Australian Government

Office of the Australian Information Commissioner

Notifiable data breaches report

January to June 2022

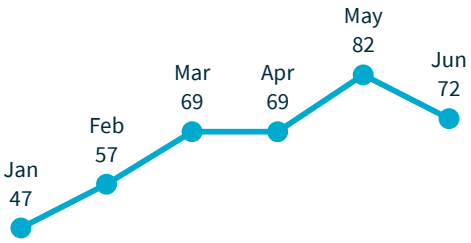
10 November 2022

OAIC

Snapshot

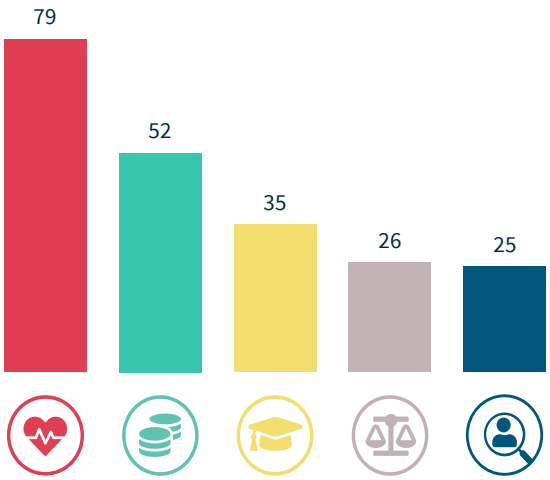
396
notifications

Down 14%



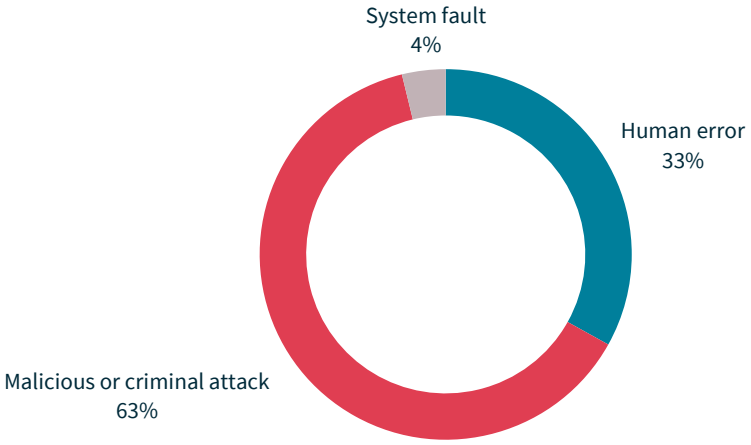
Top 5 sectors to notify data breaches

- Health service providers
- Finance (incl. superannuation)
- Education
- Legal, accounting & management services
- Recruitment agencies



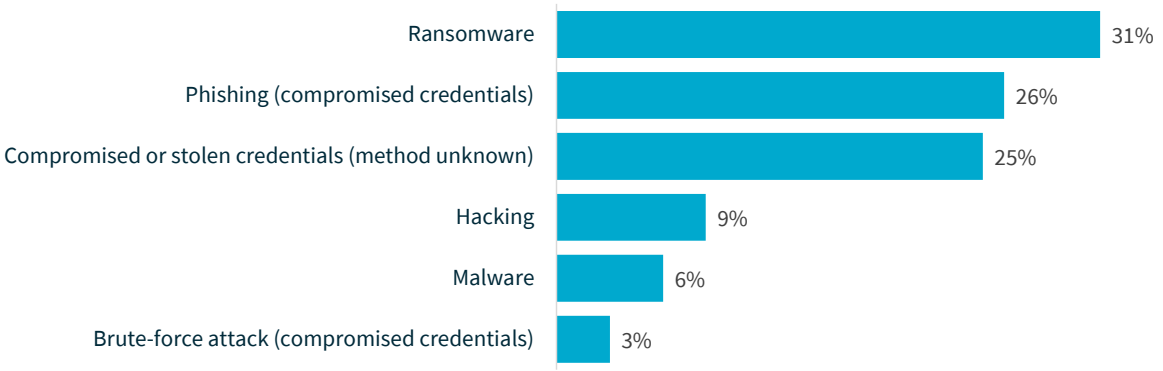
65%
of data breaches affected
100 people or fewer

Sources of data breaches



41% of all data breaches resulted from cyber security incidents (162 notifications)

Cyber incident breakdown



Top causes of human error breaches

Personal information emailed to the wrong recipient 38%

Unintended release or publication 24%

Personal information mailed to the wrong recipient 8%

Contents

About this report

The Office of the Australian Information Commissioner (OAIC) periodically publishes statistical information about notifications received under the Notifiable Data Breaches (NDB) scheme to help entities and the public understand privacy risks identified through the scheme. This report captures notifications made under the NDB scheme from 1 January to 30 June 2022.

Statistical comparisons are to the period 1 July to 31 December 2021 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 in this report unless otherwise specified.

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 at the end of this report.

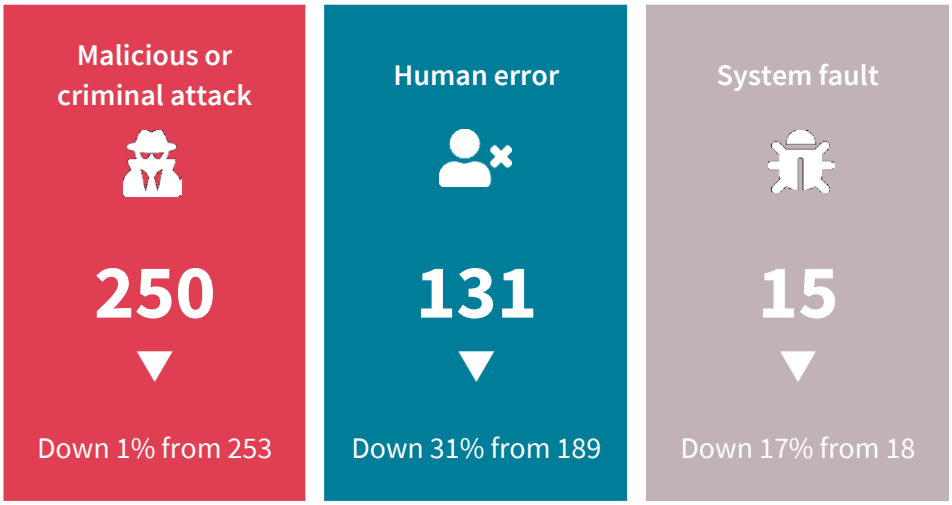
Notifications made under the *My Health Records Act 2012* are not included as they are subject to specific notification requirements set out in that Act.

Statistics in this report are current as of 30 September 2022. Some data breach notifications are being assessed and adjustments may be made to related statistics. This may affect statistics for the period January to June 2022 published in future reports. Similarly, statistics from before January 2022 in this report may differ from statistics published in previous NDB reports.

Executive summary

The NDB scheme was established in February 2018 to improve consumer protection and drive better security standards for protecting personal information. Under the scheme, any organisation or government agency covered by the *Privacy Act 1988* that experiences an eligible data breach must notify affected individuals and the OAIC.

The OAIC publishes twice-yearly reports on notifications received under the NDB scheme to track the leading sources of data breaches and highlight emerging issues and areas for ongoing attention by regulated entities.



Key findings for the January to June 2022 reporting period:

- 396 breaches were notified compared to 460 in July to December 2021 (14% decrease).
- Malicious or criminal attack remains the leading source of breaches accounting for 250 notifications (63% of the total), down 1% in number from 253.
- Data breaches resulting from human error accounted for 131 notifications (33% of the total), down 31% in number from 189.
- Health remains the highest reporting sector notifying 20% of breaches, followed by finance (13%).
- Contact information remains the most common type of personal information involved in breaches.
- 91% of breaches affected 5,000 individuals or fewer, while 65% affected 100 people or fewer.
- 71% of entities notified the OAIC within 30 days of becoming aware of an incident.

Notifications received January to June 2022 – All sectors

The OAIC received 396 notifications this reporting period. This is a 14% decrease compared to the previous 6 months.

There was significant variation month to month in the number of notifications received. The lowest monthly total was 47 notifications in January and the highest was 82 notifications in May. January 2021 is the only other month since the scheme began in which the OAIC received fewer than 50 notifications.

Table 1 – Notifications received in the 2021–22 financial year

Reporting period	Number of notifications
July to December 2021	460
January to June 2022	396
2021–22 financial year	**856**

Chart 1 – Notifications received by month from January 2020 to June 2022

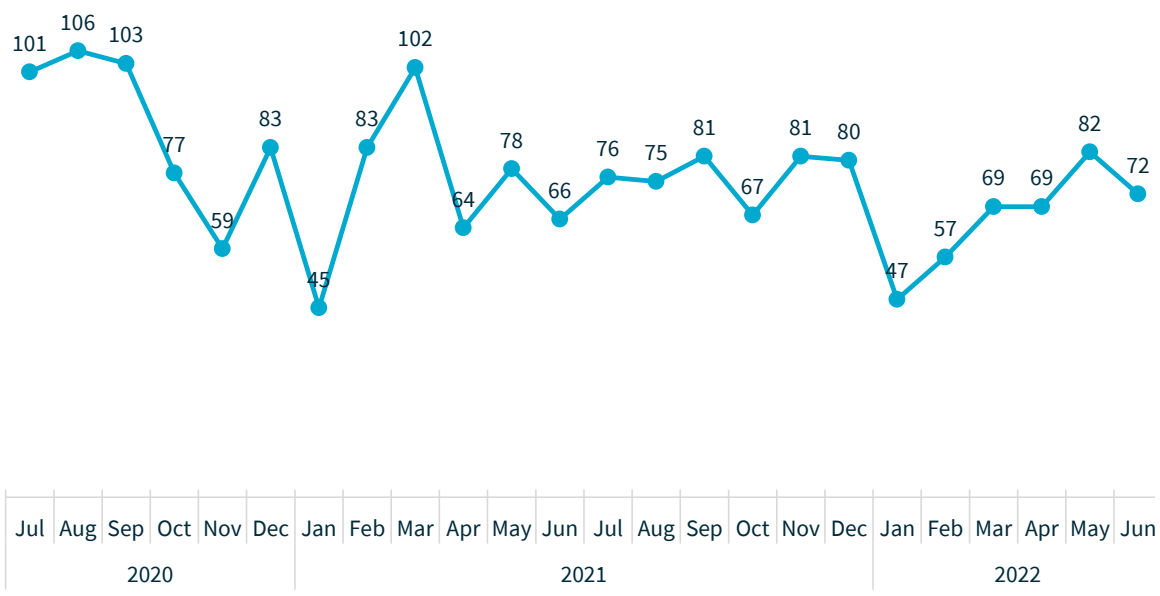
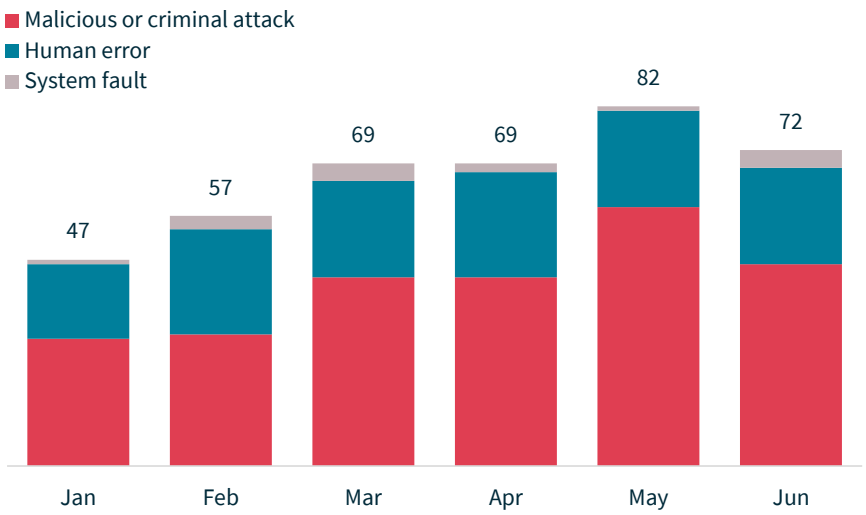


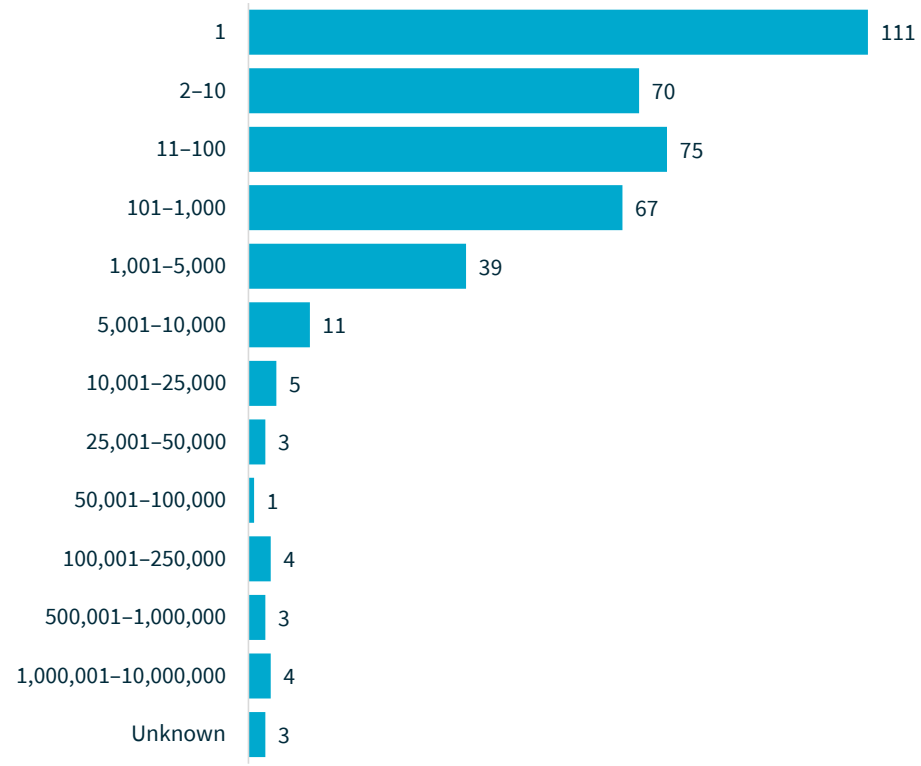
Chart 2 – Notifications received by month showing the sources of breaches



Number of individuals affected by breaches

Consistent with previous reports, most data breaches (91%) involved the personal information of 5,000 individuals worldwide or fewer. Breaches affecting 100 individuals worldwide or fewer comprised 65% of notifications and breaches affecting between 1 and 10 individuals worldwide accounted for 46% of notifications.

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 the notifying entities.

Large scale data breaches

In this reporting period, there was an increase in data breaches that reportedly impacted a larger number of Australians.

There were 24 data breaches reported to affect 5,000 or more Australians, compared with 18 breaches of this scale in July to December 2021. Four of these breaches were reported to affect 100,000 or more Australians, compared with one breach in the previous reporting period.

Number of Australians affected by breaches	Jul–Dec 2021	Jan–Jun 2022
5,001–10,000	7	9
10,001–25,000	5	5
25,001–50,000	2	3
50,001–100,000	3	3
100,001–250,000	1	3
1,000,001–10,000,000	0	1

Twenty-three of the 24 breaches that affected more than 5,000 Australians were caused by cyber incidents, with the remaining breach resulting from a system fault. Nine were ransomware incidents, 9 were due to compromised credentials, 3 were due to hacking and 2 were malware incidents.

This underlines the significant impact of cyber incidents on individuals in this reporting period, and the importance of entities taking appropriate protective measures against a range of cyber threats. The Australian Cyber Security Centre has useful guidance for entities on improving their cyber resilience and protecting the personal information they hold from cyber threats.

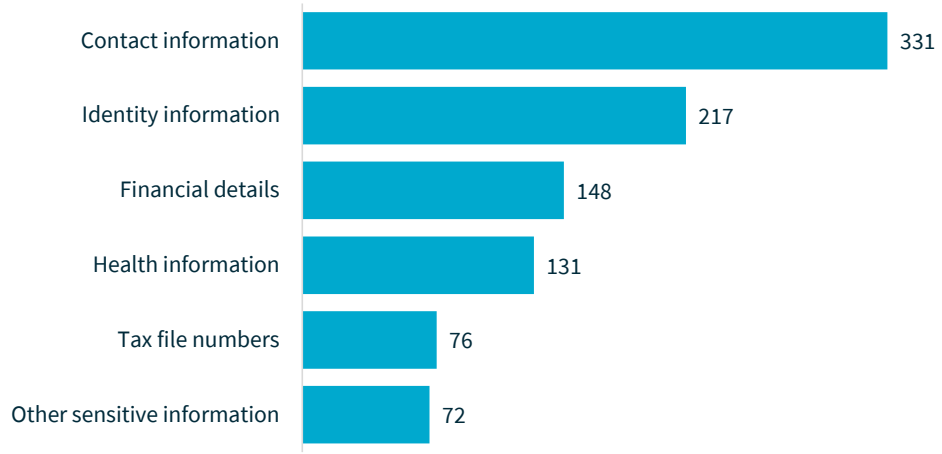
Kinds of personal information involved in breaches

Contact information, identity information and financial details continue to be the most common types of personal information involved in data breaches.

Most breaches (84%) involved contact information, such as an individual's name, home address, phone number or email address.

This is distinct from identity information, which was exposed in 55% of breaches and includes an individual's date of birth, passport details and driver licence details. Financial details, such as bank account and credit card numbers, were involved in 37% of breaches.

Chart 4 – Kinds of personal information involved in breaches



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

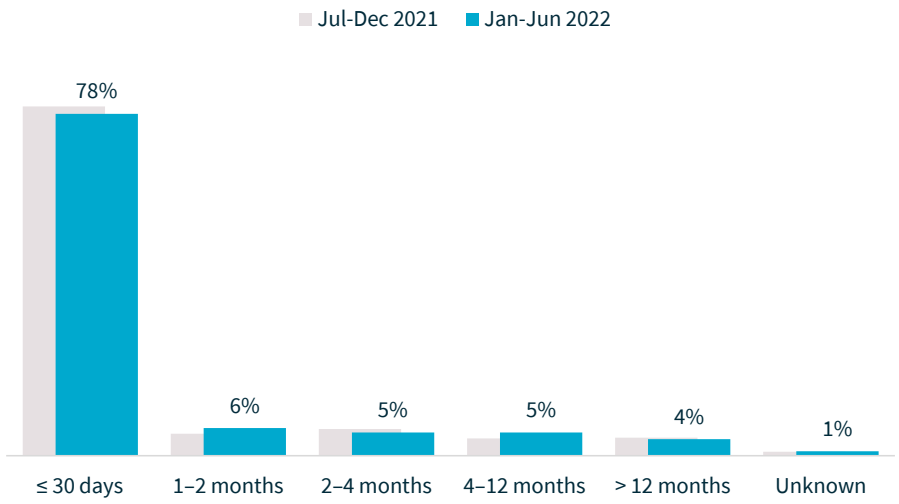
Time taken to identify breaches

As part of complying with Australian Privacy Principle 11, entities should take reasonable steps to ensure they detect data breaches in a timely manner.

The figures in this section relate to the time between an incident occurring and the entity becoming aware of it. They do not relate to the time taken by the entity to assess whether an incident qualified as an eligible data breach.[1]

In the reporting period, 78% of breaches were identified by the entity within 30 days of it occurring, compared to 80% in July to December 2021.

Chart 5 – Time taken to identify breaches

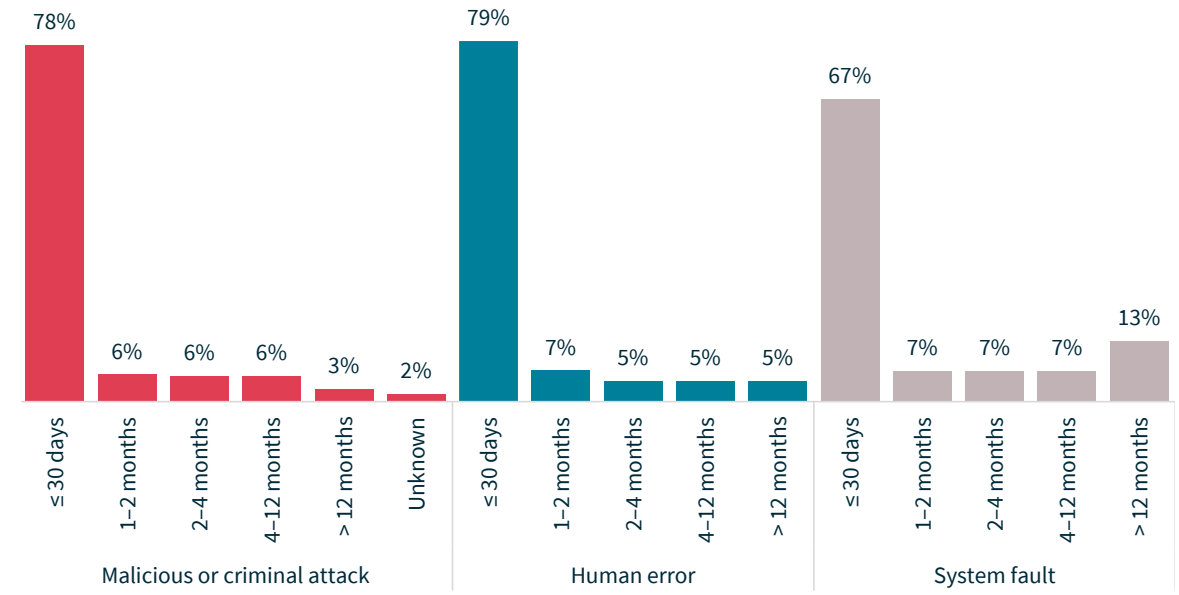


For notifications in the 'Unknown' category, the entity was unable to identify the date the breach occurred.

The time it takes entities to identify breaches has varied significantly depending on the source of the breach. There was less variation in this reporting period, however a notable proportion of entities that experienced system faults (13%) did not become aware of the incident for over a year.

[1] The Privacy Act requires entities to take reasonable steps to conduct a data breach assessment within 30 days of becoming aware there are grounds to suspect they may have experienced an eligible data breach. Once the entity forms a reasonable belief that there has been an eligible data breach, they must prepare a statement and provide a copy to the OAIC as soon as practicable.

Chart 6 – Time taken to identify breaches by source of breach



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

Timely assessment of suspected eligible data breaches

Since the introduction of the NDB scheme, there have been instances of entities taking several months to complete an assessment and notify affected individuals of an eligible data breach.

Section 26WH of the Privacy Act requires entities to carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that an eligible data breach has occurred. Entities are required to take all reasonable steps to complete this assessment within 30 days.

An entity should commence a s 26WH assessment if it experiences a data breach and is aware of anything that objectively - from the viewpoint of a reasonable person in the entity's position - would give rise to reasonable grounds to suspect that an incident was an eligible data breach. An entity's suspicion may be formed by reference to anything relevant to the breach and surrounding circumstances of which the entity is aware.

Scenario

An entity became aware of a ransomware attack that encrypted a number of files on its corporate network, although the entity did not initially know which files were affected. At this initial point, the entity had reasonable grounds to suspect an eligible data breach.

The entity undertook a s 26WH assessment to determine whether the breach was an eligible data breach. The entity engaged an IT consultant to undertake an assessment of the incident. The IT consultant identified the entity's customer information had been accessed and exfiltrated, and some of this published on the dark web. Based on this assessment, the entity concluded this was an eligible data breach.

To ensure affected individuals were notified as soon as practicable, the entity notified all potentially affected individuals whose information may have been involved in the breach, including both those whose personal information was accessed and exfiltrated as well as those whose personal information was discovered on the dark web. As part of this notification, the entity specified the kinds of information involved in the breach and provided individuals with relevant recommendations about the steps they should take in response.

Time taken to notify the OAIC of breaches

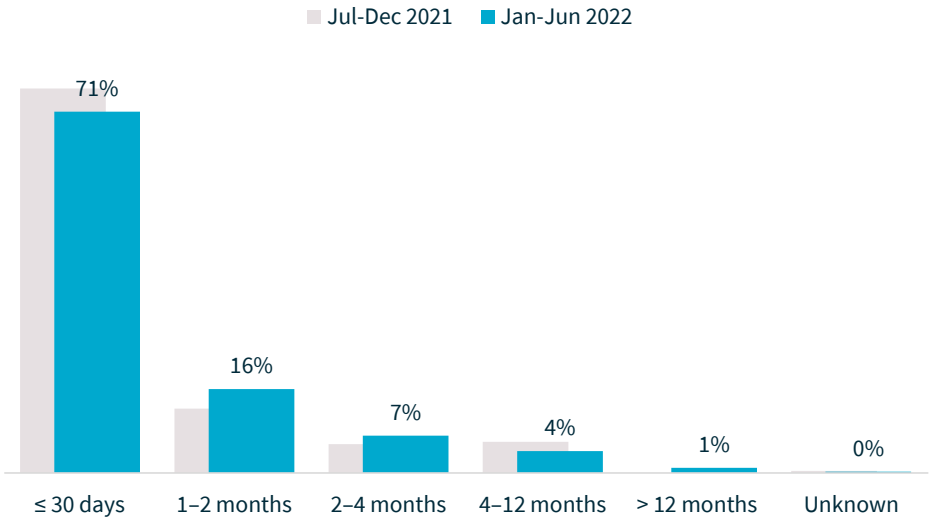
A key objective of the NDB scheme is to protect individuals by enabling them to respond quickly to a data breach to mitigate the risk of harm. Delays in assessment and notification reduce the opportunities for an individual to take steps to prevent harm.

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.

In the reporting period, 71% of entities notified the OAIC within 30 days of becoming aware of an incident, compared to 75% in the previous period. Four entities took more than 12 months from when they became aware of an incident to notify the OAIC.

Some entities notified individuals at the same time as the OAIC or shortly after. This approach helps individuals take timely steps to protect themselves from harm. Some entities notified the OAIC and then there was a delay before they notified individuals.

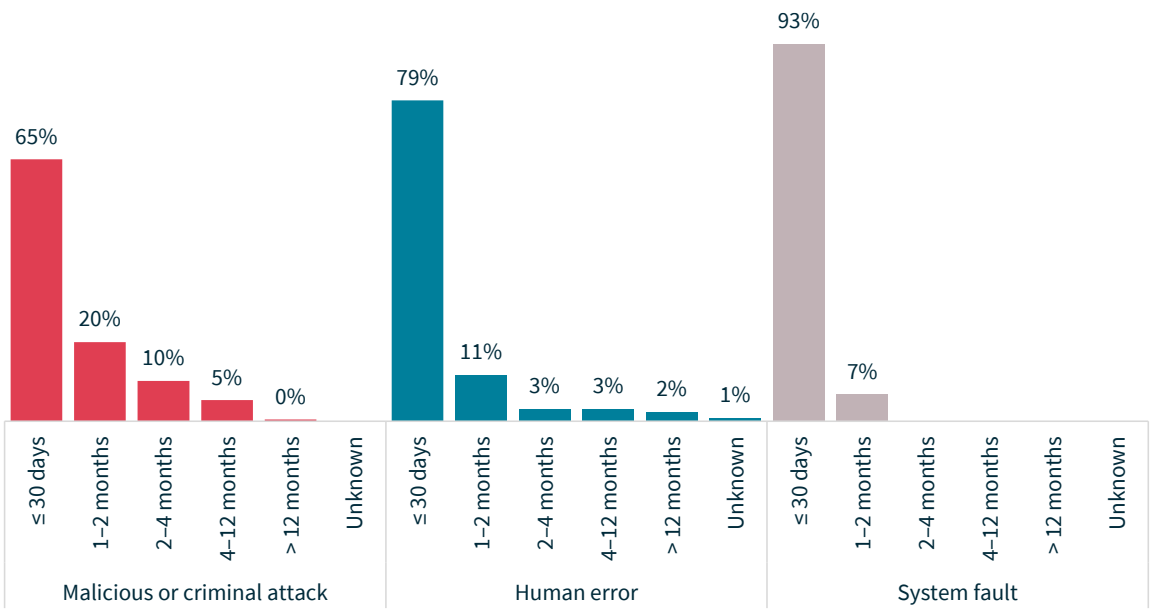
Chart 7 – Time taken to notify the OAIC of breaches



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

There was some variance by source of breach in the time taken to notify the OAIC after an incident was identified. For system fault breaches, 93% of entities notified the OAIC within 30 days compared to 79% for human error breaches and 65% for breaches caused by malicious or criminal attacks.

Chart 8 – Time taken to notify the OAIC of breaches by source of breach



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

Website notification

Under the NDB scheme, entities covered by the Privacy Act must notify affected individuals and the OAIC of an eligible data breach as soon as practicable.

An entity can notify affected individuals of an eligible data breach by notifying the contents of a statement:

- to all affected individuals
- only to individuals who are at risk from the eligible data breach.

If neither of these options are practicable, the entity must publish a statement on its website and take reasonable steps to publicise its contents. Some ways entities may achieve this are:

- making an announcement to the media, on social media or through other channels where affected individuals are likely to engage
- ensuring the statement is prominently placed on the relevant website and can be easily located and indexed by search engines.

A key objective of the NDB scheme is to protect individuals by enabling them to respond quickly to a data breach to minimise the risk of harm. The method of communication should seek to ensure that individuals can trust and act upon the information provided.

If identifying contact details of affected individuals or preparing tailored notifications is impracticable and will cause extended delay in notifying affected individuals, it is likely that website notification will be needed. It may be that this can be followed up with notification to individuals.

Scenario

A health service provider experienced a ransomware incident that involved unauthorised access to its systems and records.

Based on a review of audit logs, the disability services provider determined 50 individuals were at risk of serious harm due to the kinds of personal information involved.

The health service provider directly notified 36 of these individuals via email or direct message on relevant social media platforms. However, it did not hold up-to-date contact information for 14 of the affected individuals. As such, rather than sourcing up-to-date contact information for those 14 individuals at that time, which may have delayed notification, the disability services provider decided to make a public statement.

The health service provider published the statement on its website, social media and print newsletter while it continued its efforts to contact the 14 individuals directly. It ensured this was likely to be accessible to the affected individuals by providing a version in Auslan.

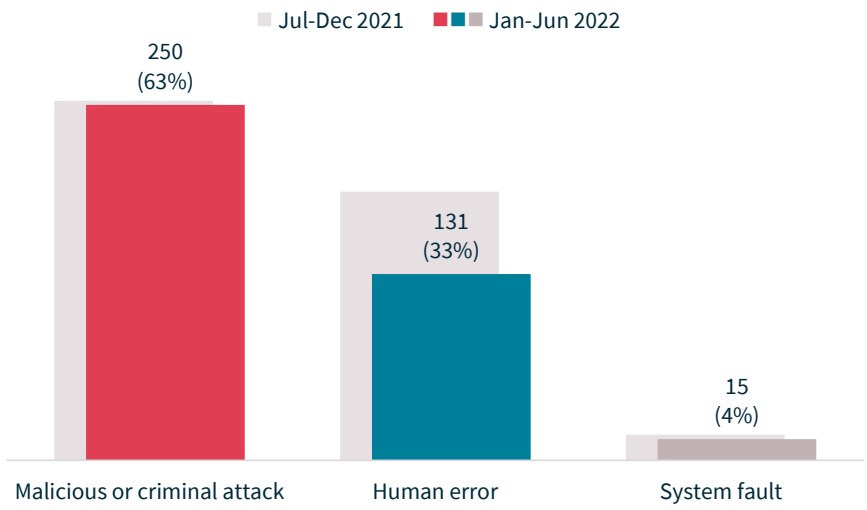
Source of breaches

Consistent with previous reports, malicious or criminal attack was the largest source of data breaches notified to the OAIC, accounting for 250 breaches (down from 253).

Human error remained a major source of breaches, accounting for 131 notifications (down from 189).

System faults accounted for the remaining 15 breaches (down from 18).

Chart 9 – Source of data breaches



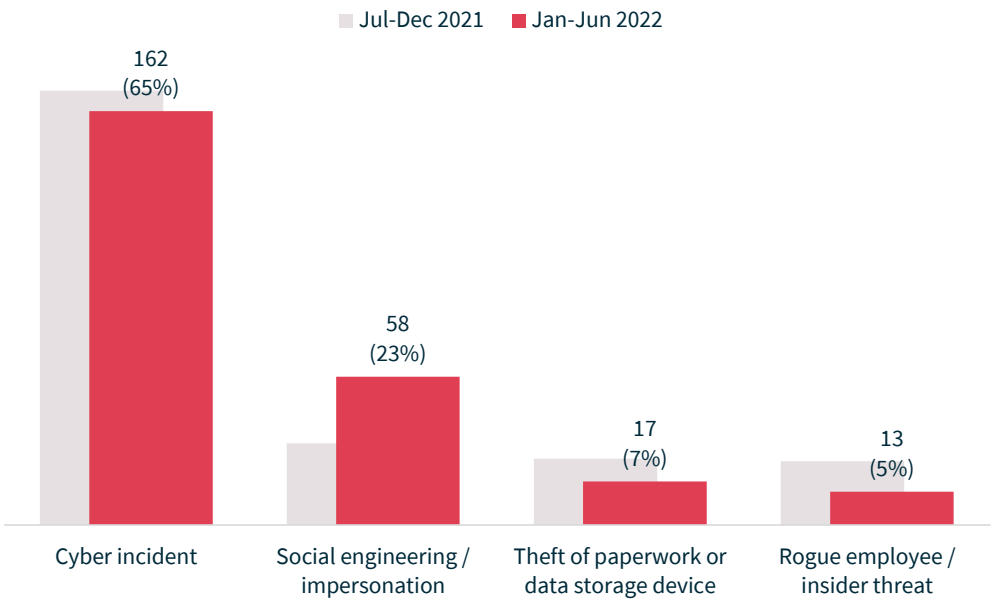
Malicious or criminal attacks

The number of breaches attributed to a malicious or criminal attack decreased by 1%. The proportion of total breaches caused by malicious or criminal attack increased from 55% to 63%.

The majority of breaches (65%) in this category involved cyber incidents (162 notifications).

Social engineering or impersonation accounted for 58 notifications, theft of paperwork or data storage device for 17 notifications and actions taken by a rogue employee or insider threat for 13 notifications.

Chart 10 – Malicious or criminal attack breakdown



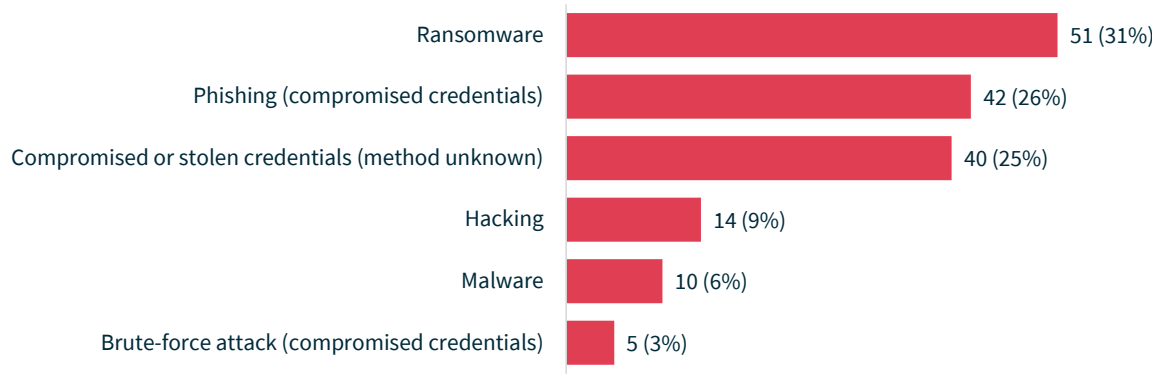
Cyber incidents

In this reporting period, 65% of breaches attributed to malicious or criminal attack – or 41% of all breaches (162 notifications) – resulted from cyber security incidents.

The top sources of cyber incidents were ransomware (51 notifications), phishing (42 notifications) and compromised or stolen credentials (method unknown) (40 notifications).

Just over half (54%) of cyber incidents involved malicious actors gaining access to accounts using compromised or stolen credentials.

Chart 11 – Cyber incident breakdown

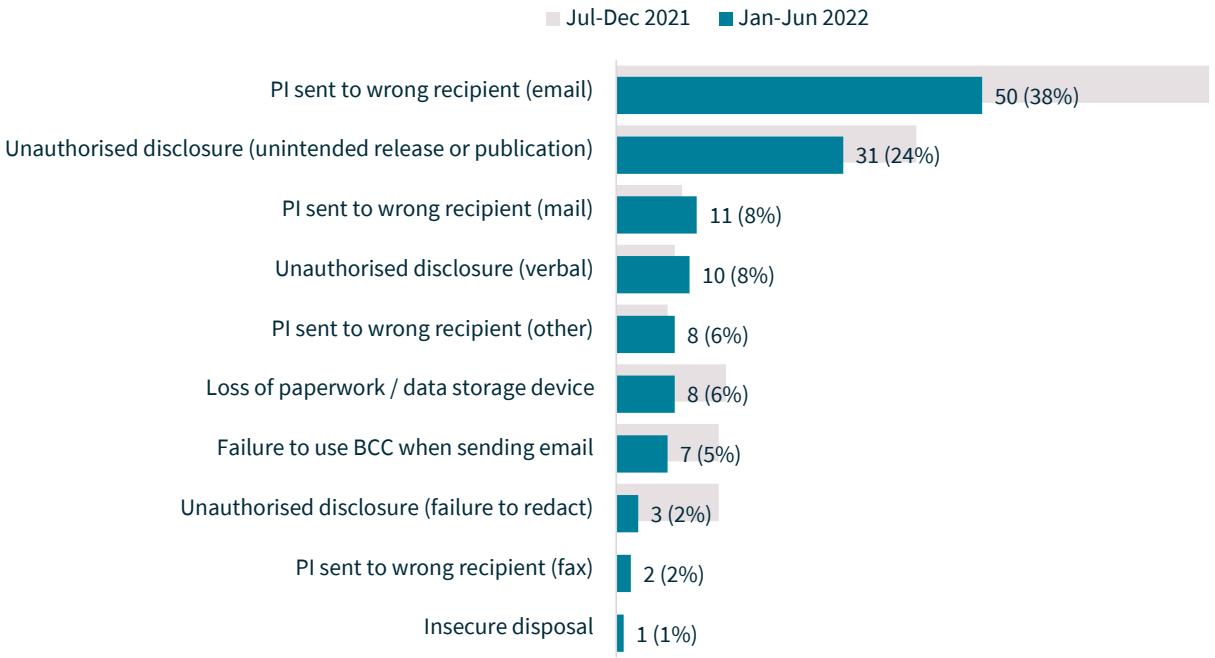


Human error

The reporting period saw a significant decrease in human error breaches in terms of the total number of notifications – down 31% from 189 to 131 – and proportionally – down from 41% to 33% of all breaches.

Just over half (54%) of human error breaches involved personal information being sent to the wrong recipient either by email, mail, fax or another method.

Chart 12 – Human error breakdown



Certain human error breaches affect larger numbers of individuals. In this reporting period, unintended release or publication affected an average 134 people per breach, while verbal disclosure affected one person on average per breach.

Table 2 – Human error breakdown by average number of affected individuals

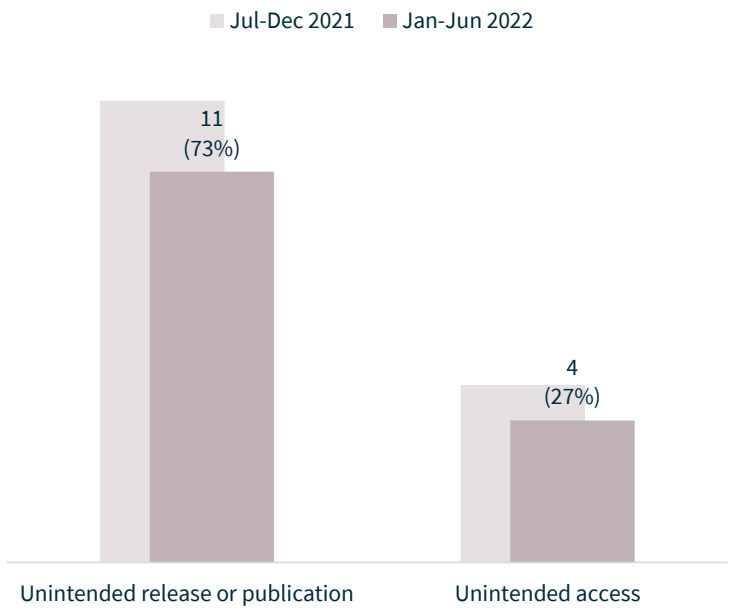
Source of breach	Number of notifications	Average number of affected individuals
Unauthorised disclosure (unintended release or publication)	31	134
Failure to use BCC when sending email	7	116
PI sent to wrong recipient (email)	50	62
PI sent to wrong recipient (mail)	11	48
Insecure disposal	1	41
PI sent to wrong recipient (other)	8	21
Loss of paperwork/data storage device	8	19
Unauthorised disclosure (failure to redact)	3	7
PI sent to wrong recipient (fax)	2	3
Unauthorised disclosure (verbal)	10	1
Total	**131**	**68**

System faults

System fault breaches include incidents that occur due to a business or technology process error and accounted for 4% of all notifications. The proportion of breaches attributed to system faults has been consistent since the NDB scheme began.

Unintended release or publication of personal information due to a system fault caused 11 breaches. Unintended access to personal information because of a system fault caused 4 breaches.

Chart 13 – System fault breakdown



Data breaches involving more than one entity

Where a single data breach incident affects multiple entities, the OAIC may receive multiple notifications relating to the same incident. This is occurring more frequently.

Notifications relating to the same incident are counted as a single notification in this report to avoid information being duplicated. However, the volume of secondary notifications provides an indication of the level of multi-party breach reporting. This reporting period, the number of secondary notifications received increased by 100% compared with the previous period.

When more than one entity holds personal information that is subject to a data breach, all affected entities may have obligations under the NDB scheme. However, only one of the affected entities needs to make an assessment of the suspected eligible data breach under s 26WH of the Privacy Act and notify the OAIC and affected individuals.

A number of factors may influence which entity notifies the OAIC and affected individuals. Generally, the OAIC recommends the entity with the most direct relationship with affected individuals notifies them.

Entities should work together to ensure the requirements of the NDB scheme are met. In some instances, the entity with the most information about the data breach will not be the entity with the most direct relationship with affected individuals. It may be that the entity with the most information about the data breach is best placed to complete the assessment, and the entity (or entities) with the most direct relationship with affected individuals is best placed to notify the OAIC and affected individuals.

Each entity that holds personal information involved in an eligible data breach needs to be able to demonstrate they are meeting the requirements of the NDB scheme. Assigning the roles and responsibilities of each entity upfront will support a quick and efficient data breach response.

Scenario

A cloud service provider experienced a malware attack that involved their systems being accessed by a threat actor. The cloud service provider's assessment identified a large volume of data may have been exfiltrated, including information stored for its client organisations.

The cloud service provider informed its client organisations, notified the OAIC and provided the OAIC with the identity and contact details of affected client organisations. It also published information about the data breach on its website.

The cloud service provider did not have a direct relationship with or knowledge of each of its client organisations' customers (the affected individuals). For this reason, the cloud service provider gave each client organisation access to its assessment and a copy of the client organisation's data that may have been involved in the attack. The cloud service provider asked each client organisation to notify affected individuals of the breach as required by the NDB scheme, which the client organisations proceeded to do.

Comparison of top 5 sectors

Health service providers and the finance industry have consistently reported the most data breaches of all sectors since the NDB scheme began.

Health service providers reported 79 data breaches (20% of notifications). The second largest source of notifications was the finance sector (13%).

The other sectors in the top 5 by notifications were education (9%), legal, accounting and management services (7%) and recruitment agencies (6%).

Table 3 – Top 5 sectors by notifications

Sector	Number of notifications
Health service providers[2]	79
Finance[3]	52
Education[4]	35
Legal, accounting and management services	26
Recruitment agencies[5]	25
Total	**217**

This section compares notifications made under the NDB scheme by these sectors, which accounted for 55% of all notifications.

[2] A health service provider generally includes any private sector entity that provides a health service within the meaning of section 6FB of the Privacy Act, regardless of annual turnover.

[3] This sector includes banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

[4] This sector includes private education providers only.

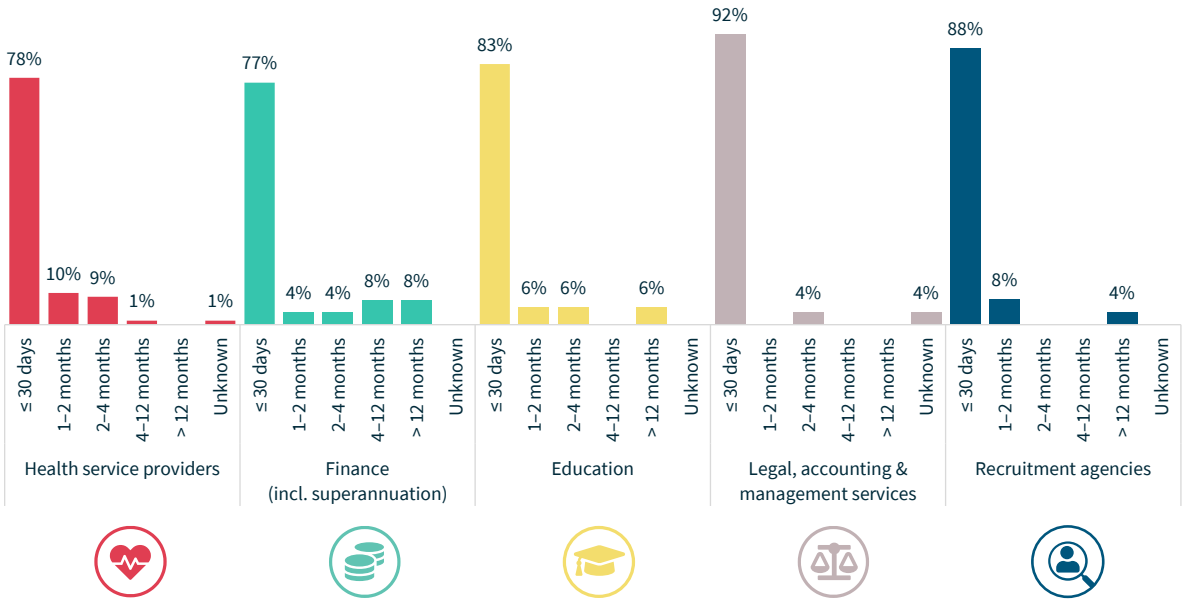
[5] This is the first reporting period in which recruitment agencies have been reported as a separate sector. They were previously considered part of the 'personal services' sector.

Time taken to identify breaches – Top 5 sectors

There was some variation by industry sector in the time taken by entities to identify incidents.

In the reporting period, 92% of legal, accounting and management service entities identified the incident within 30 days of it occurring. This figure was 77% for the finance sector.

Chart 14 – Time taken to identify breaches – Top 5 sectors



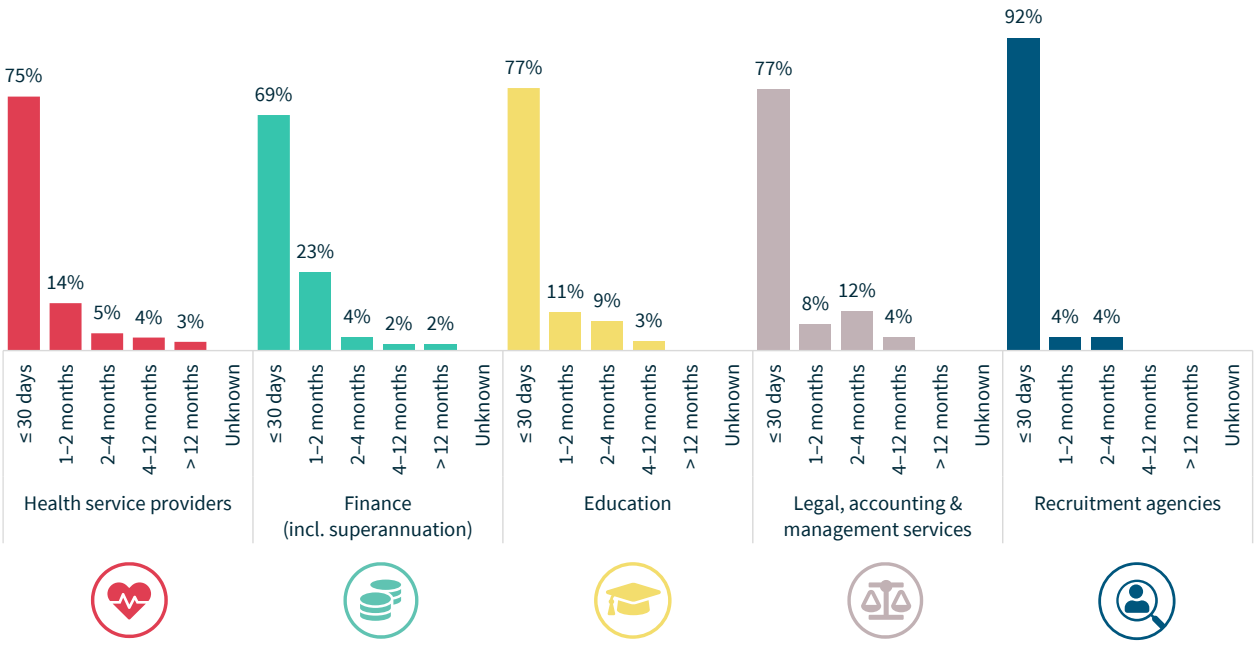
For notifications in the 'Unknown' category, the entity was unable to identify the date the breach occurred.

Time taken to notify the OAIC of breaches – Top 5 sectors

There was also some variation by industry sector in the time taken by entities to notify the OAIC of a data breach.

Ninety-two per cent of notifications from recruitment agencies were made within 30 days of the entity becoming aware of the incident. This figure was 69% for the finance sector.

Chart 15 – Time taken to notify the OAIC of breaches – Top 5 sectors



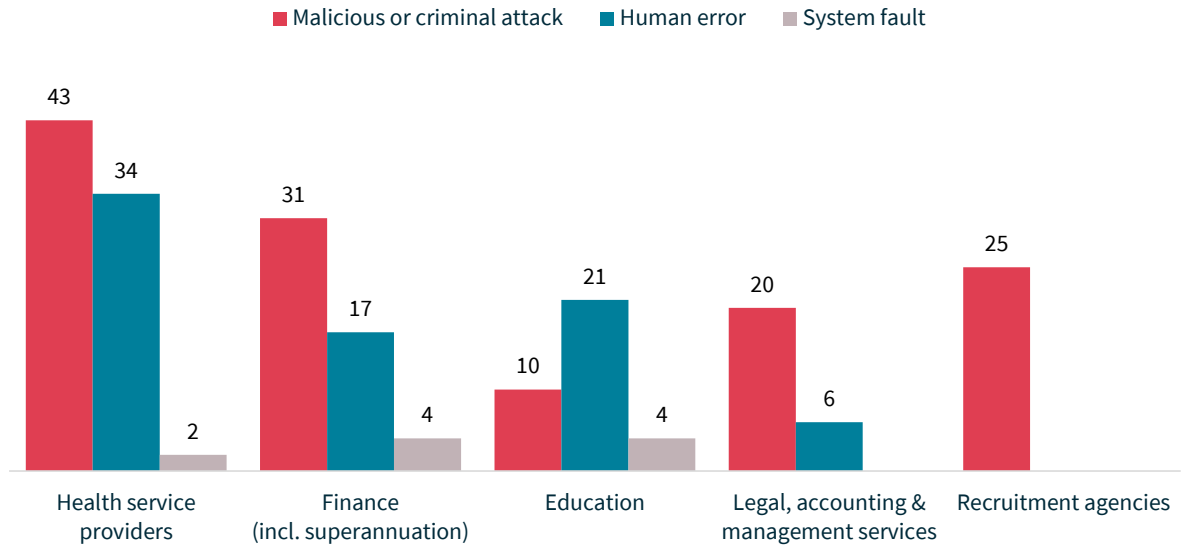
For notifications in the 'Unknown' category, the entity was unable to identify the date the breach occurred.

Source of breaches – Top 5 sectors

Malicious or criminal attack was the top cause of data breaches notified by the top 5 sectors. It was the source of all breaches notified by recruitment agencies, 77% of legal, accounting and management services breaches, 60% of finance sector breaches and 54% of health sector breaches.

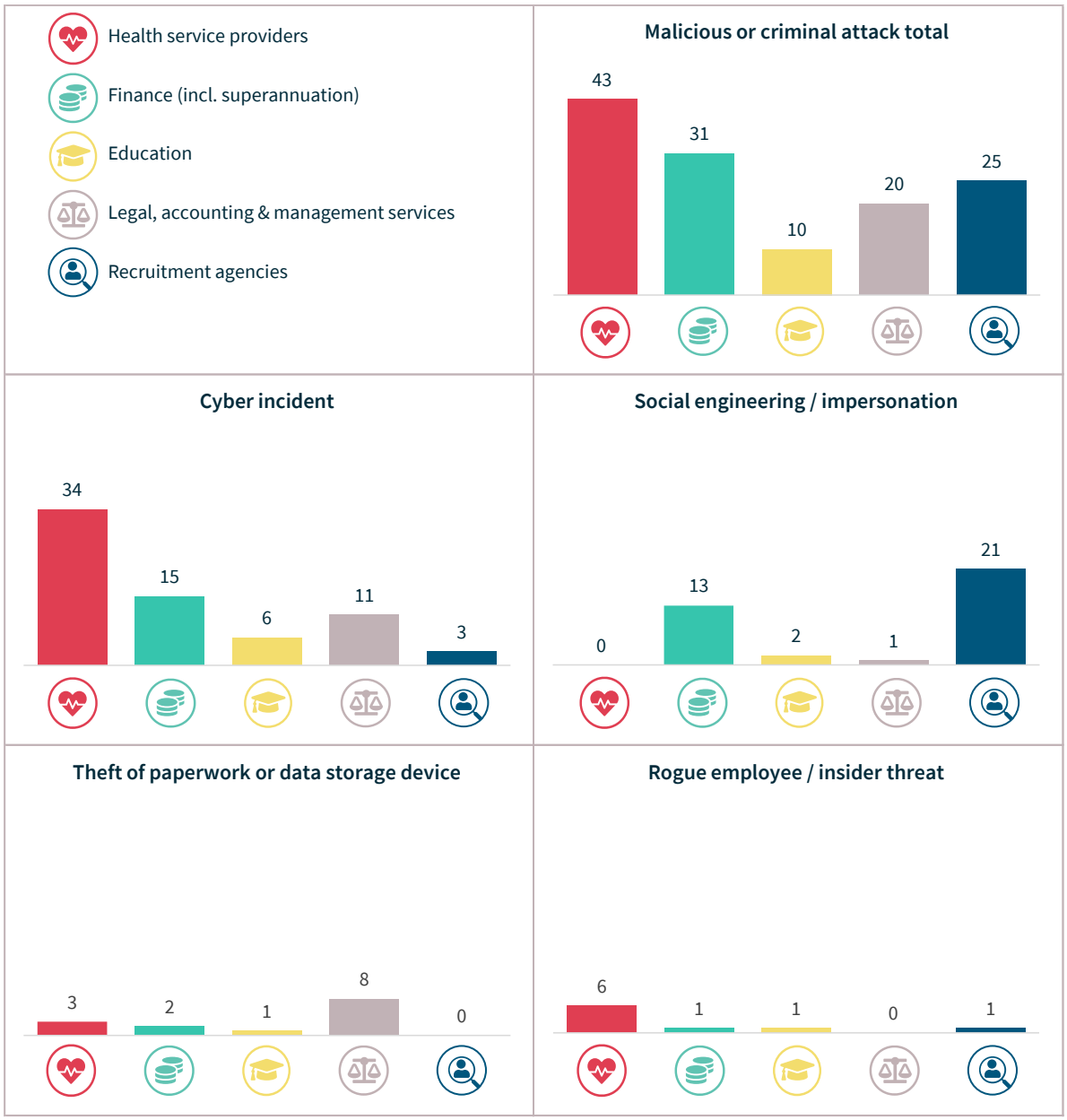
Education was the only sector in the top 5 to notify more breaches caused by human error (64% of notifications) than malicious or criminal attack (27%).

Chart 16 – Source of breaches – Top 5 sectors



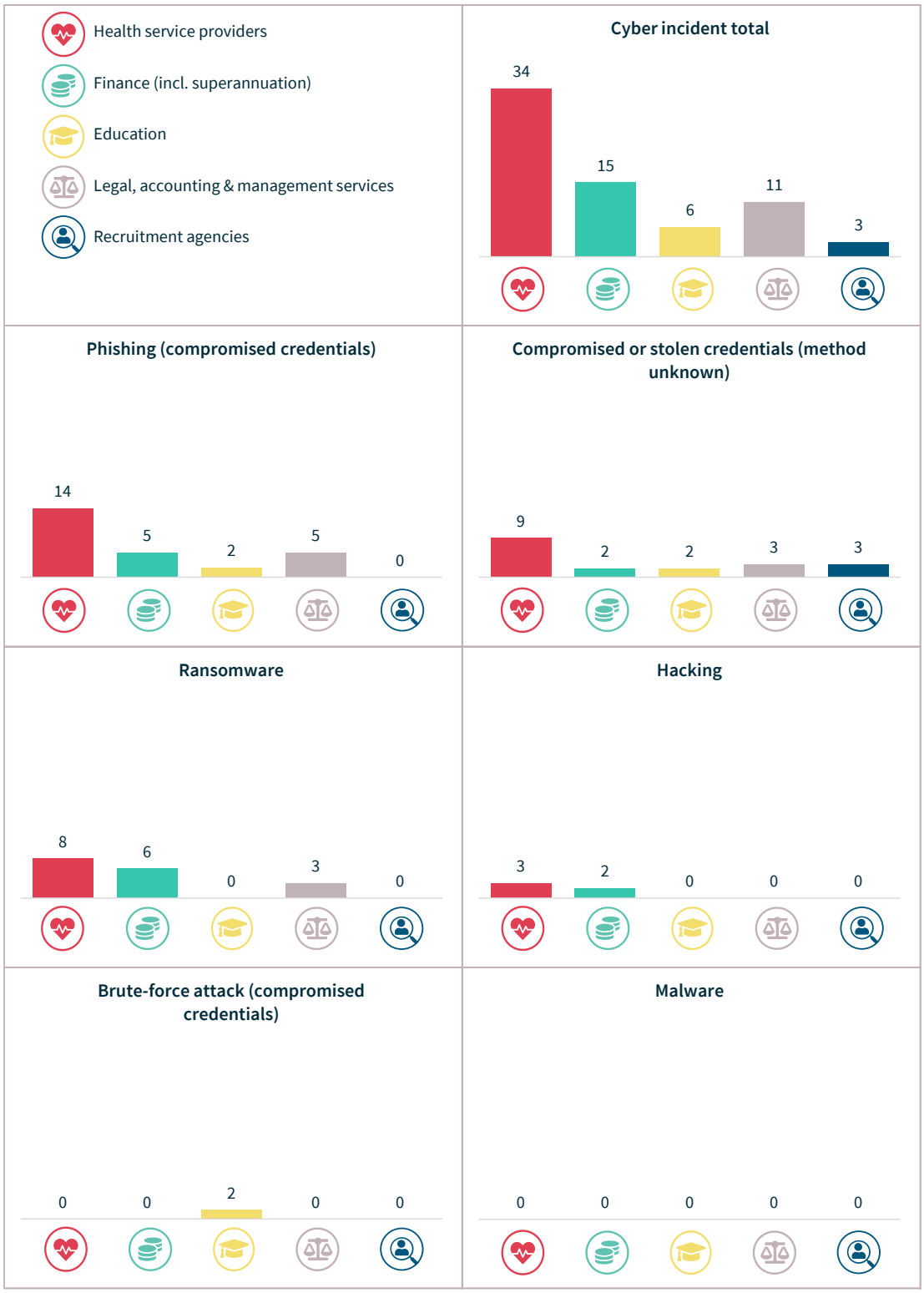
Malicious or criminal attack breaches – Top 5 sectors

Chart 17 – Malicious or criminal attacks breakdown – Top 5 sectors



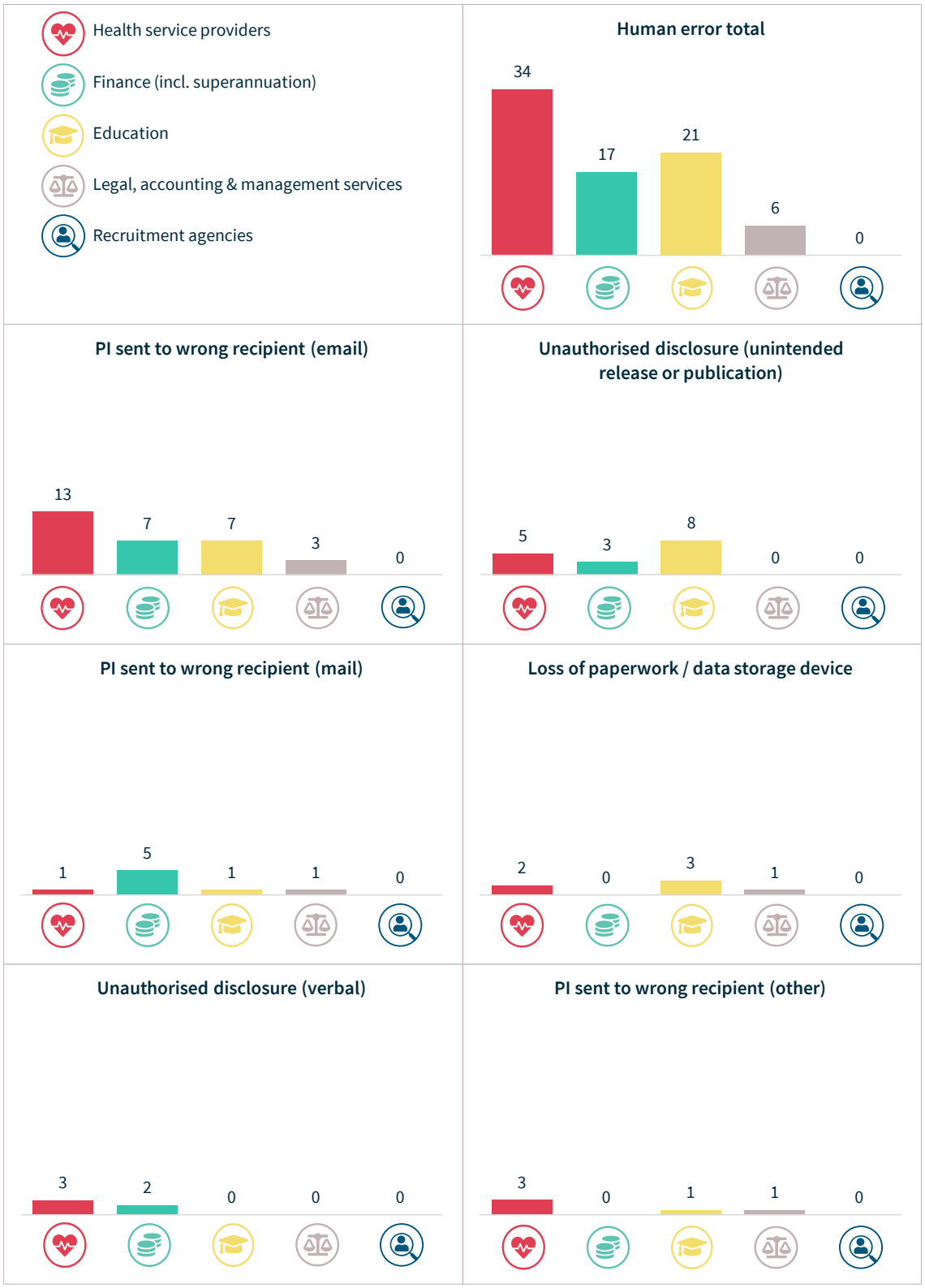
Cyber incident breaches – Top 5 sectors

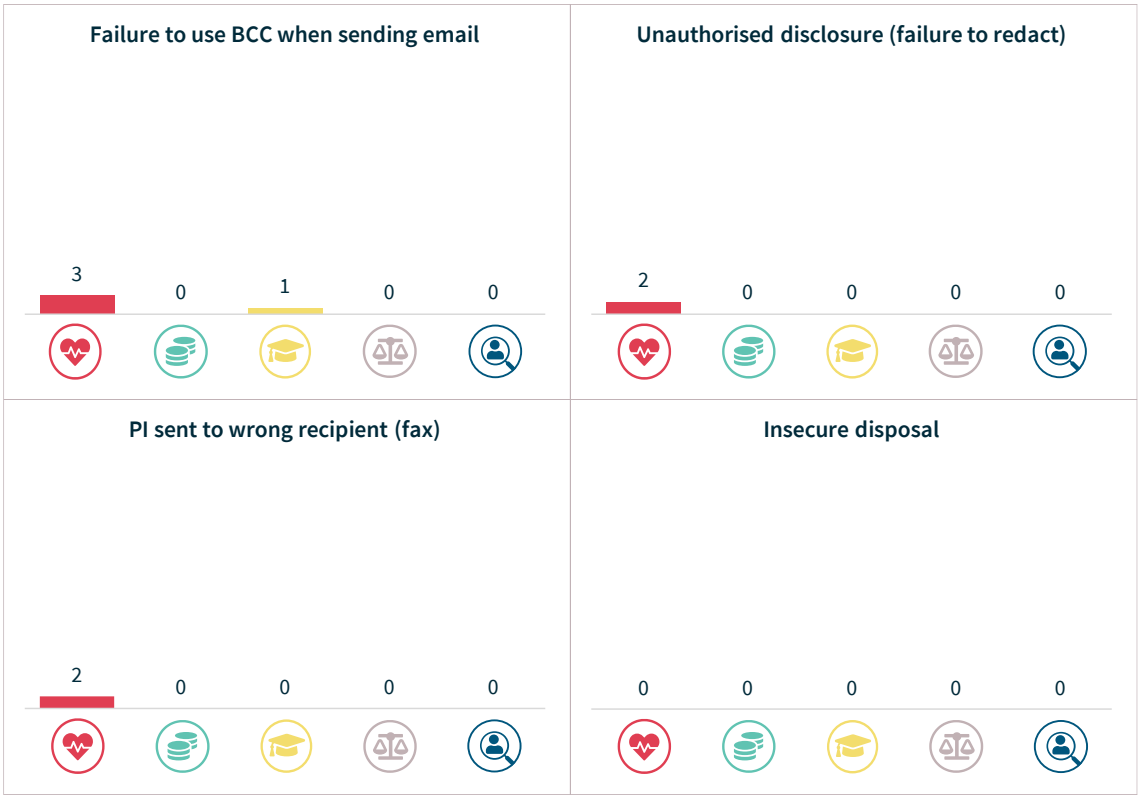
Chart 18 – Cyber incident breakdown – Top 5 sectors



Human error breaches – Top 5 sectors

Chart 19 – Human error breakdown – Top 5 sectors



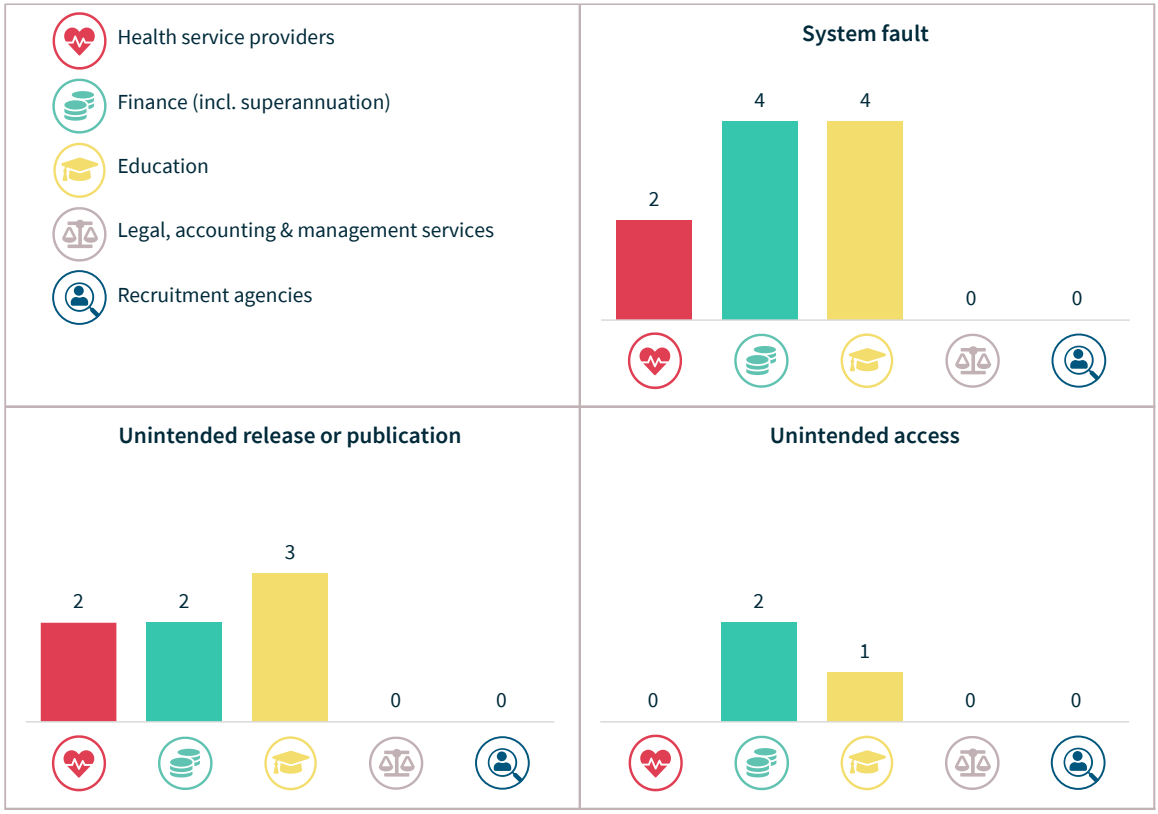

Failure to use BCC when sending email
3
0
1
0
0
Unauthorised disclosure (failure to redact)
2
0
0
0
0
PI sent to wrong recipient (fax)
2
0
0
0
0
Insecure disposal
0
0
0
0
0

System fault breaches – Top 5 sectors

Of the top 5 sectors, only 3 – health service providers, finance and education – notified data breaches resulting from a system fault.

Most system fault breaches involved the unintended release or publication of personal information, such as automated messages sent to incorrect recipients or online forms or profiles automatically linked or populated with incorrect personal information.

Chart 20 – System fault breakdown – Top 5 sectors



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 • this is likely to result in serious harm to one or more individuals • 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 section 6 of the Privacy Act
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 section 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 • health or genetic information • some aspects of biometric information.

Term	Definition
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 address 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
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

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