Information Security Incident Insights Forum

Victorian Information Security Network (**VISN**)
April 2024

OVIC
Office of the Victorian
Information Commissioner

Please note: This event is being recorded

Acknowledgment of Country

Sean Morrison

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.

Commissioner’s welcome

Sean Morrison

Information Commissioner

Incident Insights Reports

[Report for 1 July 2023 to 31 December 2023](https://ovic.vic.gov.au/information-security/security-insights/)

Report for 1 January to 30 June 2023

Report for 1 July to 31 December 2022

Report for 1 January to 30 June 2022

Report for 1 July 2021 to 31 December 2021

Report for 1 January 2021 to 30 June 2021

Report for 1 July 2020 to 31 December 2020

Report for 29 October 2019 to 30 June 2020

OFFICIAL

INFORMATION FOR AGENCIES

Incident Insights Report

1 July 2023 – 31 December 2023

Overview of this report

OFFICIAL

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

Information Security Unit

Anthony Corso
Assistant Commissioner – Information Security

Office of the Victorian
Information Commissioner

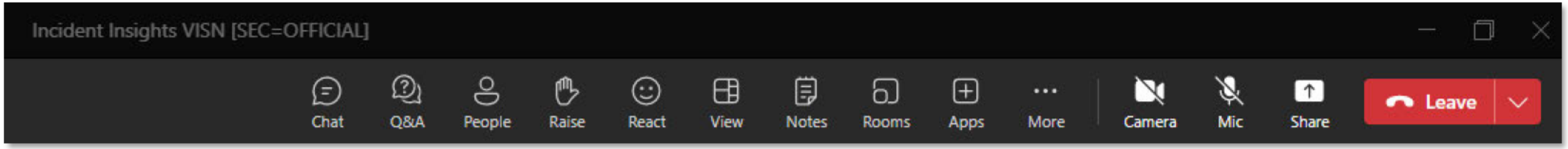
Housekeeping

Cameras and mics have been muted for attendees. If your Teams is running slow, try disconnecting from your VPN.

Today’s session **is being recorded.**

A copy of OVIC’s **slides** and the **recording** will be made available in the coming days on OVIC’s website.

Join the conversation



Regular **chat** functionality in Teams has been **activated** in this forum.

Type your question into the **Teams Q&A channel**.
You can choose to be **anonymous or leave your name displayed**.

Each speaker will answer questions following their presentation.
If you prefer to ask your question verbally **raise your hand.**

What we’ll explore today

- A bit about the Information Security Incident Notification Scheme
- The latest Incident Insights Report – themes and trends
- Guest speaker from Verizon – John Hines
- Session close

The Information Security Incident Notification Scheme

Anthony Corso
Assistant Commissioner, Information Security - OVIC

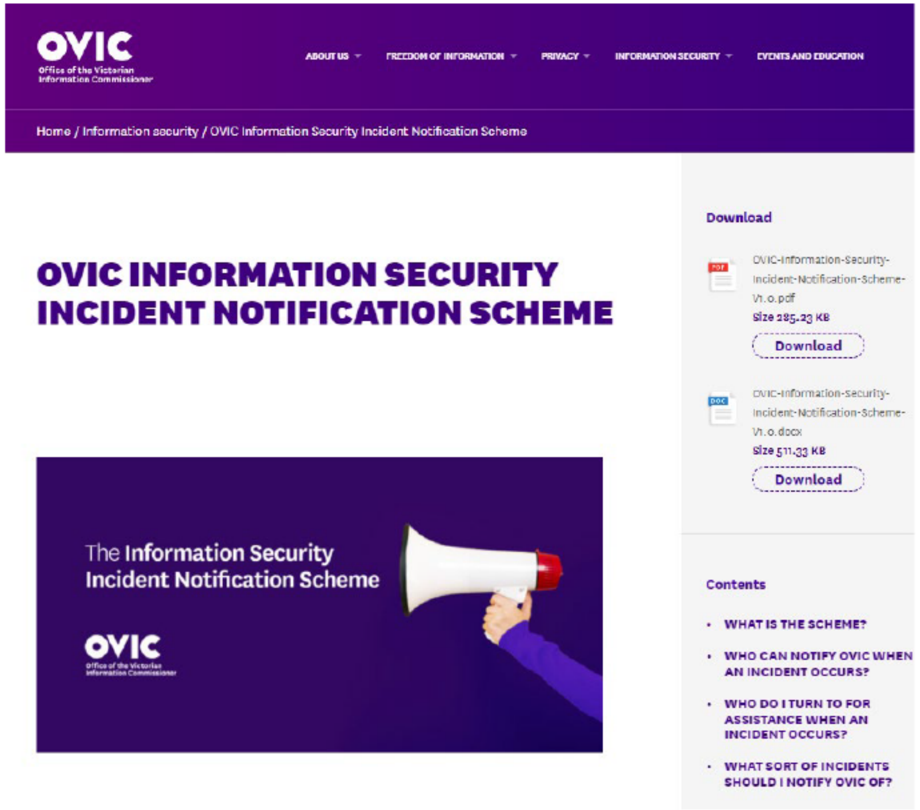
OVIC
Office of the Victorian
Information Commissioner

What is the Incident Notification 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.

What sort of incidents need to be notified to OVIC?

- Under VPDSS element E9.010, VPS organisations are required to notify OVIC of any adverse impact on the **confidentiality, integrity, or availability** of public sector information with a **business impact level (BIL) of 2 (limited) or higher**.
- This includes information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET.



Home / Information security / OVIC Information Security Incident Notification Scheme

OVIC INFORMATION SECURITY INCIDENT NOTIFICATION SCHEME

The Information Security Incident Notification Scheme

OVIC

Download

OVIC-Information-Security-Incident-Notification-Scheme-V1.0.pdf
Size 285.23 KB

OVIC-Information-Security-Incident-Notification-Scheme-V1.0.docx
Size 511.33 KB

Contents

- WHAT IS THE SCHEME?
- WHO CAN NOTIFY OVIC WHEN AN INCIDENT OCCURS?
- WHO DO I TURN TO FOR ASSISTANCE WHEN AN INCIDENT OCCURS?
- WHAT SORT OF INCIDENTS SHOULD I NOTIFY OVIC OF?

Themes and trends from the latest Incident Insights Report

Anna Harris
Principal Advisor, Information Security - OVIC

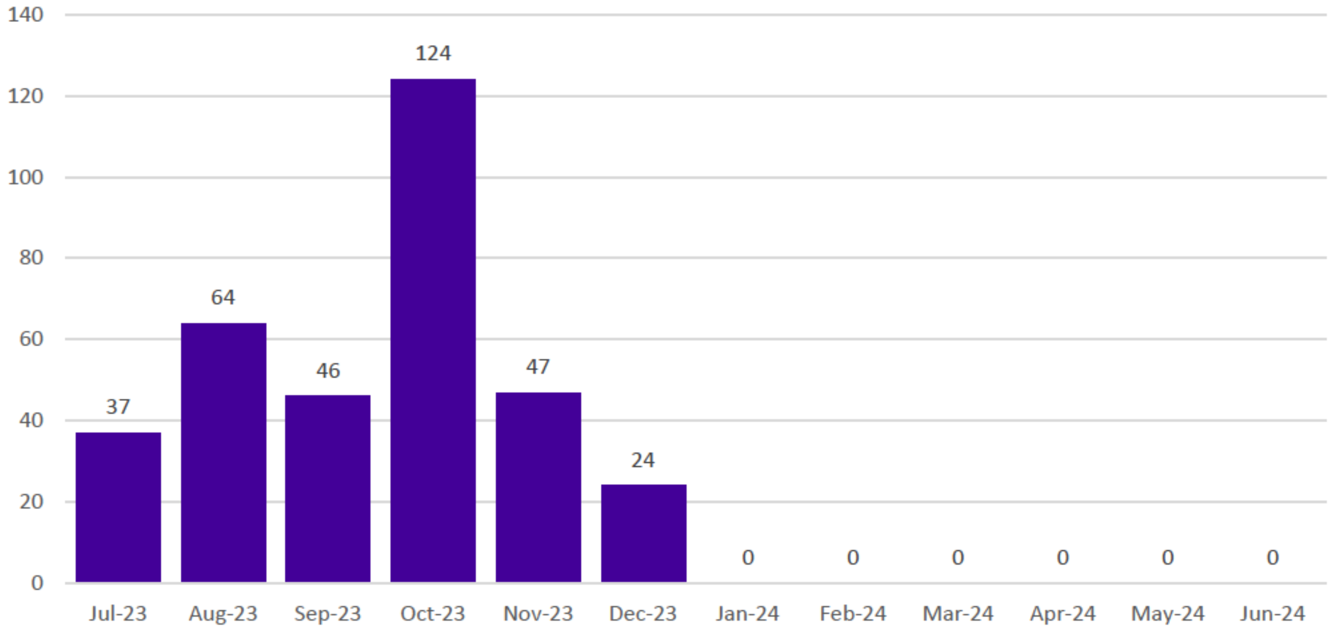
Office of the Victorian Information Commissioner

Themes and trends

- Volume
- Information format
- Information type
- Business Impact Level (BIL)
- Security attributes
- Control areas
- Threat actors
- Threat types

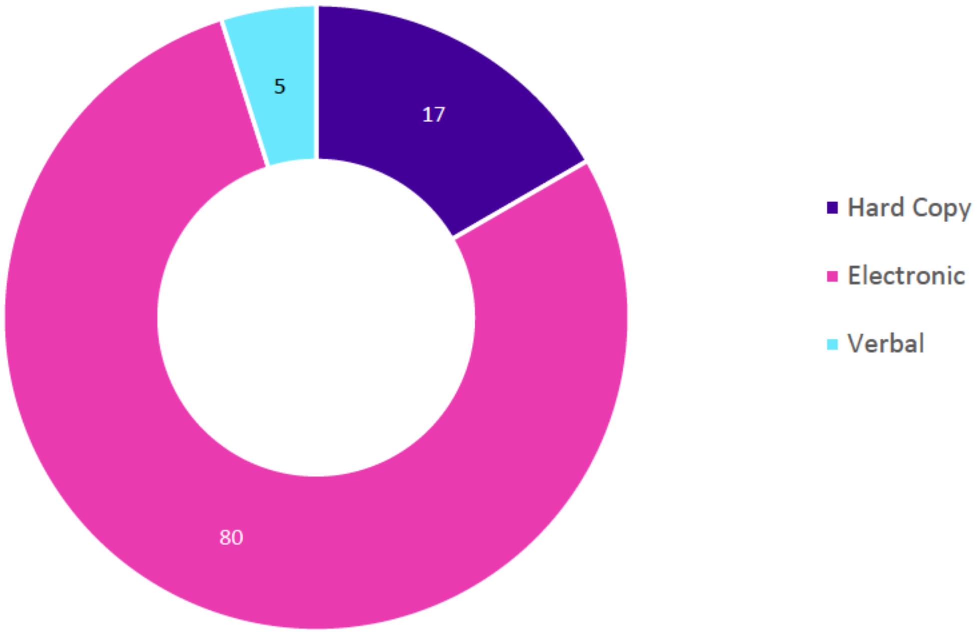
Volume - Notifications by month

- OVIC received **342** notifications between **1 July** to **31 December 2023**.
- This is a **20%** increase compared to the previous notification period.



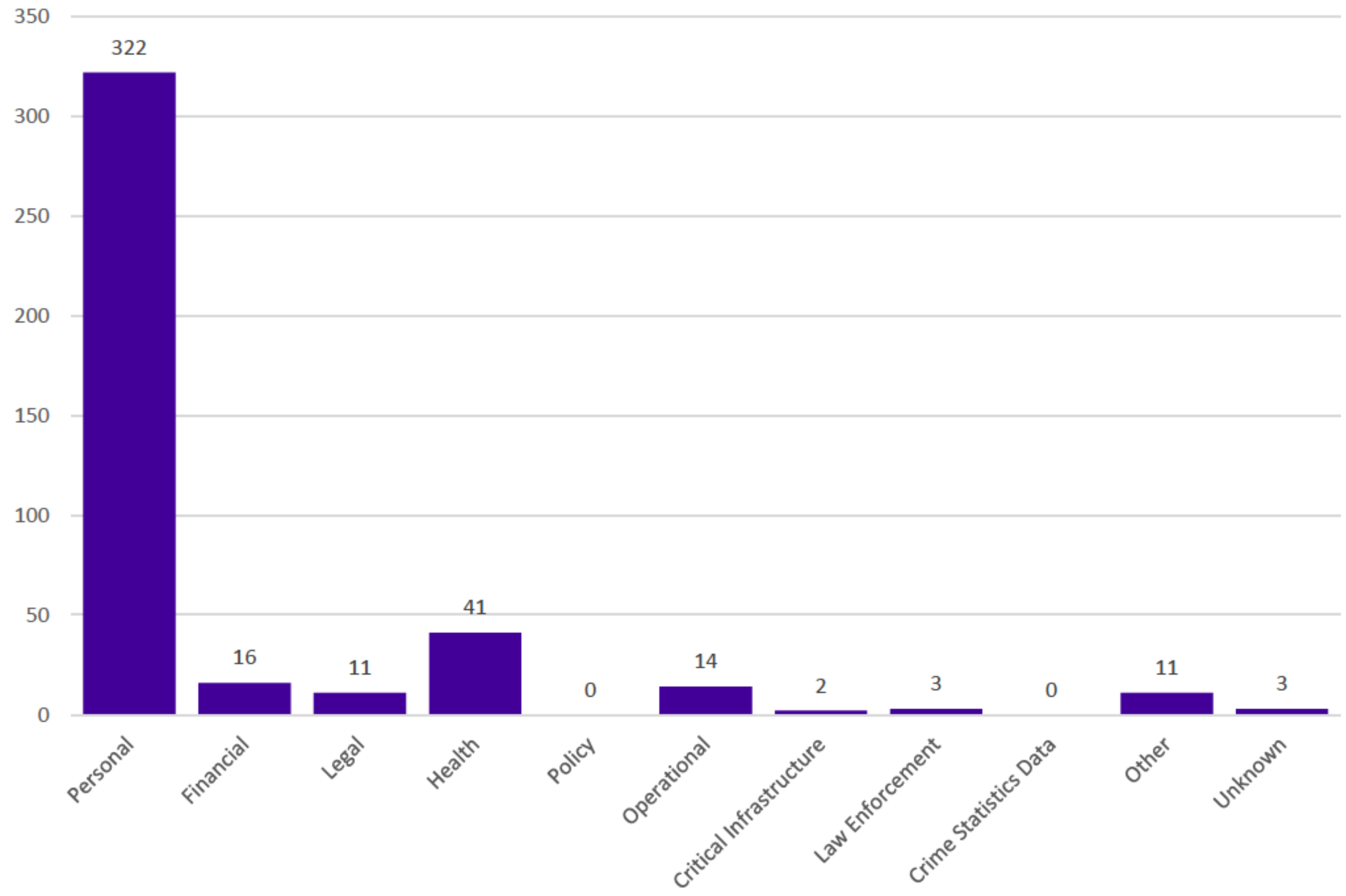
Information format

- **273** notifications indicate compromises of **electronic information**.
- More than half of the incidents affecting electronic information related to emails - predominantly **sending emails to the incorrect recipient**.
- **56%** of incidents involving hard copy information were related to **mail**.



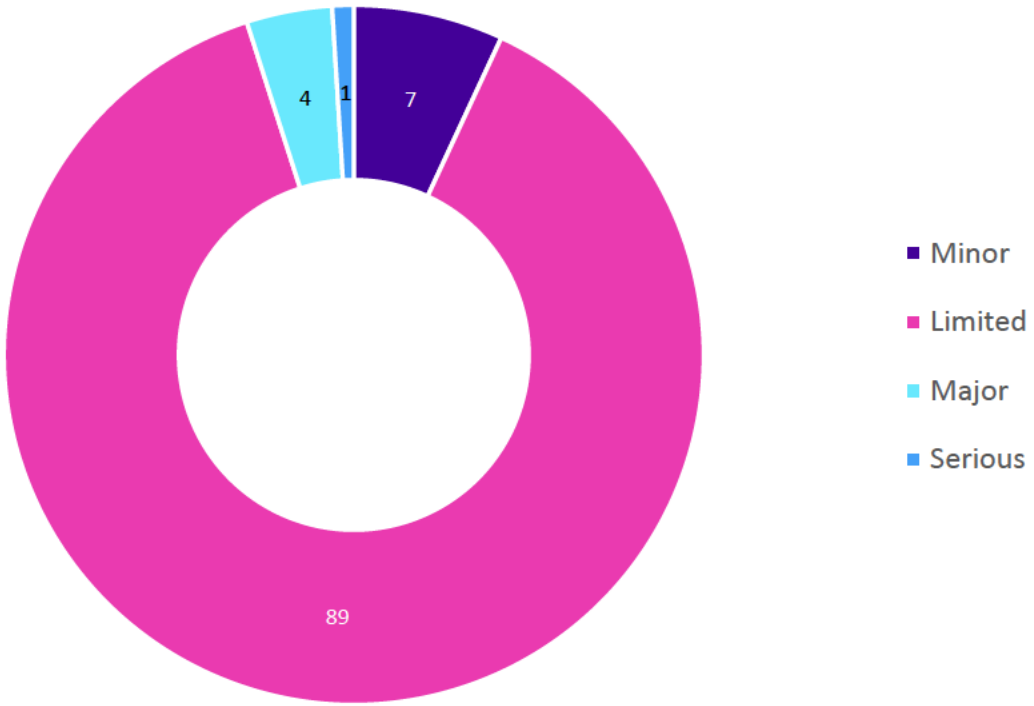
Information type

- **94%** incident notifications indicate compromises of **personal** information.
- **19%** incident notifications involved more than one information type.
- There were **11** notifications that selected **Other** e.g., claim numbers, credentials, project and committee documents.



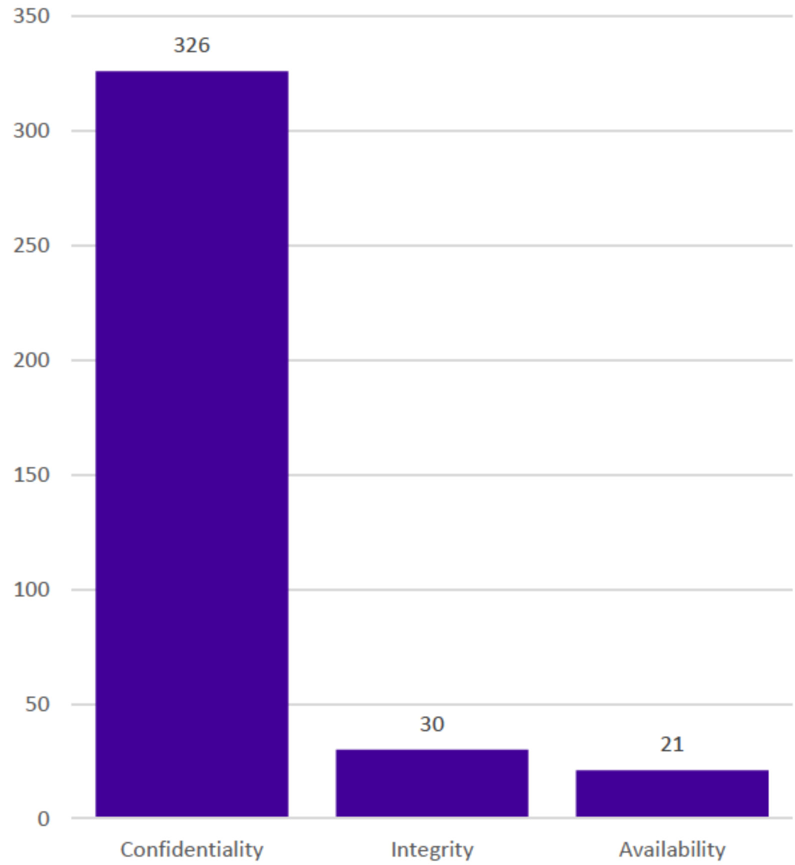
Business Impact Level (BIL)

- **89%** of incidents were assessed as impacting BIL 2 information (Limited harm or damage).
- **12** incident notifications nominated BIL 3.
- If in doubt of the BIL just notify.



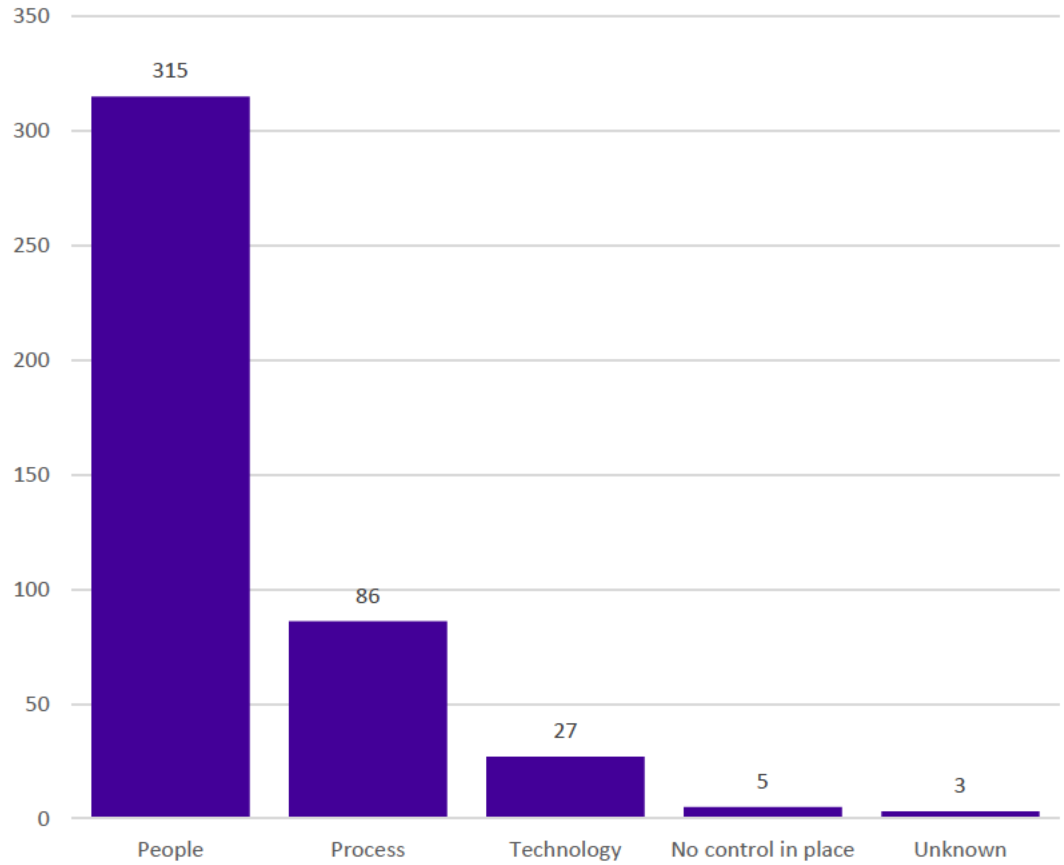
Security attributes

- **326** incident notifications indicate compromises of the **confidentiality** of information.
- **9%** of incident notifications selected more than one option for this field.



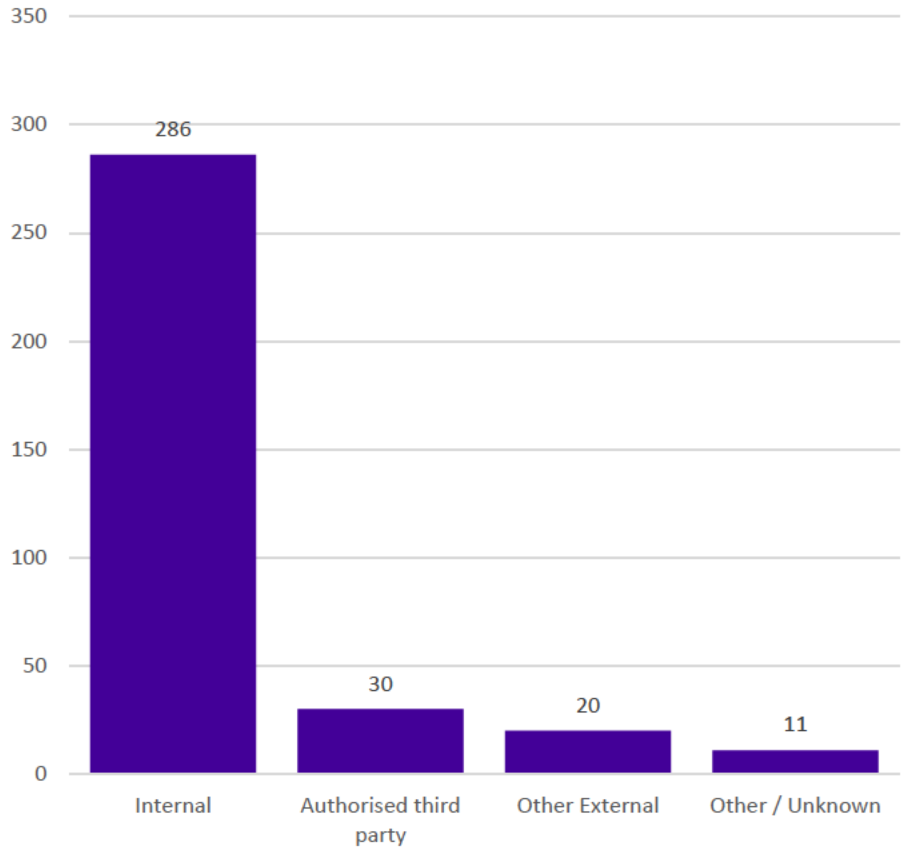
Control areas

- **315** notifications related to **people**.
- **86** notifications related to **process.**
- **27** notifications related to **technology**.
- **6** notifications where all three control areas were nominated as causal factors.



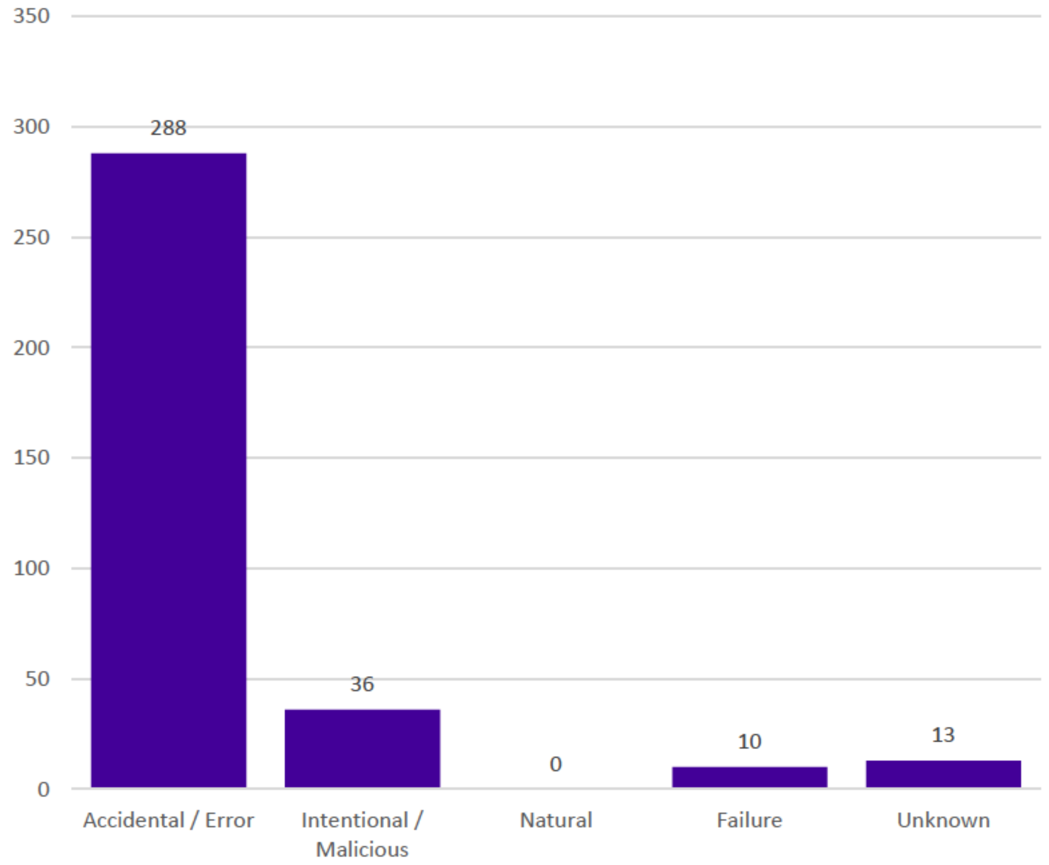
Threat actors

- **84%** of notifications related to **internal staff**.
- **9%** of notifications related to **authorised third parties** such as contracted service providers.
- **11** notifications indicated that the threat actor could not be ascertained.



Threat types

- **84%** of notifications related to **accidental actions**.
- **11%** of notifications related to **intentional actions**.



Risk statements

The risk of…	caused by…	resulting in…	
Employee payroll information shared without employee consent with a superannuation fund	System change triggering an override function and subsequently incorrectly processing data reverting employees to the default fund and informing the fund	Impact on public services (reputation of, and confidence in, the organisation) Impact to individuals whose personal information was affected	C I
Inability to access public sector information	System crash following a staff member rebooting one network device after a configuration change which caused a chain reaction on the rest of the network leading to connectivity issues	Impact on service delivery Impact on public services (reputation of, and confidence in, the organisation)	A
Inadvertent release of client information	Public sector organisation not redacting documents	Impact on public services (reputation of, and confidence in, the organisation) Impact to individuals whose personal information was affected	C

Questions for OVIC?

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

DBIR

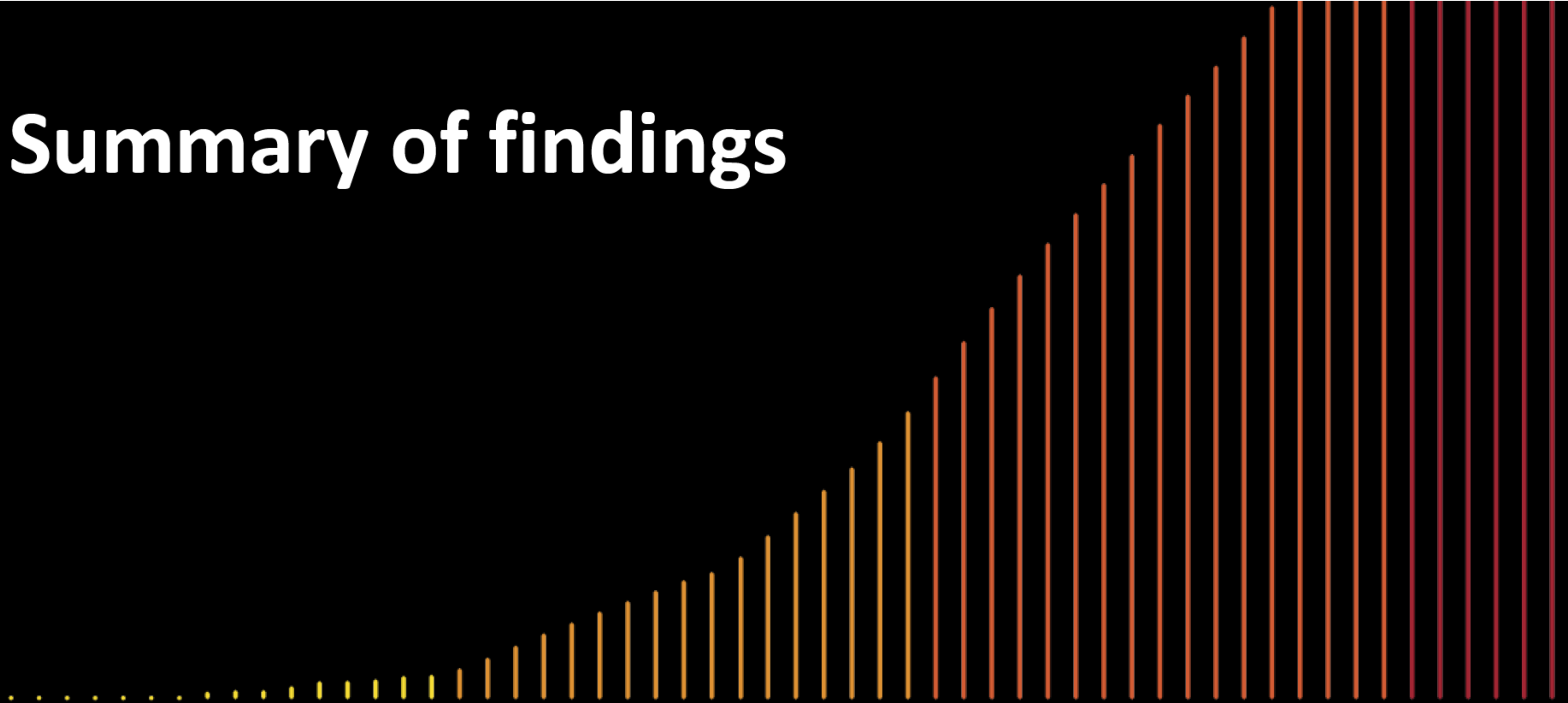
2023 Data Breach Investigations Report Presentation

John Hines

Head of Cyber Security | Asia Pacific and Japan

The authoritative source of cybersecurity breach information

Summary of findings



A comprehensive look at data security patterns

16

years

81

countries

16,312

incidents reviewed in our 2023 report

5,199

data breaches analyzed in the 2023 report

It’s been a busy year for cybercriminals—and those who fight them. Here’s what we saw.

Key paths to data breaches:

Stolen credentials

Phishing

Exploitation of vulnerabilities

Who are the culprits?

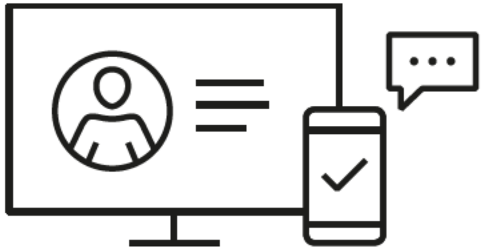
Organized crime is the leading source of cyberattacks.

74% of all breaches include the human element, through Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

What are the motives?

#1 The number 1 motive was Financial gain, which was the driver for 95% of attacks.

#2 The number 2 motive was Espionage—but a very distant second place.



Pretexting rose.

50% of all Social Engineering incidents in 2022 involved Pretexting—an invented scenario that tricks someone into giving up information or committing an act that may result in a breach.

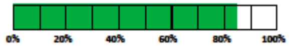
What we found:

24%

0%
20%
40%
60%
80%
100%

24% of all cyberattacks involved Ransomware.

83%



83% of breaches were by External actors, typically looking for money and data.

19%

0%
20%
40%
60%
80%
100%

19% of breaches came from Internal actors, who caused both intentional and unintentional harm.

More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

Top data-driven findings

74% of all breaches included the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering.

83% of breaches involved external actors, and the primary motivation for attacks continues to be overwhelmingly Financially driven, at 95% of breaches.

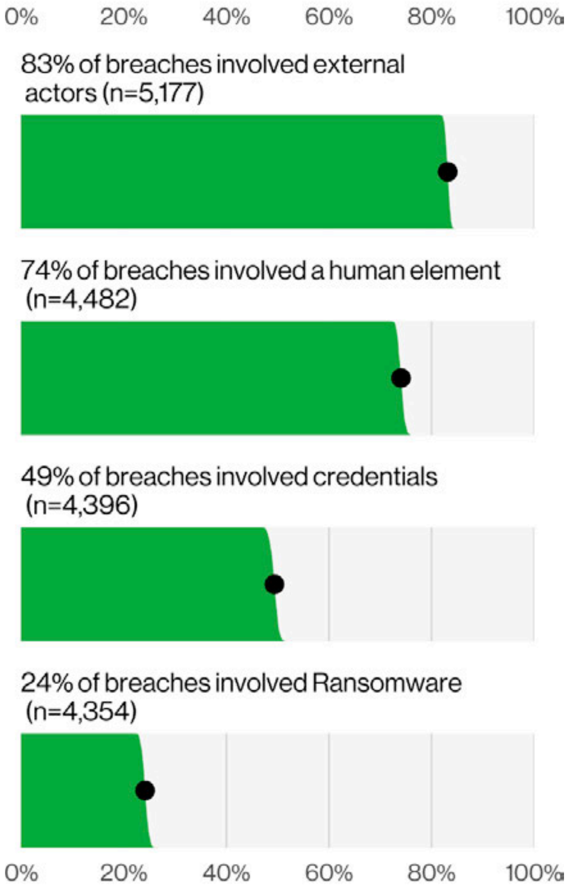


Figure 1. Select key enumerations

Ransomware

Ransomware continues its reign as one of the top Action types present in breaches, and while it did not actually grow, it did hold statistically steady at 24%. Ransomware is ubiquitous among organizations of all sizes and in all industries.

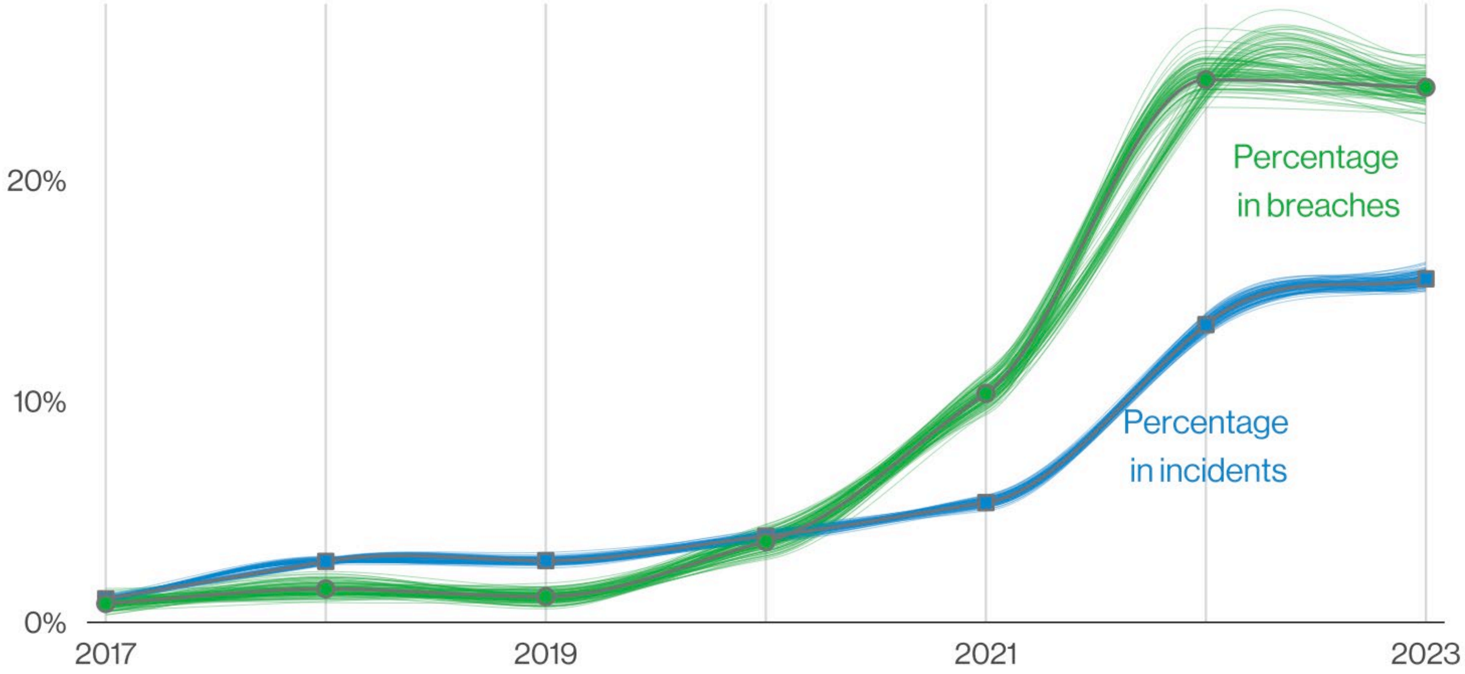


Figure 2. Ransomware action variety over time

Business Email Compromise (BEC)

Social Engineering attacks are often very effective and extremely lucrative for cybercriminals. BEC attacks (which are most of our pretexting attacks) have almost doubled across our entire incident dataset and now represent more than 50% of incidents within the Social Engineering pattern.

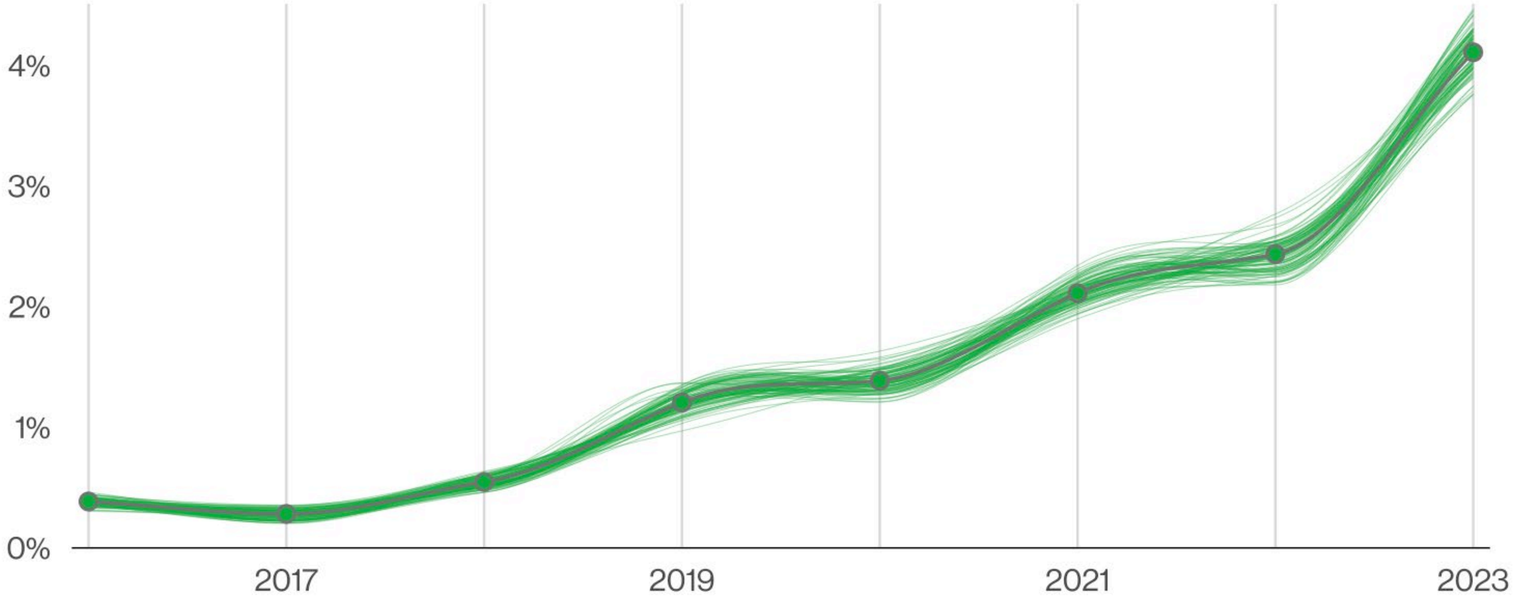


Figure 3. Pretexting incidents over time

Ways in

External actors leveraged a variety of techniques to gain entry to an organization, such as Use of stolen credentials (49%), Phishing (12%) and Exploiting vulnerabilities (5%). This is very much in line with last year's results, so what about Log4j? Wasn't it impactful?

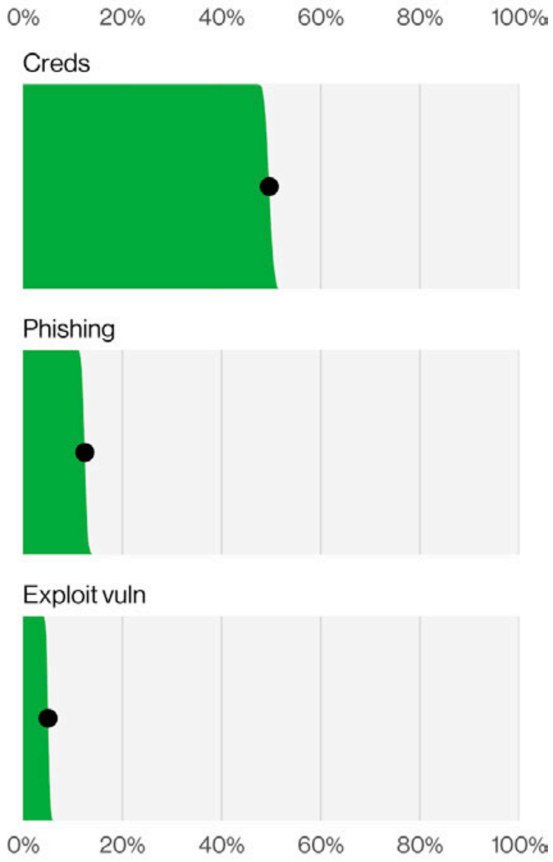


Figure 4. Select enumerations in non-Error, non-Misuse breaches (n=4,291)

Log4j

Log4j was identified as the culprit in 90% of breaches where a vulnerability exploitation was the way in and our contributors explicitly documented what vulnerability was exploited.

More than 32% of all Log4j scanning activity over the course of the year happened within 30 days of its release (with the biggest spike of activity occurring within 17 days).

Takeaway: Quick patch response by industry mitigated what could have been a much bigger disaster.

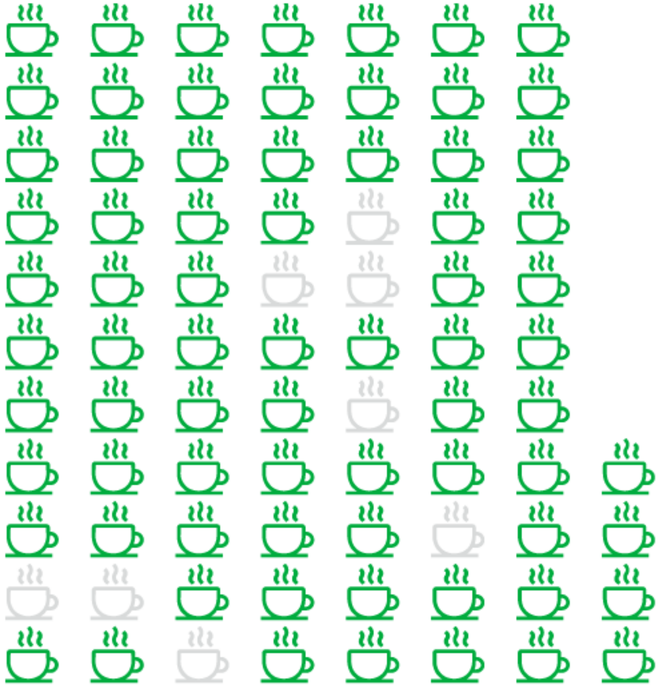


Figure 5. Percentage of identified Exploit vuln that was Log4j (n=81). Each glyph represents an incident.

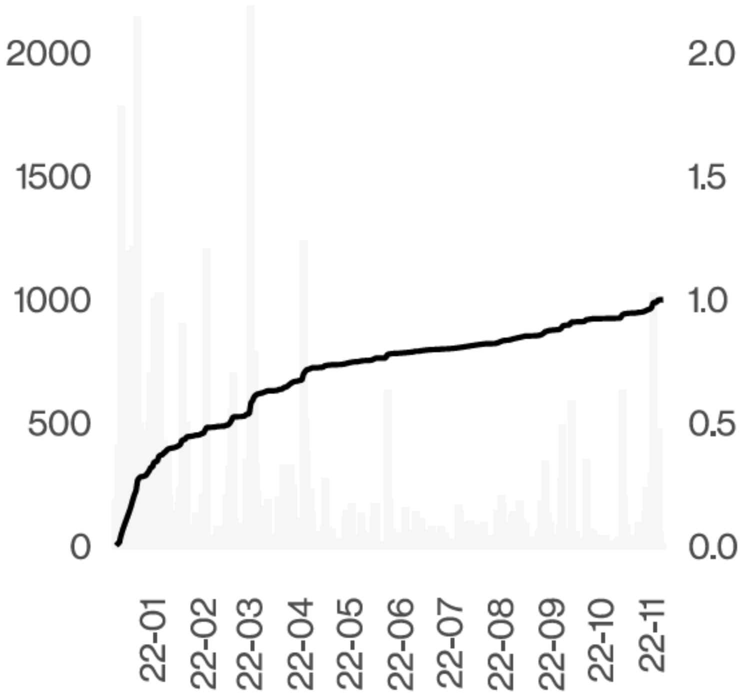
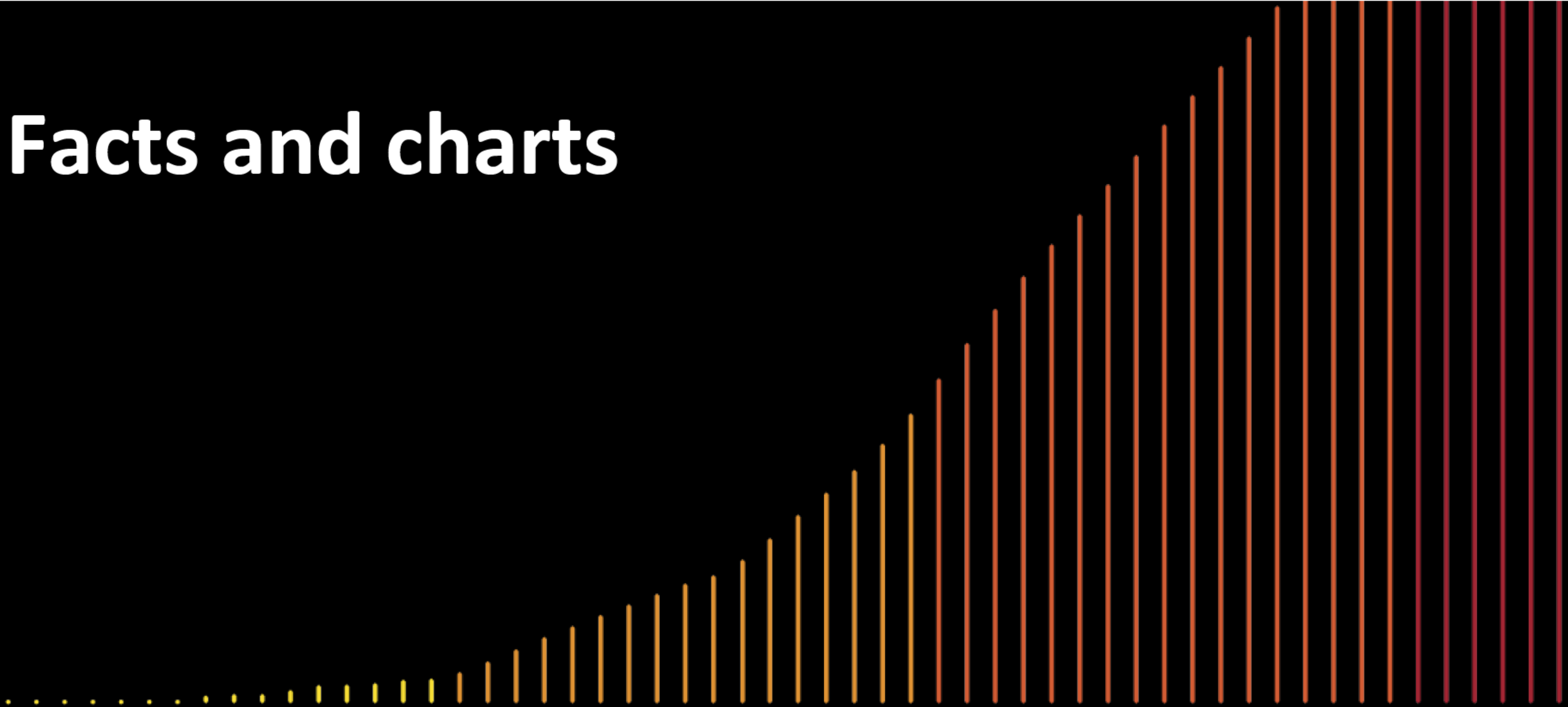


Figure 6. Percentage of Log4j scanning for 2022

Facts and charts



Incident patterns

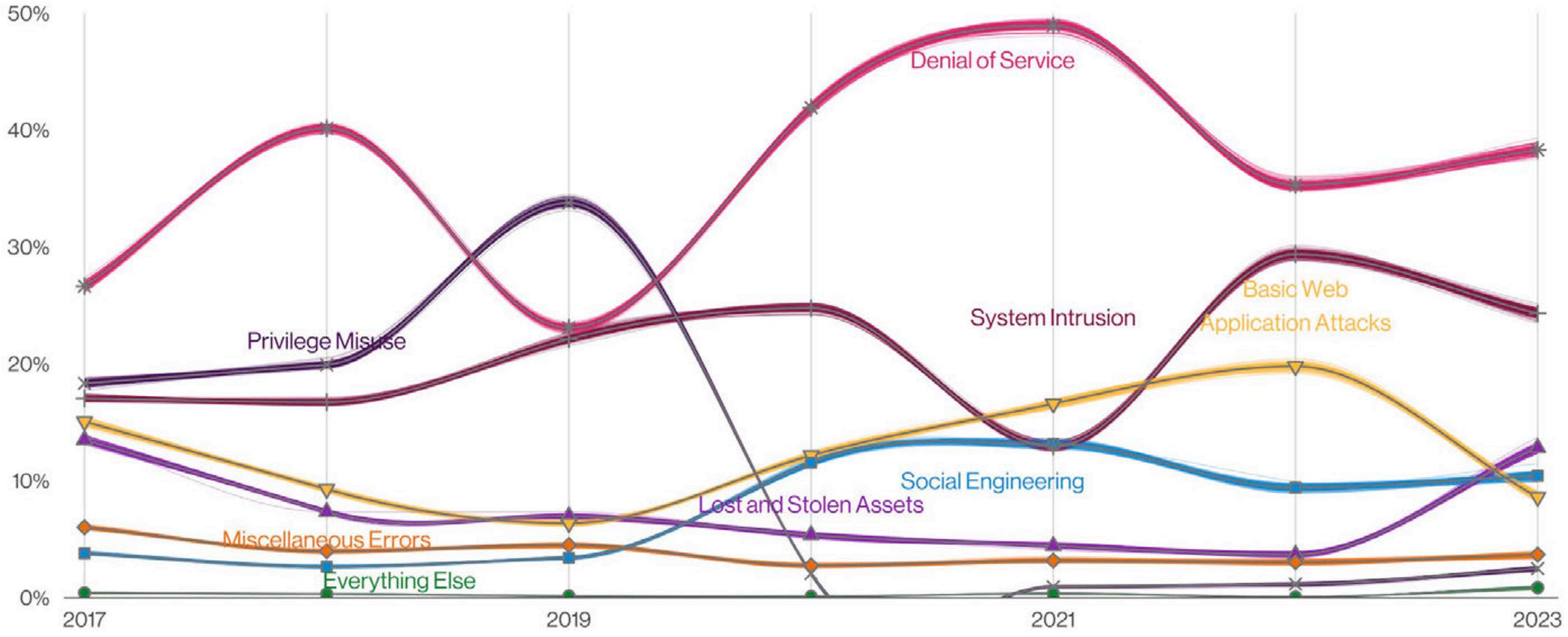


Figure 7. Patterns over time in incidents

Breach patterns

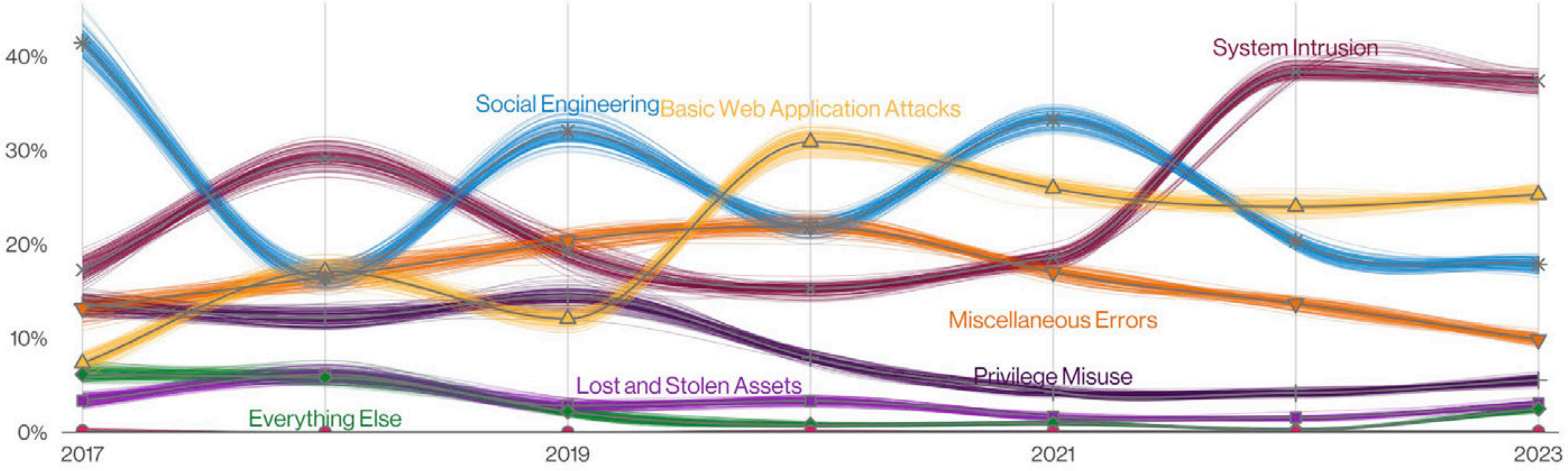


Figure 8. Patterns over time in breaches

System Intrusion

80% of System Intrusion incidents involved Ransomware as attackers continue to leverage a bevy of different techniques to compromise an organization and monetize their access.

91% of our industries have Ransomware as one of their top three actions.

While only 7% of Ransomware incidents reported losses to the FBI Internet Crime Complaint Center (IC3), the median loss more than doubled from last year to $26,000, with 95% of incidents causing losses ranging between $1 and $2.25 million.

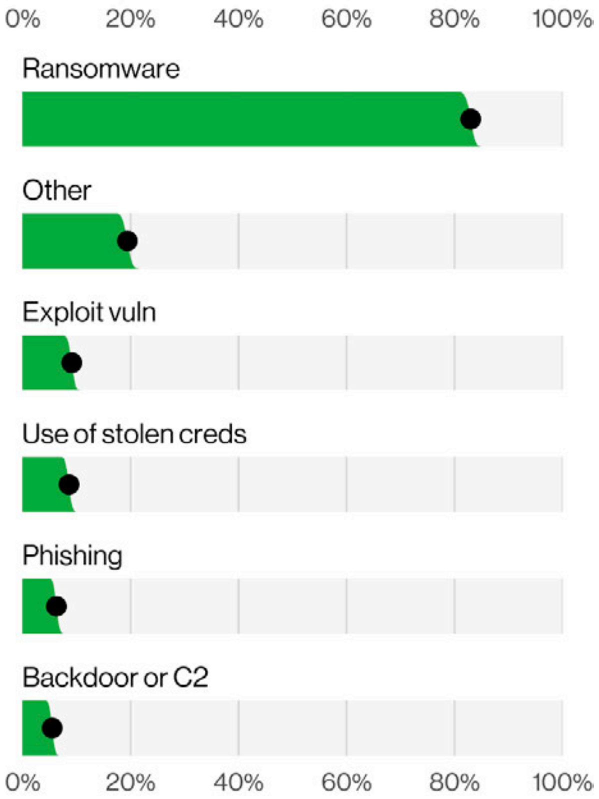


Figure 9. Action varieties in System Intrusion incidents (n=2,700)

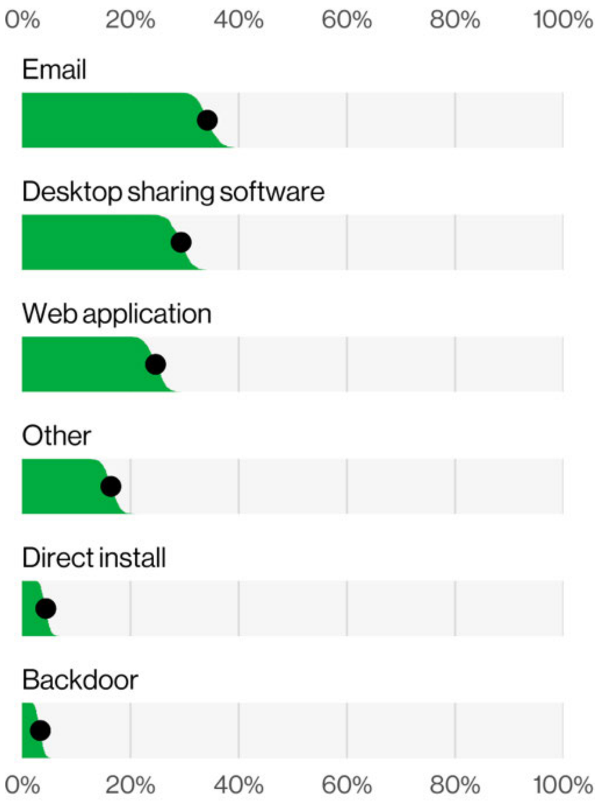


Figure 10. Action vectors for Ransomware (n=690)

Social Engineering

Social Engineering incidents have increased from the previous year largely due to the use of Pretexting—a tactic commonly used in BEC—which almost doubled since last year.

Social Engineering accounts for 17% of breaches and 10% of incidents.

Based on FBI IC3 data, the median amount stolen in a BEC has increased over the last couple of years to $50,000.

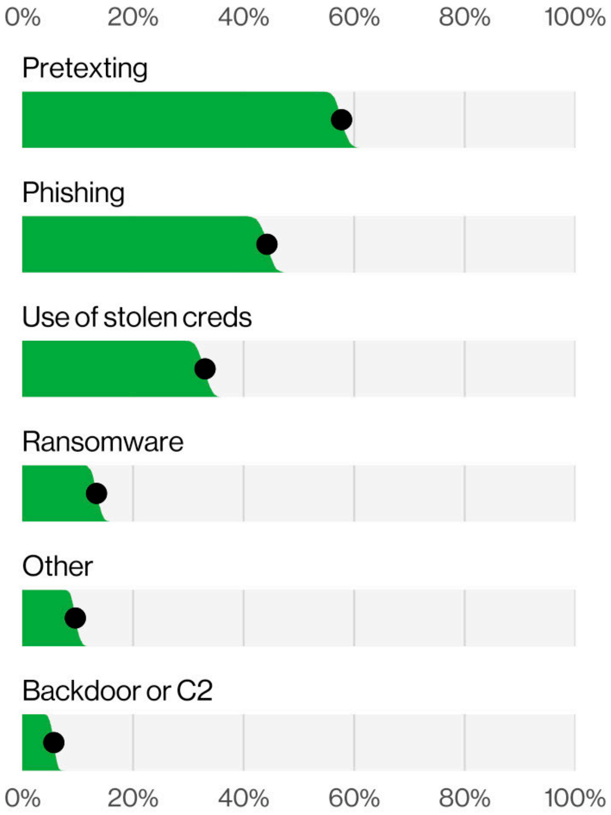


Figure 11. Action varieties in Social Engineering incidents (n=1,696)

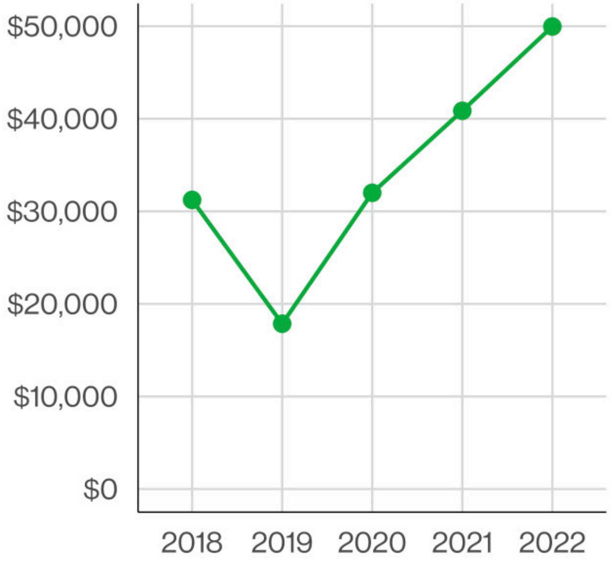


Figure 12. Median transaction size for BECs (n=73,420). Based on FBI IC3 complaints where a transaction occurred.

Basic Web Application Attacks

While representing approximately one-fourth of our dataset, Basic Web Application Attacks breaches and incidents tend to be largely driven by attacks against credentials and then leveraging those stolen credentials to access a variety
of resources.

86% of Basic Web Application Attacks breaches involve the Use
of stolen credentials.

10% of breaches in this pattern involve the Exploitation of a vulnerability.

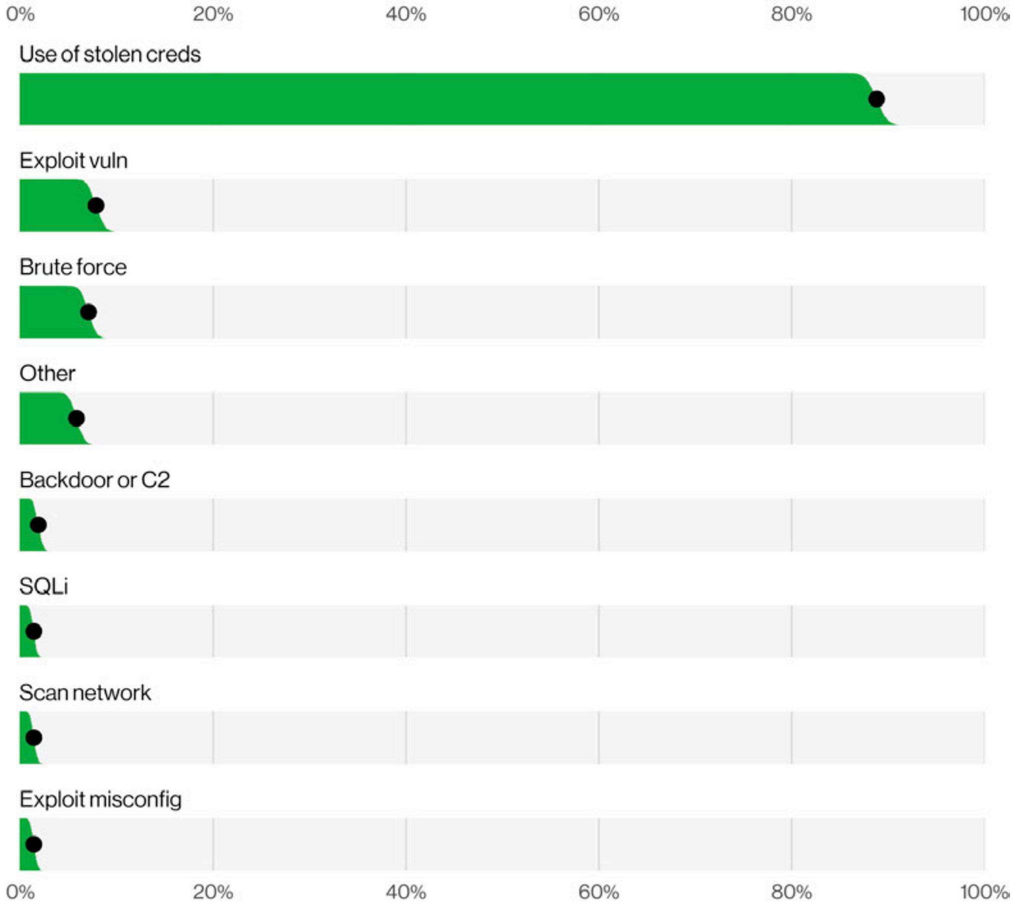


Figure 13. Top action varieties for Basic Web Application Attacks breaches (n=1,287)

Miscellaneous Errors

Error-related breaches are proportionally down to 9% as opposed to 13% last year.

The majority of errors that lead to breaches are committed by Developers and System admins.

Data compromised included Personal (89%), Medical (19%) and Bank (10%).

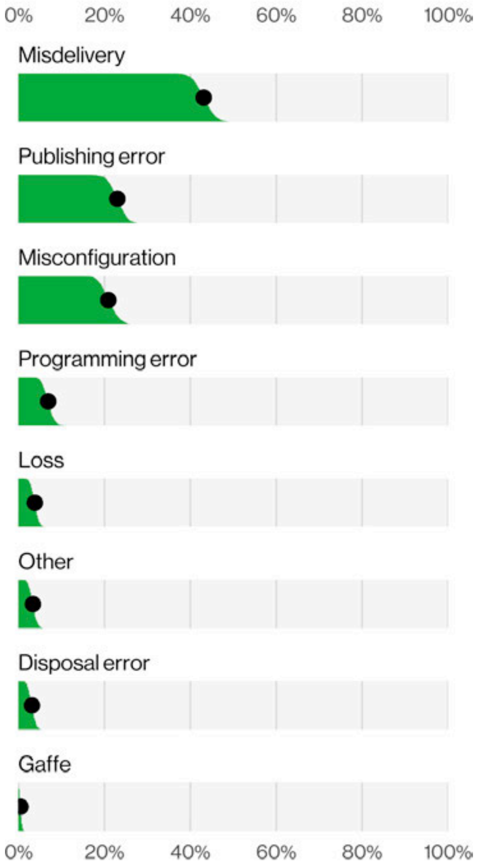


Figure 14. Top action varieties in Miscellaneous Errors breaches (n=450)

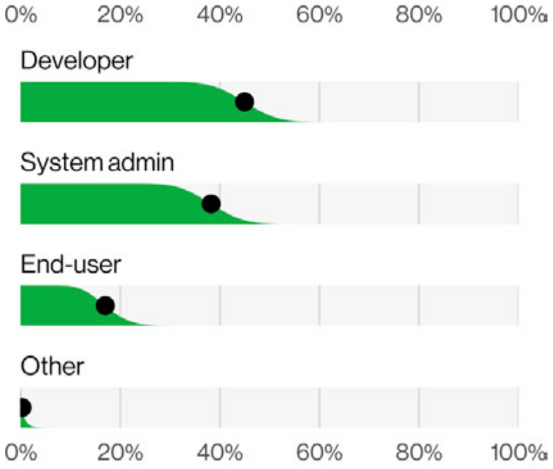
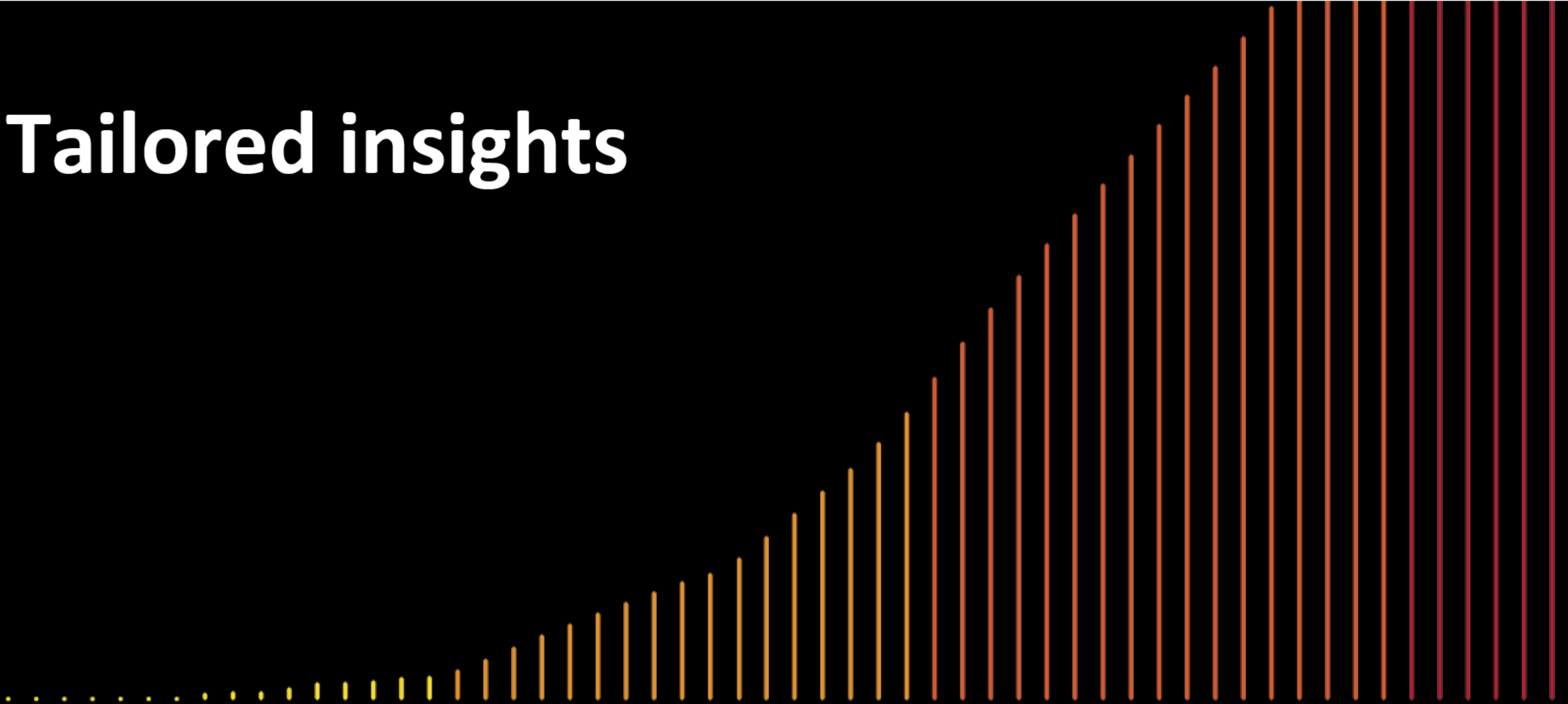


Figure 15. Top actor varieties in Miscellaneous Errors breaches (n=89)

Tailored insights



Public Administration (NAICS 92)

Frequency	3,273 incidents, 584 with confirmed data disclosure
Top patterns	System Intrusion, Lost and Stolen Assets, and Social Engineering represent 76% of breaches
Threat actors	External (85%), Internal (30%), Multiple (16%) (breaches)
Actor motives	Financial (68%), Espionage (30%), Ideology (2%) (breaches)
Data compromised	Personal (38%), Other (35%), Credentials (33%), Internal (32%) (breaches)
What is the same?	This sector continues to be targeted by Financially motivated external threat actors as well as spying Nation-states that are interested in what their rivals are doing. Personal data remains the most often stolen data type.

This is a sector where the Espionage motivation is the highest.

While ransomware continues to be an issue that disrupts the smooth running of government entities, we did see a slight decrease from last year's total.

Evidence of collusion with multiple Actor breaches was significant at 16% in this sector. Given that the overall dataset has just 2% of these kinds of cooperative breaches, it is concerning that Internal and External actors are combining forces to steal data from the public sector.

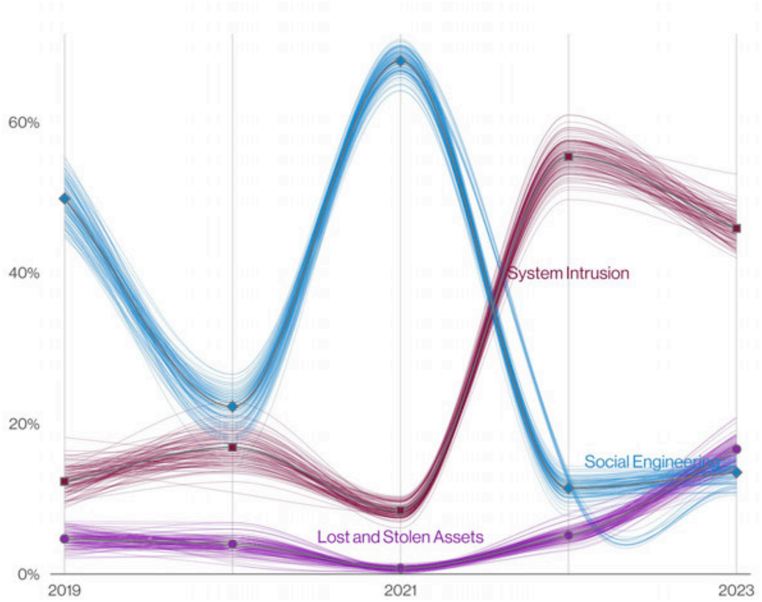


Figure 24. Patterns in Public Administration

Regions

Regions - details

Region	Frequency	Top patterns	Threat actors	Actor motives	Data compromised
APAC	699 incidents, 164 with confirmed data disclosure	Social Engineering, System Intrusion and Basic Web Application Attacks represent 93% of breaches	External (92%), Internal (9%), Partner (2%), Multiple (2%) (breaches)	Financial (61%), Espionage (39%), Convenience (2%), Grudge (2%), Secondary (1%) (breaches)	Internal (56%), Secrets (42%), Other (33%), Credentials (29%) (breaches)
EMEA	2,557 incidents, 637 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 97% of breaches	External (98%), Internal (2%), Multiple (1%) (breaches)	Financial (91%), Espionage (8%), Ideology (1%), Fun (1%) (breaches)	Credentials (53%), Internal (37%), System (35%), Other (15%) (breaches)
LAC	535 incidents, 65 with confirmed data disclosure	System Intrusion, Social Engineering and Basic Web Application Attacks represent 94% of breaches	External (95%), Internal (5%), Partner (2%), Multiple (2%) (breaches)	Financial (93%), Espionage (11%), Ideology (2%) (breaches)	System (55%), Internal (32%), Classified (23%), Credentials (23%), Other (19%) (breaches)
NA	9,036 incidents, 1,924 with confirmed data disclosure	System Intrusion, Basic Web Application Attacks and Social Engineering represent 85% of breaches	External (94%), Internal (12%), Multiple (9%), Partner (2%) (breaches)	Financial (99%), Espionage (1%), Grudge (1%) (breaches)	Credentials (67%), Internal (50%), Personal (38%), Other (24%) (breaches)

Questions?

DBIR: verizon.com/dbir
Email: dbir@verizon.com

If you are interested in becoming a contributor to the annual Verizon DBIR (and we hope you are), the process is very easy and straightforward. Please email us at dbircontributor@verizon.com.

verizon

Final thoughts

Rachel Dixon
Deputy Commissioner, Privacy and Data Protection

OVIC
Office of the Victorian
Information Commissioner

Deputy Commissioner’s Final Thoughts

Deputy Commissioner
Privacy and Data Protection

Find out more

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

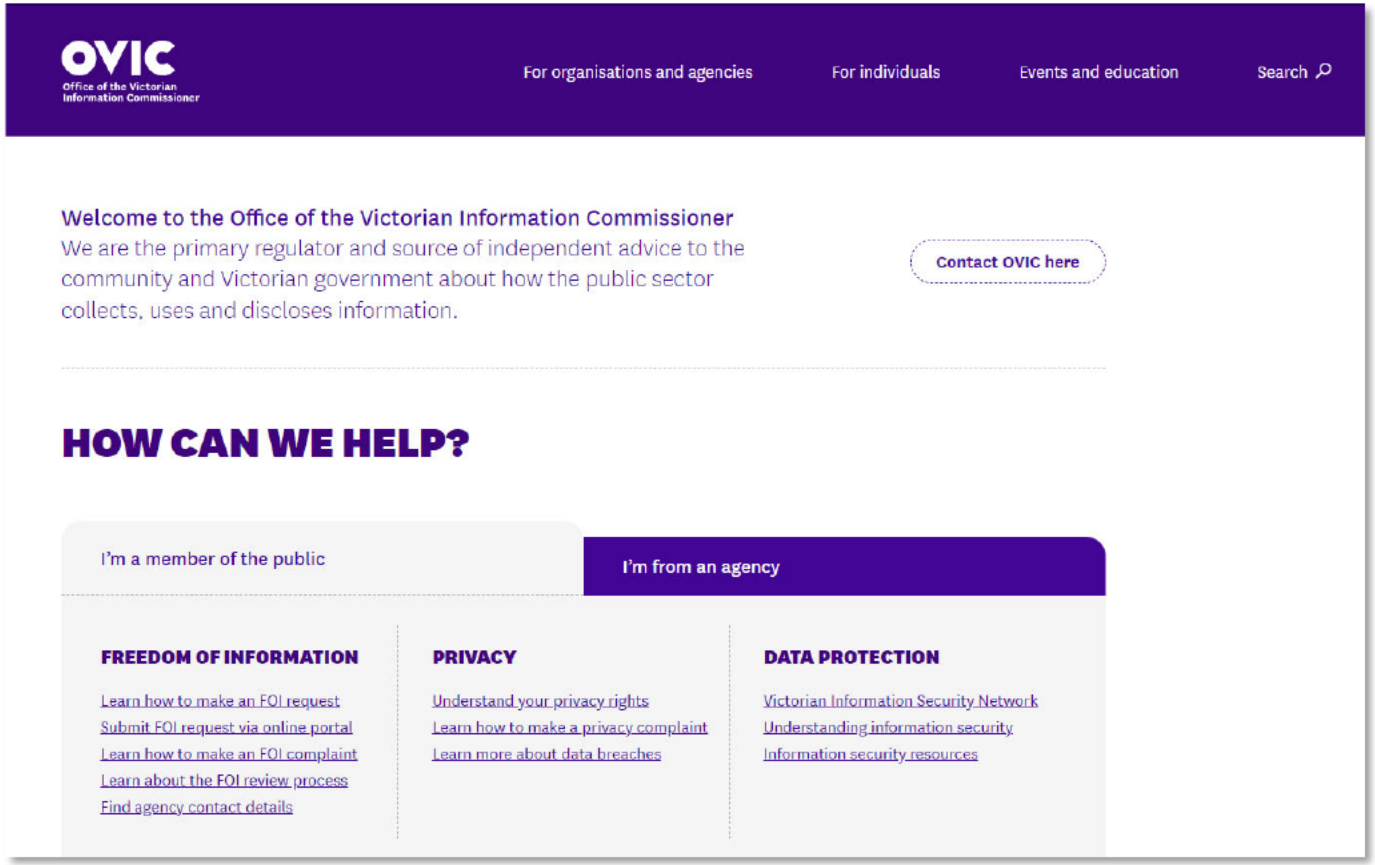
ovic.vic.gov.au

Contact the Information Security Unit by emailing

security@ovic.vic.gov.au

incidents@ovic.vic.gov.au

Or call **1300 00 OVIC**



OVIC
Office of the Victorian Information Commissioner
For organisations and agencies
For individuals
Events and education
Search

Welcome to the Office of the Victorian Information Commissioner

We are the primary regulator and source of independent advice to the community and Victorian government about how the public sector collects, uses and discloses information.

HOW CAN WE HELP?

I'm a member of the public
I'm from an agency

FREEDOM OF INFORMATION

- Learn how to make an FOI request
- Submit FOI request via online portal
- Learn how to make an FOI complaint
- Learn about the FOI review process
- Find agency contact details

PRIVACY

- Understand your privacy rights
- Learn how to make a privacy complaint
- Learn more about data breaches

DATA PROTECTION

- Victorian Information Security Network
- Understanding information security
- Information security resources

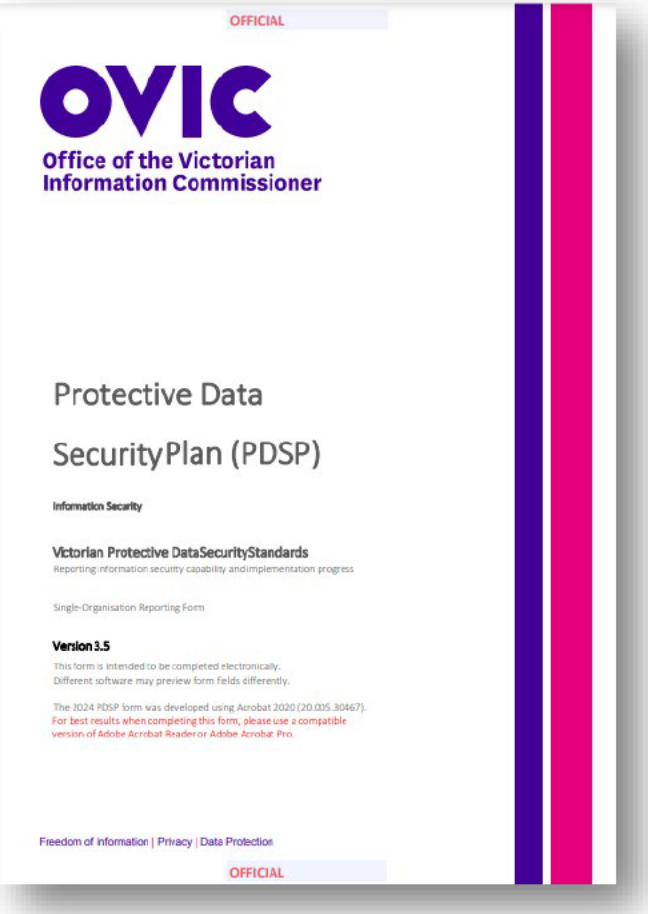
Protective Data Security Plan V3.5 released – April 2024

The 2024 Protective Data Security Plan (PDSP) form has recently been updated.

OVIC identified minor issues with version 3.4 of the PDSP form and has **released a version 3.5 as a replacement.**

If you have downloaded a copy of the PDSP form before 9th of April 2024, please ensure you download and use version 3.5 of the PDSP form.

To download a copy of Version 3.5 of the 2024 PDSP form navigate here - https://go.vic.gov.au/4cNpVEG



OFFICIAL

OVIC
Office of the Victorian
Information Commissioner

Protective Data

SecurityPlan (PDSP)

Information Security

Victorian Protective DataSecurityStandards
Reporting information security capability andimplementation progress

Single-Organisation Reporting Form

Version 3.5
This form is intended to be completed electronically.
Different software may preview form fields differently.

The 2024 PDSP form was developed using Acrobat 2020 (20.005.30467).
For best results when completing this form, please use a compatible version of Adobe Acrobat Reader or Adobe Acrobat Pro.

Freedom of Information | Privacy | Data Protection

OFFICIAL