Australian Government

Office of the Australian Information Commissioner

Notifiable data breaches report

July to December 2024

13 May 2025

OAIC

Contents

The OAIC has published a blog post as a companion to this report. The blog post draws attention to common attack methods, how the OAIC responds to reported breaches and how we will report data breach statistics in the future.

Statistics notes

- This paper captures notifications received under the Notifiable Data Breaches scheme from 1 July to 31 December 2024.
- Statistics in this paper are current as of 11 February 2025, other than data for the 'Consumer Data Right data' category in chart 4, which is current as of 11 March 2025. Some data breach notifications are being assessed, and adjustments may be made to related statistics. This may affect statistics for the period July to December 2024 published in future reports. Similarly, statistics from before July 2024 in this paper may differ from those published in other publications.
- Statistical comparisons are to the period 1 January to 30 June 2024 unless otherwise indicated.
- Percentages in charts may not total 100% due to rounding.
- Where data breaches affect multiple entities, the OAIC may receive multiple notifications relating to the same incident. Notifications relating to the same incident are counted as a single notification (referred to as a 'primary notification') in this report to avoid information being duplicated, unless otherwise specified. The volume of secondary notifications may be indicative of the level of multi-party breach reporting. Secondary notifications may relate to a primary notification received in a prior reporting period.
- The source of any given breach is based on information provided by the reporting entity. Where more than one source has been identified or is possible, the dominant or most likely source has been selected. Source of breach categories are defined in the glossary.
- Notifications made under the *My Health Records Act 2012* (Cth) are not included as they are subject to specific notification requirements set out in that legislation.

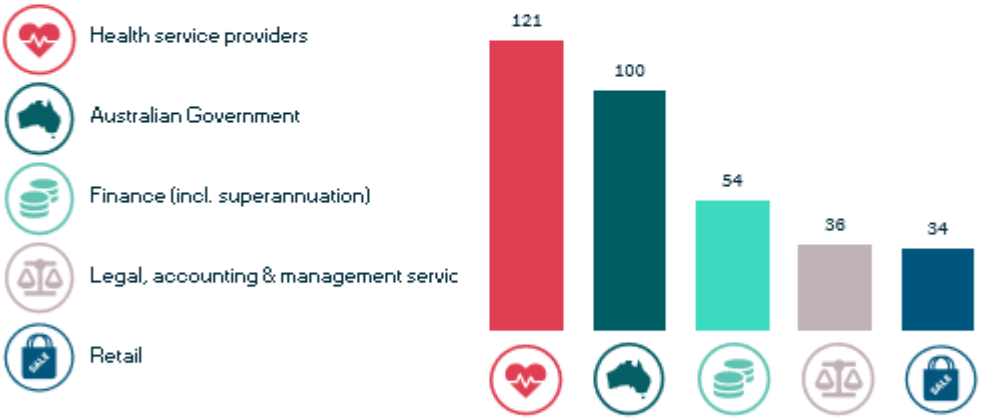
Snapshot

↑ **595**
notifications

Up 15% compared to January – June 2024

Some data breaches affect more than one entity. The OAIC received an additional 20 secondary data breach notifications

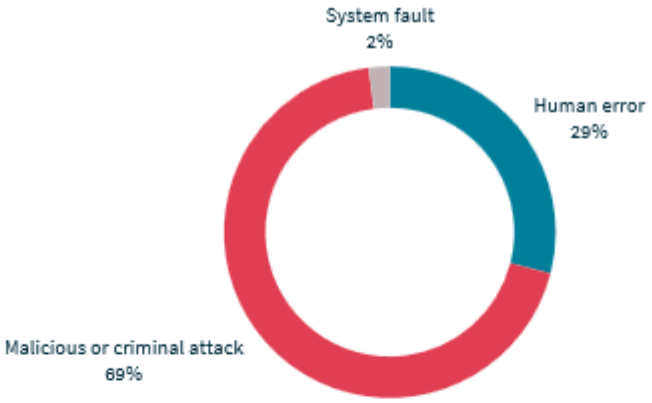
Top 5 sectors to notify data breaches



63%

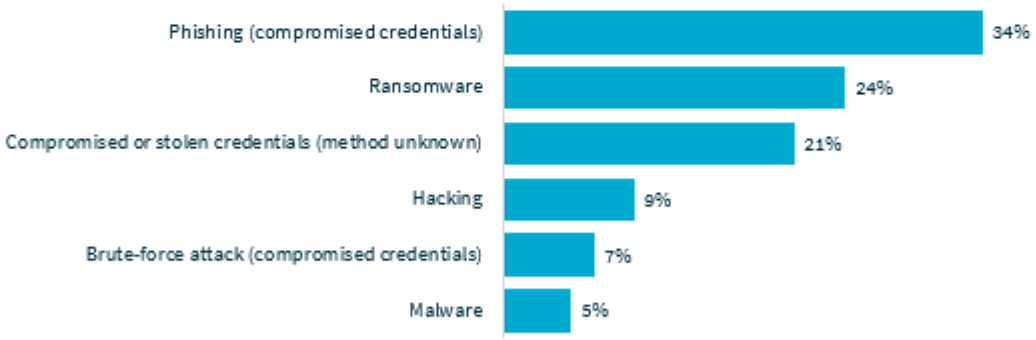
of data breaches affected 100 people or fewer

Sources of data breaches



42% of all data breaches resulted from cyber security incidents (247 notifications; 61% of malicious or criminal attacks)

Cyber incident breakdown

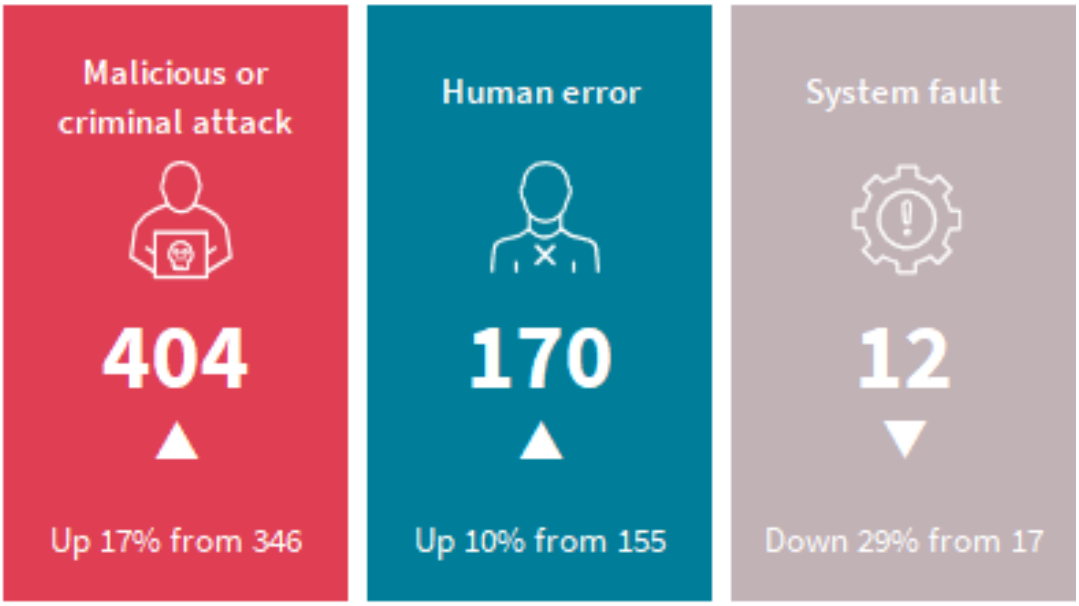


Top causes of human error breaches

PI sent to wrong recipient (email) 42%

Unauthorised disclosure (unintended release or publication) 23%

Failure to use BCC when sending email 8%



All graphics, charts and tables depicting sources of breaches include only notifications classified as ‘Malicious or criminal attack’, ‘Human error’ or ‘System fault’. Notifications where the source of breach was categorised as ‘Currently unknown’ or ‘Other’ have been excluded.

Statistics

Notifications received

Table 1 – Notifications received in 2024

Reporting period	Number of notifications
January to June 2024	518
July to December 2024	**595**
Total	**1,113**

Chart 1 – Notifications received by month from January 2023 to December 2024

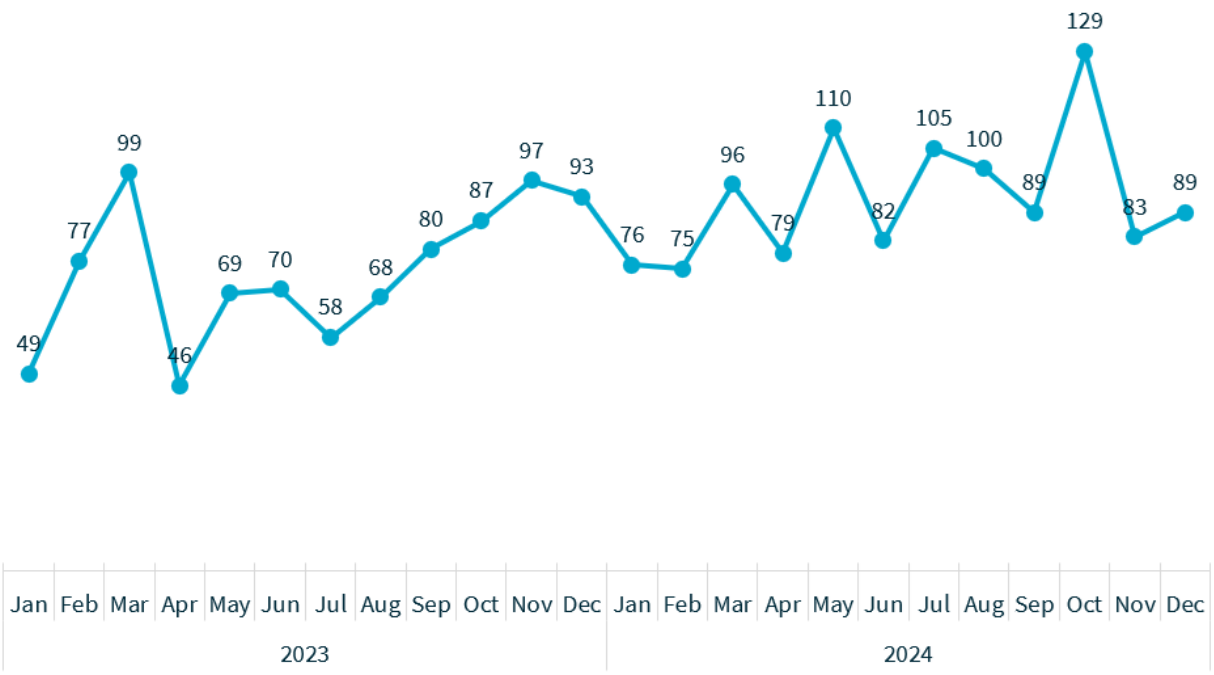
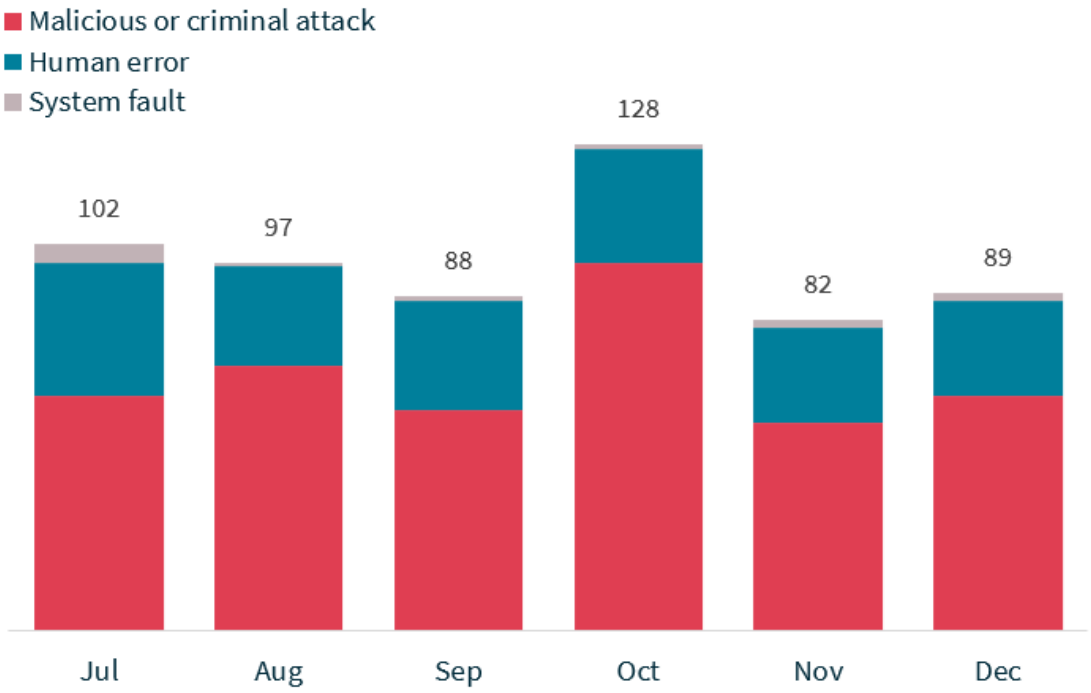
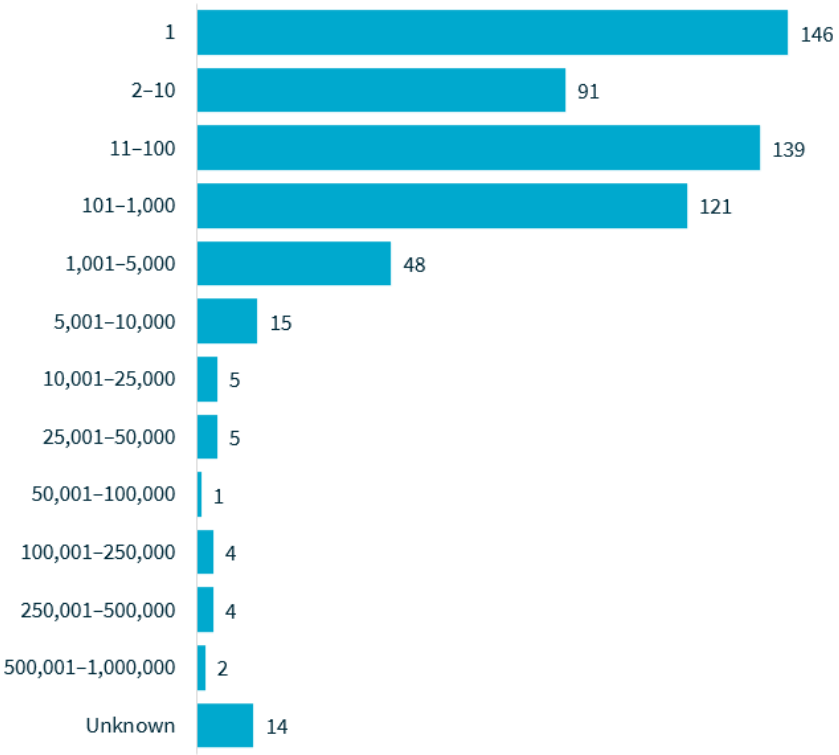


Chart 2 – Notifications received by month showing the sources of breaches



Number of individuals affected by breaches

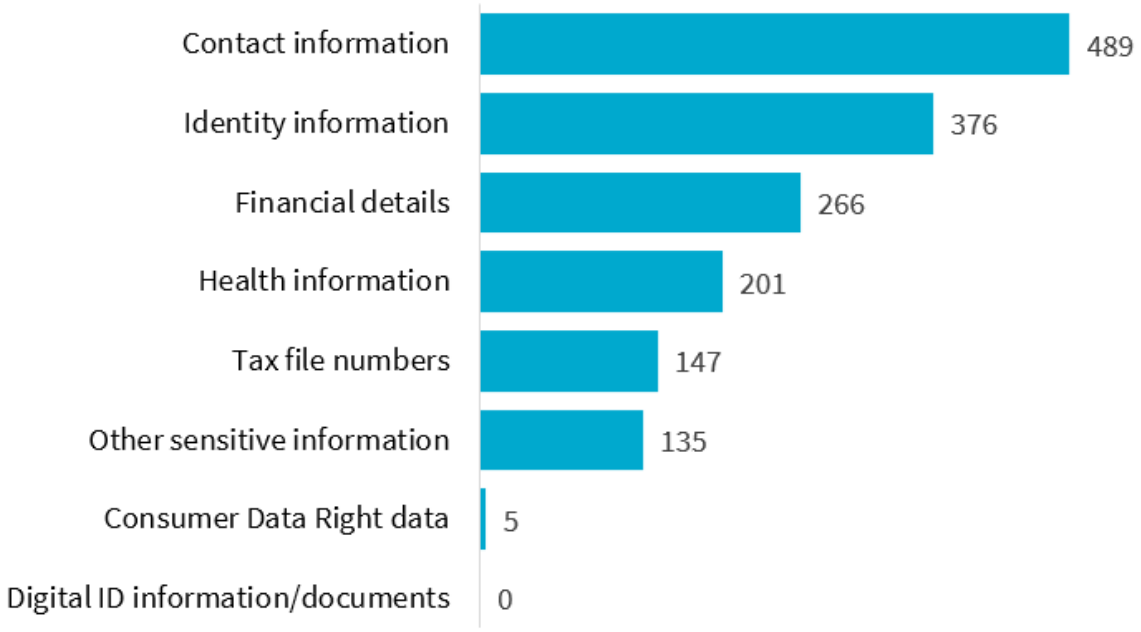
Chart 3 – Number of individuals worldwide affected by breaches



These figures reflect the number of individuals worldwide whose personal information was compromised in data breaches notified to the OAIC, as estimated by notifying entities.

Kinds of personal information involved in breaches

Chart 4 – Kinds of personal information involved in breaches

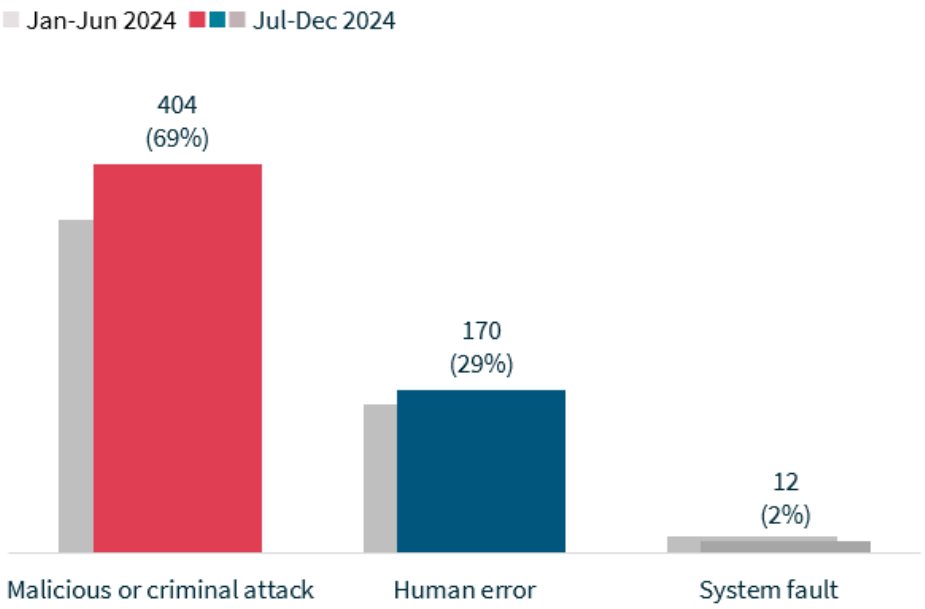


Data breaches may involve more than one kind of personal information.

The data for the 'Consumer Data Right data' category is current as of 11 March 2025.

Source of breaches

Chart 5 - Source of data breaches



Malicious or criminal attacks

Chart 6 – Causes of breaches resulting from malicious or criminal attacks

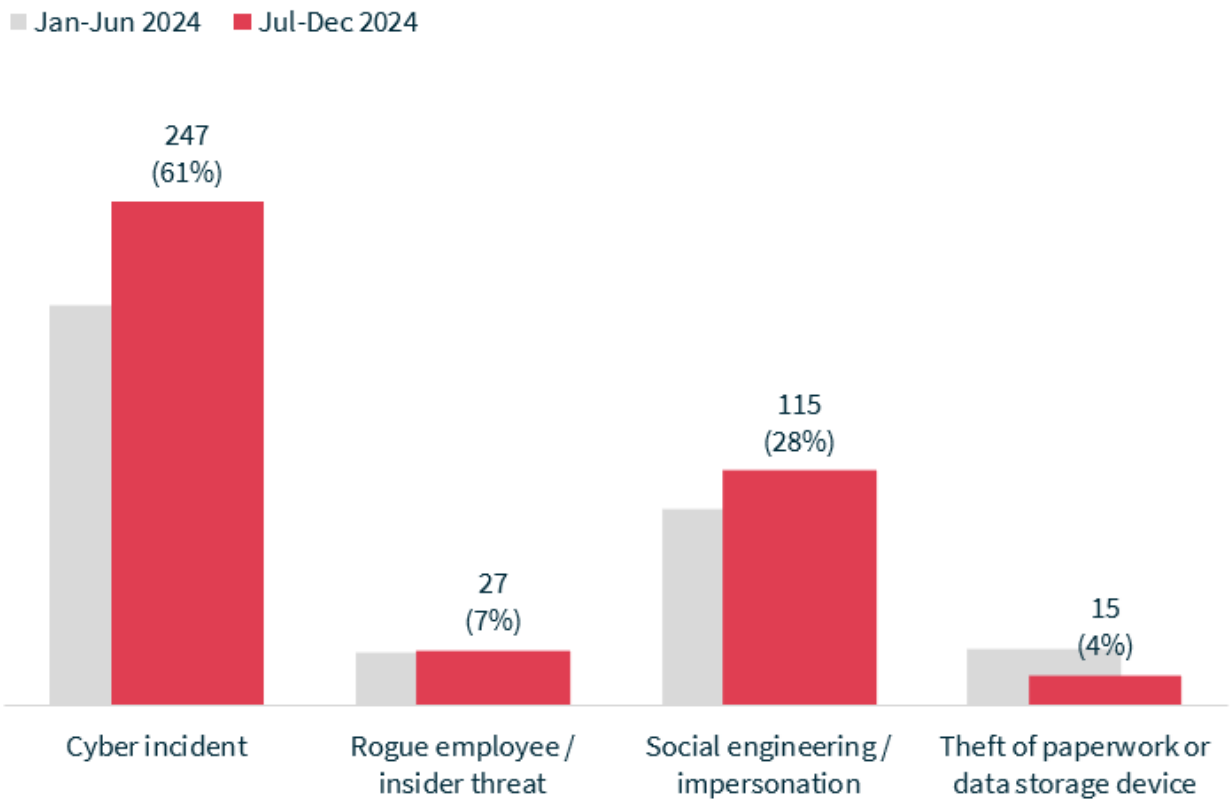


Table 2 – Malicious or criminal attack breakdown by median and average numbers of affected individuals worldwide

Source of breach	Number of notifications	Median number of affected individuals	Average number of affected individuals
Cyber incident	247	182	15,357
Social engineering / impersonation	115	41	1,683
Rogue employee / insider threat	27	18	416
Theft of paperwork or data storage device	15	19	168
Total	**404**	**81**	**9,655**

Cyber incidents

Chart 7 - Cyber incident breakdown

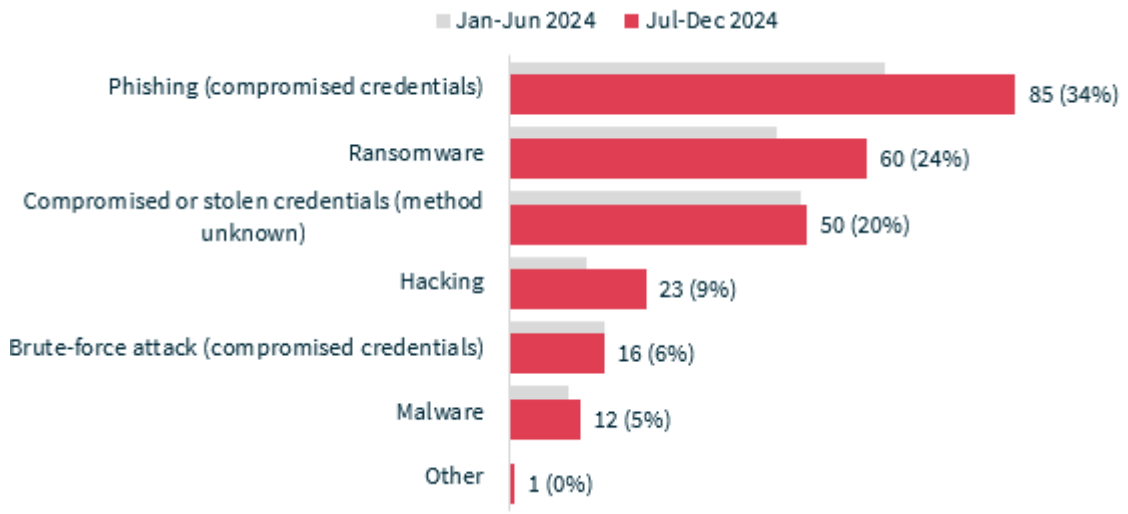


Table 3 – Cyber incident breakdown by median and average numbers of affected individuals worldwide

Source of breach	Number of notifications	Median number of affected individuals	Average number of affected individuals
Malware	12	2,229	6,358
Ransomware	60	819	26,878
Hacking	23	329	19,924
Brute-force attack (compromised credentials)	16	224	21,135
Compromised or stolen credentials (method unknown)	51	89	24,672
Phishing (compromised credentials)	84	77	1,220
Other	1	50	50
Total	**247**	**182**	**15,357**

Human error

Chart 8 – Human error breakdown

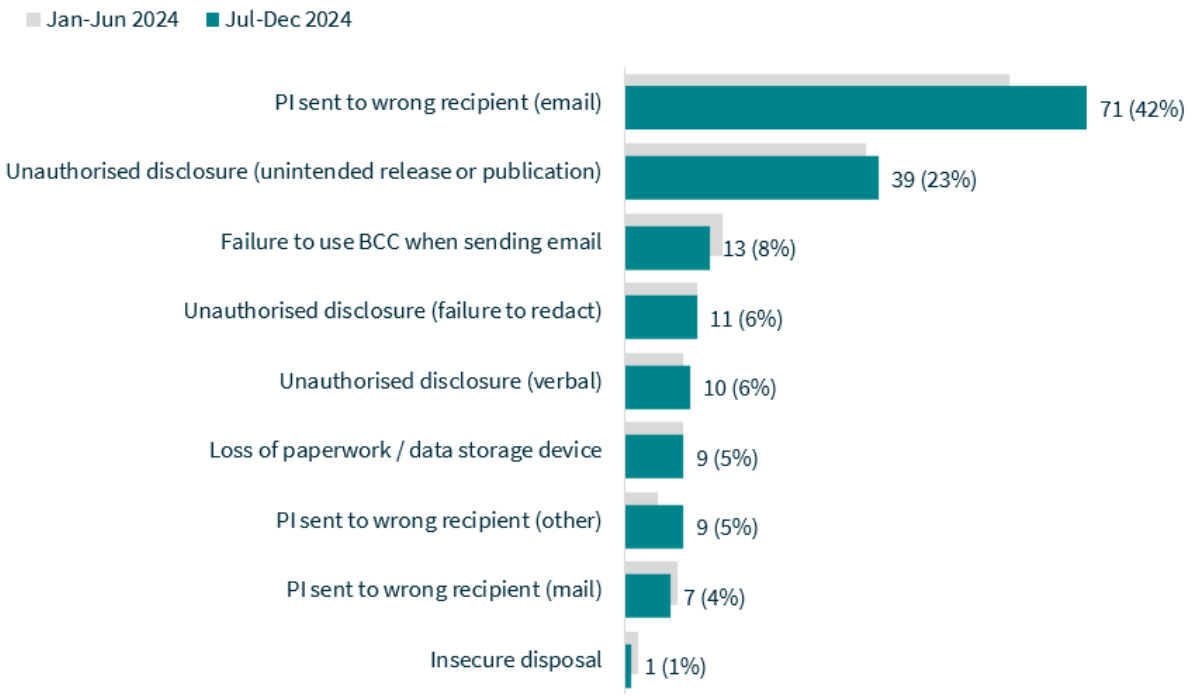
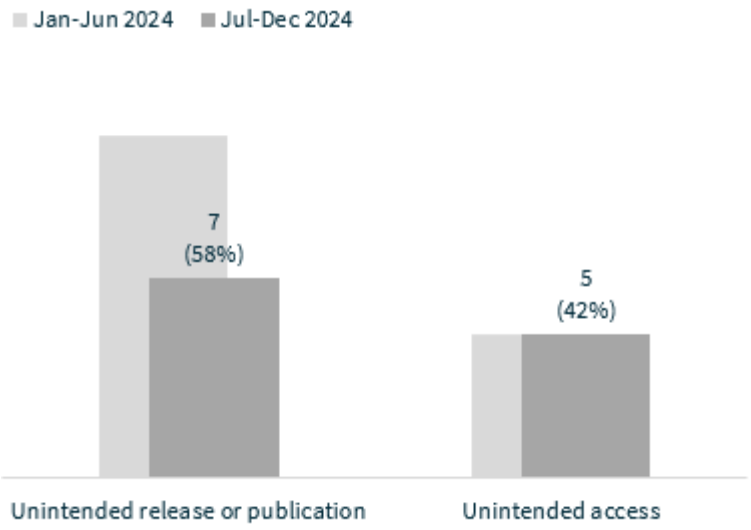


Table 4 – Human error breakdown by median and average numbers of affected individuals worldwide

Source of breach	Number of notifications	Median number of affected individuals	Average number of affected individuals
Insecure disposal	1	150	150
Failure to use BCC when sending email	13	47	244
Loss of paperwork / data storage device	9	2	23
Unauthorised disclosure (unintended release or publication)	39	1	211
Unauthorised disclosure (failure to redact)	11	1	26
PI sent to wrong recipient (email)	71	1	17
PI sent to wrong recipient (other)	9	1	10
PI sent to wrong recipient (mail)	7	1	1
Unauthorised disclosure (verbal)	10	1	1
Total	**170**	**1**	**79**

System faults

Chart 9 – System fault notifications



Time taken to identify breaches

This section conveys the time between an incident occurring and the entity becoming aware of it. The figures do not relate to the time taken by the entity to assess whether an incident qualified as an eligible data breach.

For notifications in the 'unknown' category, the entity was unable to identify the date the breach occurred.

Chart 10 – Time taken to identify breaches

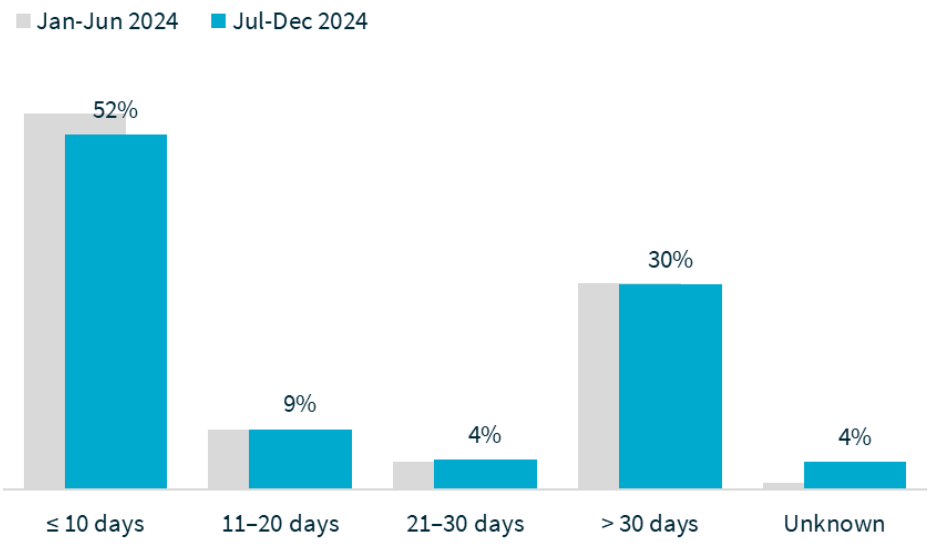
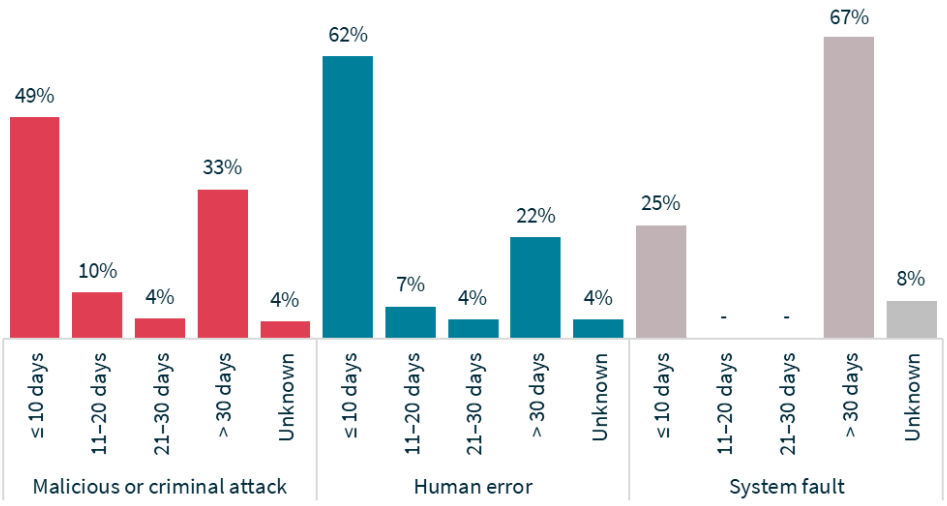


Chart 11 - Time taken to identify breaches by source of breach



Time taken to notify the OAIC of breaches

The figures in this section relate to the time between when an entity became aware of an incident and when they notified the OAIC. They do not relate to the time between when the entity determined the incident to be an eligible data breach and when they notified the OAIC.

Chart 12 – Time taken to notify the OAIC of breaches

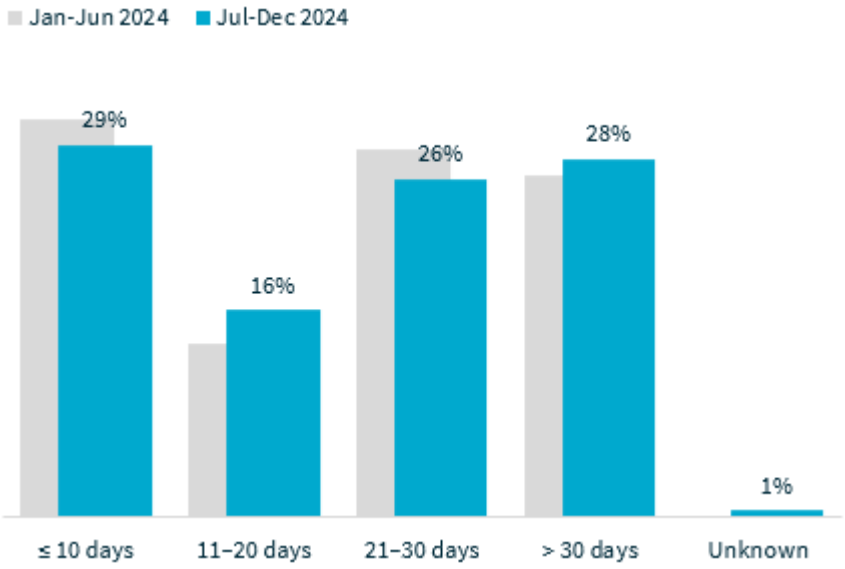
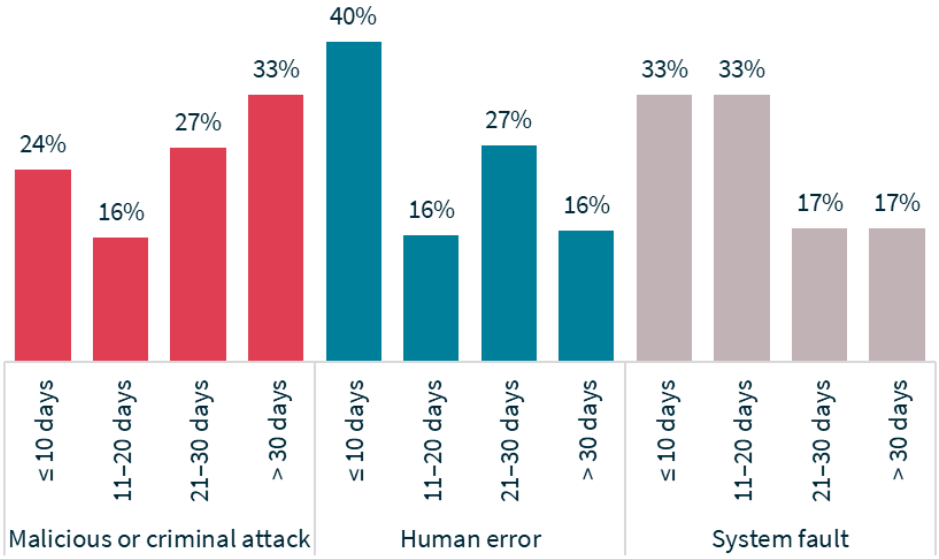


Chart 13 – Time taken to notify the OAIC of breaches by source of breach



Comparison of top 5 sectors

Table 5 – Top 5 sectors by notifications

Sector	Number of notifications	Percentage of all notifications received
Health service providers	121	20%
Australian Government	100	17%
Finance (incl. superannuation)	54	9%
Legal, accounting and management services	36	6%
Retail	34	6%
Total	**345**	**58%**

A health service provider generally includes any private sector entity that provides a health service within the meaning of s 6FB of the *Privacy Act 1988*, regardless of annual turnover.

The finance sector includes banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

Chart 14 – Source of breaches – Top 5 sectors

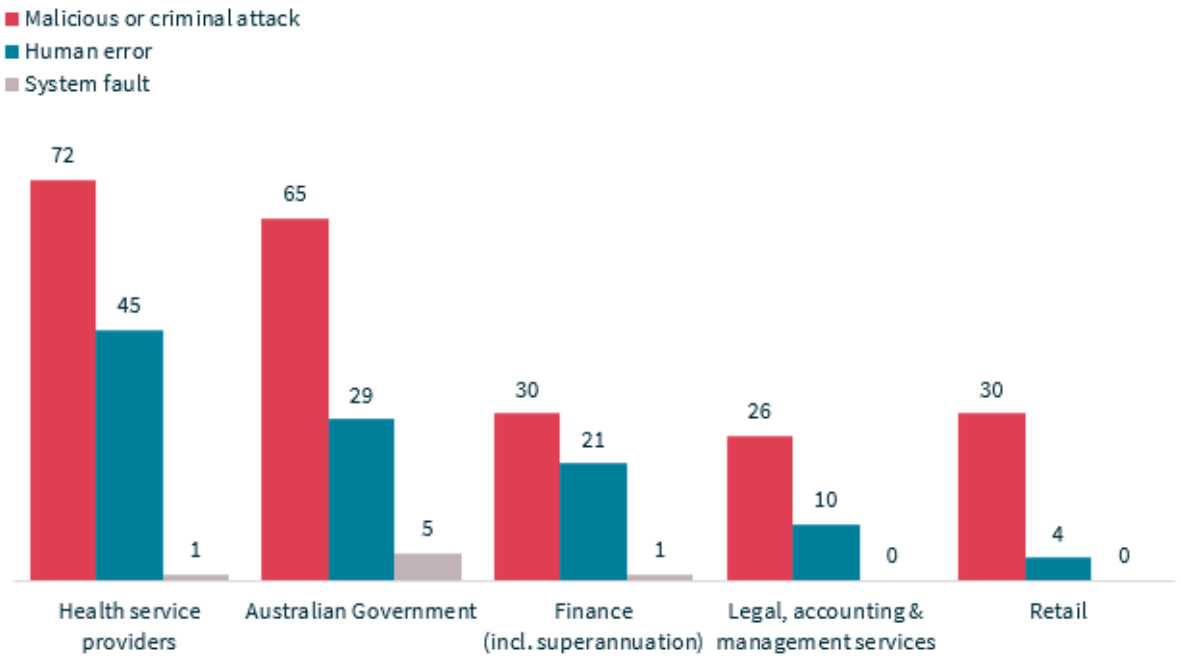


Chart 15 – Source of breaches – Top 5 sectors

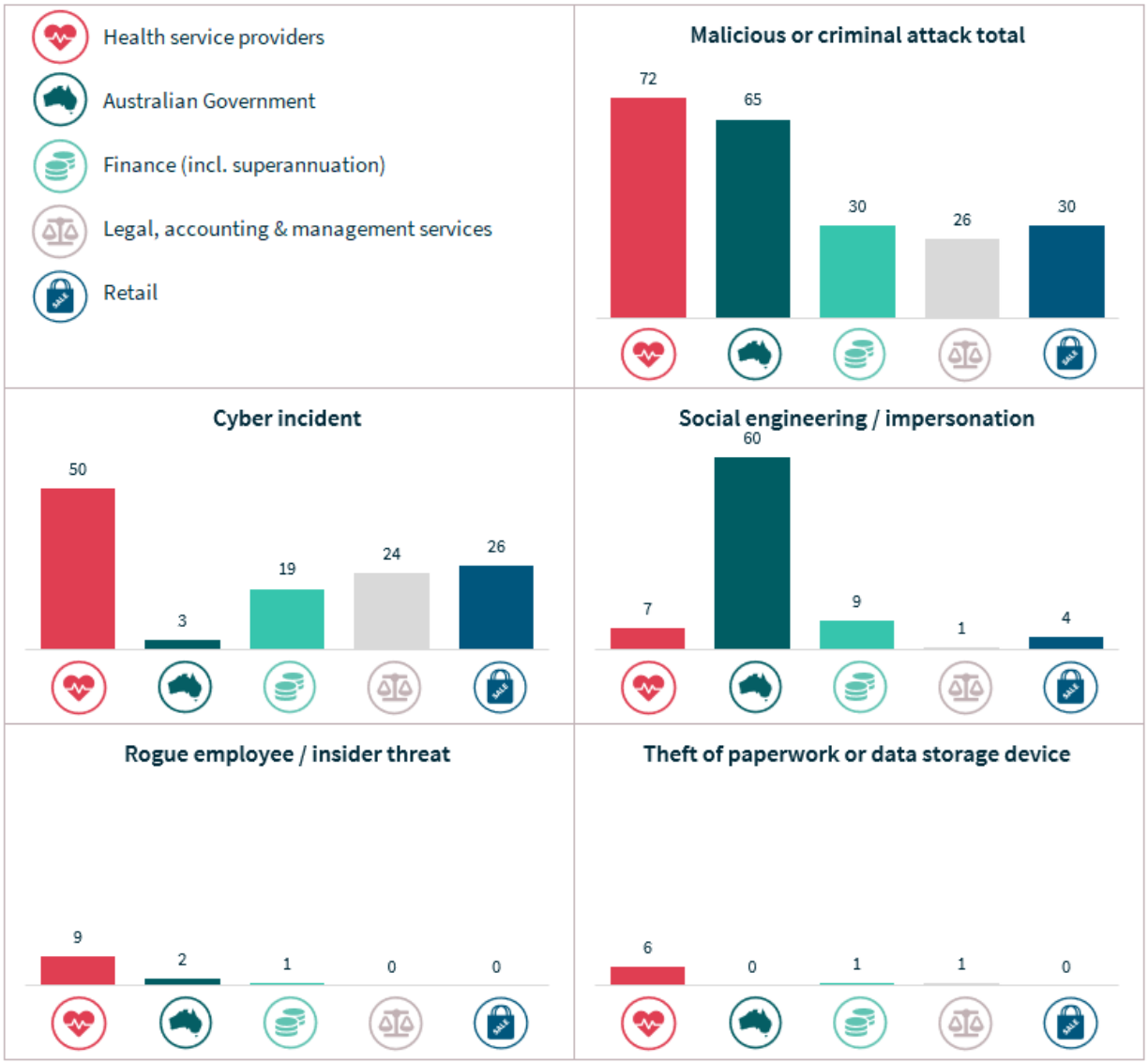


Chart 16 – Cyber incident breakdown – Top 5 sectors

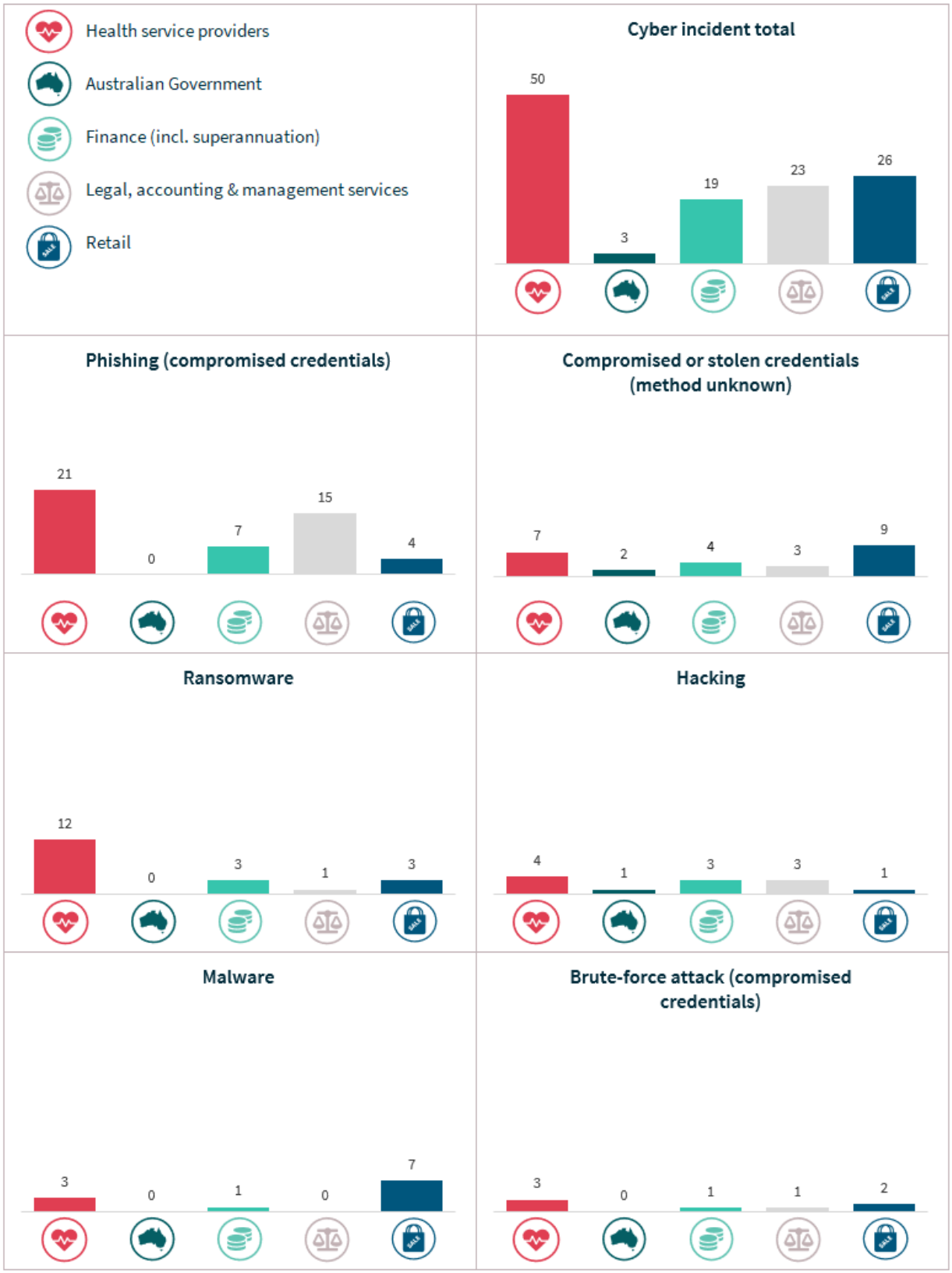
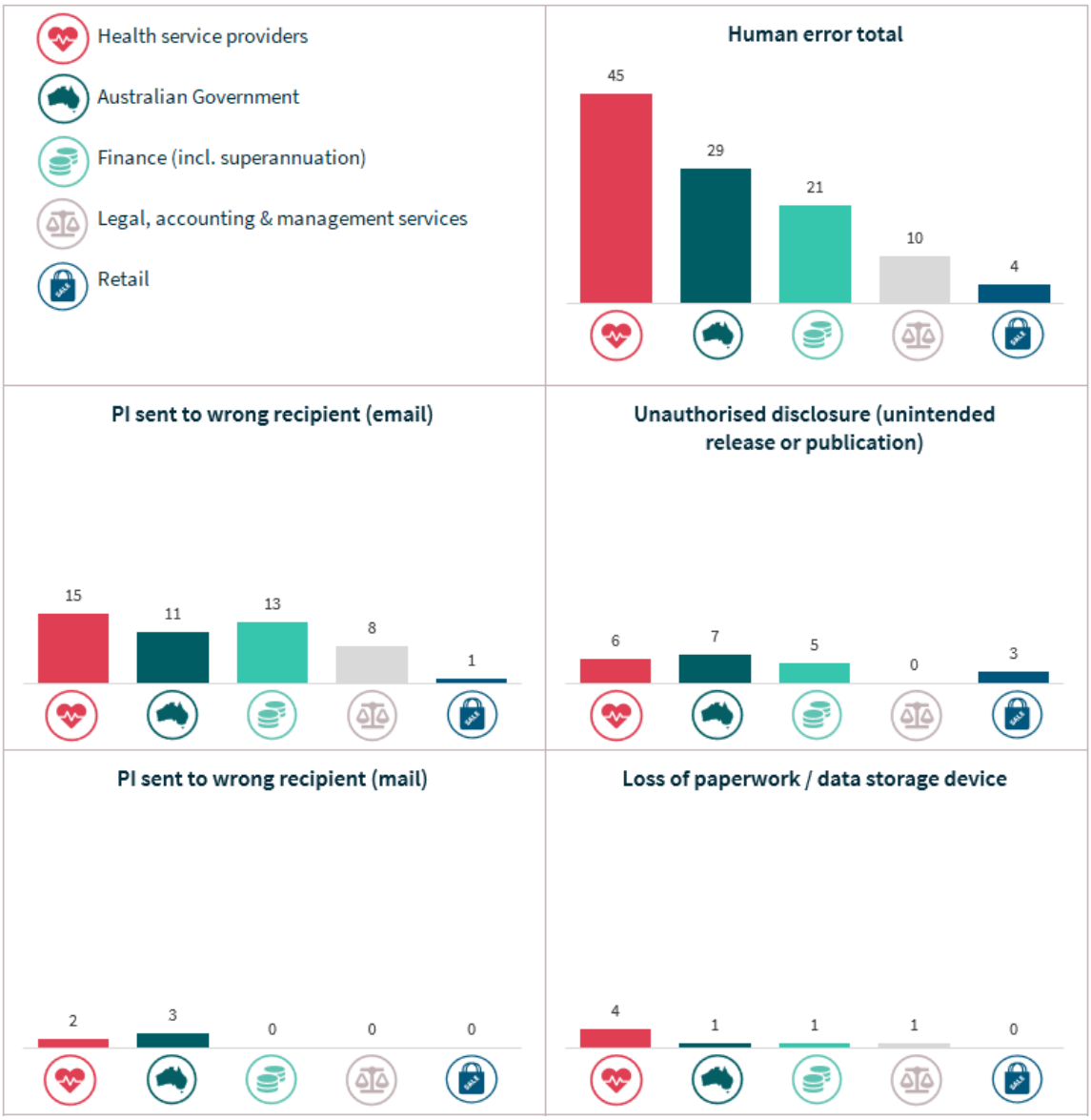


Chart 17 – Human error breakdown – Top 5 sectors




Unauthorised disclosure (verbal)
4
2
1
0
0
Failure to use BCC when sending email
5
1
0
0
0
Unauthorised disclosure (failure to redact)
5
1
0
0
0
PI sent to wrong recipient (other)
3
3
1
1
0
Insecure disposal
1
0
0
0
0
PI sent to wrong recipient (fax)
0
0
0
0
0

Chart 18 – System fault breakdown – Top 5 sectors

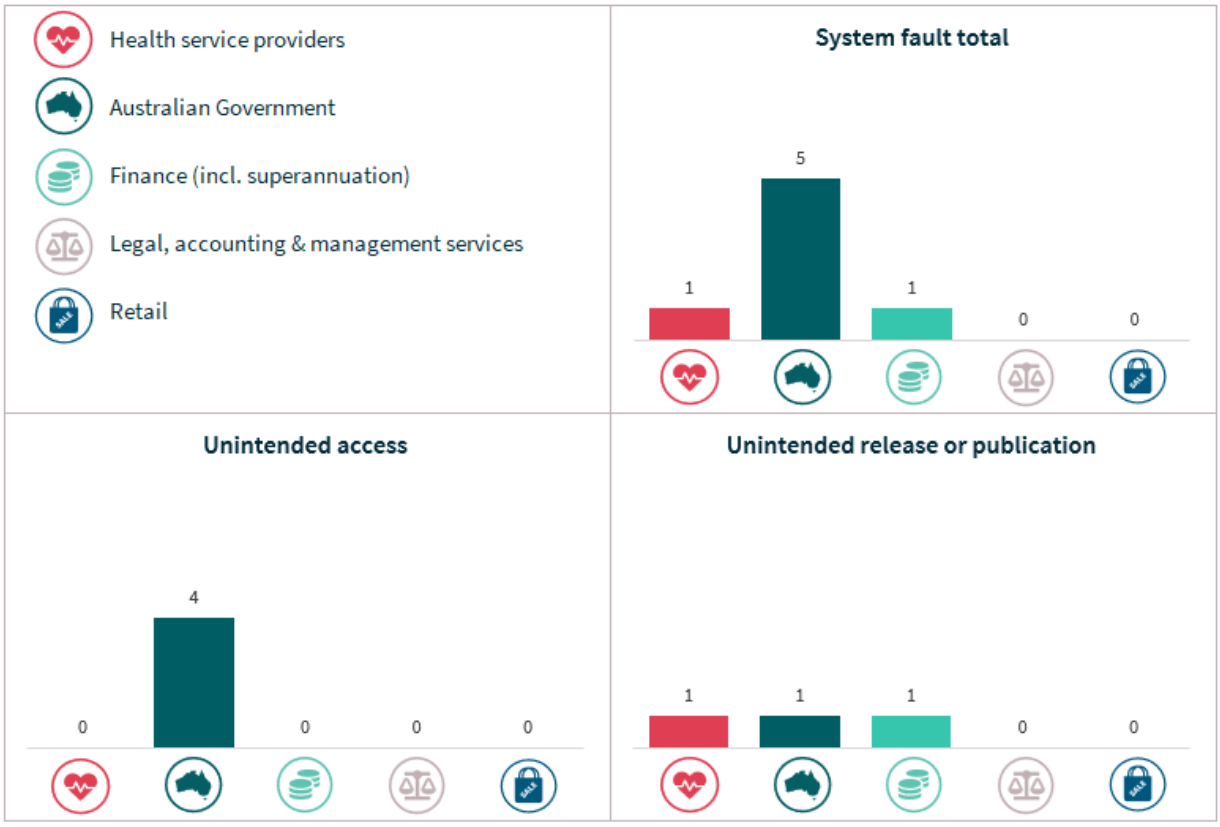
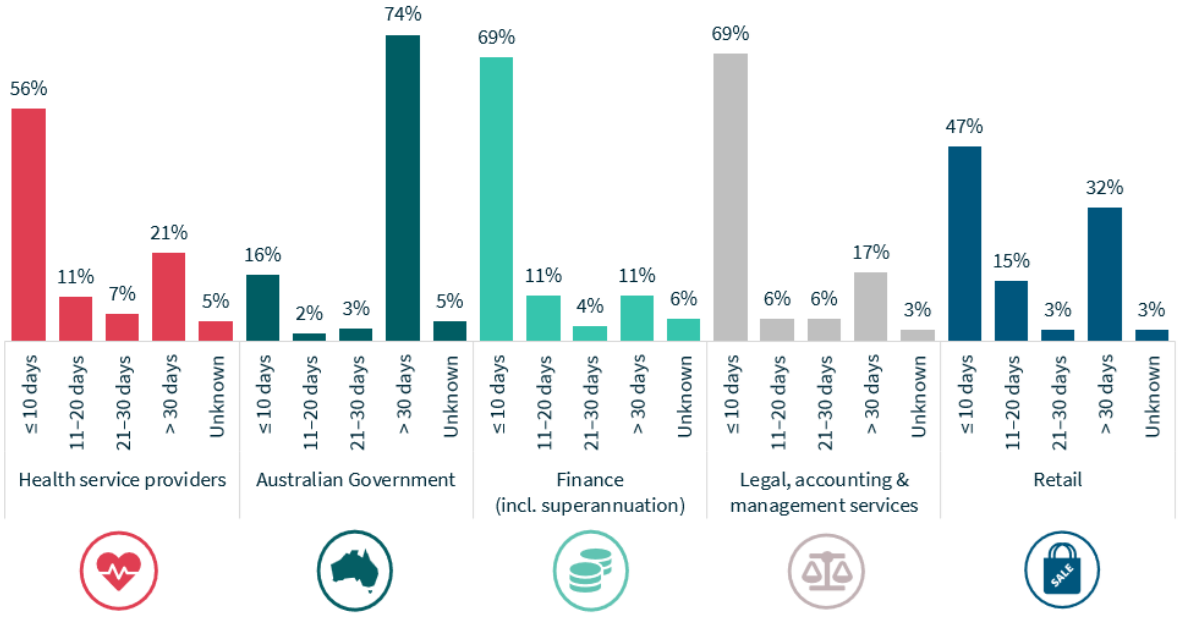
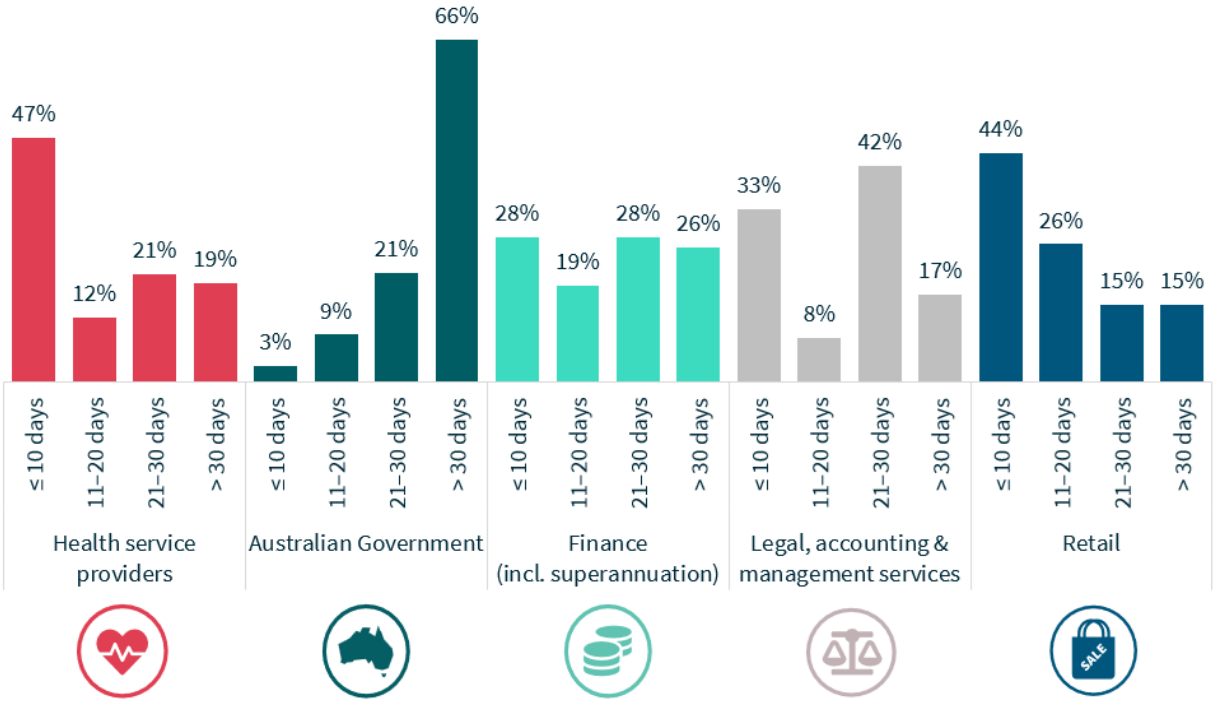


Chart 19 – Time taken to identify breaches – Top 5 sectors



For notifications in the 'unknown' category, the entity was unable to identify the date the breach occurred.

Chart 20 – Time taken to notify breaches – Top 5 sectors



For notifications in the 'unknown' category, the entity was unable to advise the OAIC the date it became aware of the incident.

Glossary

Term	Definition
Contact information	Information that is used to contact an individual, for example, a home address, phone number or email address
Eligible data breach	An eligible data breach occurs when: • Personal information has been lost, or accessed or disclosed without authorisation • It is likely to result in serious harm to one or more individual • The organisation or Australian Government agency has not been able to prevent the likely risk of serious harm with remedial action
Financial details	Information relating to an individual's finances, for example, bank account or credit card numbers
Health information	As defined in s 6 of the *Privacy Act 1988 (Cth)*
Identity information	Information that is used to confirm an individual's identity, such as a passport number, driver licence number or other government identifier
Other sensitive information	Sensitive information, other than health information, as defined in s 6 of the Privacy Act, for example, sexual orientation, political or religious views
Personal information (PI)	Information or an opinion about an identified individual or an individual who is reasonably identifiable
Sensitive information	Sensitive information is personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record

Term	Definition
	• health or genetic information • some aspects of biometric information
Tax file number	An individual's personal reference number in the tax and superannuation systems, issued by the Australian Taxation Office
Human error	An unintended action by an individual directly resulting in a data breach, for example, inadvertent disclosure caused by sending a document containing personal information to the incorrect recipient
Failure to use BCC when sending email	Sending an email to a group by including all recipient emails addresses in the 'To' field, thereby disclosing all recipient email addresses to all recipients
Insecure disposal	Disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin
Loss of paperwork/data storage device	Loss of a physical asset containing personal information, for example, leaving a folder or a laptop on a bus
PI sent to wrong recipient (email)	Personal information sent to the wrong recipient via email, for example, as a result of a misaddressed email or having a wrong address on file
PI sent to wrong recipient (fax)	Personal information sent to the wrong recipient via facsimile machine, for example, as a result of an incorrectly entered fax number or having a wrong fax number on file
PI sent to wrong recipient (mail)	Personal information sent to the wrong recipient via postal mail, for example, as a result of a transcribing error or having a wrong address on file
PI sent to wrong recipient (other)	Personal information sent to the wrong recipient via channels other than email, fax or mail, for example, delivery by hand or uploading to web portal
Unauthorised disclosure (failure to redact)	Failure to effectively remove or de-identify personal information from a record before disclosing it

Term	Definition
Unauthorised disclosure (unintended release or publication)	Unauthorised disclosure of personal information in a written format, including paper documents or online
Unauthorised disclosure (verbal)	Disclosing personal information verbally without authorisation, for example, calling it out in a waiting room
Malicious or criminal attack	A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain
Brute-force attack (compromised credentials)	A typically unsophisticated and exhaustive process to determine a cryptographic key or password that proceeds by systematically trying all alternatives until it discovers the correct one
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
Hacking (other means)	Unauthorised access to a system or network (other than by way of phishing, brute-force attack or malware), often to exploit a system's data or manipulate its normal behaviour
Malware	Short for 'malicious software'. A software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malware include trojans, viruses and worms
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Rogue employee/ insider threat	An attack by an employee or insider acting against the interests of their employer or other entity
Phishing (compromised credentials)	Untargeted, mass messages sent to many people asking for information, encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide information or download malicious content
Social engineering/ impersonation	An attack that relies heavily on human interaction to manipulate people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations
Theft of paperwork or data storage device	Theft of paperwork or data storage device

Term	Definition
System fault	A business or technology process error not caused by direct human error