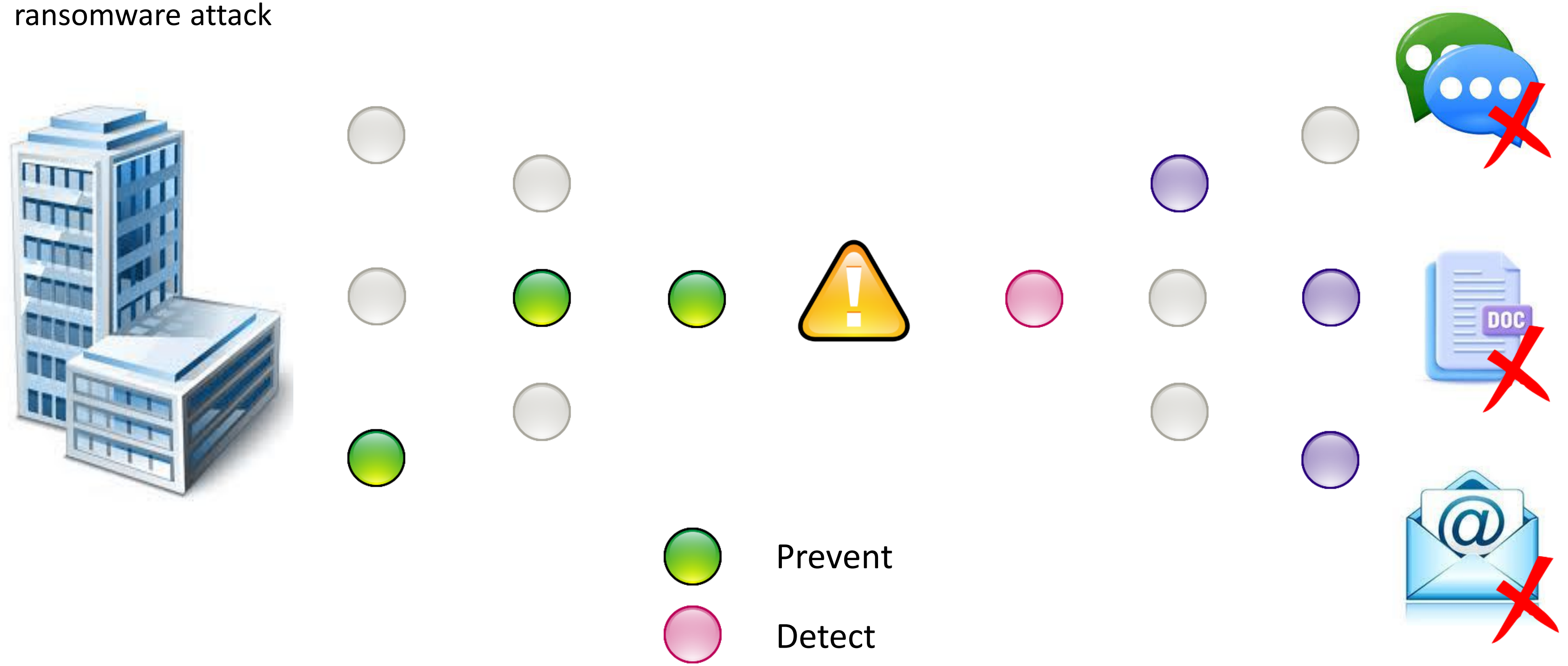


What controls may detect and/or correct ….

Cause
Third party suffering a ransomware attack

Event
Loss of client files

Resulting in
Impact to service delivery



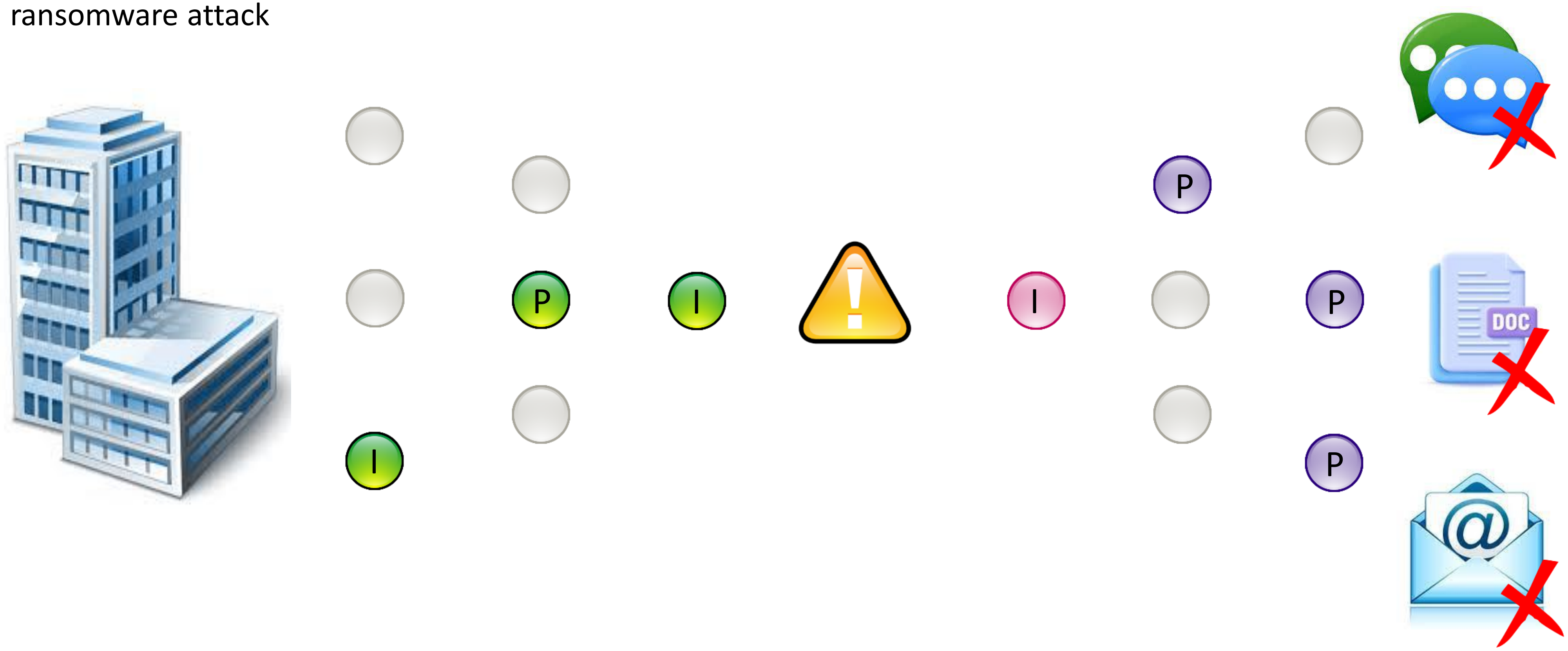
- 🟢 Prevent
- 🔴 Detect
- 🟣 Correct

What controls are implemented/planned….

Cause
Third party suffering a ransomware attack

Event
Loss of client files

Resulting in
Impact to service delivery



Update risk registers and PDSP!

Element	Description	Entity Risk Ref	Supporting Control Library	Status	Proposed Completion
E11.160	The organisation manages malware prevention and detection software for ICT systems	**Risk Ref** A1254	P	Partial (Most)	2022/23
E11.180	The organisation manages backup processes and procedures (e.g., schedule, isolation, storage, testing,retention).	**Risk Ref** A1254	P P	Partial (Some)	2022/23
E11.110	The organisation logs system events and actively monitors these to detect potential security issues (e.g., intrusion detection/ prevention systems (IDS/ IPS)).	**Risk Ref** A1254	I	Implemented	Completed/BAU
E5.030	The organisation delivers information security training and awareness to …….	**Risk Ref** A1254	I P	Partial (Most)	2023/24
E11.120	The organisation uses secure system administration practices.	**Risk Ref** A1254	I	Implemented	Completed/BAU

The risk of (event): loss of client files
caused by: a third party suffering a ransomware attack
resulting in: impact to service delivery.

With thanks from the Deputy Commissioner

Rachel Dixon
Deputy Commissioner
Privacy and Data Protection

It is sound planning that invariably earns us the outcome we want; without it, even the gods are unlikely to look with favour on our designs.

Herodotus, “The Histories,” Book Eight

Feedback and Questions

Please provide any **feedback** you have on today’s session.

slido

Go to slido.com

Code: **MarchVISN**

For those with **questions** following this forum, please email:

security@ovic.vic.gov.au