Australian Government

Office of the Australian Information Commissioner

Notifiable data breaches report

January to June 2023

5 September 2023

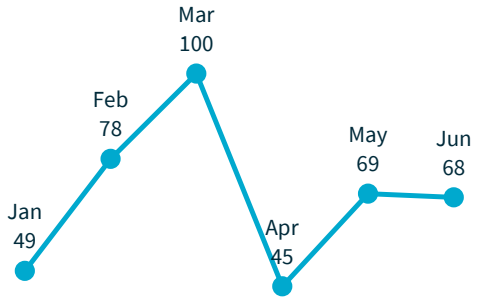
OAIC

Contents

Snapshot

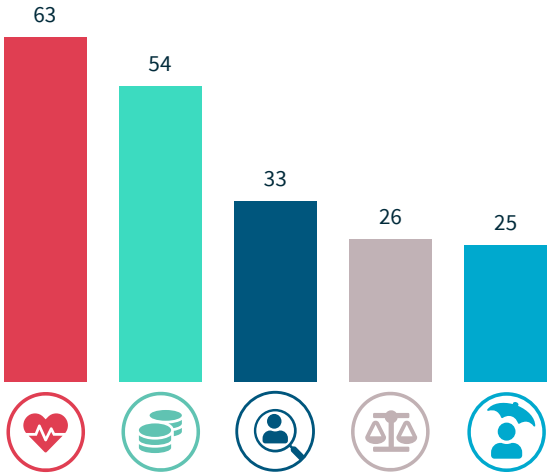
409
notifications

Down 16%



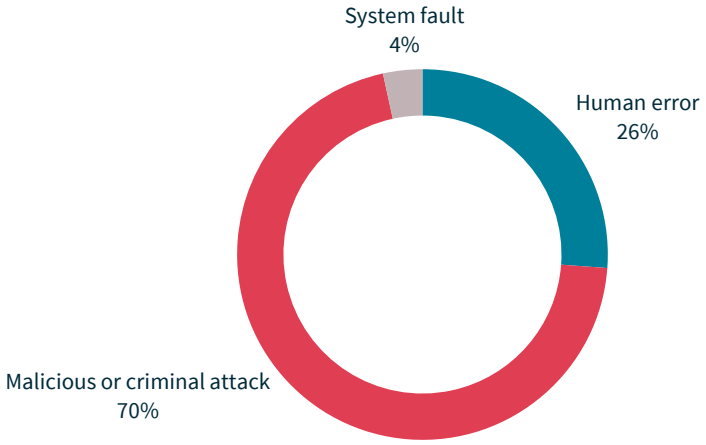
Top 5 sectors to notify data breaches

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



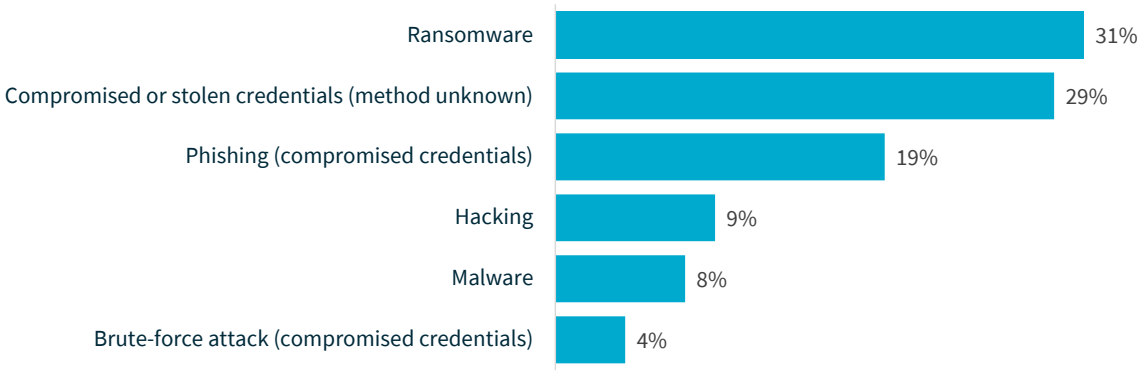
63%
of data breaches affected
100 people or fewer

Sources of data breaches



42% of all data breaches resulted from cyber security incidents (172 notifications)

Cyber incident breakdown



Top causes of human error breaches

PI sent to wrong recipient (email) 46%

Unauthorised disclosure (unintended release or publication) 18%

Loss of paperwork / data storage device 9%

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 January to 30 June 2023.

Statistical comparisons are to the period 1 July to 31 December 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.

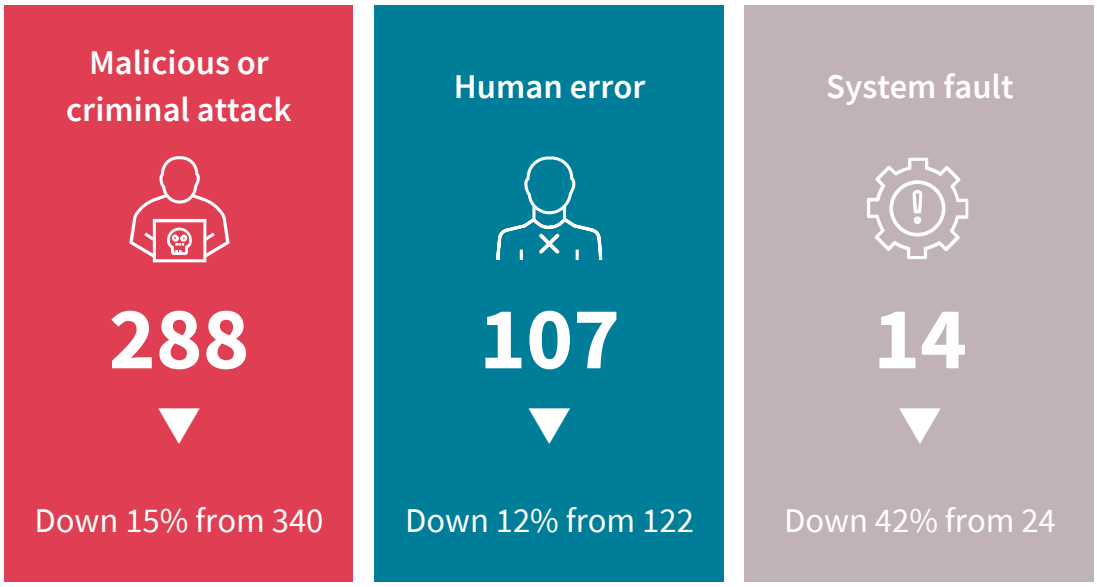
Notifications made under the *My Health Records Act 2012* are not included as they are subject to specific notification requirements set out in that legislation.

Statistics in this report are current as of 1 August 2023. 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 2023 published in future reports. Similarly, statistics from before January 2023 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 to 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.



Key findings for the January to June 2023 reporting period:

- 409 breaches were notified compared with 486 in July to December 2022 – a 16% decrease.
- Malicious or criminal attacks remained the leading cause (70%) of data breaches.
- Human error breaches were the fastest to be identified with 81% identified in 30 days or fewer. Only 57% of system faults were identified in the same timeframe.
- The health and finance sectors remained the top reporters of data breaches. Health reported 63 breaches (15% of all notifications) and finance 54 breaches (13% of all notifications).
- The majority of breaches (63%) affected 100 or fewer people.

Notifications received January to June 2023 – All sectors

The OAIC received 409 notifications this reporting period – a 16% decrease compared with July to December 2022. Since the start of the NDB scheme in February 2018, the OAIC has observed a trend where more notifications are received in the second half of the calendar year.

Following a typically low number of notifications in January (49), there was a peak in notifications in March (100). This was followed by a much lower number of notifications in April (45), which equals the lowest monthly total since the NDB scheme commenced (45 notifications were received in January 2021).

Table 1: Notifications received in the 2022–23 financial year

Reporting period	Number of notifications
July to December 2022	486
January to June 2023	409
Total	**895**

Chart 1: Notifications received by month from July 2021 to June 2023

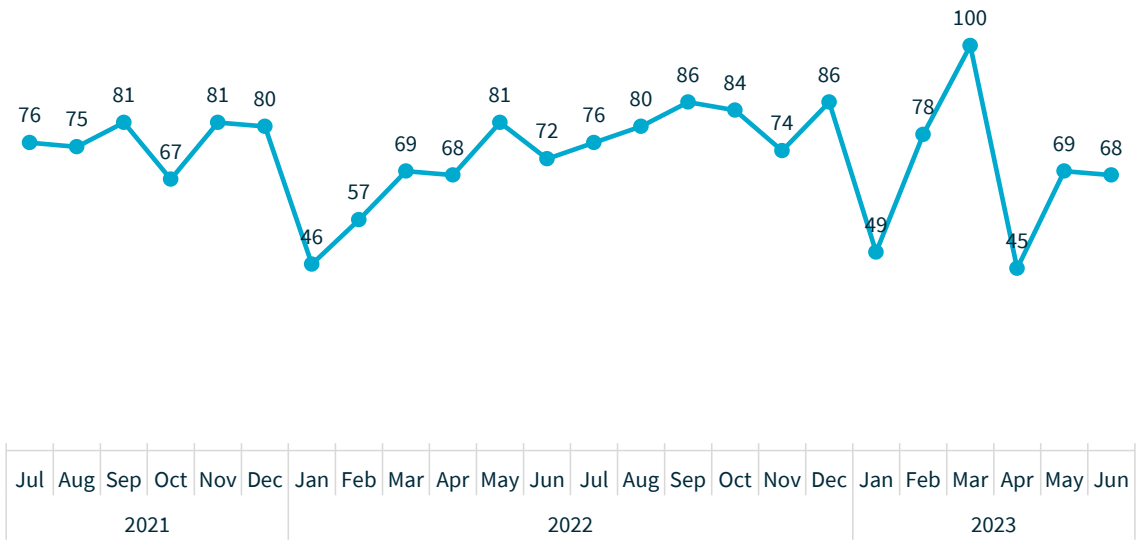
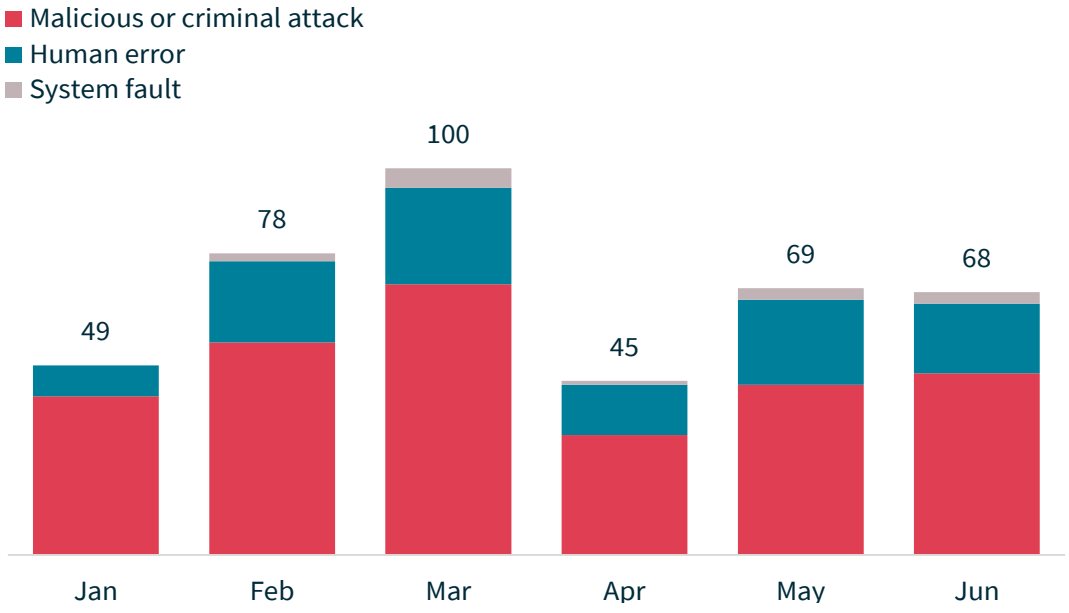


Chart 2: Notifications received by month showing the sources of breaches



Awareness and impact of data breaches among the community

According to the OAIC Australian Community Attitudes to Privacy Survey (ACAPS) 2023, three-quarters (74%) of Australians feel data breaches are one of the biggest privacy risks they face today.

Almost half (47%) of Australians said they had been told by an organisation that their information was involved in a data breach in the 12 months prior to completing the survey in March 2023. A similar proportion (51%) know someone who was affected by a breach.

Three-quarters (76%) of those whose data was involved in a breach said they experienced harm as a result. More than half (52%) reported an increase in scams or spam texts or emails. Three in ten (29%) said they had to replace key identity documents, such as a driver's licence or passport. Around 1 in 10 said they experienced significant issues such as emotional or psychological harm (12%), financial or credit fraud (11%) or identity theft (10%).

Nearly half (47%) of Australians said they would close their account or stop using a product or service provided by an organisation that experienced a data breach. However, most Australians are willing to remain with a breached organisation provided the organisation promptly takes action, such as quickly putting steps in place to prevent customers experiencing further harm from the breach and making improvements to their security practices. Only 12% of Australians said there is nothing an organisation could do that would influence them to stay after a data breach.

There is a range of ways organisations can protect personal information. A quarter (26%) of Australians believe the most important step is for organisations to only collect the information necessary to provide the product or service. Australians view the second most important thing organisations can do is take proactive steps to protect the information they hold (24%).

The OAIC commissioned Lonergan Research to undertake ACAPS 2023. The survey was conducted in March 2023 with a nationally representative sample of 1,916 unique respondents aged 18 and older.

To read the full report, visit oaic.gov.au/acaps

A maturing regulatory approach

The NDB scheme is now a mature model and the OAIC expects entities to have strong practices in place to protect personal information. Entities are also expected to have processes to ensure a timely response and compliance with the requirements of the scheme should a data breach occur.

The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* provided the Commissioner with new and increased regulatory powers. This includes the power to require a person or an entity to provide information and documents relevant to a suspected or actual eligible data breach (s 26WU).

The OAIC works closely with notifying entities to facilitate compliance with the NDB scheme. The OAIC is prioritising regulatory action in instances of serious or repeated non-compliance with the requirements of the NDB scheme. The OAIC's *Privacy regulatory action policy* sets out other factors the OAIC takes into account in deciding when to take regulatory action.

The scenarios below are examples of circumstances in which the OAIC may take regulatory action to obtain information in relation to a suspected or actual eligible data breach.

Scenario 1

An entity notified the OAIC of a suspected eligible data breach involving unauthorised access to personal information stored on one of its servers.

The entity advised it was unable to confirm if the incident was an eligible data breach or answer any questions until its analysis was completed. The entity also advised it would take 10 to 12 weeks to complete its assessment and notify any affected individuals it might identify.

While regulatory action was ultimately not required in this case, in circumstances such as this, it would be open to the Commissioner to exercise her power under s 26WU(3) of the Privacy Act, requiring the entity by written notice to answer any relevant questions about the data breach within a specific timeframe. This could include questions about the particular kind(s) of personal information typically stored on the impacted server, which is information that should be considered when conducting an assessment of whether there are reasonable grounds to *believe* that an eligible data breach has occurred.

Scenario 2

The OAIC became aware of a suspected eligible data breach involving an IT service provider. The entity confirmed it had experienced a ransomware incident that compromised the information of 20 health service provider clients, including their patients' treatment information.

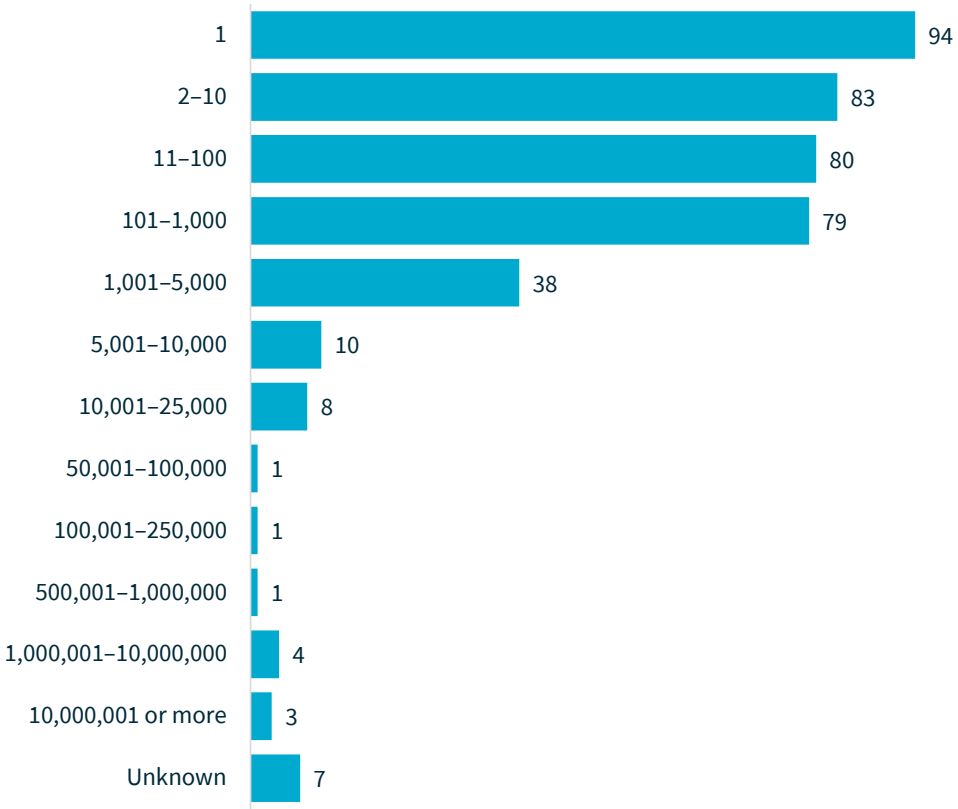
The entity notified the impacted health service providers of the breach, presuming they would notify affected individuals if required. The entity declined to provide the health service providers' details to the OAIC, claiming it did not have consent to disclose the information.

In the circumstances, the Commissioner exercised her power under s 26WU(3) to issue a written notice, requiring the entity to provide a list of the health service providers impacted by the data breach. Following receipt of the notice, the entity provided the information required. This information enabled the Commissioner to ensure the affected individuals were notified and that all entities involved in the data breach complied with the NDB scheme.

Number of individuals worldwide affected by breaches

Most data breaches (91%) involved the personal information of 5,000 or fewer individuals worldwide. Breaches affecting 100 or fewer individuals comprised 63% of notifications and breaches affecting between 1 and 10 individuals accounted for 43% of notifications, similar to previous reporting periods.

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.

Large-scale data breaches

The OAIC continues to be notified of breaches that affect a large number of Australians.

In the first half of 2023, there were 23 breaches that affected over 5,000 Australians, compared with 42 in the previous period – a 45% decrease. The OAIC considers the decline reflects the overall (16%) decrease in the number of notifications received this period.

While there was a decrease in the number of breaches that affected over 5,000 Australians, 2 of the breaches reported in this period affected more than 1 million Australians and one affected more than 10 million. This is the first breach notified under the NDB scheme to affect more than 10 million Australians.

Table 2: Number of Australians affected by breaches

Number of Australians affected by breaches	Jul–Dec 2022	Jan–Jun 2023
5,001–10,000	14	9
10,001–25,000	9	5
25,001–50,000	6	2
50,001–100,000	3	3
100,001–250,000	2	1
250,001–500,000	1	0
500,001–1,000,000	1	0
1,000,001–10,000,000	6	2
10,000,001 or more	0	1
Total number of breaches affecting over 5,000 Australians	**42**	**23**

Cyber incidents were the cause of a significant proportion of large-scale breaches reported to the OAIC. Twenty-one of the 23 breaches that affected over 5,000 Australians in this period were caused by cyber incidents. Of these, 7 were caused by ransomware, 7 by compromised or stolen credentials (method unknown), 4 by hacking and 1 each by brute-force attack, malware and phishing (compromised credentials).

The remaining 2 breaches that affected over 5,000 Australians in this period were caused by a rogue employee or insider threat and theft of paperwork or a data storage device.

It is vital that entities continue to take appropriate and proactive steps to protect against and respond to a range of cyber threats. The Australian Cyber Security Centre considers the most effective way to defend against cyber threats is to implement the Essential Eight cyber security strategies.

The OAIC has published guidance on securing personal information and data breach preparation and response to assist entities to protect their information against cyber threats.

Kinds of personal information involved in breaches

Consistent with previous reports, contact, identity and financial information remain the most common kinds of personal information involved in data breaches.

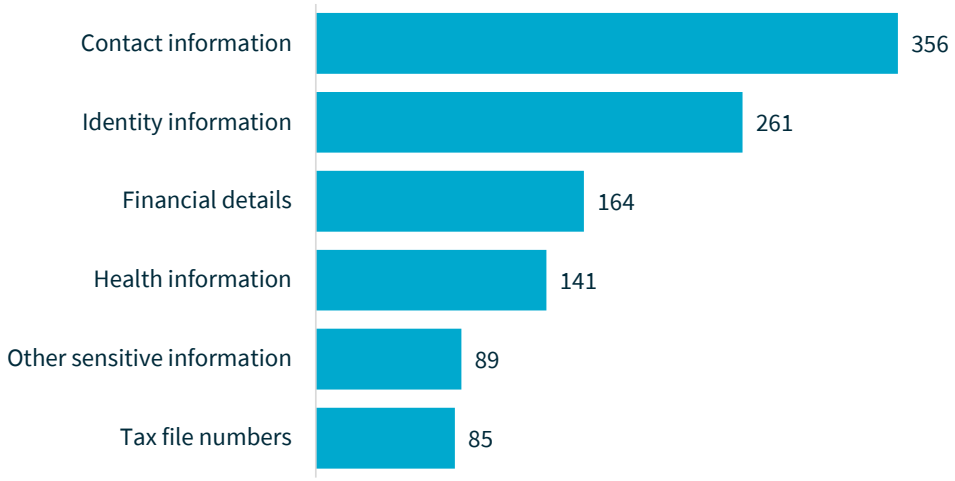
The proportions of breaches involving these kinds of personal information are similar to previous reports.

Most breaches (87%) 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 64% of breaches, and includes individuals' date of birth, passport details and driver licence details.

Financial details, such as bank account and credit card numbers, were involved in 40% 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

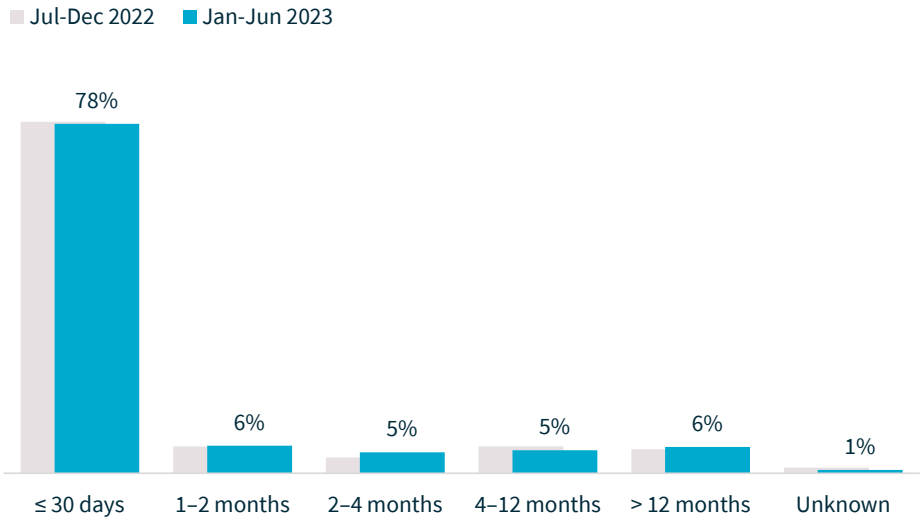
The NDB scheme aims to protect individuals by requiring that they are notified when they are at risk of serious harm from a data breach. Prompt notification enables individuals to take further steps to protect themselves, such as being alert to scams. Delays in identifying, assessing and notifying breaches may increase the risk of individuals experiencing harm.

Under Australian Privacy Principle (APP) 11, entities must take reasonable steps 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 to prevent and 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]

This reporting period, 78% of breaches were identified by the entity within 30 days of it occurring, consistent with the previous period.

Chart 5: Time taken to identify breaches



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

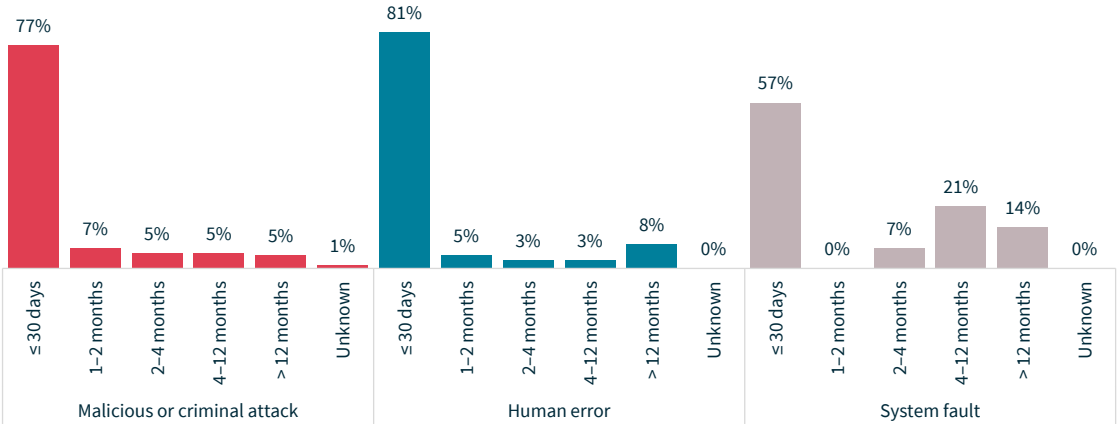
The time taken by entities to identify breaches varies depending on the source of breach.

In this period, human error breaches (81% identified within 30 days) were the fastest to be identified, followed by malicious or criminal attacks (77%).

[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.

Consistent with previous reports, system faults were the slowest to be identified. A notable proportion of entities that experienced system faults (14%) did not become aware of the incident for over a year. The circumstances that result in an organisation's delayed awareness of a system fault are usually complex. System faults include system errors that occur only in very specific circumstances that are difficult for the organisation to identify and investigate.

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.

Privacy by design to prevent and detect data breaches

Entities should have processes and systems in place to proactively identify and manage privacy risks and security vulnerabilities. Even minor risks and vulnerabilities can result in serious data breaches and undermine community trust in entities.

Human error was the cause of 26% of breaches this reporting period. There is often an element of human error in data breaches predominantly caused by malicious or criminal attacks and system faults. For example:

- Ransomware attacks are often preceded by a successful phishing attack on one or more individual(s) whose compromised credentials are then leveraged by a threat actor.
- Some system faults occur because relevant programming or settings for a device or software program were improperly set or insufficiently tested.

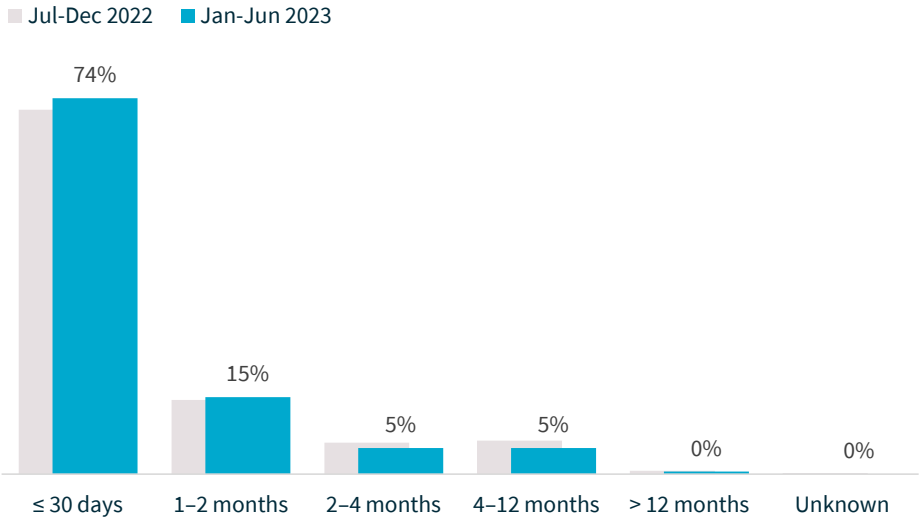
Entities should assume human error will occur and design for it. The OAIC encourages entities to embed good privacy practices into all aspects of their functions and activities. This includes designing systems and processes that anticipate and minimise the risk of human error.

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.

From January to June 2023, 74% of entities notified the OAIC within 30 days of becoming aware of an incident, similar to 72% in the previous period.

Chart 7: Time taken to notify the OAIC of breaches



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

Conducting reasonable and expeditious assessments by being flexible and adaptive

Entities are required to undertake a reasonable and expeditious assessment of a suspected eligible data breach and take all reasonable steps to complete the assessment within 30 days (s 26WH).

The OAIC expects the amount of time and effort entities expend on an assessment is proportionate to the likelihood that an eligible data breach has occurred and its apparent severity.

This period, 26% of entities took more than 30 days to notify the OAIC of data breaches. The OAIC has observed this delay in notification may be due to some entities adopting a fixed-method or sequential approach to assessing and responding to data breaches.

Examples include when an entity:

- assesses whether there are reasonable grounds to believe an eligible data breach has occurred only after completing a forensic investigation, rather than doing the assessment and investigation at the same time
- conducts iterative and increasingly complex and technical reviews of the data involved to identify exactly what occurred and who was impacted, when the apparent severity of the breach and the volume of data is clear.

Generally, the steps in response to any data breach should be taken simultaneously or in quick succession. Entities should also consider whether all the steps are necessary, if any can be combined, or if they need to be re-ordered to ensure the most reasonable and prompt assessment outcome.

Scenario 1

An entity was compromised by a ransomware attack, which resulted in the encryption of data containing personal information. The entity commenced a forensic investigation that identified the root cause was a phishing email, and data was successfully exfiltrated by the threat actor.

Upon conclusion of the forensic investigation, the entity commenced cross-checking and validation exercises to identify exactly what personal information had been exfiltrated. The entity undertook the forensic investigation and assessment sequentially rather than in parallel, which delayed the notification to affected individuals by 5 months, increasing their risk of harm.

Scenario 2

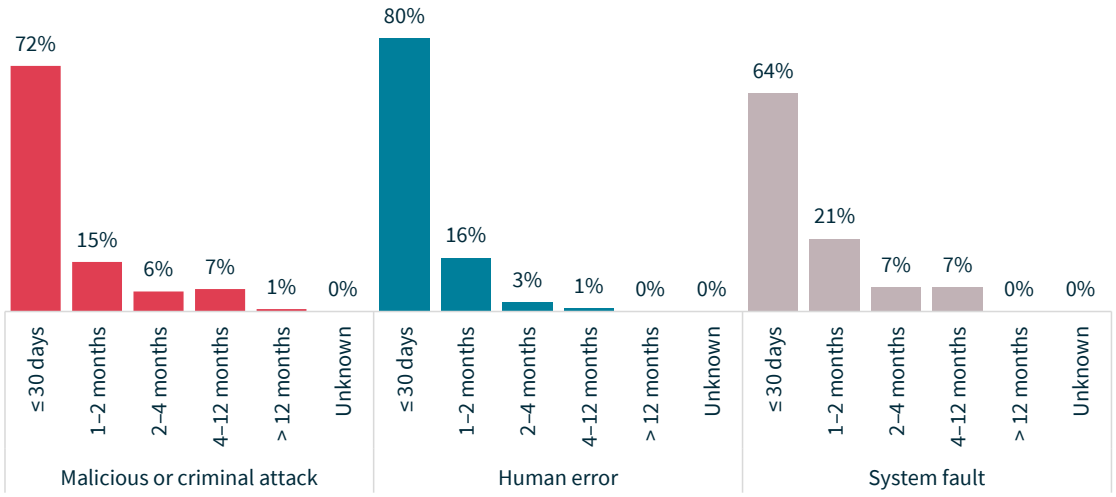
An entity became aware of unauthorised access to its IT system. The entity commenced a forensic IT investigation and data review, which concluded that an eligible data breach had occurred.

The entity took steps to contain the breach and notified affected individuals as soon as practicable to reduce the risk of serious harm. As the entity undertook an investigation of the data breach and its assessment under the NDB scheme in parallel, it was able to quickly identify there were reasonable grounds to believe an eligible data breach had occurred. This enabled it to promptly determine the kinds of personal information involved and to notify affected individuals within 20 days of becoming aware of the breach.

The time taken to notify the OAIC of data breaches based on source of breach saw some variation when compared to the previous report.

Malicious or criminal attack and human error breaches were reasonably comparable, but system faults saw the most variation. This period, 64% of system faults were notified within 30 days, a decrease from the previous period which saw 71% of such breaches being notified within the same timeframe.

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.

Preventing risks arising from working in changed environments

Working environments have evolved over the last three years, including an increase in remote and hybrid work.

The OAIC has guidance to assist entities to assess privacy risks in changed working environments. Entities are strongly encouraged to conduct a privacy impact assessment and address identified risks arising from their employees' and contractors' work environments. This may include consideration of:

- how 'security aware' employees and contractors are and whether training or other measures to improve capability and understanding are needed
- remote working policies and procedures and whether these clearly address a range of relevant matters, including physical security and access security
- the risks and benefits of 'bring your own device' (BYOD) for employees, requiring exclusive use of entity issued and managed devices for work or a combination of both
- processes and policies in place to enforce regular password updates, minimum password complexity requirements and mandatory multi-factor authentication for all employees and contractors.

Scenario

An entity experienced a cyber incident where personal and commercially sensitive information was stolen. This occurred because a threat actor leveraged a security vulnerability on an employee's BYOD to obtain their work credentials and remotely login to the entity's systems at the same time as the employee.

As a result, the threat actor also appeared to be a genuine user and their activities, including unauthorised access to personal information, went undetected until after the data theft.

In this circumstance, the likelihood of the threat actor accessing the information may have been reduced had the entity proactively enforced strong encryption on sensitive personal information, enforced multi-factor authentication and either issued a company device or required minimum security requirements on the employee's BYOD.

Entities that permit BYOD should review their IT security policy to ensure it addresses risks arising from BYOD and that they educate their employees on how to securely use BYOD to prevent data breaches of work systems.

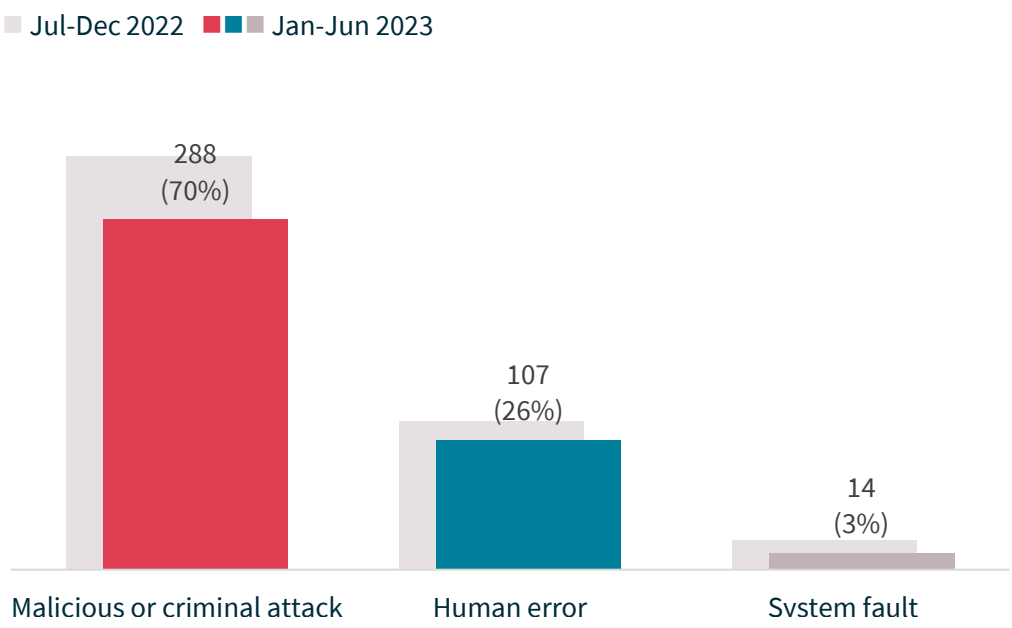
Source of breaches

Overall, fewer data breach notifications were received this period, with breaches caused by malicious or criminal attacks decreasing in number by 15%, human error by 12% and system faults by 42%.

Proportionally, the sources of breaches were relatively consistent with the previous period:

- 70% were malicious or criminal attacks, the same proportion as the previous period.
- 26% were human error breaches, compared to 25% the previous period.
- 3% were system faults, compared to 5% the previous period.

Chart 9: Source of data breaches

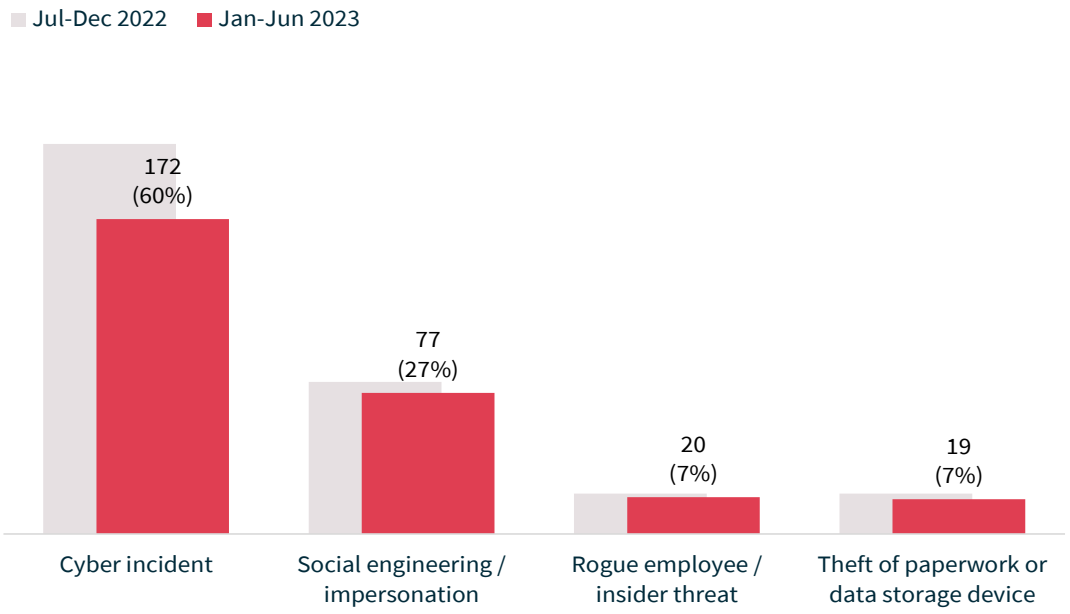


Malicious or criminal attacks

The majority (60%) of breaches caused by malicious or criminal attacks were cyber incidents. There were 172 breaches resulting from cyber incidents, down 19% in number from 213 in July to December 2022. Forty-two per cent of all data breaches resulted from cyber incidents, compared with 44% in the previous period.

As a subset of all malicious or criminal attacks notified to the OAIC during this period, social engineering or impersonation attacks accounted for 27%, theft of paperwork or data storage device for 7% and actions taken by a rogue employee or insider threat for 7%. These proportions are generally consistent with previous reports.

Chart 10: Malicious or criminal attack breakdown



Remaining vigilant to social engineering and impersonation

Nearly 1 in 5 data breaches in the first half of 2023 were caused by social engineering or impersonation.

The increased incidence of large-scale data breaches in the previous year elevates the likelihood of a mosaic effect, which is when separate pieces of information become significant when combined with other types of information. For example, millions of individuals' personal information might be collated or aggregated from multiple sources, including the dark web, to build a more complete understanding or new insight into specific individuals or a group of individuals.

With this capability and knowledge in hand, threat actors are more capable of:

- impersonating many different individuals, gaining trust and bypassing existing authentication measures to access accounts
- accessing multiple systems and accounts using compromised credentials, particularly where employees or individuals have reused the same password – or a predictable pattern of passwords – to commit credential stuffing attacks and access accounts.

The OAIC strongly encourages all entities to review and strengthen their access security and ICT security measures, including identity management and authentication.

Entities should also actively foster a security and privacy-aware culture to ensure staff are well-equipped to identify and respond to fraud and credential stuffing attacks, and so customers know what to do if they are concerned they may have been the subject of an attack.

The scenarios below demonstrate the importance of proactively implementing strong and multiple forms of identity management and authentication, and taking reasonable steps to ensure information is accessed only by authorised persons.

Scenario 1

A retail entity's customer portal was subjected to a credential stuffing attack, resulting in unauthorised access to 500 customer accounts, which included identity information. At the time of the incident, the entity's identity authentication for customer accounts was limited to email address and password.

Following an investigation, the entity formed a suspicion that the customers' credentials were obtained in a data breach of another entity and that the threat actor(s) leveraged this information to bypass their identity authentication measures.

The entity notified all affected customers of the data breach and uplifted its identity authentication measures to include mandatory multi-factor authentication for all customers.

Scenario 2

An entity that facilitates access to health services via a digital platform experienced a data breach in which a threat actor registered with the platform using the genuine professional registration details of a health services provider. The threat actor then impersonated a health service provider and accepted appointments from individuals, gaining access to their personal and sensitive information.

The entity became suspicious after receiving complaints from individuals and conducted an investigation, resulting in identification of the fraud registration and removal of the threat actor's access to the platform.

The entity notified affected individuals and implemented more stringent identity verification measures for registering healthcare providers on its platform.

Cyber incidents affected on average a significantly higher number of individuals worldwide compared to other types of breaches caused by malicious or criminal attacks. Cyber incidents reported to the OAIC affected 319,761 individuals on average, in comparison to the next highest average of 845 individuals affected by a breach caused by a rogue employee or insider threat.

Table 3: Malicious or criminal attack breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Cyber incident	172	319,761	215
Rogue employee / insider threat	20	845	3
Theft of paperwork or data storage device	19	690	29
Social engineering / impersonation	77	108	7
Total	**288**	**186,951**	**59**

Assessing breaches with limited or no evidence

Data breaches caused by cyber security incidents are often complex and generally tend to affect more individuals than other types of malicious or criminal attacks.

It is imperative that entities have effective measures in place to detect, prevent and respond to cyber incidents. This includes having an up-to-date data breach response plan and appropriate audit and logging capabilities so entities can quickly undertake a meaningful and informed assessment of a data breach.

In the July to December 2022 report, the OAIC cautioned entities against relying on the presumed motivations of threat actors and absence of evidence of unauthorised access when assessing cyber incidents. Reliance on these factors can adversely affect the accuracy of a data breach assessment.

The OAIC also encourages entities to:

- **Take a cautious approach**. If an entity suspects a data breach has occurred but is unable to eliminate that suspicion quickly and confidently, the entity should consider proceeding on the presumption that there has been a data breach. Notification obligations are triggered once there are reasonable grounds to *believe* that an eligible data breach has occurred. Conclusive or positive evidence of unauthorised access, disclosure or loss is not required for an entity to assess that an eligible data breach has occurred.

- **Consider all relevant factors and risks of harm**. Entities need to assess a range of relevant factors, when assessing the likelihood of serious harm (s 26WG). Given the objective of the scheme is to promote notification, entities' assessments should weigh in favour of notifying the OAIC and affected individuals.
- **Focus on unauthorised access**. Given the clear risks posed by exfiltration, the OAIC appreciates that initial priority may be given to assessing exfiltrated data and notifying individuals to whom it relates. However, an eligible data breach can occur based on unauthorised access alone and individuals' data can be stolen by less traceable means, such as screenshots. Therefore, entities should not rely on data exfiltration as the determinative factor for deciding whether an eligible data breach has occurred. Entities need to consider all the information that was accessed by a threat actor, or the information that was accessible to them.

The following scenarios are examples of how entities can successfully assess incidents based on the available information, including when there is little or no evidence.

Scenario 1

An entity deployed an update to its customer portal on its website. However, the update contained a bug, which meant individuals who logged in via the portal could see each other's details.

Within 24 hours of deploying the update, the entity became aware of the bug, contained it and commenced an assessment of whether there were reasonable grounds to believe an eligible data breach had occurred. As part of its assessment, the entity referred to its activity logs and quickly determined 29 individuals who had logged into the portal within the previous 24 hours had been affected by the incident. The entity notified these individuals.

The activity logs enabled the entity to quickly conduct an evidence-based assessment of the data breach and to promptly notify the affected individuals.

Scenario 2

An entity experienced a ransomware attack on one of its servers, resulting in data being exfiltrated by a threat actor(s).

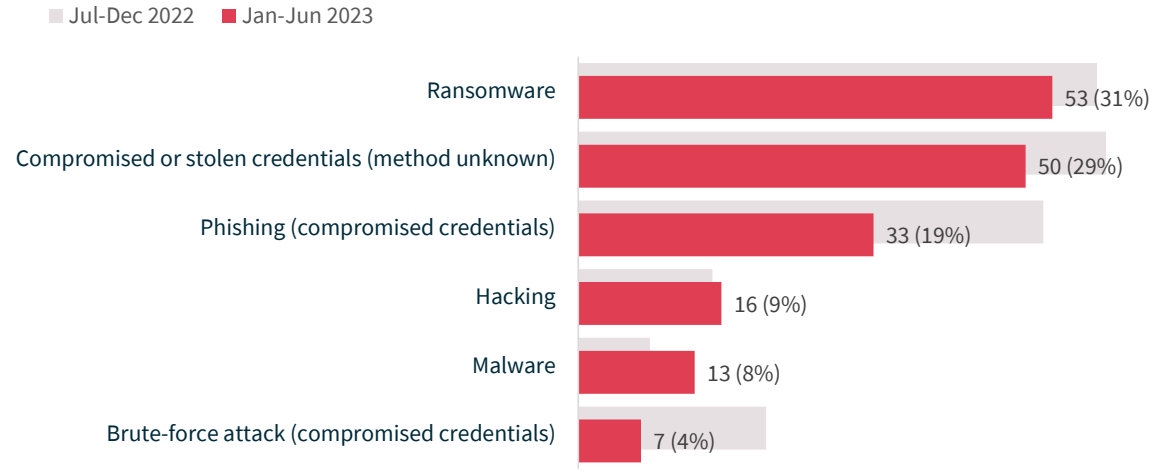
Cyber security specialists conducted a forensic analysis of the incident on the entity's behalf and determined what specific information was exfiltrated from the server. However, they were unable to determine with certainty what other personal information may have been accessed during the incident.

As the entity was unable to confirm the extent of any unauthorised access, it took a cautious approach and presumed all personal information stored on the server at the time of the incident was potentially accessed by the threat actor(s). As such, the entity notified all potentially affected individuals, enabling them to take steps to reduce their risk of harm.

Cyber incidents

Ransomware remained the top source of cyber incidents (31%; 53 notifications), followed by compromised or stolen credentials (method unknown) (29%; 50 notifications) and phishing (19%; 33 notifications).

Chart 11: Cyber incident breakdown



Particular kinds of cyber incidents affect a larger number of individuals worldwide. In this reporting period, brute-force attacks (7 notifications) affected the most individuals on average at 1,667,293. This was followed by compromised or stolen credentials for which the method was unknown (50 notifications), which affected 658,794 individuals on average. Ransomware attacks (53 notifications) affected 206,861 individuals on average.

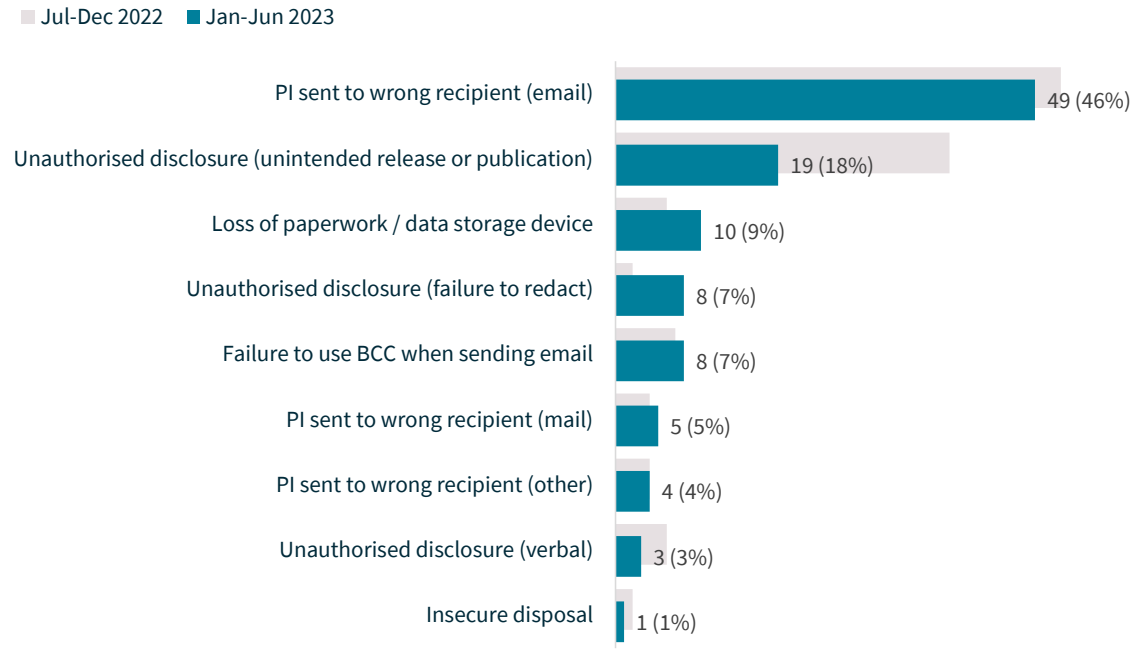
Table 4: Cyber incident breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Brute-force attack (compromised credentials)	7	1,667,293	58
Compromised or stolen credentials (method unknown)	50	658,794	92
Ransomware	53	206,861	517
Hacking	16	4,945	1,300
Malware	13	3,936	227
Phishing (compromised credentials)	33	1,109	150
Total	**172**	**319,761**	**215**

Human error

Like the previous reporting period, personal information being emailed to the wrong recipient was the most common cause of human error breaches in the first half of 2023. More than half (54%) of human error breaches resulted from personal information being sent to the wrong recipient, whether by email (46% of human error data breaches), post (5%) or other (4%) means.

Chart 12: Human error breakdown



Certain kinds of human error breaches also affected larger numbers of individuals worldwide. Failure to use BCC when sending an email (8 notifications) affected an average of 453 individuals. This was followed by 4 breaches caused by personal information being sent to the wrong recipient by means other than email, mail or fax, which affected 276 individuals on average.

Table 5: Human error breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Failure to use BCC when sending email	8	453	185
PI sent to wrong recipient (other)	4	276	1
Unauthorised disclosure (unintended release or publication)	19	86	14
Insecure disposal	1	80	80
Loss of paperwork/data storage device	10	69	31

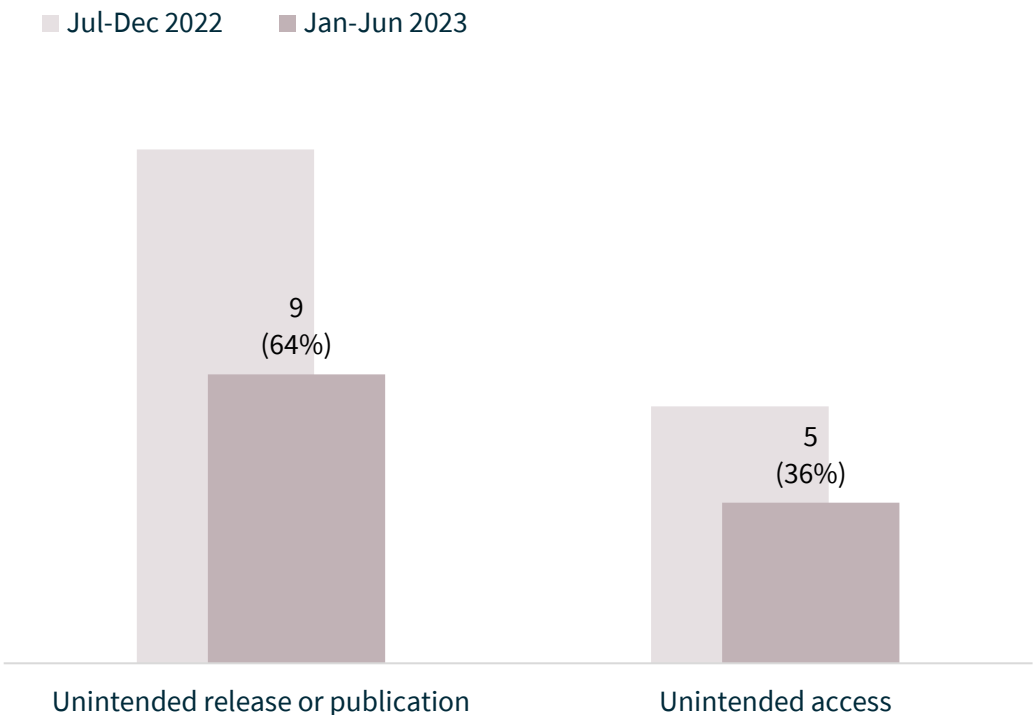
PI sent to wrong recipient (email)	49	38	1
Unauthorised disclosure (failure to redact)	8	3	2
PI sent to wrong recipient (mail)	5	2	1
Unauthorised disclosure (verbal)	3	1	1
Total	**107**	**84**	**2**

System faults

The majority (64%) of system fault breaches involved the unintended release or publication of personal information. Examples of issues that may lead to this include systems and databases that are misaligned or operate asynchronously, and untested system and infrastructure changes.

Unintended access to personal information because of a system fault caused 5 breaches (36% of system faults). Examples of causes include system synchronisation issues and webform, portal or platform design issues that result in users seeing each other's information.

Chart 13: System fault breakdown



Data governance to mitigate the effects of data breaches

Over the last year, the OAIC has generally observed an increase in the number of data breaches affecting more than one entity.

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 the 'primary notification') in this report to avoid information being duplicated.

While the overall number of data breaches, including primary notifications, trended downward this reporting period, the average number of secondary notifications increased. Of the 8 primary notifications, 7 were caused by malicious or criminal attacks and involved a service provider relationship. Three were also large-scale data breaches.

Table 6: Comparison of primary and secondary notifications

	Jan–Jun 2022	Jul–Dec 2022	Jan–Jun 2023
Primary notifications	7	17	8
Secondary notifications*	22	42	30

* Secondary notifications may relate to a primary notification received in a prior period.

There are significant risks with outsourcing the handling of personal information to service providers and contractors. It is important that entities have an information governance framework in place that incorporates the requirements of the Australian Privacy Principles. The information governance framework should cover contractors and service providers that have access to or handle personal information on the entity's behalf.

The scenario below demonstrates how appropriate information governance can mitigate the effects and severity of a data breach.

Scenario

An entity that provides services to employees and customers (the affected individuals) of other organisations (client organisations) experienced a cyber incident that resulted in the personal information of several thousand individuals being exfiltrated and published on the dark web.

Once aware of the incident, the entity undertook an assessment and identified several client organisations were impacted, some of which were no longer using the entity's services. This meant the entity needed to consider the data it held about individuals for all client

organisations, not just those to which it was still providing services. This resulted in a lengthy and involved assessment process.

In this instance, the complexity and scale of the breach may have been reduced if the entity and client organisations had taken appropriate steps at an earlier time to ensure information was deidentified or destroyed when it was no longer needed.

Effective information governance

The OAIC recommends entities consider the information life cycle and review personal information holdings at least annually to determine:

- **What specific personal information is being collected, who is collecting it and whether the collection is necessary.** For example, entities should consider sighting identity documents rather than copying and saving them. Information cannot be compromised in a data breach if it was never collected.
- **How the personal information is being handled and stored and whether this is occurring in an organised and consistent way.** Entities that understand their personal information holdings are better positioned to quickly respond to and assess a data breach.
- **What security measures are in place to protect personal information and whether any additional measures are needed.** For example, entities should consider whether additional authentication requirements are required to secure systems containing sensitive personal information.
- **Whether personal information is still needed and if it should be destroyed or deidentified.** Entities with routine retention and destruction policies can substantially reduce the costs and privacy risks associated with holding excess data, including duplicate, low value and historical personal information that may be out of date, inaccurate or misleading.

Comparison of top 5 sectors

This section compares notifications received by the top 5 sectors by notifications, which accounted for 49% 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 63 data breaches (15% of all notifications). The second largest source of notifications was the finance sector, which reported 54 data breaches (13% of all notifications). Recruitment agencies reported the third highest number of breaches after having the fifth highest in the previous reporting period.

The other sectors in the top 5 by notifications were recruitment agencies (8%), legal, accounting and management services (6%) and insurance (6%).

Table 7: Top 5 sectors by notifications

Sector	Number of notifications	Percentage of all notifications received
Health service providers	63	15%
Finance[3]	54	13%
Recruitment agencies	33	8%
Legal, accounting and management services	26	6%
Insurance	25	6%
Total	**201**	**49%**

[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.

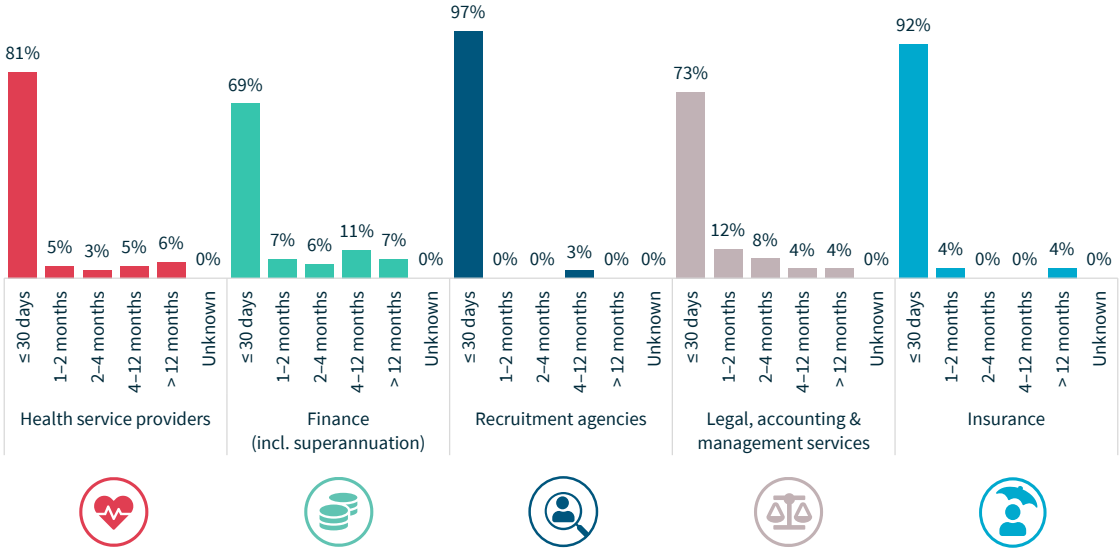
[3] This sector includes banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

Time taken to identify breaches – Top 5 sectors

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

In the reporting period, 97% of recruitment agencies identified the incident within 30 days of it occurring, compared to 69% 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.

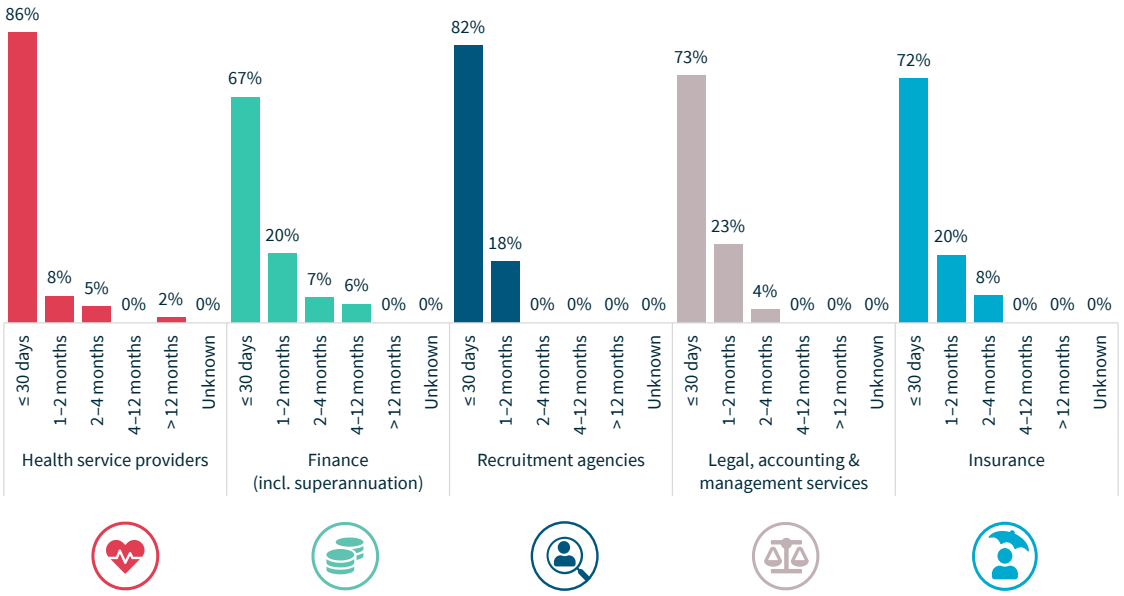
Time taken to notify the OAIC of breaches – Top 5 sectors

Each industry sector again showed variation in how long it took entities to notify the OAIC of a data breach.

Eighty-six per cent of notifications in the health sector were made within 30 days of the entity becoming aware of the incident, compared to only 67% for entities in the finance sector.

Two percent of health service providers took more than 12 months to notify the OAIC of a data breach.

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

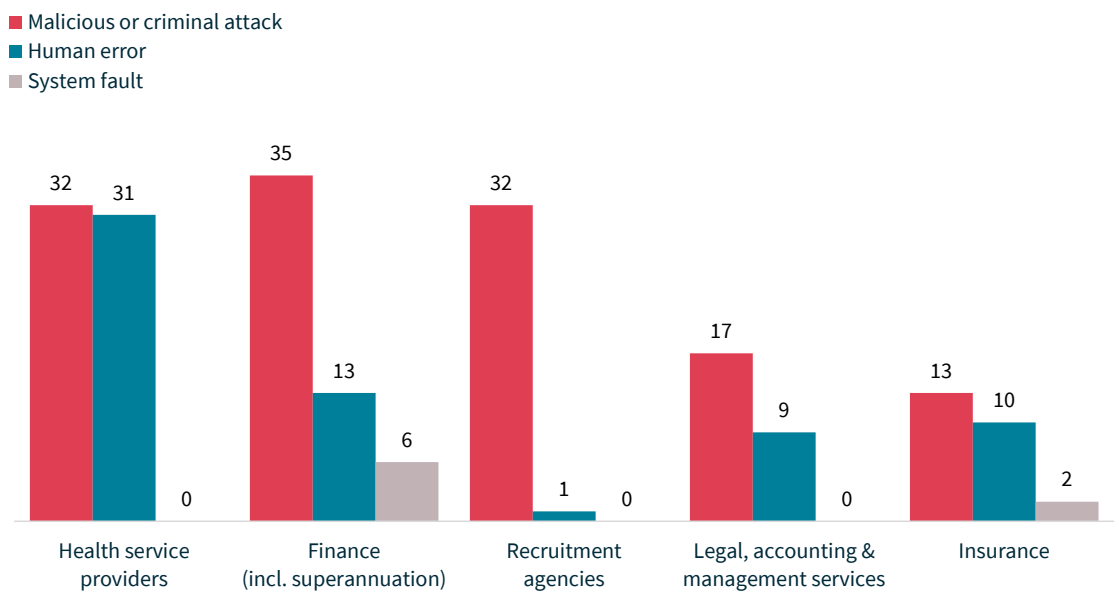


For notifications in the 'unknown' category, the entity was unable to identify the date the breach occurred.

Source of breaches – Top 5 sectors

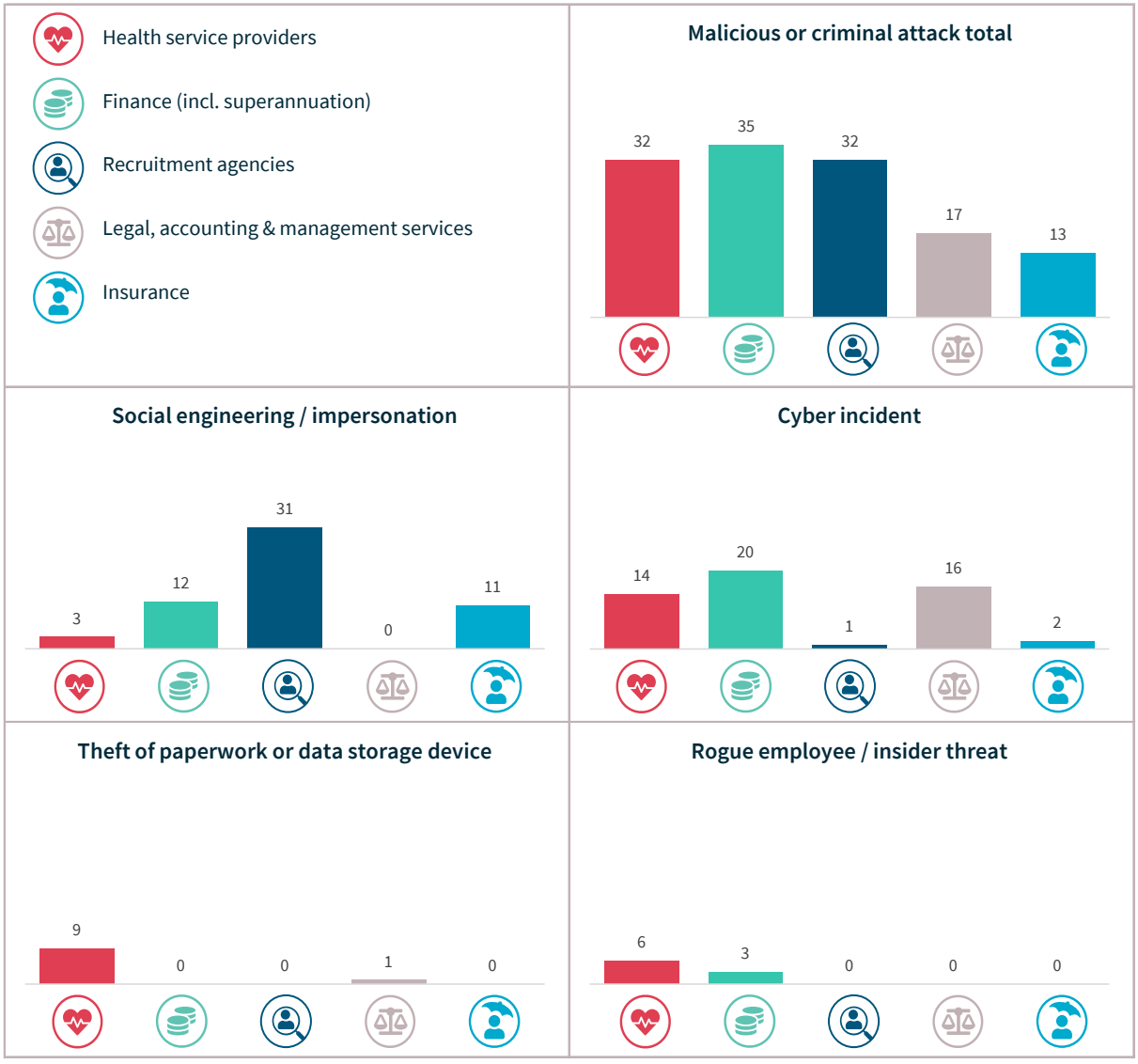
As with the previous reporting period, malicious or criminal attack remained the leading cause of data breaches notified by the top 5 sectors. It was the source of 97% of breaches notified by recruitment agencies, 65% for both legal, accounting and management services and finance, 52% of breaches notified by the insurance sector and 51% by health service providers.

Chart 16: Source of breaches – Top 5 sectors



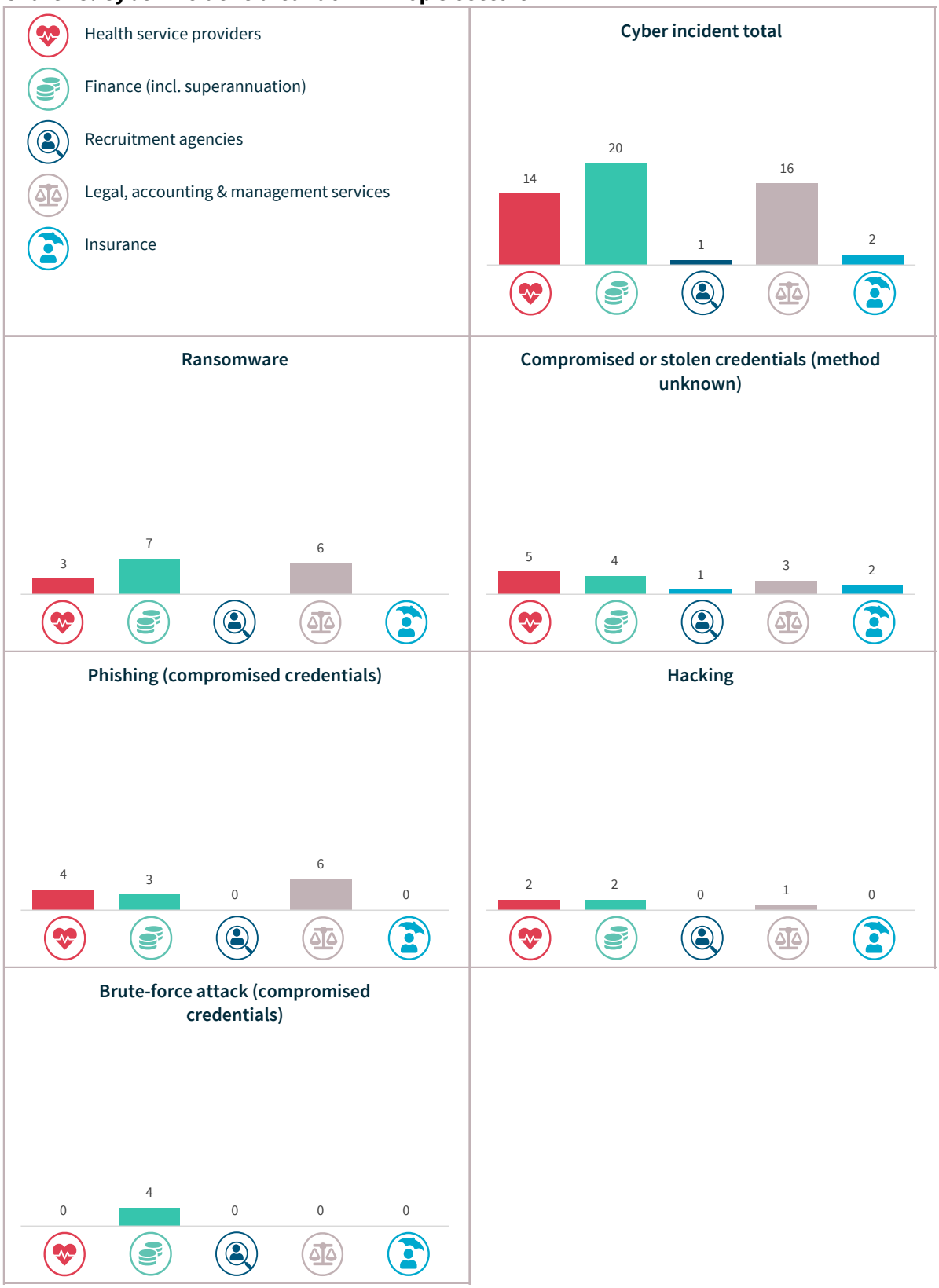
Malicious or criminal attack breaches – Top 5 sectors

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



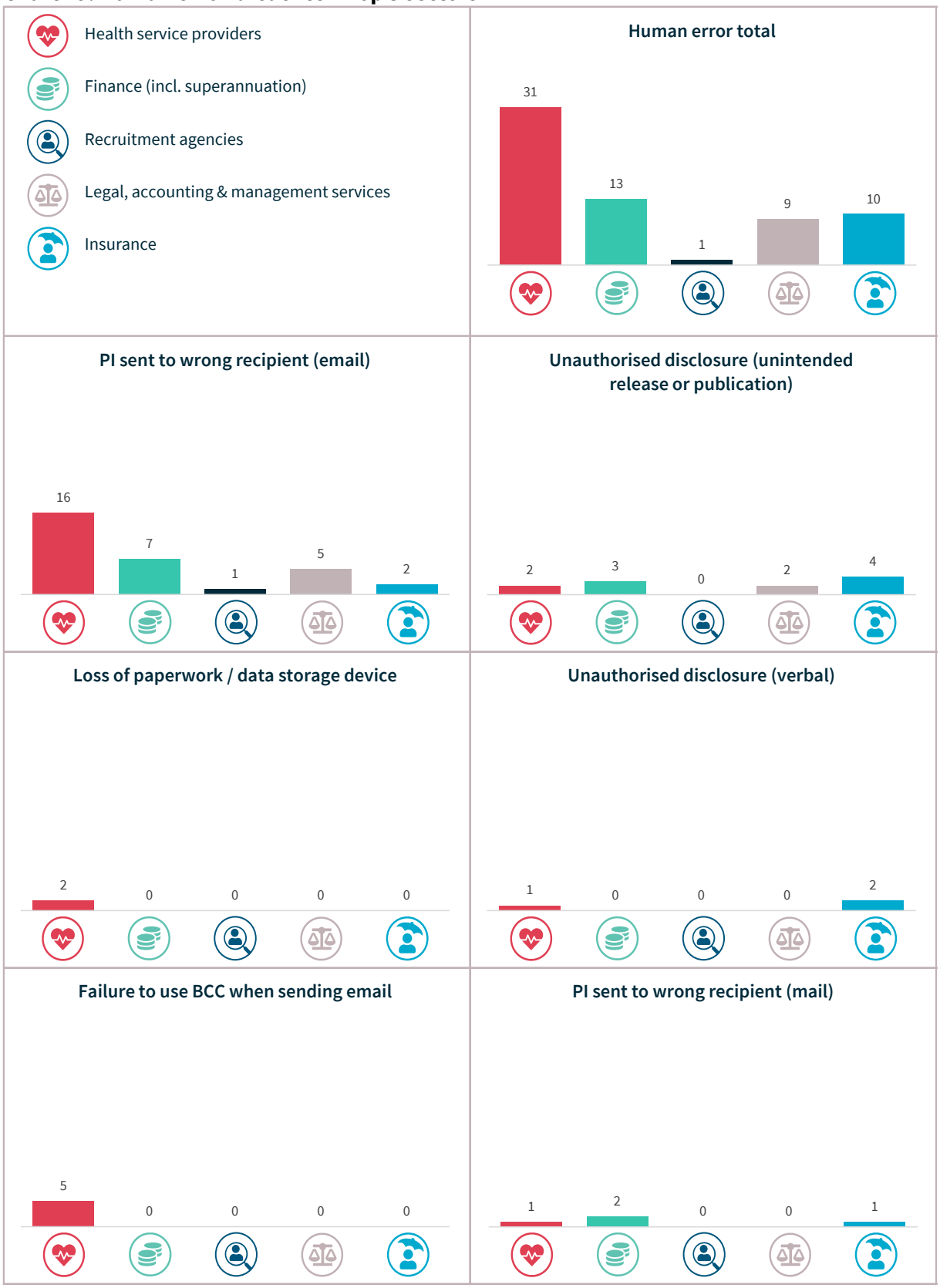
Cyber incident breaches – Top 5 sectors

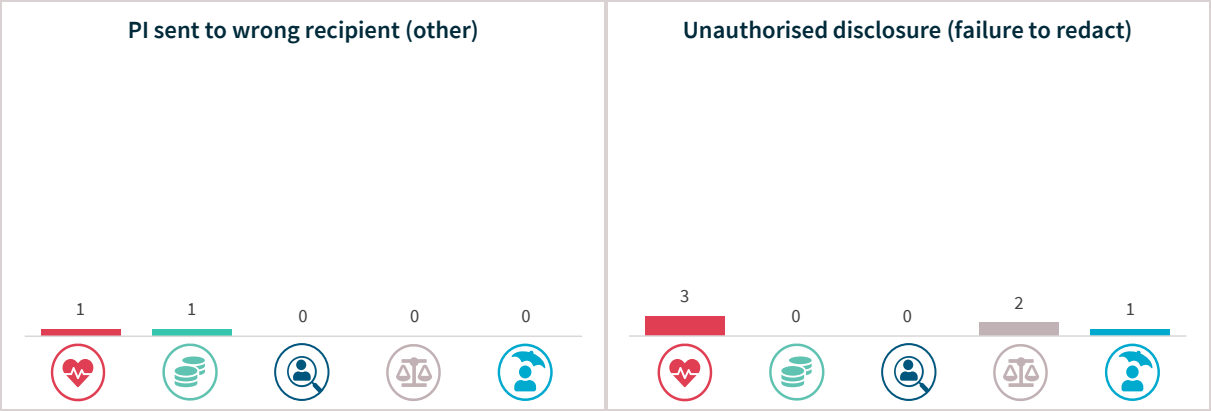
Chart 18: Cyber incident breakdown – Top 5 sectors



Human error breaches – Top 5 sectors

Chart 19: Human error breaches – Top 5 sectors

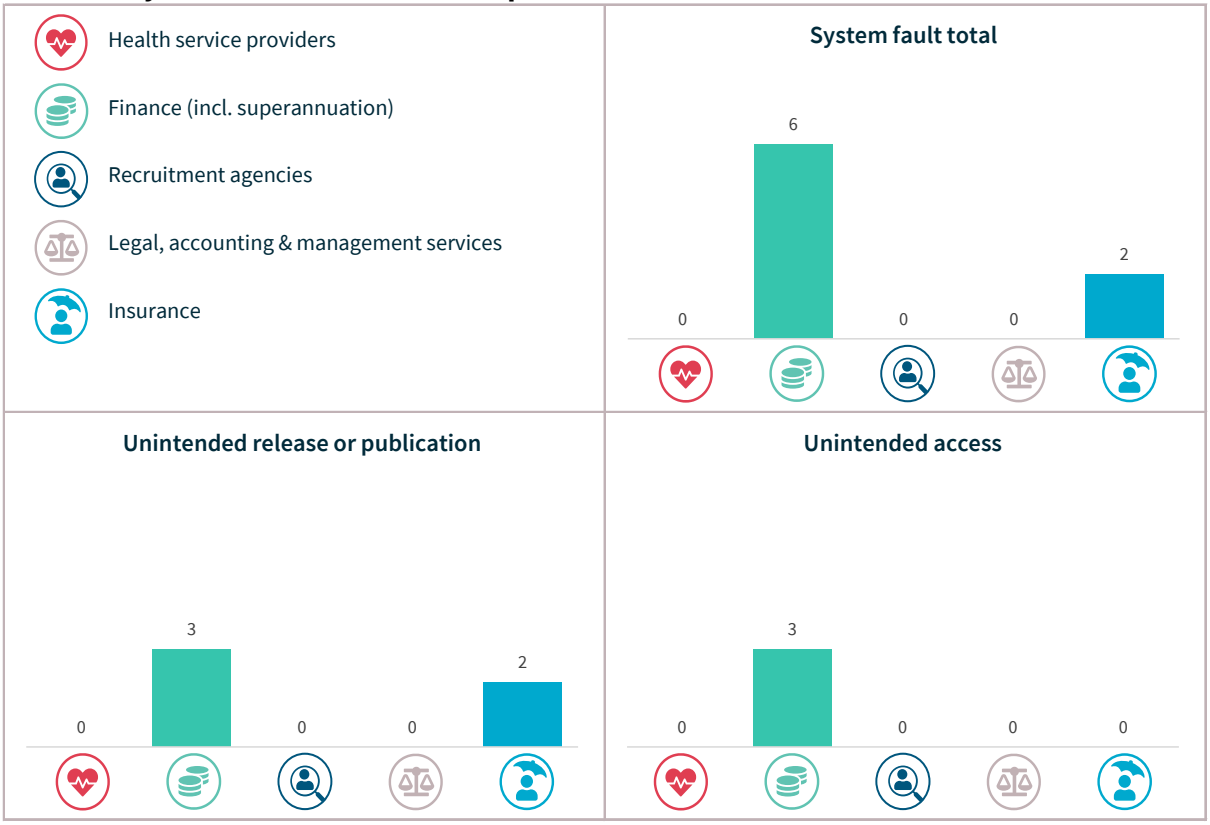




System fault breaches – Top 5 sectors

Only 2 of the top 5 sectors, finance and insurance, notified data breaches resulting from system faults.

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 • 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
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
Credential stuffing	A type of cyber incident in which a threat actor collects and uses compromised credentials, often obtained in other data breach incidents or from the dark web, to access other systems and accounts without authorisation. A threat actor may automate logins for a large number of compromised credentials
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

Term	Definition
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