Australian Government

Office of the Australian Information Commissioner

Notifiable data breaches report

July to December 2022

1 March 2023

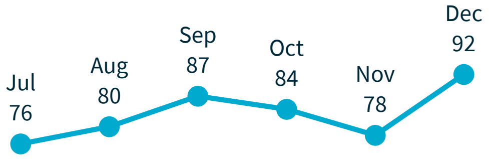
OAIC

Contents

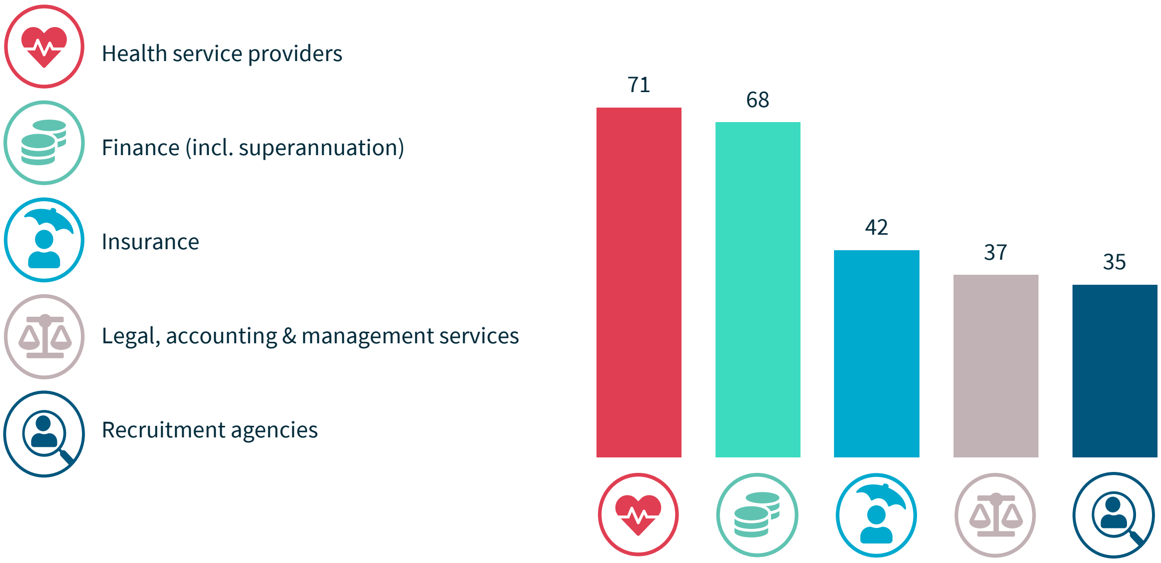
Snapshot

↑ **497** notifications

Up 26%



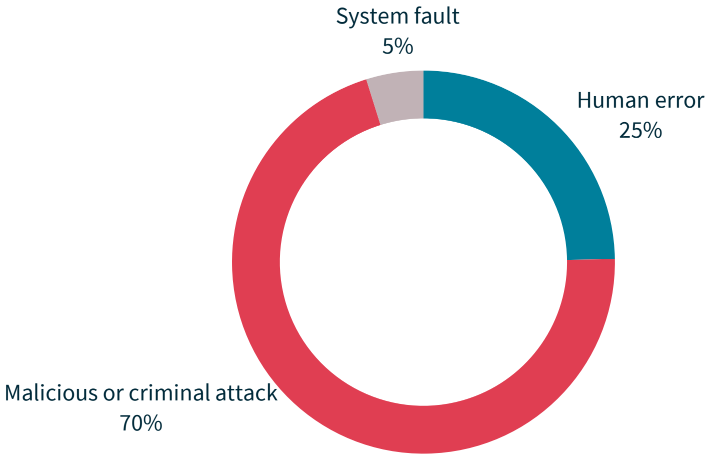
Top 5 sectors to notify data breaches



62%

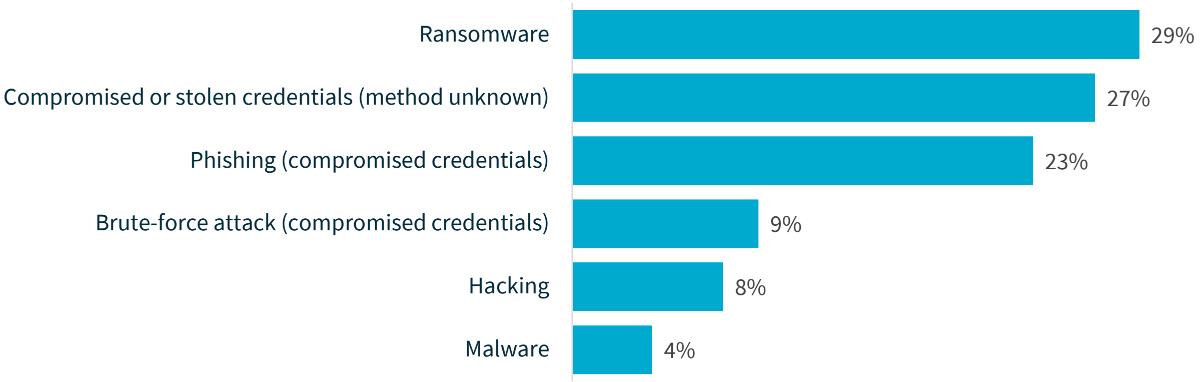
of data breaches affected 100 people or fewer

Sources of data breaches



45% of all data breaches resulted from cyber security incidents (222 notifications)

Cyber incident breakdown



Top causes of human error breaches

PI sent to wrong recipient (email) 42%

Unauthorised disclosure (unintended release or publication) 33%

Failure to use BCC when sending email 6%

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 received under the NDB scheme from 1 July to 31 December 2022.

Statistical comparisons are to the period 1 January to 30 June 2022 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.

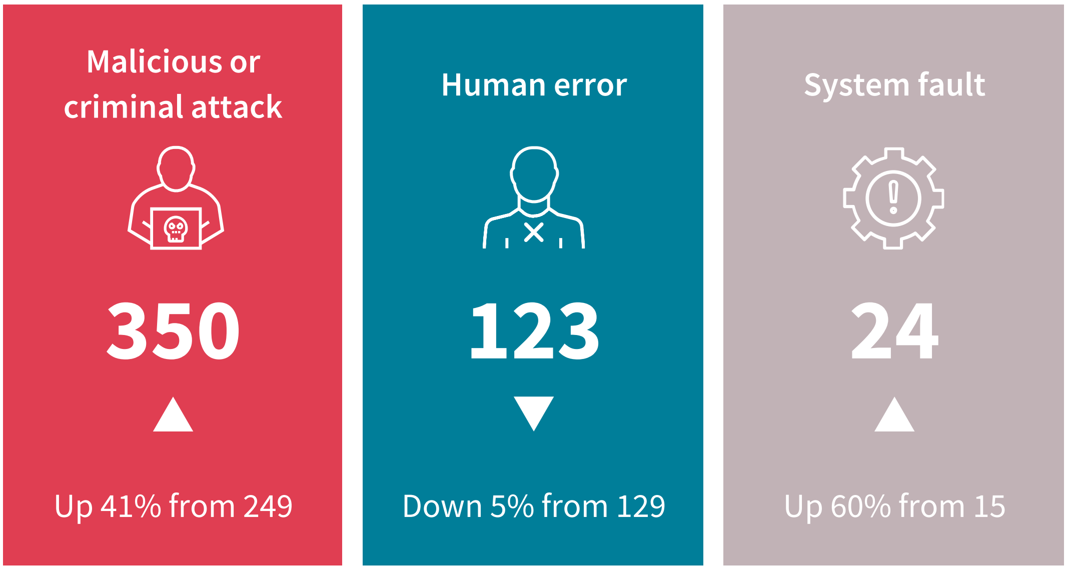
Notifications made under the *My Health Records Act 2012* are not included as they are subject to specific notification requirements set out in that legislation.

Statistics in this report are current as of 29 January 2023. 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 2022 published in future reports. Similarly, statistics from before July 2022 in this report may differ from those published in other reports.

Executive summary

The NDB scheme was established in February 2018 to drive better security standards and accountability for protecting personal information and improve consumer protection. 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 regulated entities' ongoing attention.



Malicious or criminal attack

350 ▲

Up 41% from 249

Human error

123 ▼

Down 5% from 129

System fault

24 ▲

Up 60% from 15

Key findings for the July to December 2022 reporting period:

- 497 breaches were notified compared with 393 in January to June 2022 – a 26% increase.
- There was a 41% increase in data breaches resulting from malicious or criminal attacks. Malicious or criminal attacks accounted for 350 notifications – 70% of all notifications.
- Human error was the cause of 123 notifications (25% of all notifications), down 5% in number from 129.
- Of all sectors, health reported the most breaches (71), followed by finance (68).
- Contact information remains the most common type of personal information involved in breaches.
- The majority (88%) of breaches affected 5,000 individuals or fewer.
- 71% of entities notified the OAIC within 30 days of becoming aware of an incident.

Notifications received July to December 2022 – All sectors

The OAIC received 497 notifications this reporting period – a 26% increase compared with January to June 2022.

After a low number of notifications in the first few months of 2022, the number of notifications received trended upwards across the calendar year. The lowest monthly total this reporting period was 76 notifications in July and the highest was 92 notifications in December.

Table 1 – Notifications received in 2022

Reporting period	Number of notifications
January to June 2022	393
July to December 2022	497
Total	**890**

Chart 1 – Notifications received by month from January 2021 to December 2022

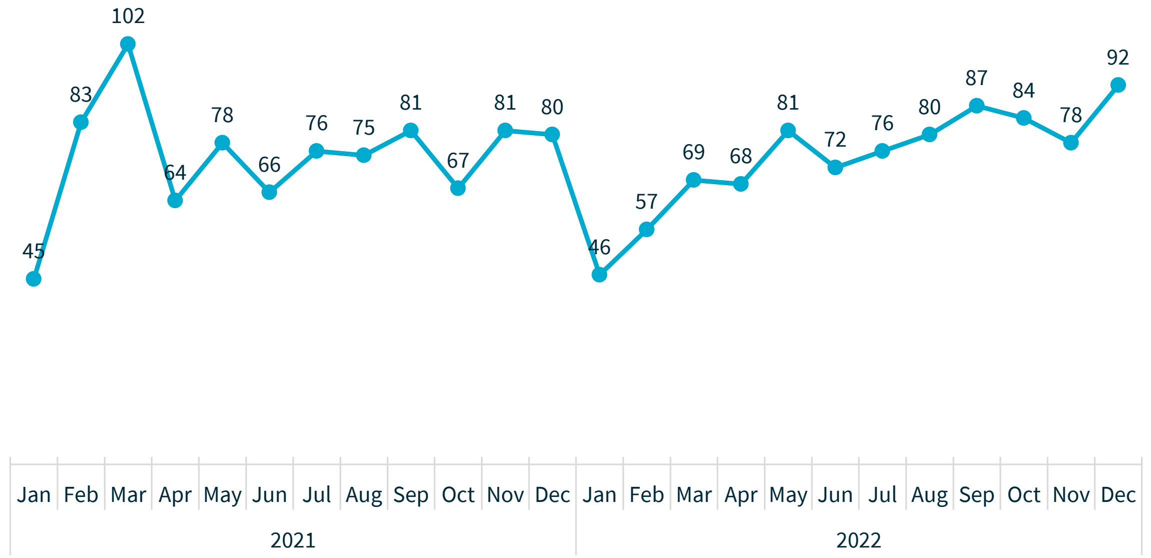
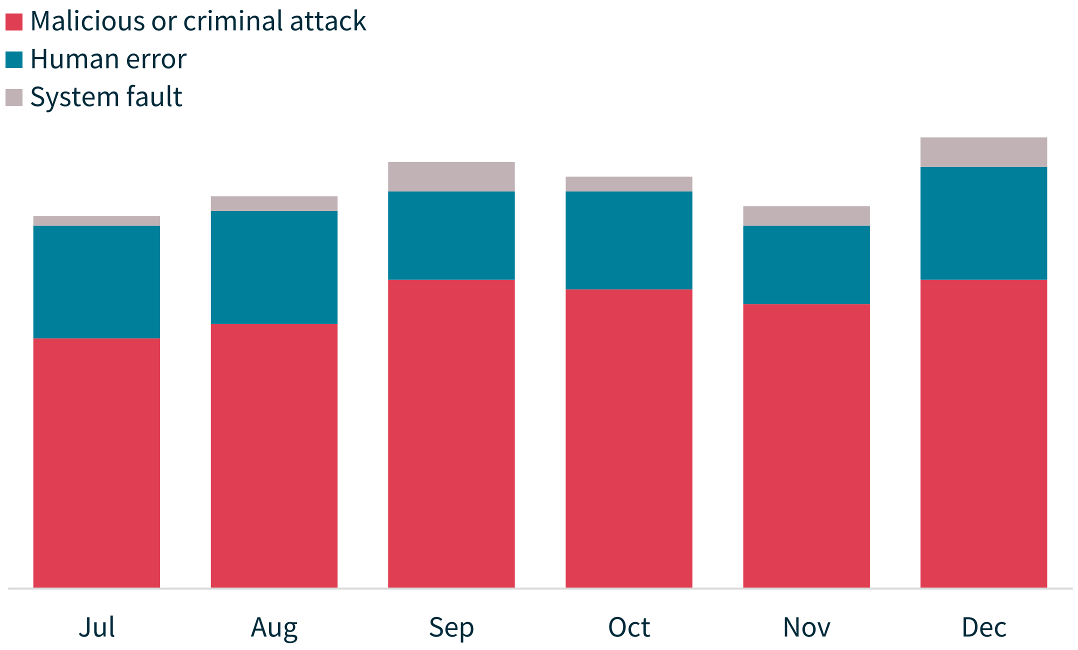


Chart 2 – Notifications received by month showing the sources of breaches



Regulatory approach

This reporting period, there were several large-scale data breaches that impacted millions of Australians' personal information, as well as a 26% increase in breaches overall. The response to these incidents demonstrated the high level of community concern about the protection of individuals' personal information.

In 2022, the OAIC welcomed the passing of the Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022. This law came into effect on 12 December 2022 and, among other things:

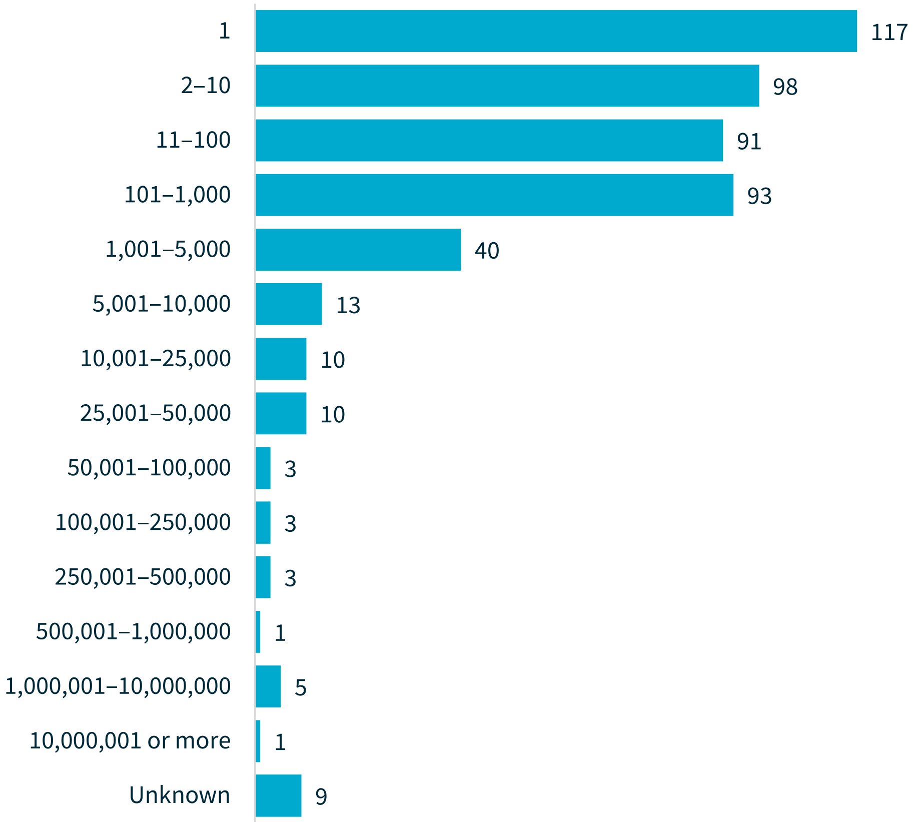
- provides the Commissioner with new and greater powers to quickly share information with other authorities about data breaches (s 33A)
- provides the Commissioner with a new power to obtain information and documents relevant to an actual or suspected eligible data breach (s 26WU)
- enables the Commissioner to conduct an assessment of the ability of an entity to comply with the NDB scheme, including the extent to which the entity has processes and procedures in place to assess suspected eligible data breaches, and provide notice to the Commissioner and individuals at risk from such breaches (s 33C(1)(ca))
- significantly increases penalties for serious or repeated privacy breaches, which includes non-compliance with the NDB scheme (s 13G).

The OAIC continues to work with entities to facilitate voluntary compliance and to ensure best privacy practice and prevent privacy breaches, including data breaches. However, entities should be aware that these new powers are intended to strengthen the NDB scheme and enhance the Commissioner's enforcement powers. Where appropriate, the Commissioner will use these regulatory powers to ensure compliance with the NDB scheme.

Number of individuals worldwide affected by breaches

Consistent with previous reports, most data breaches (88%) involved the personal information of 5,000 or fewer individuals worldwide. Breaches affecting 100 or fewer individuals comprised 62% of notifications and breaches affecting between 1 and 10 individuals accounted for 43% of notifications.

Chart 3 – Number of individuals 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.

Large-scale data breaches

The January to June 2022 report noted an increase in data breaches that impacted a larger number of Australians. This trend continued into the second half of the year.

Some of the large-scale data breaches reported this period attracted significant public interest. This interest may have raised awareness of the requirement for entities covered by the Privacy Act to notify the OAIC and individuals about eligible data breaches and increased the number of notifications in the second half of the reporting period.

There were 40 breaches that affected over 5,000 Australians this period, compared with 24 last report (a 67% increase). Five of these breaches affected over 1 million Australians, compared with 1 in the previous period.

Number of Australians affected by breaches	Jan–Jun 2022	Jul–Dec 2022
5,001–10,000	9	12
10,001–25,000	5	8
25,001–50,000	3	6
50,001–100,000	4	4
100,001–250,000	2	2
250,001–500,000	0	2
500,001–1,000,000	0	1
1,000,001–10,000,000	1	5
Total number of breaches affecting over 5,000 Australians	**24**	**40**

Cyber incidents continue to have a significant impact on individuals. Thirty-three of the 40 breaches that affected over 5,000 Australians were caused by cyber incidents. Of the 33 cyber incidents, 15 were caused by ransomware, 10 by compromised or stolen credentials, 7 by hacking and 1 by malware.

A further 2 incidents were caused by a rogue employee or insider threat, 2 were caused by social engineering and 1 was caused by theft of paperwork or a data storage device.

Entities must take appropriate and proactive steps to protect against and respond to a range of cyber threats. The Australian Cyber Security Centre (ACSC) considers the most effective way to defend against cyber threats is to implement the Essential Eight cyber security strategies. For further advice on protecting personal information and responding to cyber incidents, see the ACSC cyber incident response plan guidance, template and checklist and the OAIC's guidance on securing personal information and data breach preparation and response.

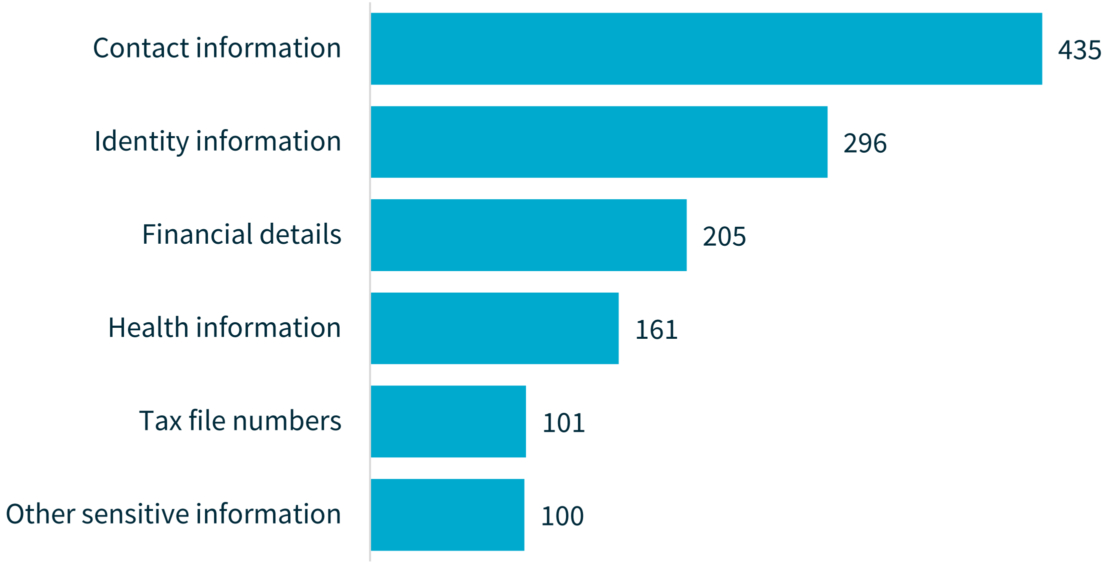
Kinds of personal information involved in breaches

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

Most breaches (88%) 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 60% 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 41% 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

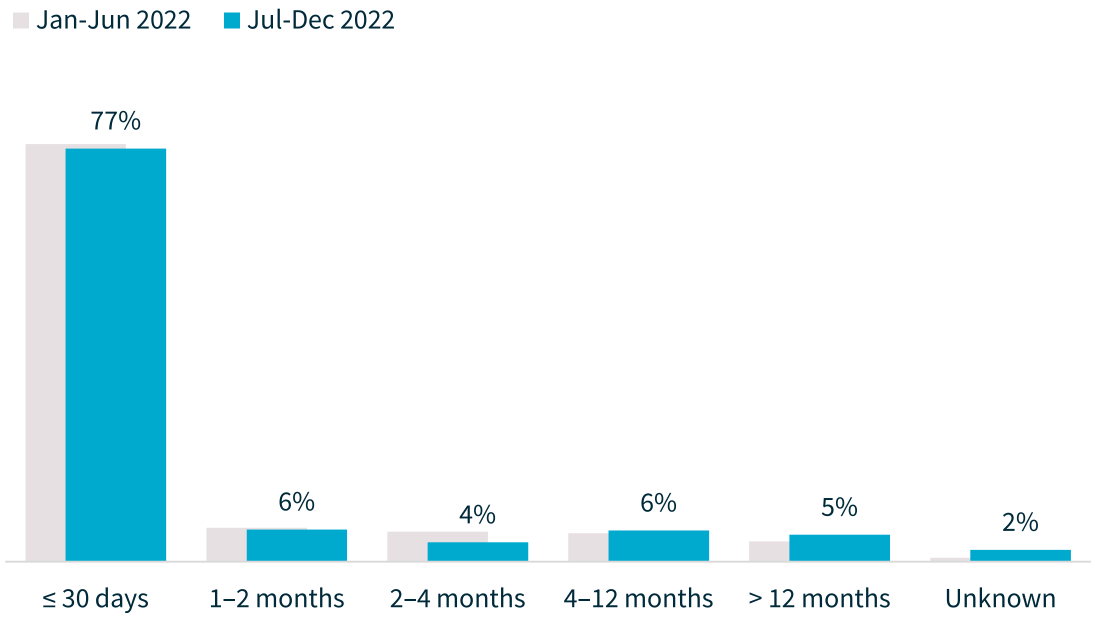
A key objective of the NDB scheme is to protect individuals by enabling them to respond quickly to a data breach to mitigate the risk of harm. Delays in identifying, assessing and notifying breaches reduce the opportunities for an individual to take steps to prevent harm.

Under Australian Privacy Principle 11, entities must take such steps as are reasonable in the circumstances to protect the information they hold from misuse, interference and loss, and from unauthorised access, modification or disclosure. As part of complying with APP 11, entities should ensure they have measures in place to promptly detect data breaches.

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, 77% of breaches were identified by the entity within 30 days of it occurring, similar to the previous period (78%).

Chart 5 – Time taken to identify breaches



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

[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.

Using monitoring and audit logs to quickly assess a suspected breach

Understanding data holdings can reduce the time and resources an entity requires to effectively assess a data breach and support incident response.

Entities that have sufficient audit and activity logging capabilities enabled on their networks, email servers and accounts are better prepared to assess and determine the information accessed and exfiltrated, or likely accessed and exfiltrated, by a threat actor if a data breach occurs.

The following scenarios highlight the difference that having monitoring and audit logs in place can have when dealing with a data breach incident.

Scenario

An entity experienced a phishing attack and an employee's email account was compromised.

The entity's preliminary review of the contents of the compromised email account indicated it contained a large quantity of personal information, ranging from contact information to picture copies of driver licences and passports.

Based on a review of audit logs, the entity determined the extent of information in the account that was accessed and that the threat actor had only sent themselves a copy of a contact list, which they attempted to hide by deleting the email from the sent folder.

The entity was therefore able to promptly notify individuals on the contact list and provide information about phishing scams and how to recognise legitimate emails from the entity.

Scenario

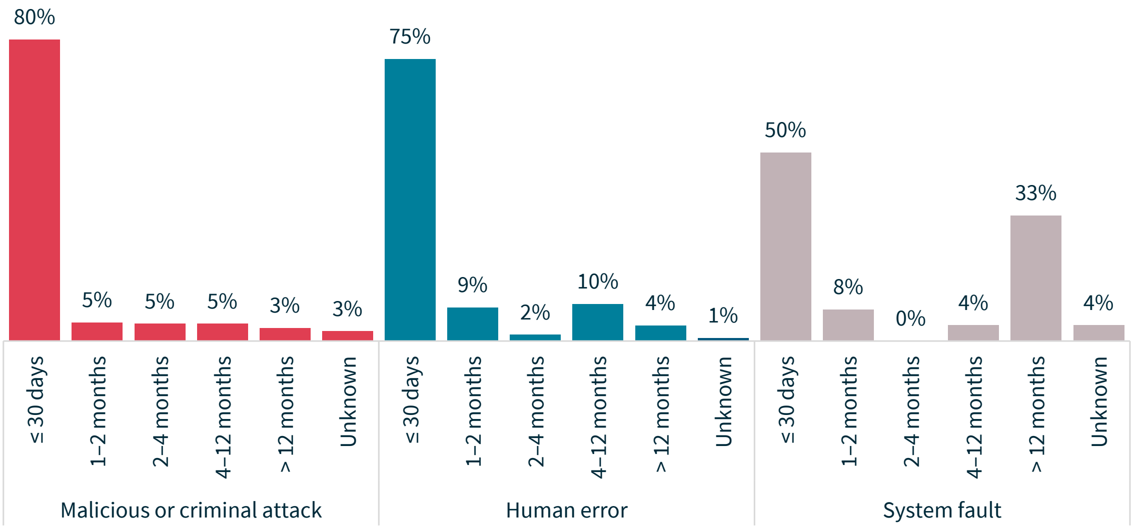
An employee's email account was compromised, which resulted in a threat actor gaining unauthorised access to the entity's database.

Cyber security specialists conducted a forensic analysis on the entity's behalf and were unable to conclude whether the threat actor had accessed personal information in the entity's database. This is because the entity had only retained audit logs for a limited period, which did not include the dates of the incident. This meant that valuable evidence of the breach had not been preserved.

As the entity was unable to confirm the extent of unauthorised access, it had to presume all personal information in the database was accessible to the threat actor and consequently had to notify all potentially affected individuals.

Across the life of the scheme, the time taken by entities to identify breaches has tended to vary depending on the source of breach. In the reporting period, entities generally identified breaches caused by malicious or criminal attack the fastest and system fault breaches the slowest. A third (33%) of system fault breaches were not identified for over a year.

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.

Detecting and preventing system faults

Entities should implement measures to monitor and promptly detect system faults, which can be caused by hardware malfunctions or software settings errors, or even by natural disasters and extreme weather conditions. Entities should also consider whether the software they use is sufficiently secure and has been developed to support privacy and prevent and limit the impact of data breaches.

Entities can assess personal information security risks by conducting a privacy impact assessment and an information security risk assessment, and regularly reviewing personal information security controls. These practices will help entities ensure they are aware of the variety of security risks and the possible impacts and can address them in designing and implementing any new or changed way of handling personal information. This will assist entities to integrate privacy considerations into risk management strategies.

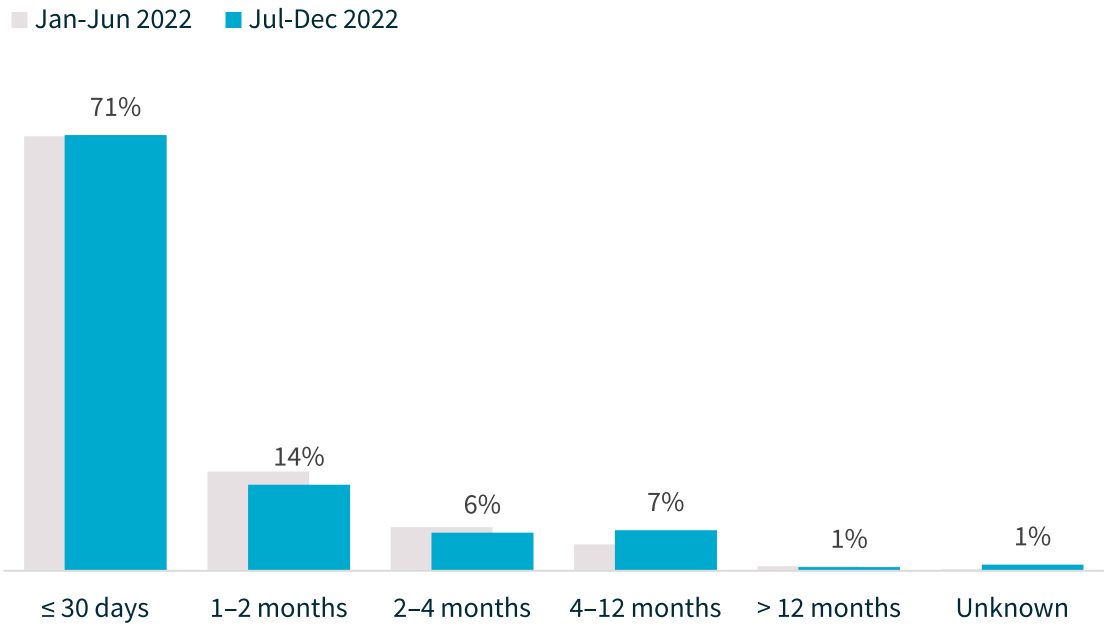
Time taken to notify the OAIC of breaches

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.

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

Entities notifying individuals at the same time as the OAIC or shortly after helps individuals take timely steps to protect themselves from harm.

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.

The importance of timely notification

Failure to notify individuals affected by a data breach in a timely manner undermines an entity's relationship with its customers or clients as it reduces their ability to take steps to mitigate risks arising from the data breach. Proactive, timely and helpful notification to affected individuals builds confidence that an entity has systems and processes in place to identify and quicky respond to data breaches and prioritises the needs of its customers or clients.

Where there are reasonable grounds to believe an eligible data breach of an entity has occurred, the Commissioner may issue a notice under s 26WR of the Privacy Act, directing an entity to prepare a statement about the data breach, provide it to the Commissioner and notify affected individuals.

The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* gave the Commissioner further powers under s 26WU to obtain information and documents regarding an actual or suspected eligible data breach of an entity and the entity's compliance with the NDB scheme. This new provision supports the OAIC's regulatory role to facilitate timely notification to affected individuals and ensure compliance with the NDB scheme.

Notifying individuals while events unfold

The Privacy Act requires entities to notify individuals about an eligible data breach, including certain information about the incident, as soon as practicable. There are 3 options for notifying individuals:

- The entity can notify each individual whose personal information was involved in the eligible data breach.
- The entity can notify only those individuals who are at risk of serious harm.
- If neither option is practicable, the entity can publish a statement on the eligible data breach on its website and publicise the statement.

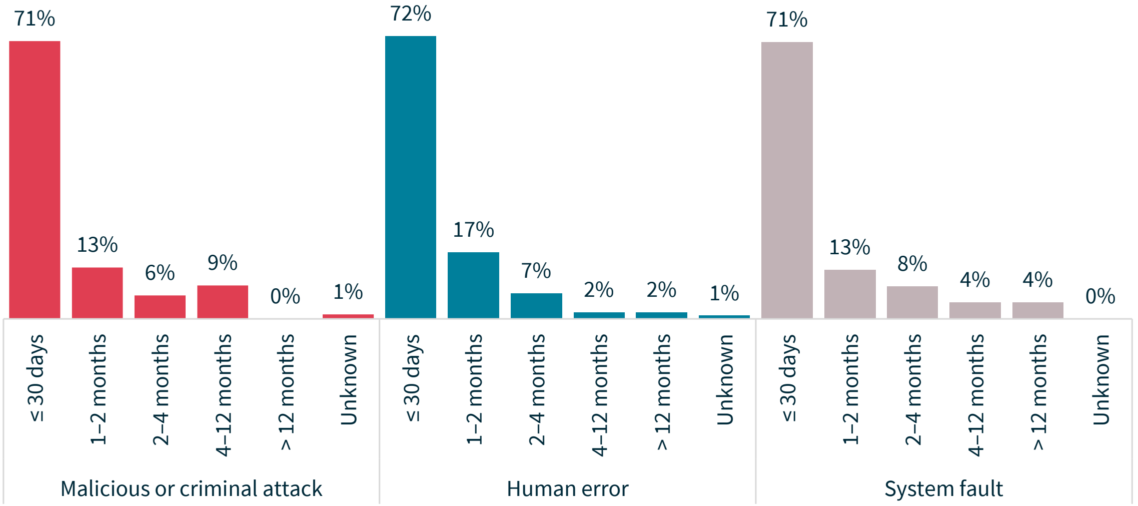
A key objective of the NDB scheme is to promote notification to individuals. The information in a notification needs to be timely, trustworthy and easy for individuals to action. Regardless of the method of notification, entities should seek to ensure the information they provide to individuals is accurate and reliable.

Where an eligible data breach is unfolding, there can be challenges in ensuring the notification to individuals is both timely and accurate. In this situation, entities may wish to consider:

- Including in their data breach response plan a strategy for when and how to communicate information about data breaches to individuals. This can assist with making decisions on notification when an incident occurs.
- When notifying individuals directly as well as providing information on their website, seeking to ensure consistent information is provided and updates are communicated clearly.
- Where an entity is unable to complete its assessment promptly and within 30 days, and there are grounds to suspect an eligible data breach may have occurred, consider erring on the side of caution and notifying affected individuals and the OAIC.

There was limited variation by source of breach in the time taken by entities to notify the OAIC after identifying an incident.

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.

A data breach response plan ensures a timely response

The Privacy Act is clear that an entity responding to a data breach must:

- carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the incident amounts to an eligible data breach, and take all reasonable steps to complete the assessment within 30 days
- notify affected individuals and the OAIC as soon as practicable after becoming aware there are reasonable grounds to believe an eligible data breach occurred.

Entities should have a data breach response plan that incorporates the requirements of the NDB scheme. A data breach response plan enables an entity to identify and respond to a data breach quickly. By responding quickly using an existing data breach response plan, an entity can decrease the impact of a breach on affected individuals, reduce the costs associated with dealing with a breach and reduce the potential reputational damage that can result.

Scenario

An entity became aware of unauthorised access to its Microsoft 365 environment. Due to the time it took to appoint a specialist forensic investigator, the entity did not commence an investigation to determine the extent of breach until 2 months later. As a result of this delay in identifying and assessing the breach, there were substantial delays in notifying the breach.

Had the entity had a data breach response plan incorporating the requirements of the NDB, it may have enabled the entity to:

- identify appropriate escalation points
- ensure remedial steps were taken immediately
- commence an investigation at an earlier stage or to take more rapid steps to appoint a specialist, so that the assessment and notification could be completed sooner.

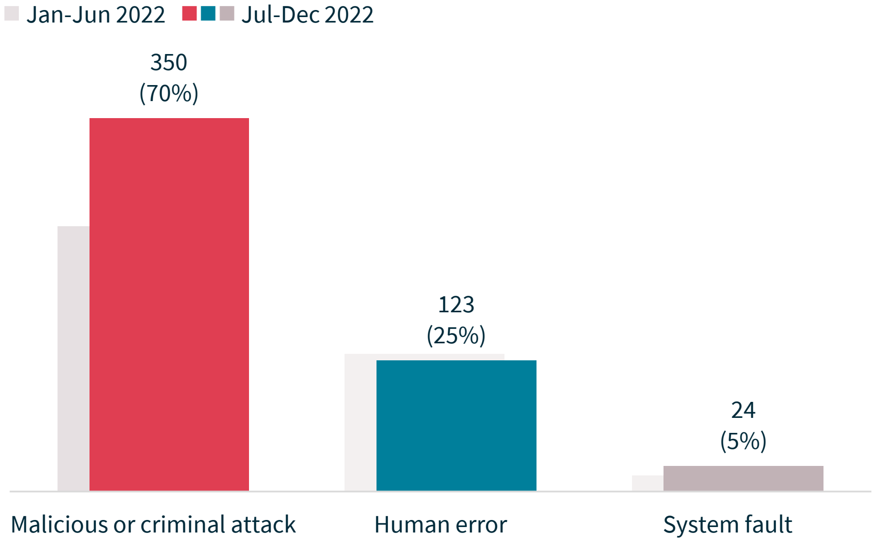
Source of breaches

There was a significant increase in breaches caused by malicious or criminal attack, both in terms of the total number of notifications received (up 41% to 350) and as a proportion of all notifications received (up from 63% to 70%).

The number of human error breaches was down 5% from 129 to 123. Human error breaches accounted for 25% of all notifications, compared with 33% the previous period.

System faults accounted for 24 breaches (up from 15), or 5% of all notifications. The proportion of breaches attributed to system faults has been consistent since the NDB scheme began.

Chart 9 – Source of data breaches

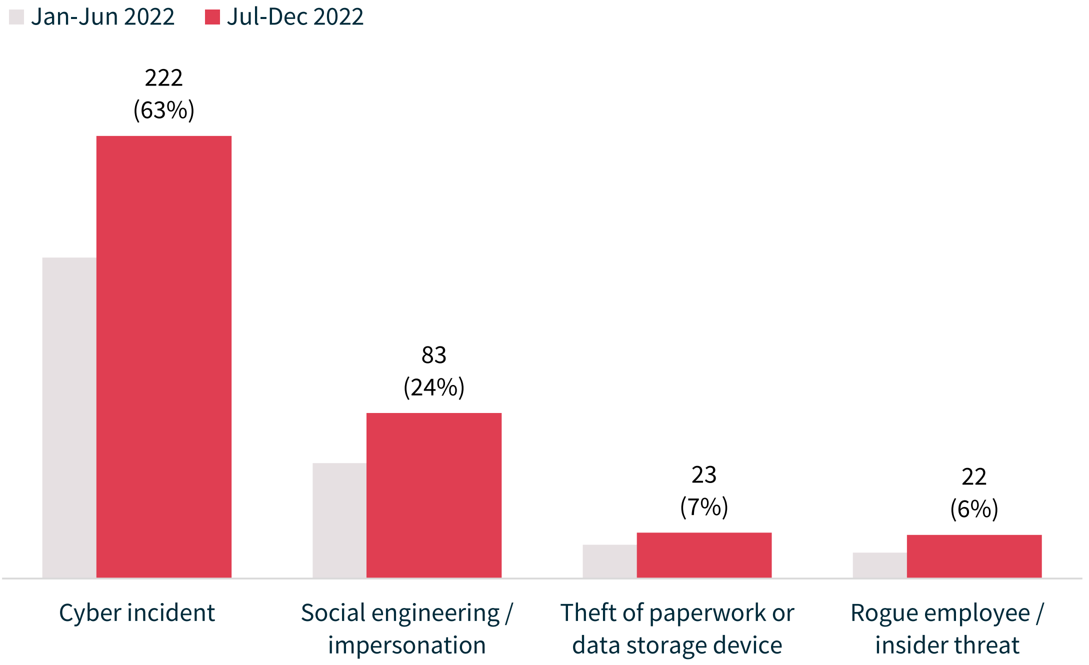


Malicious or criminal attacks

The majority (63%) of breaches caused by malicious or criminal attacks were cyber incidents. There were 222 breaches resulting from cyber incidents, up 38% from 161. Forty-five per cent of all data breaches resulted from cyber incidents, compared with 41%.

Social engineering or impersonation accounted for 24% of data breaches caused by malicious or criminal attack, theft of paperwork or data storage device for 7% and actions taken by a rogue employee or insider threat for 6%.

Chart 10 – Malicious or criminal attack breakdown

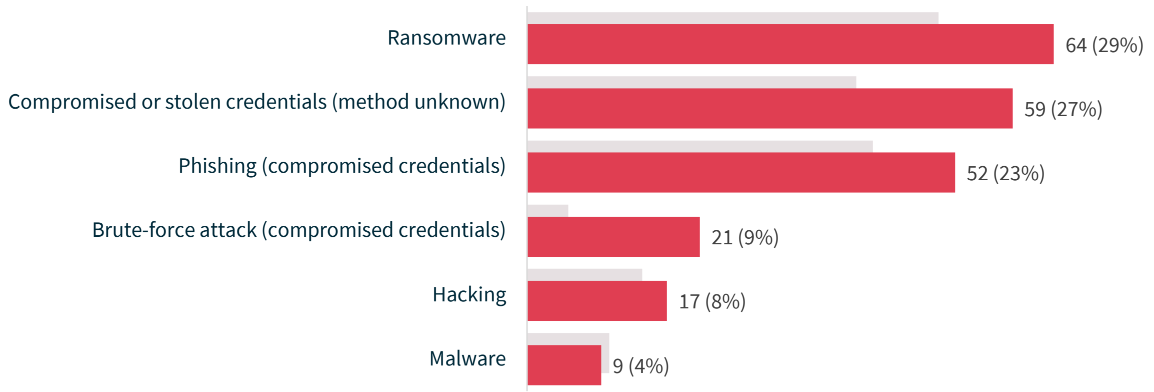


Cyber incidents

The top sources of cyber incidents were ransomware (29% of cyber incidents; 64 notifications), compromised or stolen credentials (method unknown) (27%; 59 notifications) and phishing (23%; 52 notifications).

To gain initial access to an entity's networks or systems, threat actors commonly use compromised or stolen credentials. This reporting period, 59% of cyber incidents involved malicious actors exploiting compromised or stolen credentials. If compromised credentials are used by a threat actor, and this is not prevented or promptly detected, this can lead to further kinds of data breach incidents, including ransomware attacks.

Chart 11 – Cyber incident breakdown



Evidence of cyber incident data breaches

During this reporting period, some entities indicated they considered there to be a lower risk of serious harm to affected individuals either because their investigation of a data breach did not find evidence that data had been exfiltrated, or because their perceived understanding of the threat actor's motivations led them to believe individuals were unlikely to be harmed.

In some instances, these entities later became aware of information or events that meant these assessments were inaccurate. Moreover, their initial assessment meant individuals were not notified promptly.

Entities should take a holistic approach to their assessment of whether a data breach is likely to result in serious harm to individuals. Among the factors entities should consider are:

- the likelihood that any security measures protecting the information could be overcome
- the kinds of persons who have obtained, or who could obtain, the information (s 26WG).

Whether serious harm to individuals is likely is to be determined from the perspective of a reasonable person. In determining this, entities should be cautious about relying on:

- A lack of evidence that data has been exfiltrated. In many cases, an eligible data breach can occur based on access to information alone. Moreover, some threat actors are careful to delete evidence of their actions within a system, limiting the reliability of a lack of evidence, particularly where an entity does not have adequate audit and activity logs. Finally, not locating the data on the dark web does not mean it has not been disclosed.
- A perceived understanding of a threat actor's motivations. Entities need to consider the reliability or credibility of the presumed or purported motivation of a threat actor.

Practical strategies for preventing impersonation attacks

During this reporting period, there were a number of breaches that resulted in large-scale compromises of personal information. As personal information increasingly becomes available through large-scale breaches, the likelihood of other attacks, such as targeted social engineering, impersonation fraud, phishing and scams, can increase.

Impersonation fraud involves a malicious actor impersonating another individual to gain access to an account, system, network or physical location. In most cases, the impersonator already possessed some, if not all personal information required to circumvent an entity's identity verification process.

Entities are advised to have robust controls and identity verification processes in place to minimise the risk of impersonation fraud or social engineering, including:

- training staff about identity verification processes and how to report and escalate fraud
- automatically notifying customers when there are changes to their account or failed authentication attempts, or when their account is accessed from a new device or location
- a data breach response plan that sets out clear lines of authority for escalation and decision-making in the event of any actual or suspected data breach incidents.

Where practicable, entities should also consider:

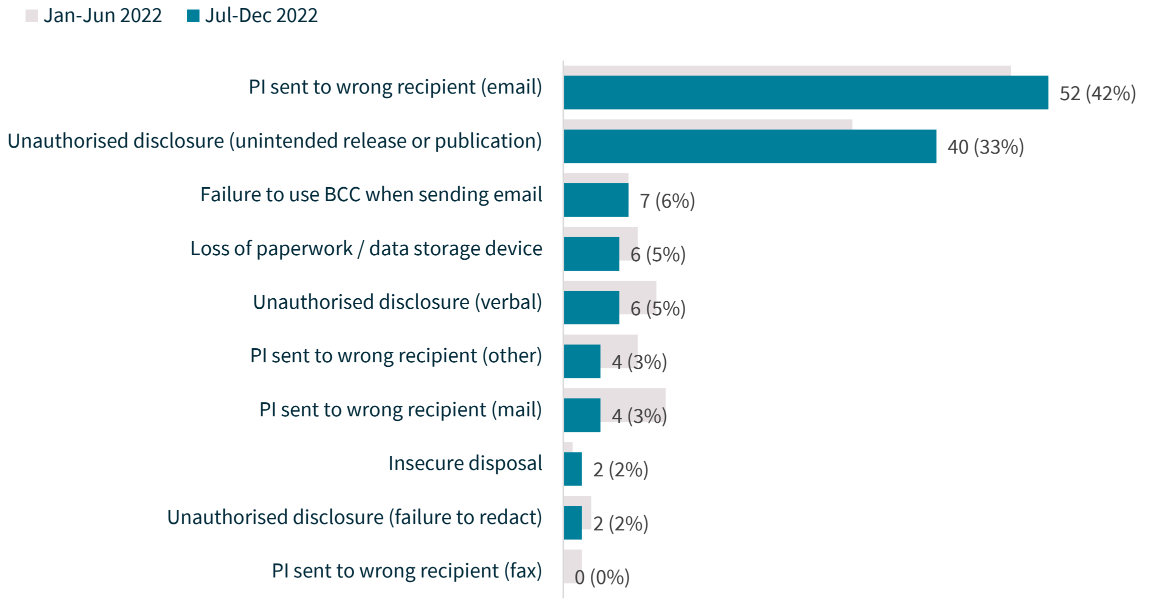
- masking personal information within customer accounts to reduce risk should the account be accessed without authorisation
- temporarily disabling online accounts that have been subjected to failed verification attempts
- hiding webform responses, for example, to ensure a login or password reset form does not reveal the validity of information entered
- enhancing capabilities to detect and prevent unusual or suspicious logins from internet service provider addresses and geolocations
- increasing the frequency of internal audit and quality assurance activities
- providing privacy training to new staff on commencement and all staff at least annually.

Entities should also be aware that a social engineering incident can constitute an eligible data breach, even if a threat actor leveraged personal information they had already obtained (for example, through another data breach) to circumvent or exploit an entity's security and identity verification processes.

Human error

Personal information being emailed to the wrong recipient was the most common cause of human error breaches. In fact, almost half (49%) of human error breaches involved personal information being sent to the wrong recipient either by email, mail 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 1,328 people per breach, while verbal disclosure affected one person on average per breach.

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

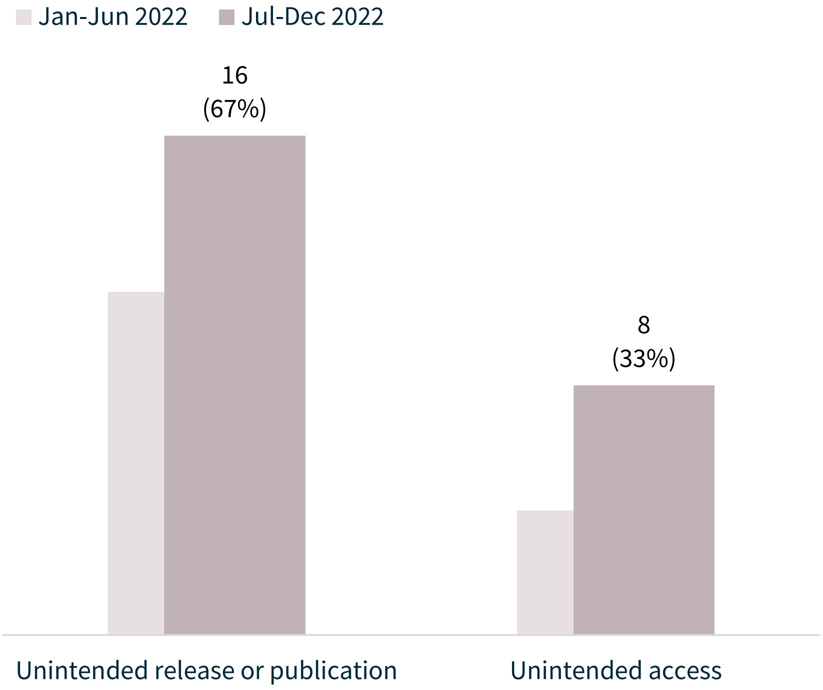
Source of breach	Number of notifications	Average number of affected individuals
Unauthorised disclosure (unintended release or publication)	40	1,328
Failure to use BCC when sending email	7	262
Insecure disposal	2	77
PI sent to wrong recipient (email)	52	66
Loss of paperwork/data storage device	6	24
PI sent to wrong recipient (mail)	4	9
Unauthorised disclosure (failure to redact)	2	2
PI sent to wrong recipient (other)	4	2
Unauthorised disclosure (verbal)	6	1
Total	**123**	**481**

System faults

The majority (67%) of system fault breaches involved the unintended release or publication of personal information. Examples of issues that may lead to this include misalignments between systems and databases, untested system and infrastructure changes, and automated messages being sent to incorrect recipients.

Unintended access to personal information because of a system fault caused 8 breaches (33% of system faults). Among other things, these breaches were attributed to the failure to maintain accurate and up-to-date access security measures, including in relation to customer accounts, and vulnerabilities in web forms and associated databases.

Chart 13 – System fault breakdown



Breaches that involve third-party service providers

When more than one entity holds personal information that is subject to a data breach, all affected entities have obligations under the NDB scheme. To meet these obligations, only one of the affected entities needs to conduct an assessment of the suspected eligible data breach under s 26WH of the Privacy Act and notify affected individuals and the OAIC. If no affected entity complies with the NDB scheme requirements, then all affected entities will be considered non-compliant.

Although only one entity is required to notify a data breach affecting multiple entities, the number of secondary notifications (notifications relating to the same data breach incident) continues to increase; 42 secondary notifications were received this period compared to 22 in January to June 2022 (a 91% increase). Moreover, 8 of the 40 large-scale data breaches that affected over 5,000 Australians this period involved a service provider relationship.

This indicates the significant data breach risks that can arise in the handling of personal information where there is a service provider or contractor relationship.

Where an entity receives services from a third-party that involve the handling of personal information, or itself provides such services to other entities, it is recommended entities:

- 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 can most effectively complete the assessment, and the entity (or entities) with the most direct relationship with affected individuals is best placed to notify affected individuals.
- Establish and implement data breach response plans to support a timely and efficient response. Where an entity deals with other entities in handling personal information, this could include strategies for managing breaches and set out roles and responsibilities, acknowledging these information flows.
- Have a service agreement or contractual arrangement in place and ensure it addresses the handling of personal information and steps to respond to a data breach. Agreements of this kind can enable multiple entities impacted by a single data breach to respond quickly and ensure affected individuals and the OAIC are notified as soon as practicable. It can be especially beneficial to have such an agreement in place where an entity handles personal information for or on behalf of a business that is not covered by the Privacy Act.

Scenario

An information technology (IT) service provider experienced a ransomware attack. Its systems were accessed by a threat actor, data was exfiltrated and a subset of the data was uploaded on a public forum.

As the IT provider had a detection and data breach response plan in place, it was able to quickly identify the breach and stop it from impacting other environments. In line with its data breach response plan, the IT provider assessed the impact of the breach, establishing the kinds of personal information involved, quickly after becoming aware of the breach.

The IT provider notified the OAIC and informed its client organisations of the incident. It also took proactive measures to ensure affected individuals were notified by the client organisations, including:

- emailing client organisations and having follow-up telephone discussions in some instances
- informing the OAIC of the client organisations impacted by the incident
- publishing a statement on its website
- directly notifying the affected individuals on behalf of certain client organisations.

These steps reduced the impact the breach had on the operation of the IT provider and its client organisations' businesses and prevented any delays in the client organisations notifying affected individuals.

Comparison of top 5 sectors

This section compares notifications received under the NDB scheme by the top 5 sectors by notifications, which accounted for 51% of all notifications.

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 71 data breaches (14% of all notifications). The second largest source of notifications was the finance sector, which reported 68 data breaches (also 14% of all notifications).

The other sectors in the top 5 by notifications were insurance (8%), legal, accounting and management services (7%) and recruitment agencies (7%).

Table 3 – Top 5 sectors by notifications

Sector	Number of notifications	Percentage of all notifications received
Health service providers[2]	71	14%
Finance[3]	68	14%
Insurance	42	8%
Legal, accounting and management services	37	7%
Recruitment agencies	35	7%
Total	**253**	**51%**

[2] 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, regardless of annual turnover.

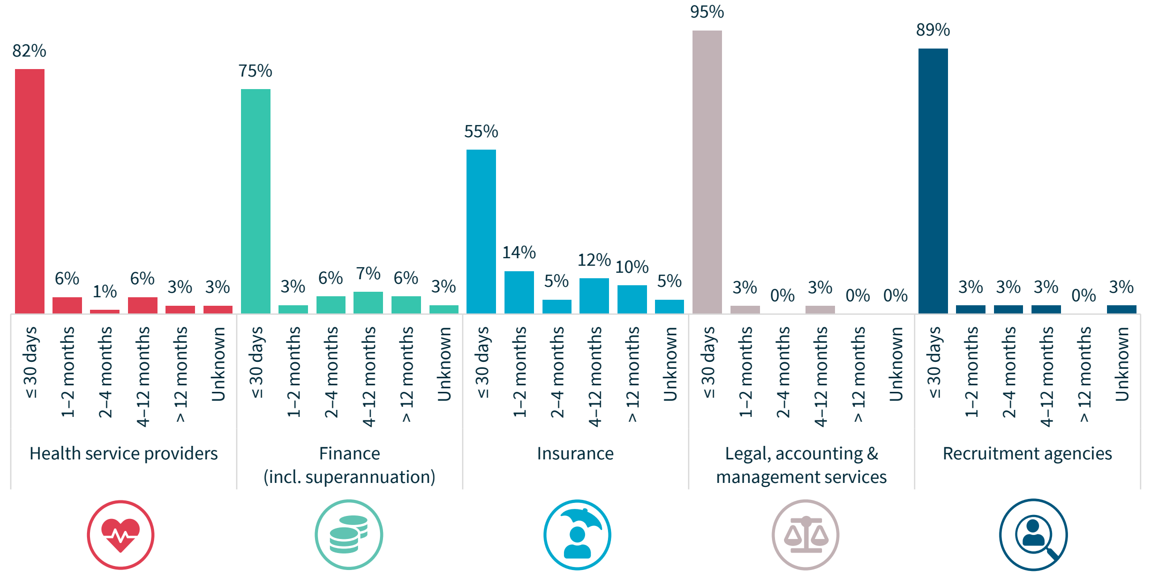
[3] This sector includes banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

Time taken to identify breaches – Top 5 sectors

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

In the reporting period, 95% of entities in the legal, accounting and management services sector identified the incident within 30 days of it occurring, while this was 55% for the insurance sector. Ten per cent of entities in the insurance sector took over 12 months to identify breaches.

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



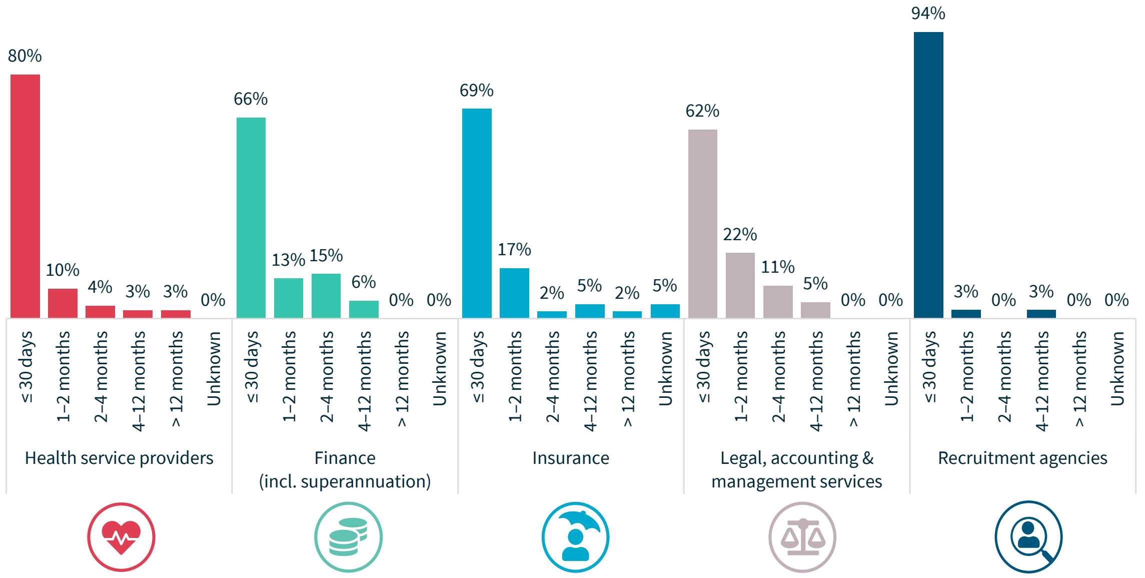
For notifications in the ‘unknown’ category, the entity was unable to identify the date the breach occurred.

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

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

Ninety-four per cent of notifications from recruitment agencies were made within 30 days of the entity becoming aware of the incident. This figure was 62% for entities in the legal, accounting and management services sector.

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

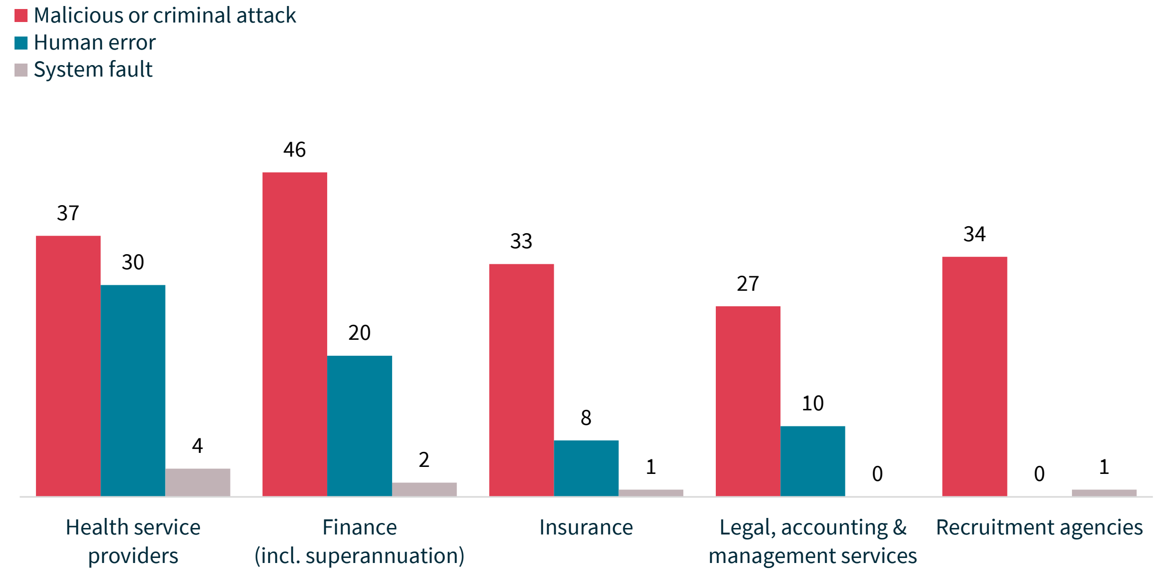


For notifications in the ‘unknown’ category, the entity was unable to identify the date the breach occurred.

Source of breaches – Top 5 sectors

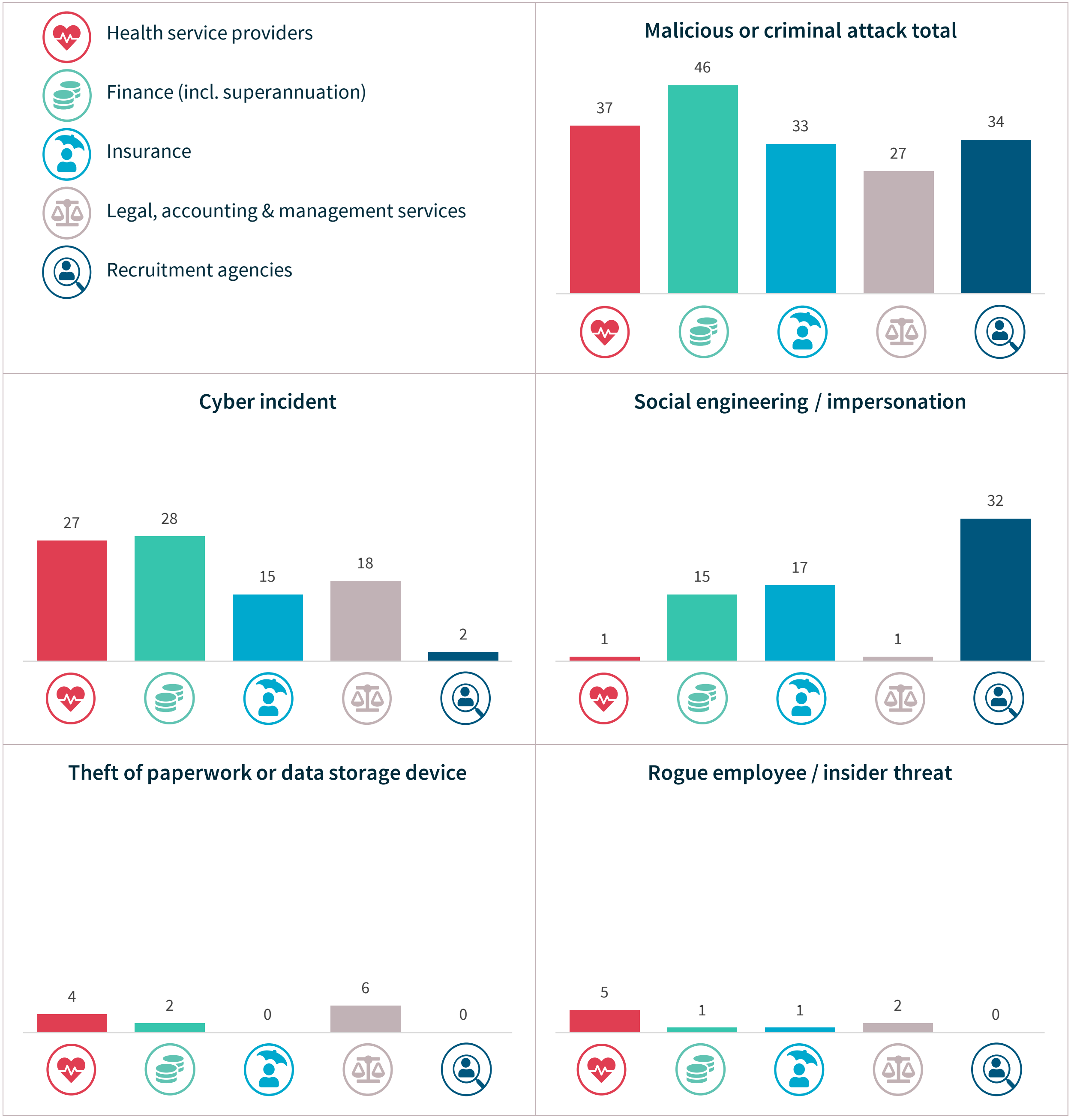
Malicious or criminal attack was the top cause of data breaches notified by the top 5 sectors. It was the source of 97% of breaches notified by recruitment agencies, 79% of insurance sector breaches, 73% of legal, accounting and management services breaches, 68% of finance sector breaches and 52% of health sector breaches.

Chart 16 – Source of breaches – Top 5 sectors



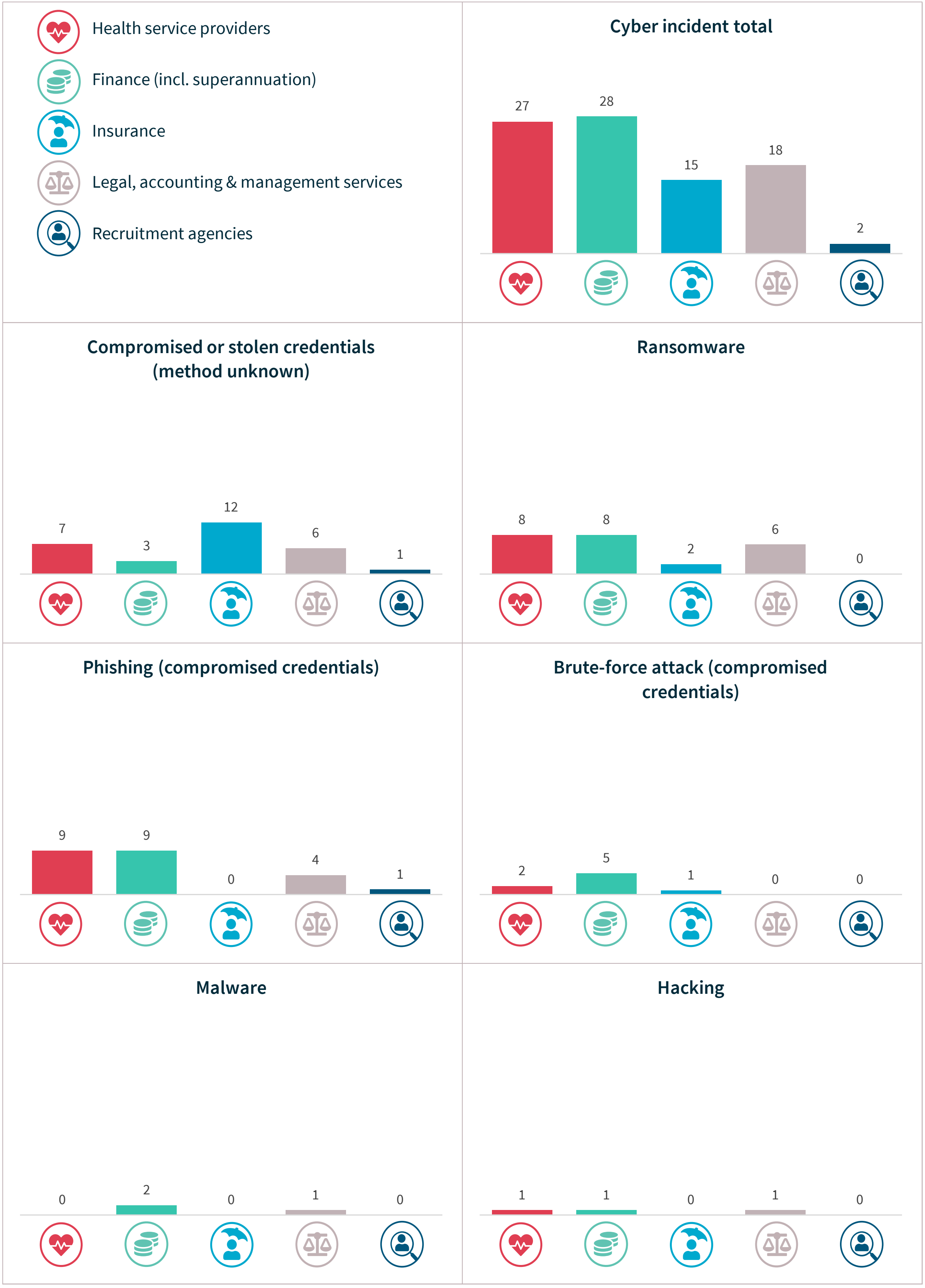
Malicious or criminal attack breaches – Top 5 sectors

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



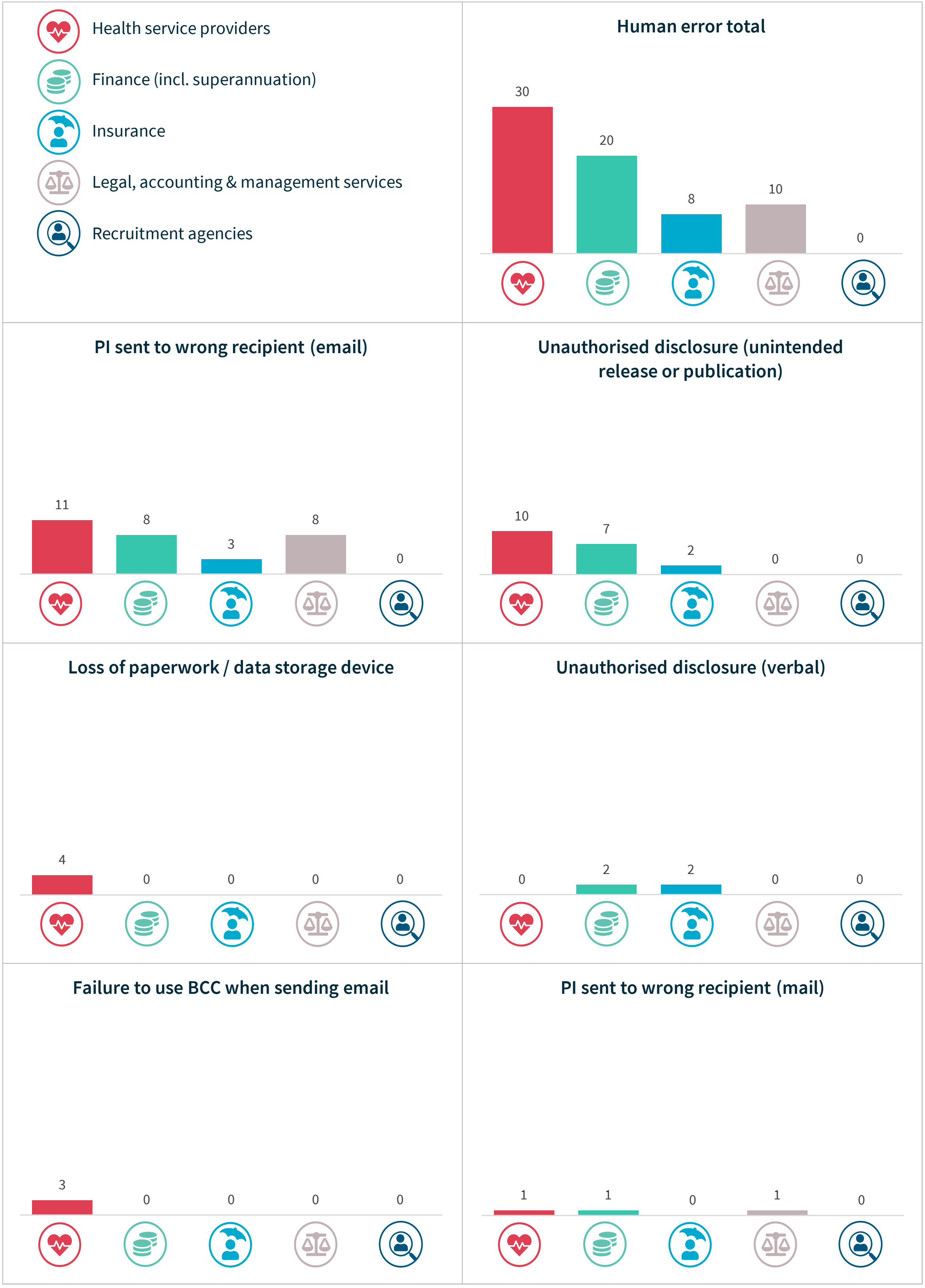
Cyber incident breaches – Top 5 sectors

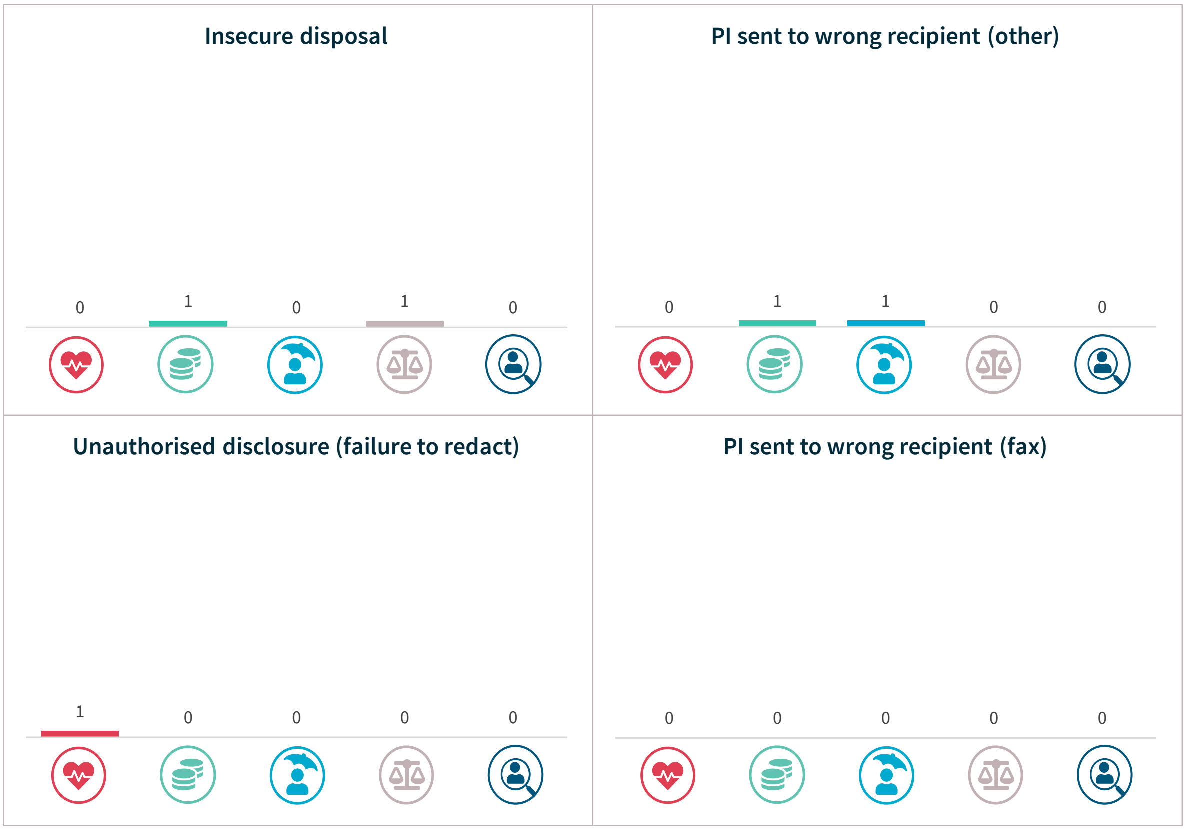
Chart 18 – Cyber incident breakdown – Top 5 sectors



Human error breaches – Top 5 sectors

Chart 19 – Human error breakdown – Top 5 sectors





Insecure disposal

PI sent to wrong recipient (other)

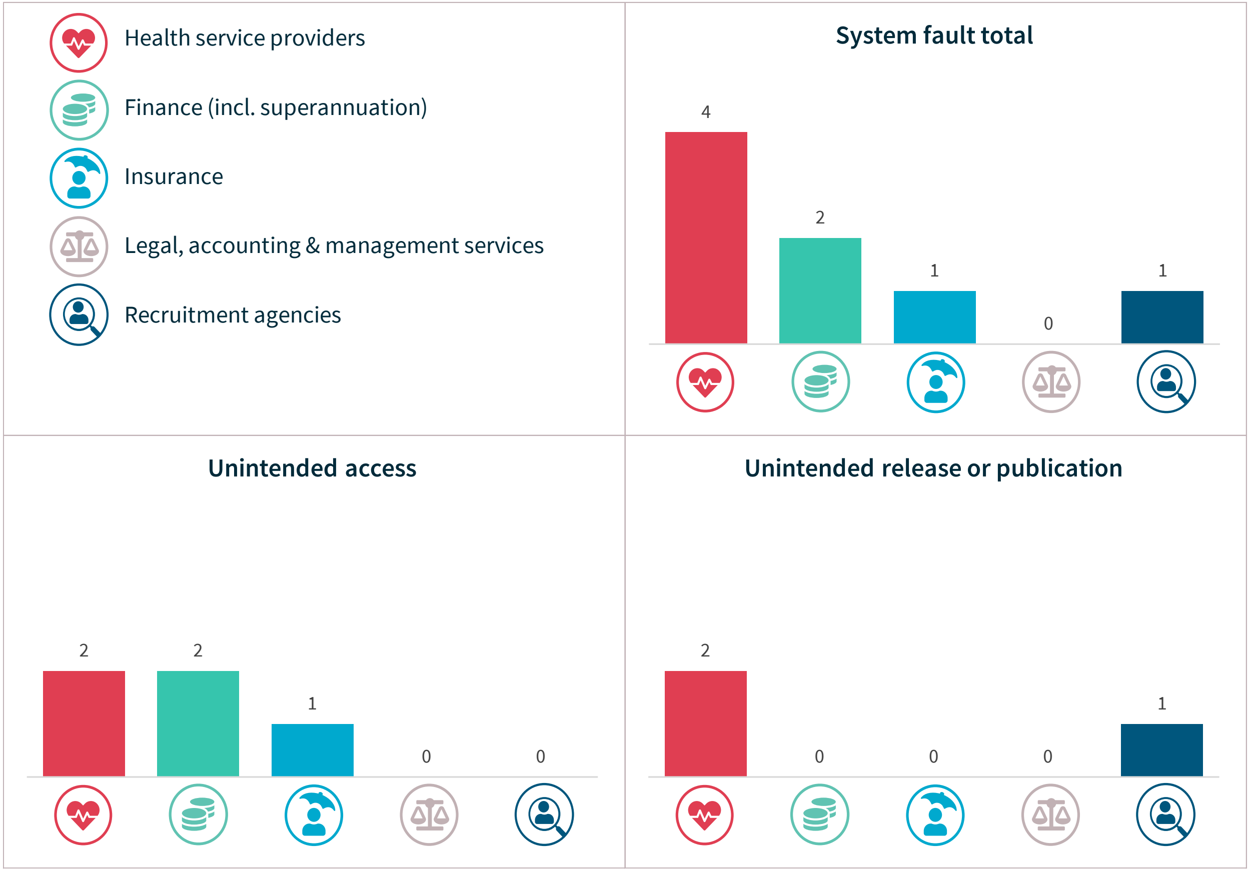
Unauthorised disclosure (failure to redact)

PI sent to wrong recipient (fax)

System fault breaches – Top 5 sectors

Four of the top 5 sectors notified data breaches resulting from a system fault, with legal, accounting and management services the exception.

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 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
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 • health or genetic information

Term	Definition
	• 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
Unauthorised disclosure (unintended release or publication)	Unauthorised disclosure of personal information in a written format, including paper documents or online

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