Australian Government

Office of the Australian Information Commissioner

Notifiable data breaches report

July to December 2023

22 February 2024

OAIC

Contents

About this report

The Office of the Australian Information Commissioner (OAIC) periodically publishes statistical information about notifications received under the Notifiable Data Breaches (NDB) scheme to help entities and the public understand privacy risks identified through the scheme. This report captures notifications received under the NDB scheme from 1 July to 31 December 2023.

Statistical comparisons are to the period 1 January to 30 June 2023 unless otherwise indicated.

Percentages in charts may not total 100% due to rounding.

Where data breaches affect multiple entities, the OAIC may receive multiple notifications relating to the same incident. Notifications relating to the same incident are counted as a single notification (referred to as a 'primary notification') in this report to avoid information being duplicated, unless otherwise specified. The volume of secondary notifications may be indicative of the level of multi-party breach reporting. Secondary notifications may relate to a primary notification received in a prior reporting period.

The source of any given breach is based on information provided by the reporting entity. Where more than one source has been identified or is possible, the dominant or most likely source has been selected. Source of breach categories are defined in the glossary at the end of this report.

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

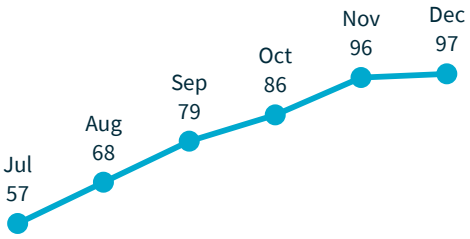
Statistics in this report are current as of 30 January 2024. Some data breach notifications are being assessed and adjustments may be made to related statistics. This may affect statistics for the period July to December 2023 published in future reports. Similarly, statistics from before July 2023 in this report may differ from those published in other reports.

Snapshot

483
notifications

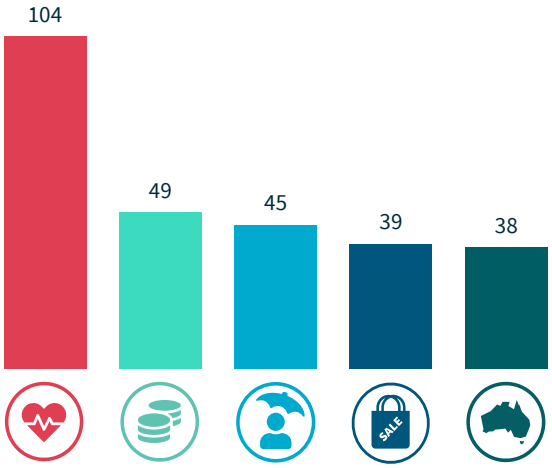
Up 19%

Some data breaches affect more than one entity. The OAIC received an additional 121 secondary data breach notifications



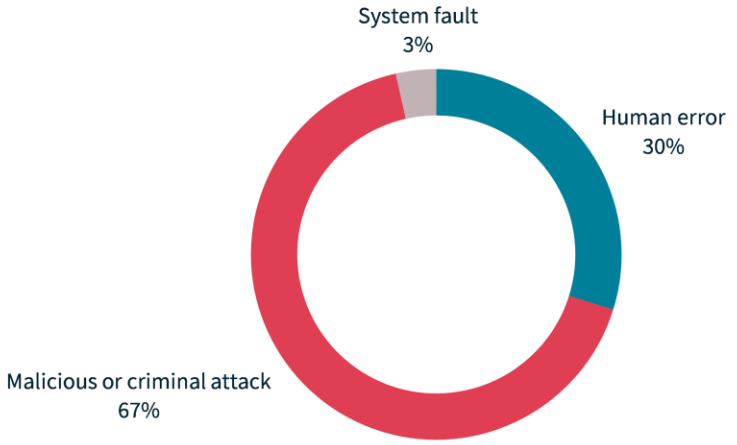
Top 5 sectors to notify data breaches

- Health service providers
- Finance (incl. superannuation)
- Insurance
- Retail
- Australian Government



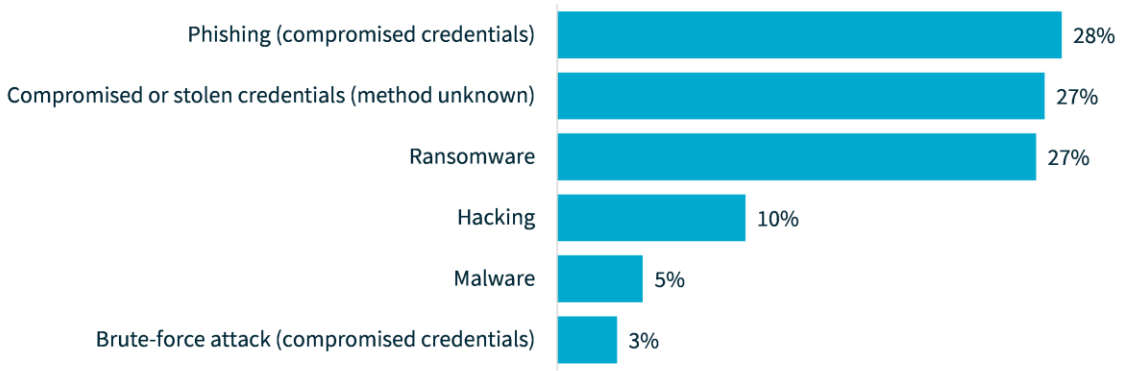
65%
of data breaches affected 100 people or fewer

Sources of data breaches



44% of all data breaches resulted from cyber security incidents (211 notifications)

Cyber incident breakdown



Top causes of human error breaches

PI sent to wrong recipient (email) 33%

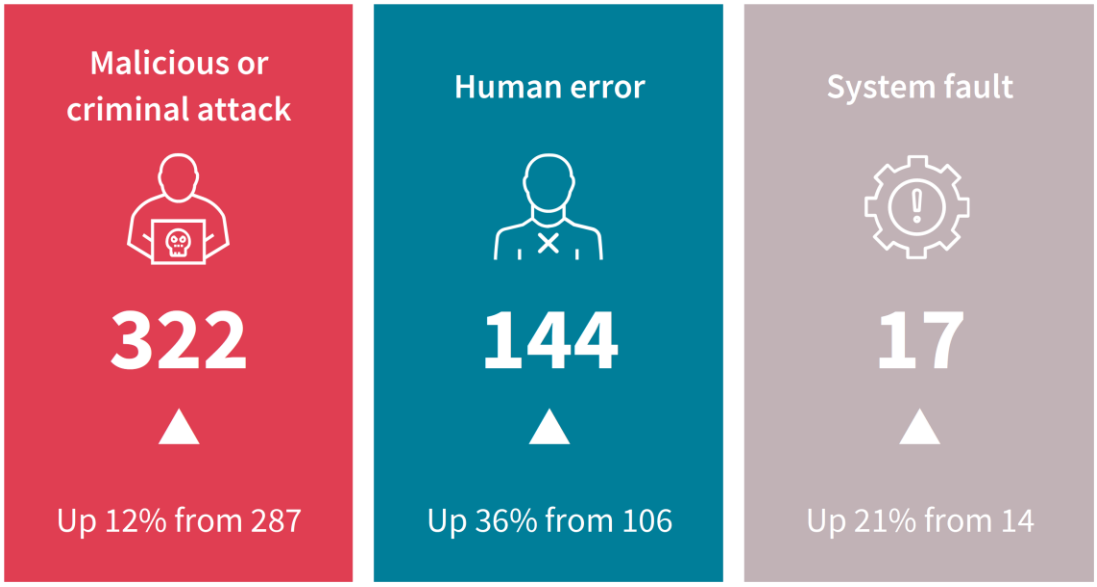
Unauthorised disclosure (unintended release or publication) 20%

PI sent to wrong recipient (mail) 10%

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* (Cth) 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 July to December 2023 reporting period:

- 483 breaches were notified, up 19% from 407 breaches in January to June 2023.
- Malicious or criminal attacks remained the leading cause (67%) of data breaches.
- The health and finance sectors remained the top reporters of data breaches. Health reported 104 breaches (22% of all notifications) and finance 49 breaches (10%).
- The majority of breaches (65%) affected 100 or fewer people.
- In addition to the 483 primary notifications, the OAIC received 121 secondary notifications, a significant increase from 29 secondary notifications in January to June 2023.

A stronger regulatory approach to NDB scheme compliance

The OAIC has identified the security of personal information as a regulatory priority and is prioritising regulatory action that addresses areas where there is the greatest risk of harm to individuals. The OAIC considers this is where there may be:

- serious failures to take reasonable steps to protect personal information
- inappropriate data retention practices
- failures to comply with the reporting requirements of the NDB scheme, particularly where the OAIC has publicised risks and mitigations.

Entities are expected to have established processes in place to ensure an effective response to data breaches and compliance with the requirements of the NDB scheme.

This expectation is reflected in 2 determinations made by the Information Commissioner in October 2023: *Datateks Pty Ltd* (Privacy) [2023] AICmr 97 and *Pacific Lutheran College* (Privacy) [2023] AICmr 98.

The determinations clarify the Commissioner's position on 2 aspects of the assessment requirement under s 26WH of the Privacy Act:

- when an entity forms a reasonable suspicion that an eligible data breach may have occurred (which then triggers the requirement to conduct a reasonable and expeditious assessment to resolve that suspicion)
- what may point to a failure to conduct an 'expeditious' assessment, such as a delay in an entity concluding its own investigation, engaging and managing the services of third parties or assessing personal information involved.

A key takeaway from these determinations is entities should have a considered and up-to-date data breach response plan. The entities in both cases did not have a data breach response plan in place before the data breach occurred.

The Commissioner ordered the entities to develop data breach response plans within a specified timeframe that addressed specific matters, such as:

- details of the entity's insurance coverage, including the extent of the coverage and the contact details of the insurer
- a process for engaging an external provider to investigate a suspected data breach where necessary, including details of the information that should be given to the provider, such as deadlines and the level of analysis required
- clear advice on the need for an investigation to be conducted expeditiously and for all reasonable steps to be taken to conclude an investigation within 30 days.

Civil penalty proceedings

On 3 November 2023, the Commissioner announced she had commenced civil penalty proceedings in the Federal Court against Australian Clinical Labs Limited (ACL) following an investigation of its privacy practices that arose from a February 2022 data breach.

The Commissioner alleges from May 2021 to September 2022, ACL seriously interfered with the privacy of millions of Australians by failing to take reasonable steps to protect their personal information from unauthorised access or disclosure and these failures left ACL vulnerable to cyber-attack.

When ACL did experience a cyber-attack that resulted in the unauthorised access and exfiltration of personal information of over 100,000 individuals, the Commissioner alleges that ACL:

- failed to conduct a reasonable and expeditious assessment (in contravention of s 26WH(2))
- failed to notify the Commissioner as soon as practicable (in contravention of s 26WK(2)).

The Federal Court can impose a civil penalty of up to $2,220,000 for each contravention (as per the penalty rate applicable from May 2021 to September 2022). Whether a civil penalty order is made, and the amount, are matters before the court.

Notifications received July to December 2023 – All sectors

The OAIC received 483 notifications during this reporting period, a 19% increase compared with January to June 2023. This is consistent with a trend observed by the OAIC since the start of the NDB scheme in February 2018 whereby more notifications are received in the second half of the calendar year.

Following a typically low number of notifications (57) in July 2023, there was a steady increase in notifications received month by month – peaking in December 2023 (97 notifications).

Table 1: Notifications received in 2023

Reporting period	Number of notifications
January to June 2023	407
July to December 2023	483
Total	**890**

Chart 1: Notifications received by month from January 2022 to December 2023

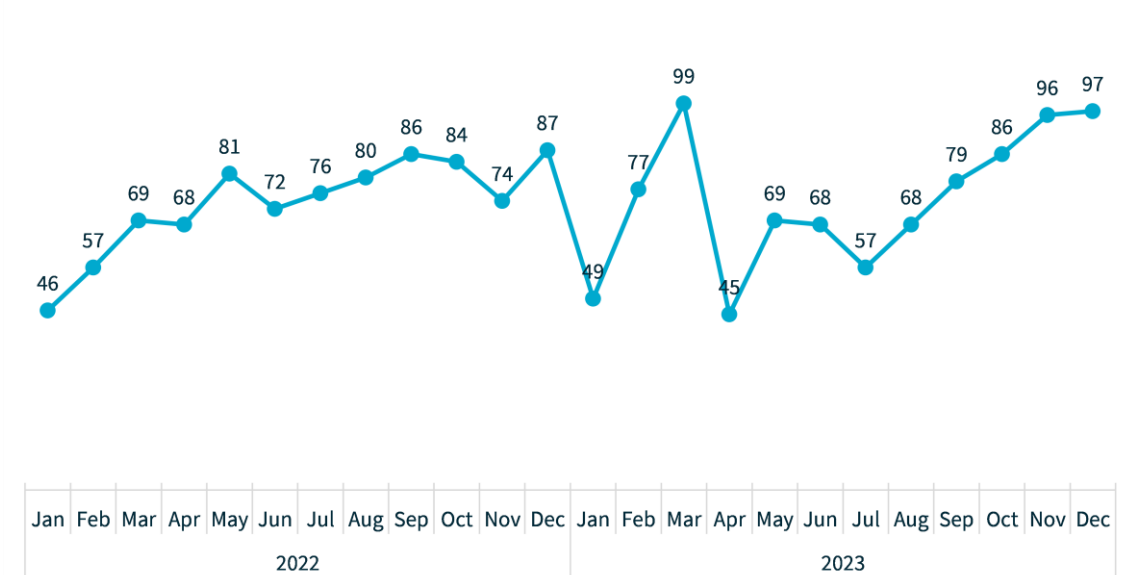
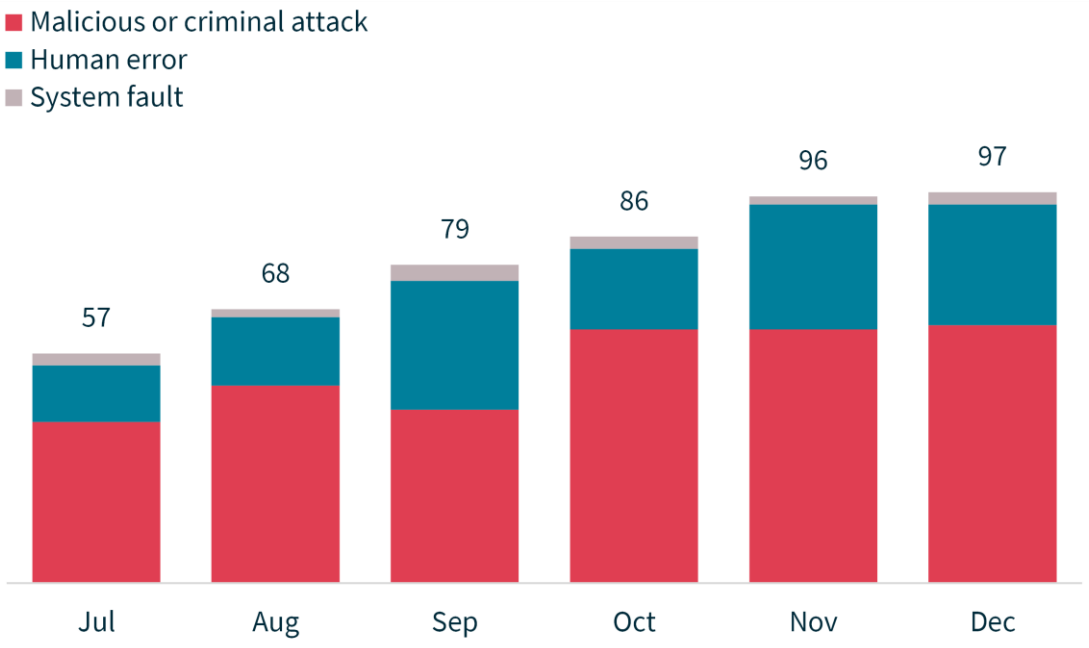


Chart 2: Notifications received by month showing the sources of breaches



Regulatory coordination

Entities may have various data breach reporting obligations. The Australian Government recently released the *Overview of cyber security obligations for corporate leaders* booklet [PDF 7.1 MB] to help corporate leaders understand and fulfil their cyber security obligations, including obligations under the Privacy Act and NDB scheme. The Australian Government has also launched a single reporting portal for cyber security incident reporting.

A coordinated approach among regulators is central to ensuring the distinct but complementary cyber regulatory frameworks work cohesively to address risks of harm and to promote a consistent whole-of-government approach to cyber security.

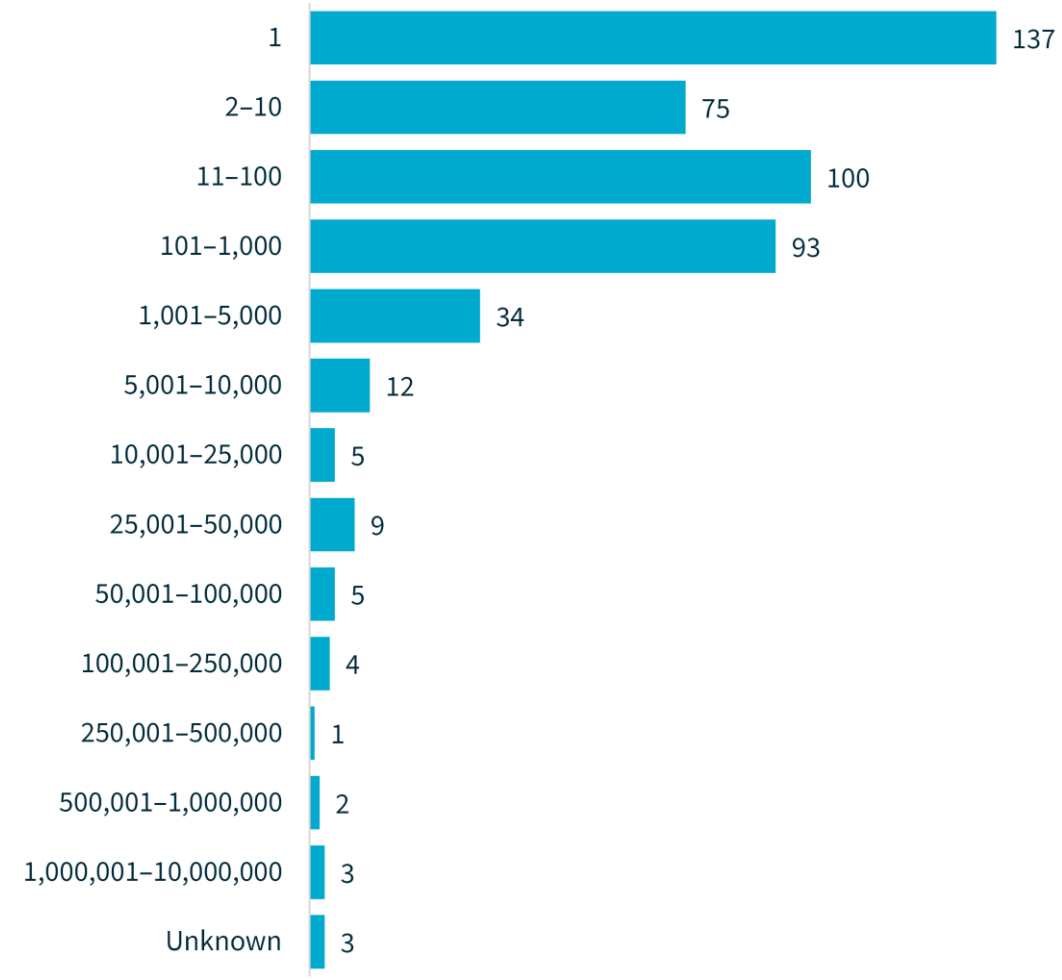
The OAIC welcomes the measures implemented by the Australian Government to streamline existing regulatory frameworks, such as the establishment of the National Coordinator for Cyber Security and the National Office for Cyber Security, and will continue to engage with the Australian Government as it implements the 2023–2030 Australian Cyber Security Strategy.

The OAIC co-chairs the Cyber Security Regulator Network (CSRN), which is a forum for Australian regulators to work together to understand, respond to and share information about cyber security risks and incidents. The CSRN works to reduce duplication or gaps in regulatory responses, so that regulatory activities are effective and efficient.

Number of individuals worldwide affected by breaches

The vast majority of data breaches (91%) during this reporting period involved personal information of 5,000 or fewer individuals worldwide. Breaches affecting 100 or fewer individuals comprised 65% of all notifications. Breaches affecting between 1 and 10 individuals accounted for 44% of all 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 affecting Australians

The OAIC received a similar number of data breaches that affected over 5,000 Australians in the second half of 2023 to those received in the first half of the year.

Table 2: Number of Australians affected by breaches

Number of Australians affected by breaches	Jan–Jun 2023	Jul–Dec 2023
5,001–10,000	11	7
10,001–25,000	5	4
25,001–50,000	3	7
50,001–100,000	3	0
100,001–250,000	1	4
250,001–500,000	0	1
500,001–1,000,000	0	1
1,000,001–10,000,000	2	2
10,000,001 or more	1	0
Total number of breaches affecting over 5,000 Australians	**26**	**26**

Cyber incidents continued to be the leading cause of data breaches that impacted a large number of Australians. Of the 26 breaches that affected over 5,000 Australians, 22 were caused by cyber incidents. The top causes were compromised or stolen credentials (9 notifications), ransomware (8 notifications) and hacking (4 notifications).

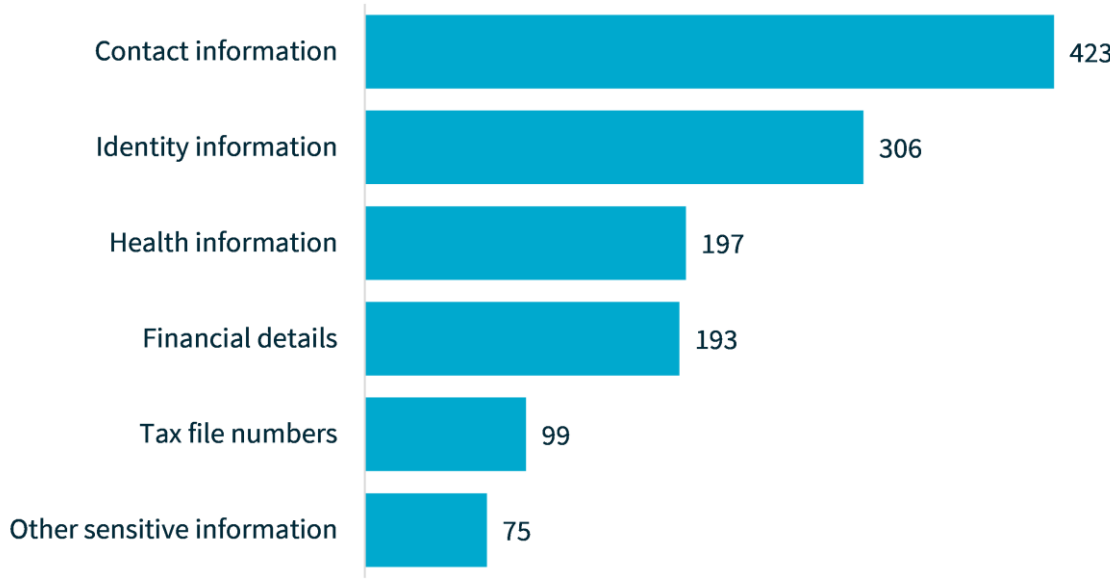
Entities need to continually review whether appropriate controls and processes are in place to defend against and mitigate data breaches caused by cyber incidents. The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) has developed prioritised mitigation strategies – the Strategies to Mitigate Cyber Security Incidents – to help entities protect themselves against various cyber threats. The most effective of these mitigation strategies is the Essential Eight.

Kinds of personal information involved in breaches

Contact and identity information continued to be the most common kinds of personal information involved in data breaches. Most data breaches (88%) involved contact information, such as an individual's name, home address, phone number and email address. This is distinct from identity information, which was exposed in 63% of breaches and includes information to confirm an individual's identity such as date of birth, passport details and other government identifiers.

Health information was exposed in 41% of data breaches in this reporting period, surpassing financial details as the third most common kind of personal information affected.

Chart 4: Kinds of personal information involved in breaches



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

Back to basics: data retention

Recent data breaches have highlighted the risks of retaining personal information for longer than needed. The more personal information an entity holds, the greater the possible scale and complexity of a data breach.

Entities should be mindful of their obligations under Australian Privacy Principle (APP) 11.2 to take reasonable steps to destroy or de-identify personal information unless:

- the entity needs the information for any purpose for which it may be used or disclosed by the entity under the APPs
- the information is contained in a Commonwealth record
- the entity is required by or under an Australian law, or a court/tribunal order, to retain the information.

Entities may have similar obligations to destroy or de-identify credit reporting information, credit eligibility information, tax file number information or Consumer Data Right data.

APP 1.2 also requires an entity to take reasonable steps to implement practices, procedures and systems relating to its functions or activities that will ensure it complies with the APPs, including APP 11.2. Entities should ensure they have systems and processes in place to regularly review whether it is still necessary to retain personal information.

For example, entities may find it useful to establish and implement a data retention policy. A data retention policy can assist an entity in identifying the different kinds of personal information it holds and determining appropriate retention periods that comply with APP 11.2. This helps to ensure that any information that is no longer required is promptly and securely destroyed. Entities should ensure data retention policies are adhered to, regularly audited and updated as required.

Scenario 1

A health service provider experienced a phishing attack that resulted in unauthorised access to the contents of multiple email accounts.

The health service provider collected a large volume of personal and sensitive information via its email accounts, meaning there was a significant number of records that required review after the breach. The health service provider did not have a data retention policy governing the storage and destruction of information collected via its email accounts. The email accounts contained historical personal information that the entity no longer required and personal information that was already captured in another record management system.

This led to a costly exercise of engaging a third-party service provider to analyse the unstructured data held within the compromised email accounts. It caused lengthy delays in conducting a data review to identify what personal information was compromised.

> Had the health service provider established and operationalised a data retention policy, it would more likely have turned its mind to whether it needed or was required to retain the historical personal information in the compromised email accounts. Had the health service provider taken the further step of destroying any personal information it no longer needed or was required to retain, it would have reduced the scale and cost of the data breach.

Time taken to identify breaches

Promptly detecting a data breach allows an entity to also quickly contain it, limiting its impact and reducing the time any malicious actors have access to systems. Examples of containment measures include shutting down systems breached, revoking or changing computer access privileges and recovering records.

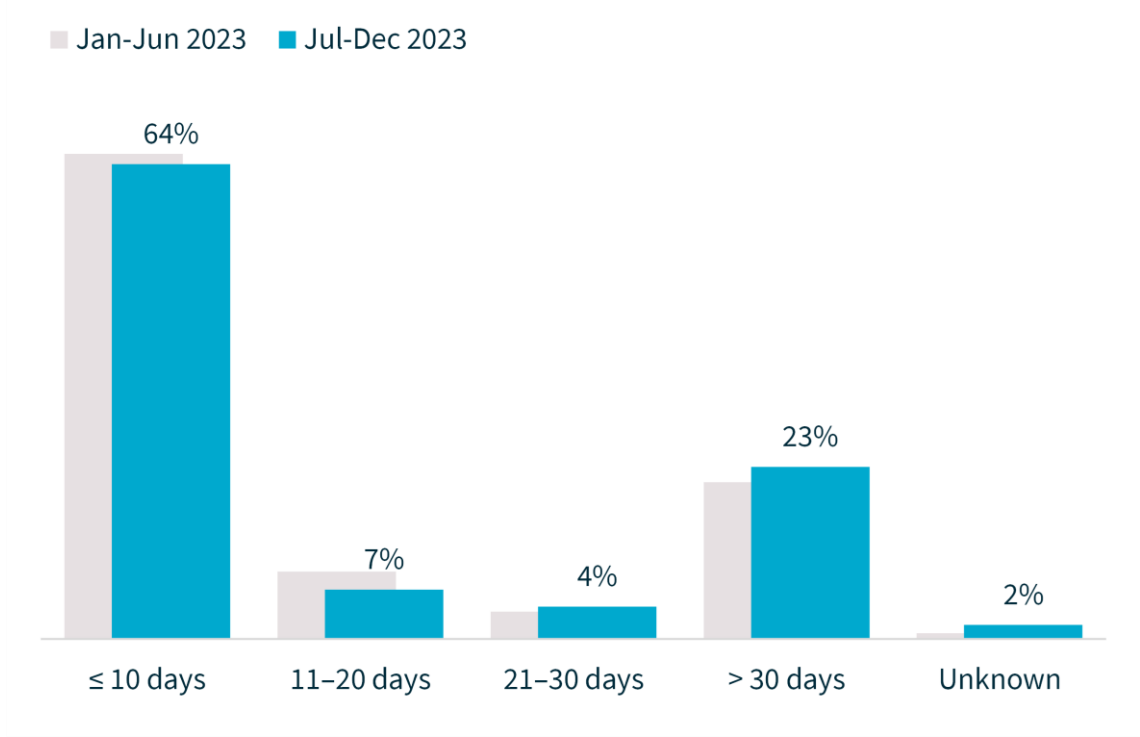
The figures in this section relate to the time between an incident occurring and the entity becoming aware of it. They do not relate to the time taken by the entity to assess whether an incident qualified as an eligible data breach.[1]

The charts for this section have changed from previous reports. Previously, the OAIC reported on the number of breaches that were identified within 30 days and above. To provide more specific details on how promptly entities identify breaches, the charts have been changed to provide information on the number of breaches identified from within 10 days to over 30 days of the incident occurring.

In this reporting period, 64% of breaches were identified by the entity within 10 days of it occurring. Around a quarter (23%) of breaches were identified over 30 days after it occurred.

[1] Section 26WH of the Privacy Act requires entities to take reasonable steps to conduct a data breach assessment within 30 days of becoming aware there are reasonable grounds to suspect they may have experienced an eligible data breach. Once the entity forms a reasonable belief that there has been an eligible data breach, they must prepare a statement and provide a copy to the OAIC as soon as practicable.

Chart 5: Time taken to identify breaches

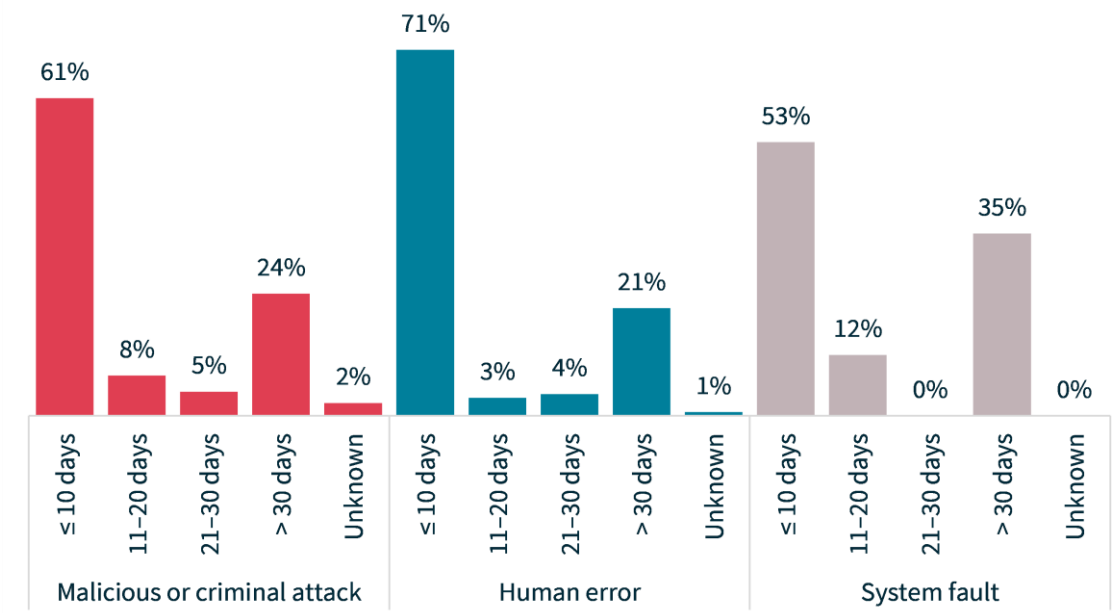


For notifications in the 'unknown' category, the entity was unable to identify the date the breach occurred.

The time taken by entities to identify breaches varied depending on the source of breach. Human error breaches (71% identified within 10 days) were the fastest to be identified, followed by malicious or criminal attacks (61%).

Consistent with previous reports, system fault breaches were the slowest to be identified (53% identified within 10 days).

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.

Reasonable and expeditious assessments of a 'suspected' eligible data breach

The requirement to conduct a reasonable and expeditious assessment is triggered when an entity is aware of reasonable grounds sufficient to cause it to form a suspicion that an eligible data breach has occurred (s 26WH(1)).

The following scenarios illustrate circumstances that would give rise to a reasonable suspicion and how the entities responded in those circumstances.

Scenario 1

An entity became aware that its IT service provider had experienced a cyber incident resulting in unauthorised access to its systems.

While it was unclear what actions the malicious actor took while they had access to the IT service provider's environment, the entity considered there was sufficient information to suspect an eligible data breach may have occurred.

The entity commenced its assessment and engaged IT forensic experts to investigate the cause and scope of the incident and external legal counsel to assist with its review of the data possibly accessible to the malicious actor.

One week later, the entity became aware of allegations that the malicious actor exfiltrated data from its network and published it on a 'leak site'. The IT forensic experts assessed the published data and confirmed personal information relating to financial loan applications was exfiltrated from the entity's systems.

In this instance, the entity commenced its assessment of the suspected eligible data breach when it became aware of the unauthorised access to its systems, rather than when it confirmed data had been exfiltrated. As a result, the entity was able to respond in a timely manner, notifying the OAIC and affected individuals within 30 days of becoming aware of the breach.

Scenario 2

A health service provider became aware that a locked paper waste bin was missing from its premises. The bin was typically used to dispose new patient forms intended for shredding. The forms contained individuals' names, dates of birth, contact information, Medicare numbers and health information.

The health service provider reported the incident to the police on the same day it became aware the bin was missing. Five months later, the police informed the entity the bin had been located at a perpetrator's house and had been tampered with and its contents were missing.

The health service provider did not notify the Information Commissioner or affected individuals until 6 months after it became aware of the incident. The health service provider had not initiated an assessment of whether there were reasonable grounds to believe an eligible data breach had occurred until the police confirmed the bin had been stolen.

In this circumstance, the time taken to notify the Commissioner and affected individuals would have been reduced had the health service provider commenced its assessment as soon as it became aware of the incident.

The health service provider's immediate action of reporting the missing bin to the police indicates it was concerned about the risks associated with the loss of the bin and its contents from the premises. The health service provider ought to have become aware that there were reasonable grounds to *suspect* there may have been an eligible data breach on the day it realised the bin was missing and notified the police. The additional certainty that may have been provided by the police's later confirmation of theft was not necessary to meet the threshold of reasonable suspicion.

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 this reporting period, 72% of entities notified the OAIC within 30 days of becoming aware of an incident, similar to 74% in the previous period.

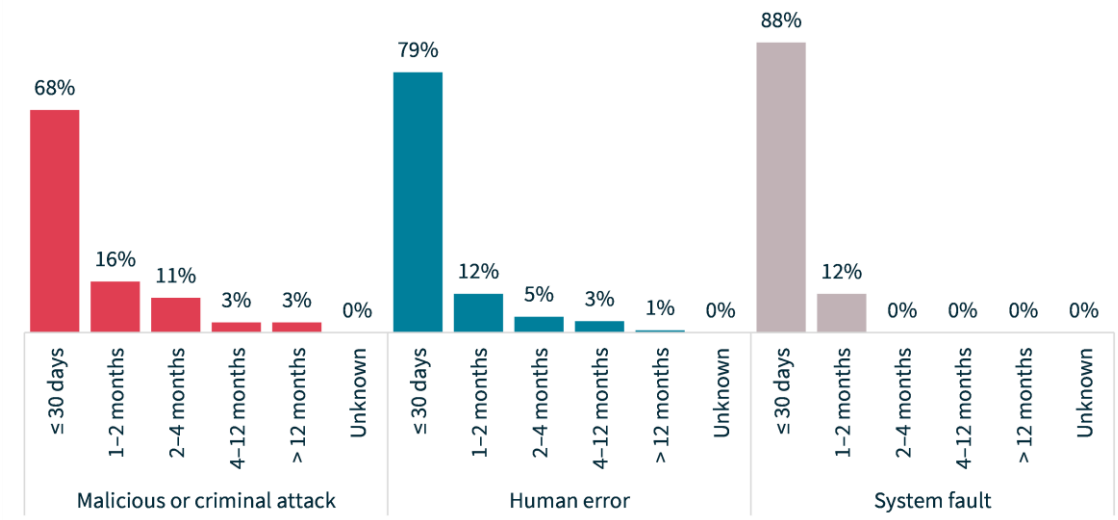
Chart 7: Time taken to notify the OAIC of breaches

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

The time it took entities to notify the OAIC also varied depending on the source of the breach, and there was some variation from the previous period.

The time it took entities to notify breaches caused by malicious or criminal attacks and human error was comparable to the previous period. The majority of system fault breaches were notified to the OAIC within 30 days of the entity becoming aware of the 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.

Putting the individual at the front and centre of a data breach response

A key objective of the NDB scheme is to ensure individuals are promptly told of data breaches so they can quickly take steps to minimise their risk of harm.

A data breach does not necessarily mean an entity will lose the trust of Australians. Our *Australian Community Attitudes to Privacy Survey 2023* found most Australians would remain with an entity that acts quickly in response to a data breach. The actions most likely to influence an individual to stay include the entity quickly putting steps in place to prevent customers experiencing further harm from the breach and making improvements to security practices. Only 12% of Australians said there was nothing an entity could do that would influence them to stay after a data breach. This demonstrates the response matters – the individual should be front and centre.

Individuals affected by a data breach expect to be informed about the incident.

The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* introduced the requirement for greater particularity in notification statements to both the OAIC and affected individuals. An entity's notification must include:

- the identity and contact details of the entity (s 26WK(3)(a))

- a description of the eligible data breach (s 26WK(3)(b))
- the particular kind or kinds of information involved in the eligible data breach (s 26WK(3)(c))
- what steps the entity recommends that individuals take in response to the eligible data breach (s 26WK(3)(d)).

An entity can meet its obligations under the NDB scheme by notifying all affected individuals (s 26WL(2)(a)) or individuals who are at risk of serious harm from the breach (s 26WL(2)(b)).

Public statements about a data breach

In circumstances where neither of these options are practicable, the entity must publish a statement on its website and take reasonable steps to publicise its contents (s 26WL(2)(c)). The OAIC expects that public statements about a data breach are timely and specific. The website statement must comply with s 26WK(3) and must not deviate from the contents of the statement that has been provided to the OAIC under s 26WK(2).

The OAIC has observed instances where a public statement about a data breach has not set out all the details outlined in s 26WK(3) of the Privacy Act, such as a description of the eligible data breach or the particular kinds of personal information involved. There have also been instances where an entity has provided a statement that is compliant with s 26WK(3) to the OAIC, but has subsequently published a website statement withholding required details.

Publishing a website statement that does not include all the required details may fall short of the notification obligations under the NDB scheme. Withholding key details in the statement may also adversely affect an affected individual's ability to make an informed decision about how best to mitigate harm.

Where directly notifying affected individuals is practicable for an entity but the entity's direct notification campaign is delayed due to difficulties in identifying contact details and preparing tailored notifications, it is also open to the entity to publish a website notification before directly notifying affected individuals.

However, a website notification is not a substitute for the entity's obligation to directly notify affected individuals. Despite any public statements that may have been published, it remains that the entity must take reasonable steps to notify the affected individuals directly as soon as practicable after it completes preparing a statement that complies with s 26WK(3).

Scenario 1

An entity became aware of a data breach involving unauthorised access to a third-party supplier's systems. The entity immediately commenced its forensic investigation of the incident in parallel with its notification campaign.

Within 2 days of becoming aware of the incident, the entity notified its entire customer base of over one million individuals of the data breach and published a statement on its website.

In its notification and published statement, the entity outlined the kinds of personal information likely to be involved, including dates of birth, contact details and gender, and outlined precautionary steps an individual may wish to take to protect themselves.

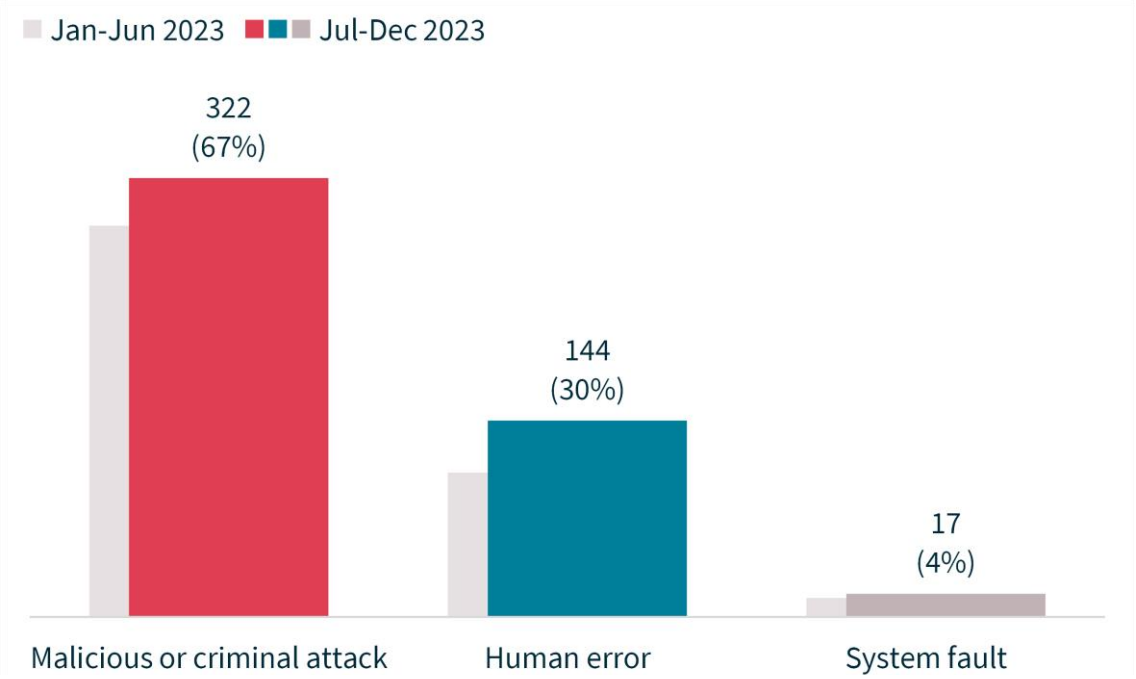
Source of breaches

Malicious or criminal attacks remained the leading source of data breaches reported to the OAIC.

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

- 67% were caused by malicious or criminal attacks, compared to 71% the previous period.
- 30% were caused by human error, compared to 26% the previous period.
- 4% were caused by system faults, compared to 3% the previous period.

Chart 9: Source of data breaches

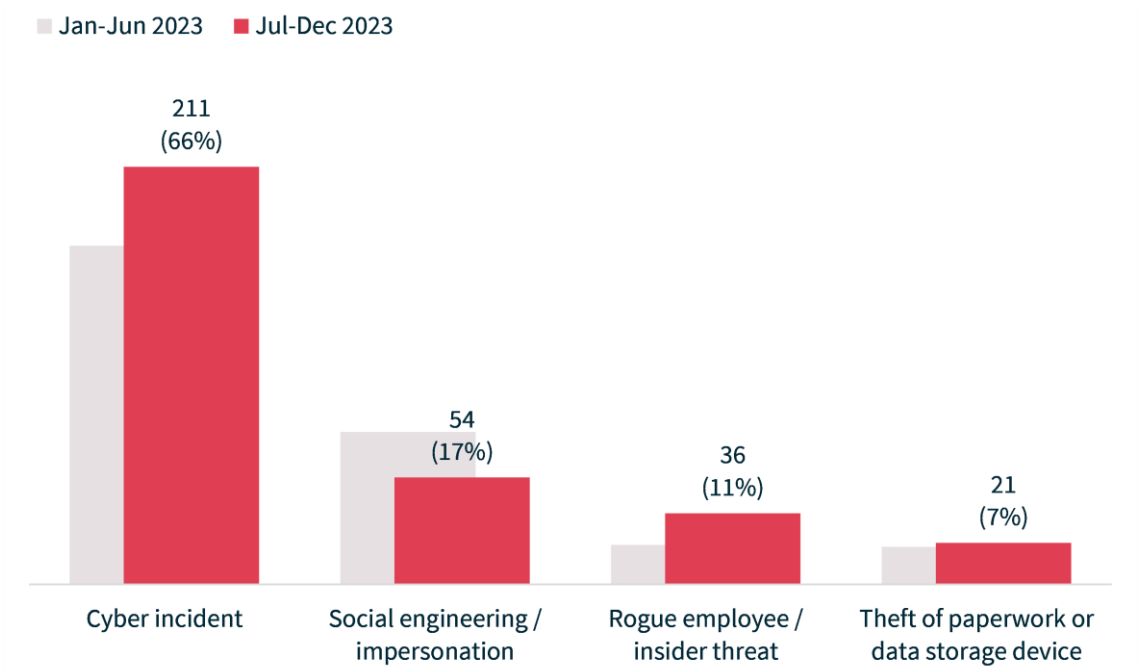


Malicious or criminal attacks

The majority (66%) of breaches caused by malicious or criminal attacks were cyber incidents. There were 211 breaches resulting from cyber incidents, up 23% in number from 171 in January to June 2023. Cyber incidents were the source of 44% of all data breaches, compared with 42% in the previous period.

Social engineering or impersonation attacks accounted for 17% of breaches caused by malicious or criminal attacks, actions taken by a rogue employee or insider threat for 11% and theft of paperwork or data storage device for 7%.

Chart 10: Malicious or criminal attack breakdown



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 56,279 individuals on average, in comparison to the next highest average of 9,080 individuals affected by a breach caused by a rogue employee or insider threat.

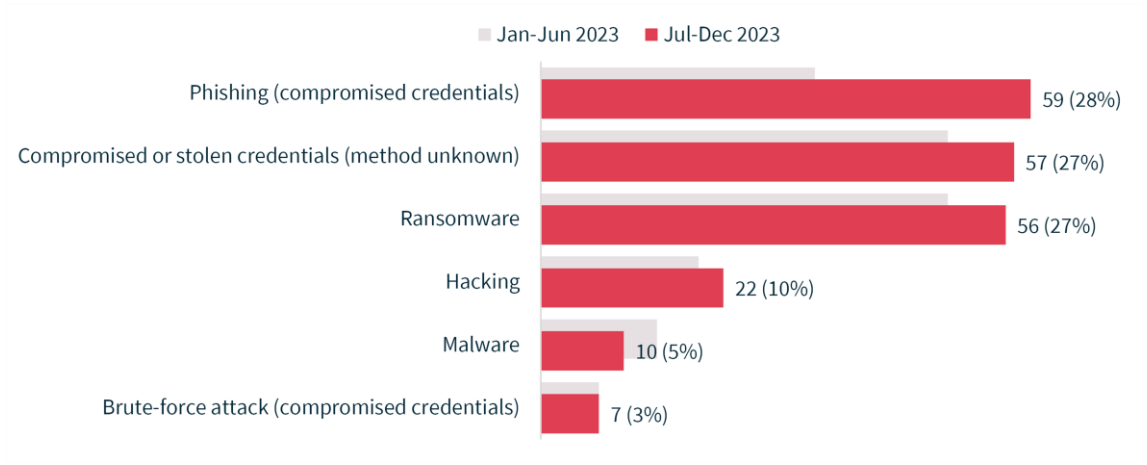
Table 3: Malicious or criminal attack breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Cyber incident	211	56,279	171
Rogue employee / insider threat	36	9,080	11
Social engineering / impersonation	54	183	4
Theft of paperwork or data storage device	21	152	48
Total	**322**	**37,346**	**58**

Cyber incidents

In this reporting period, phishing (28%, 59 notifications) took over from ransomware (27%, 57 notifications) as the top source of cyber incidents. Compromised credentials – through phishing, a brute-force attack or an unknown method – comprised 58% of all cyber incidents.

Chart 11: Cyber incident breakdown



Particular kinds of cyber incidents affect a larger number of individuals worldwide. In this period, brute-force attacks continued to impact the most individuals, affecting an average of 803,222 individuals across 7 notifications. This was followed by ransomware (56 notifications), which affected 57,900 individuals on average, and hacking (22 notifications), which affected 49,501 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	803,222	95
Ransomware	56	57,900	693
Hacking	22	49,501	879
Compromised or stolen credentials (method unknown)	57	27,320	17
Phishing (compromised credentials)	59	1,951	70
Malware	10	356	9
Total	**211**	**56,279**	**171**

Compromised or stolen credentials as the leading cause of all data breaches

Compromised or stolen account credentials caused a quarter (25%) of all data breaches in the reporting period.

Entities must remain vigilant as the increased occurrence of large-scale data breaches in recent years has heightened the risks of cyber incidents that involve the use of compromised credentials, such as credential stuffing attacks.

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

The ASD's ACSC recommends entities implement the Essential Eight cyber security strategies as a baseline defence against cyber threats. One of these mitigation strategies is multi-factor authentication.

Multi-factor authentication is one of the most effective ways entities can protect against unauthorised access. However, multi-factor authentication that is not implemented or configured properly can create security vulnerabilities that could be leveraged by malicious actors.

Entities should also encourage employees and customers to use strong passphrases to protect their accounts. Each account should have a unique passphrase, as reusing a passphrase makes each account that uses it more vulnerable.

Scenario 1

A malicious actor used compromised credentials to gain access to an employee of an entity's account. The malicious actor then deployed ransomware that resulted in the personal information of the entity's clients being encrypted and exfiltrated.

The entity had thought multi-factor authentication was in place at the time of the incident. However, its investigation later found the malicious actor accessed the network by targeting 'legacy users' that did not have multi-factor authentication applied.

As a result of the incident, the entity ensured multi-factor authentication was configured appropriately for all employees' access to the network and further enhanced its management of accounts that had privileged access to large volumes of personal information.

Mitigating the use of compromised credentials

Entities should be mindful that cyber-attacks are increasingly sophisticated. The OAIC has observed instances of malicious actors using a mix of social engineering and technical techniques to circumvent multi-factor authentication.

The ASD's ACSC's November 2023 update to the Essential Eight Maturity Model included adopting a new minimum multi-factor authentication standard that requires 'something users have', in addition to 'something users know', to address the risks associated with weaker forms of multi-factor authentication that used biometrics, security questions or 'Trusted Signals'.

Multi-factor authentication should be implemented alongside additional strategies to mitigate the use of compromised credentials, including:

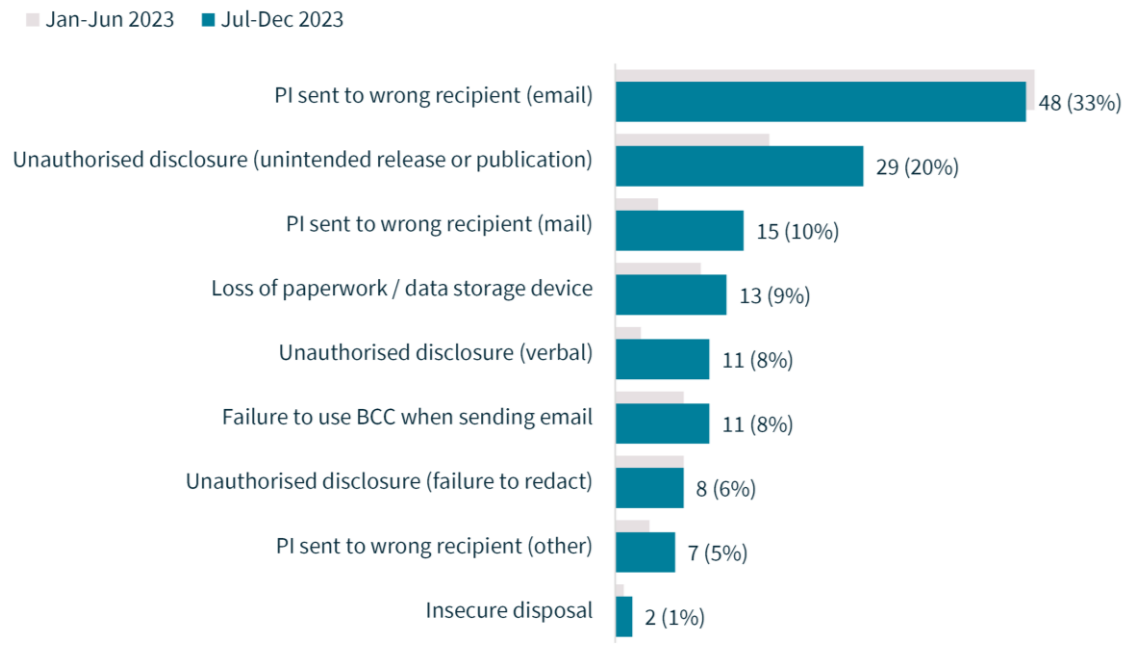
- restricting administrative privileges to operating systems and applications based on user duties and regularly revalidating the need for privileges
- enhancing capabilities to detect and prevent logins from unusual or suspicious internet service provider addresses and geolocations
- increasing the frequency of internal audit and quality assurance activities
- measures to embed good privacy practices and an understanding of cyber risks across all levels of the entity.

Entities should refer to the ASD's ACSC website for further detailed guidance.

Human error

Personal information being emailed to the wrong recipient remained the most common cause of human error breaches in the second half of 2023. Close to half (49%) of human error breaches resulted from personal information being sent to the wrong recipient by email, mail or other means.

Chart 12: Human error breakdown



Certain kinds of human error breaches also affected larger numbers of individuals worldwide. Fifteen breaches where personal information was sent to the wrong recipient by mail affected an average of 2,231 individuals. This was followed by 2 breaches that were caused by the insecure disposal of personal information, which affected 1,074 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
PI sent to wrong recipient (mail)	15	2,231	1
Insecure disposal	2	1,074	1,074
Unauthorised disclosure (unintended release or publication)	29	299	1
Loss of paperwork / data storage device	13	193	5
Failure to use BCC when sending email	11	145	66

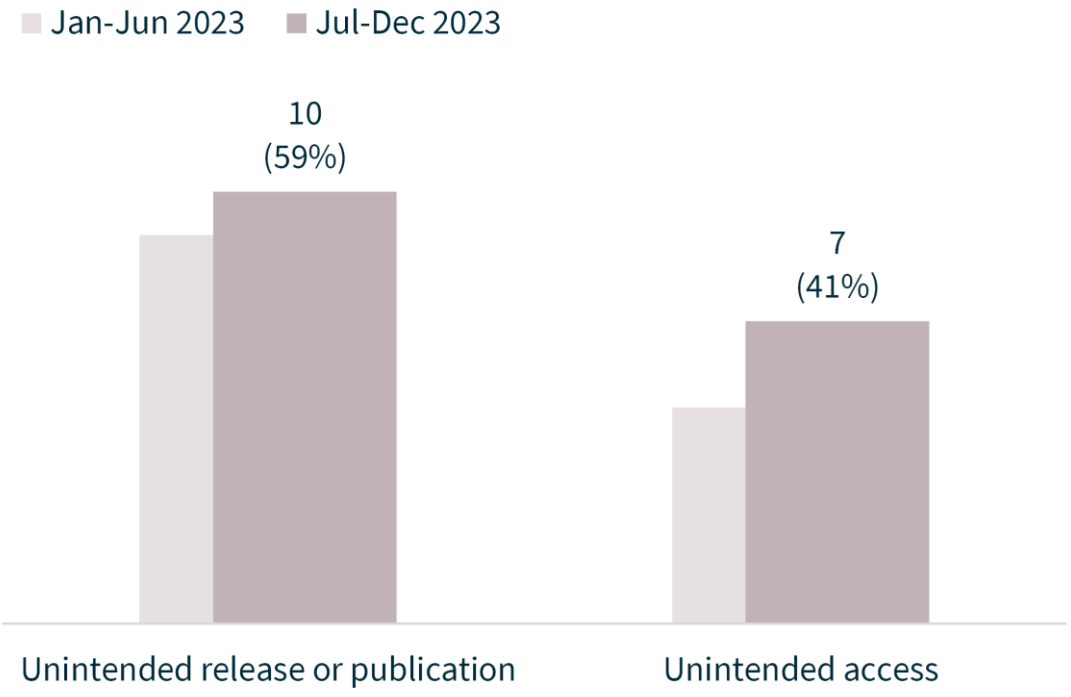
Unauthorised disclosure (failure to redact)	8	35	2
PI sent to wrong recipient (email)	48	29	1
Unauthorised disclosure (verbal)	11	1	1
PI sent to wrong recipient (other)	7	1	1
Total	**144**	**348**	**1**

System faults

The majority (59%) of system fault breaches involved the unintended release or publication of personal information. Examples of issues that may lead to this include systems or databases that are misaligned or operate asynchronously, and untested system or infrastructure changes.

Unintended access to personal information due to a system fault comprised 41% of system fault breaches. 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



Risks associated with outsourcing personal information handling

Where a single data breach affects multiple entities, the OAIC may receive multiple notifications relating to the same incident, although only one entity is required to notify a data breach affecting multiple entities.

Notifications relating to the same incident are counted as a single notification in this report to avoid information being duplicated. However, the volume of secondary notifications may be indicative of the level of multi-party breach reporting.

There was a significant increase in the number of secondary notifications (121 notifications) from the previous reporting period (29 notifications).

Most of these multi-party breaches involved a data breach of a cloud or software provider, which then impacted the clients who had outsourced their personal information handling to those providers. This highlights the significant data breach risks that can arise from outsourcing personal information handling.

Table 6: Primary and secondary notifications received from January 2022 to December 2023

Reporting period	Primary notifications where at least one secondary notification was received	Secondary notifications
January to June 2022	7	22
July to December 2022	17	41
January to June 2023	9	29
July to December 2023	6	121

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

In this reporting period, multi-party breaches involving contracted service providers highlighted 2 issues:

- the lack of data retention or destruction clauses in contractual agreements following the cessation of services
- the lack of clearly defined responsibilities should a data breach occur, including who should assess and/or notify the breach.

In our increasingly interconnected economy, where services are commonly contracted out and involve the handling of personal information, it is imperative that entities proactively mitigate

privacy risks in contractual agreements with third-party service providers. This is an important step in demonstrating an entity's compliance with APP 11 (securing personal information) and the NDB scheme.

Prior to using the services of third-party providers:

- Entities should ensure the third-party provider has baseline security and operational controls to prevent the compromise of systems that hold personal information, such as monitoring and logging capabilities for their customer infrastructure.
- Entities should ensure service agreements or contractual arrangements address:
  - the handling of personal information, including defined data retention periods and processes for destroying or de-identifying data
  - data breach response requirements, including assigning roles and responsibilities for managing a data breach and meeting regulatory reporting obligations. This should specifically address which entity is to assess a data breach should one occur and which entity is responsible for notifying affected individuals. Depending on the contractual arrangement, both responsibilities could lie with one entity or be separated between them.
- Entities should set out expectations for communication when suspicious activity is detected on systems that hold personal information.

Scenario 1

A software service provider experienced a ransomware attack that resulted in data being exfiltrated and published on the dark web, including personal information stored for a large number of client organisations.

The service provider took over 6 months to identify the personal information that related to each client and coordinate notification to affected individuals. In some instances, the client organisation had not used the service provider's services for several years and the personal information of affected individuals was collected over 10 years prior.

The scale of the incident and the lengthy data review process were impacted by the service provider not having clear retention policies in place, particularly in instances where it had ceased providing services to client organisations. The service provider advised it deleted data upon receiving a written request from its clients, though these requests were rarely made.

In this instance, both the service provider and the client organisations failed to define or enforce data retention periods, and failed to ensure personal information was de-identified or destroyed in accordance with APP 11.2. This led to the service provider retaining personal information longer than was necessary and increased the amount of personal information accessible to the malicious actor when its systems were compromised.

Comparison of top 5 sectors

This section compares notifications received by the top 5 sectors by notifications, which accounted for 57% of all data breaches.

Health service providers[2] and the finance[3] industry have consistently reported the most data breaches of all sectors since the NDB scheme began.

Health service providers reported 104 data breaches (22% of all notifications). The second largest source of notifications was the finance sector with 49 data breaches (10%). The other sectors in the top 5 were insurance (9%), retail (8%) and the Australian Government (8%).

Table 7: Top 5 sectors by notifications

Sector	Number of notifications	Percentage of all notifications received
Health service providers	104	22%
Finance	49	10%
Insurance	45	9%
Retail	39	8%
Australian Government	38	8%
Total	**275**	**57%**

[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.

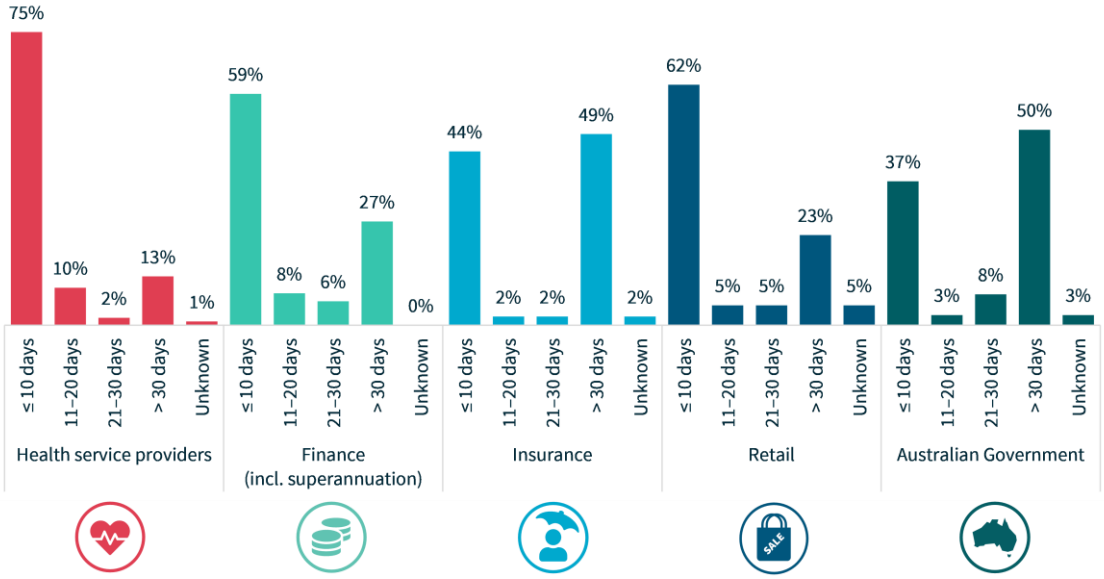
[3] This sector includes banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

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, for 75% of the notifications by health service providers, the incident was identified within 10 days of it occurring, compared to 37% of the notifications by the Australian Government.

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.

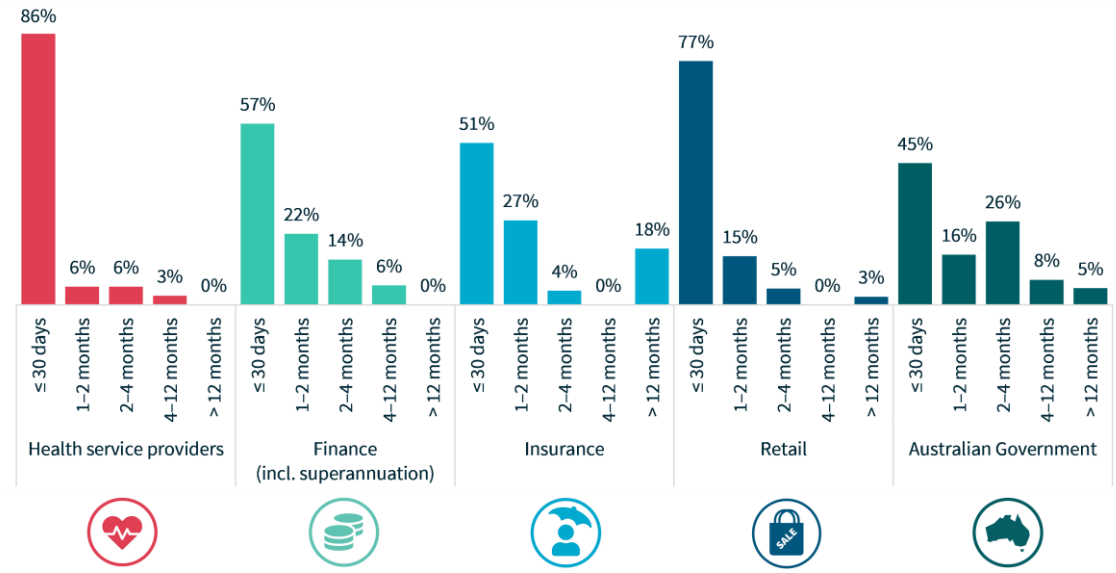
Time taken to notify the OAIC of breaches – Top 5 sectors

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

In the reporting period, 86% of notifications by the health sector were made within 30 days of the entity becoming aware of the incident, compared to 45% for the Australian Government.

It took over 12 months for 18% of breaches in the insurance sector to be notified to the OAIC, a significantly higher proportion than other sectors in the top 5.

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

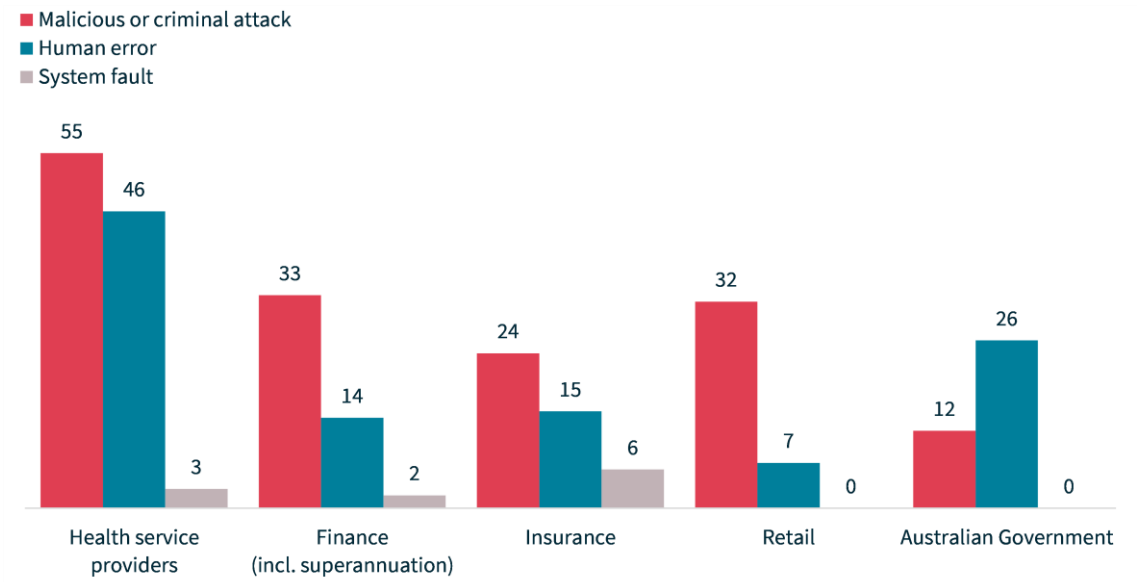


For notifications in the 'unknown' category, the entity was unable to advise the OAIC the date it became aware of the incident.

Source of breaches – Top 5 sectors

Malicious or criminal attacks remained the leading cause of data breaches notified by the top 5 sectors. They were the source of 53% of breaches notified by health service providers, 67% for the finance sector, 53% for the insurance sector and 82% for the retail sector.

Chart 16: Source of breaches – Top 5 sectors



Data breaches in the public sector

Before this report, the Australian Government had not been in the top 5 sectors by notifications since the January to June 2021 reporting period.

Australian Government agencies reported 38 data breaches, 8% of all notifications during the period.

In contrast with the other sectors in the top 5, Australian Government agencies notified more data breaches caused by human error (68%) than those caused by malicious or criminal attacks (32%).

Of the 26 human error breaches experienced by Australian Government agencies: 13 involved personal information being sent to a wrong person; 11 were a result of unauthorised disclosure of personal information; and 2 involved the loss of paperwork or a data storage device.

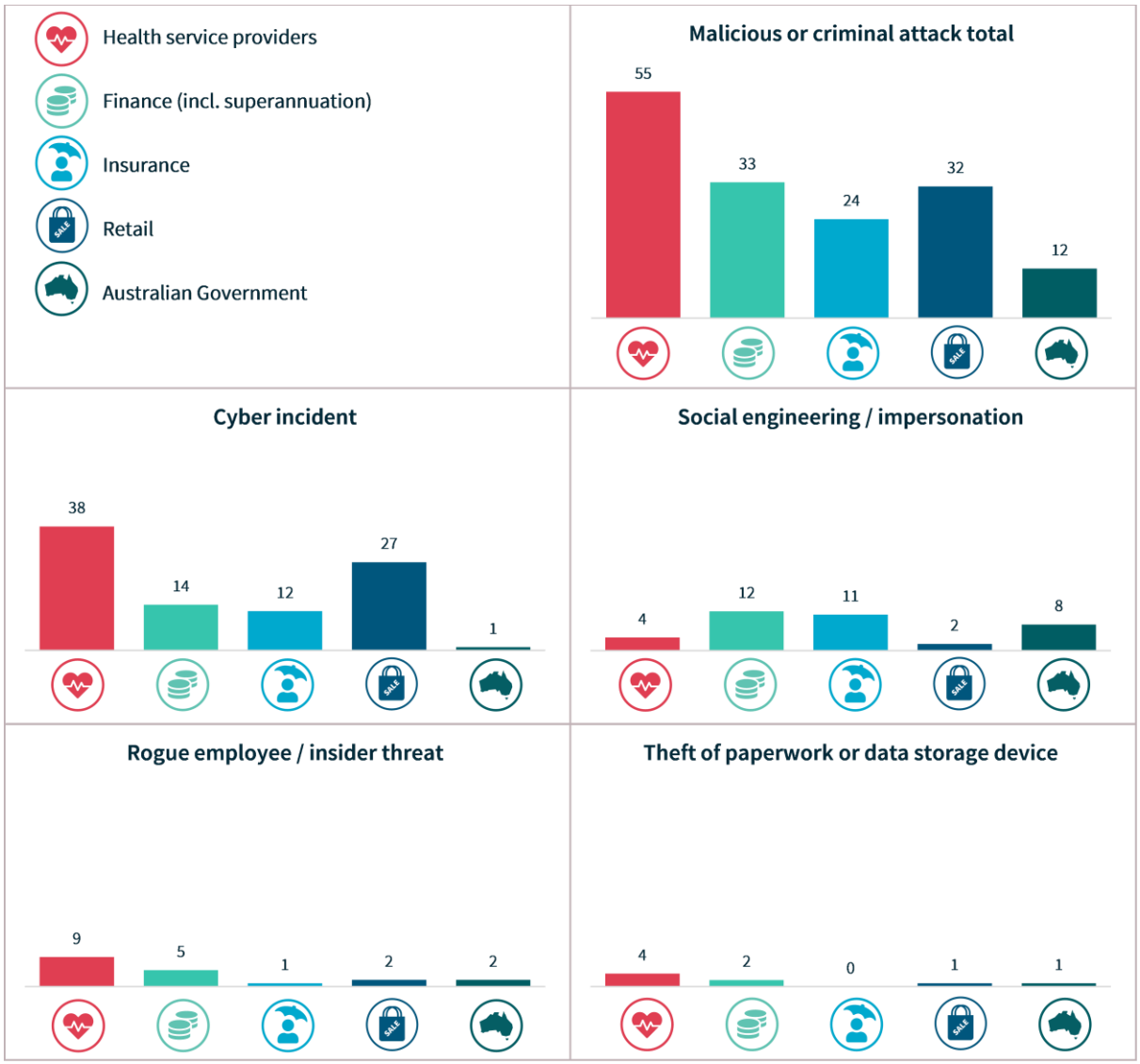
Human error breaches generally result from a failure of process or procedure. Entities should assume human error will occur and design systems and processes to minimise the risk. The risk of human error can also be reduced by educating staff about secure information handling practices (such as sending documents containing personal information via mechanisms that provide additional security controls) and putting controls in place (such as email filtering).

Of the top 5 sectors, the Australian Government had the largest proportion (50%) of notifications where the agency identified the incident over 30 days after it occurred. The Australian Government also had the largest proportion (55%) of notifications made to the OAIC more than 30 days after the agency become aware of the incident.

These statistics suggest Australian Government agencies should check they have effective systems for detecting, assessing, responding to and notifying data breaches. Such systems are fundamental to an agency's ability to meet the NDB scheme's requirements.

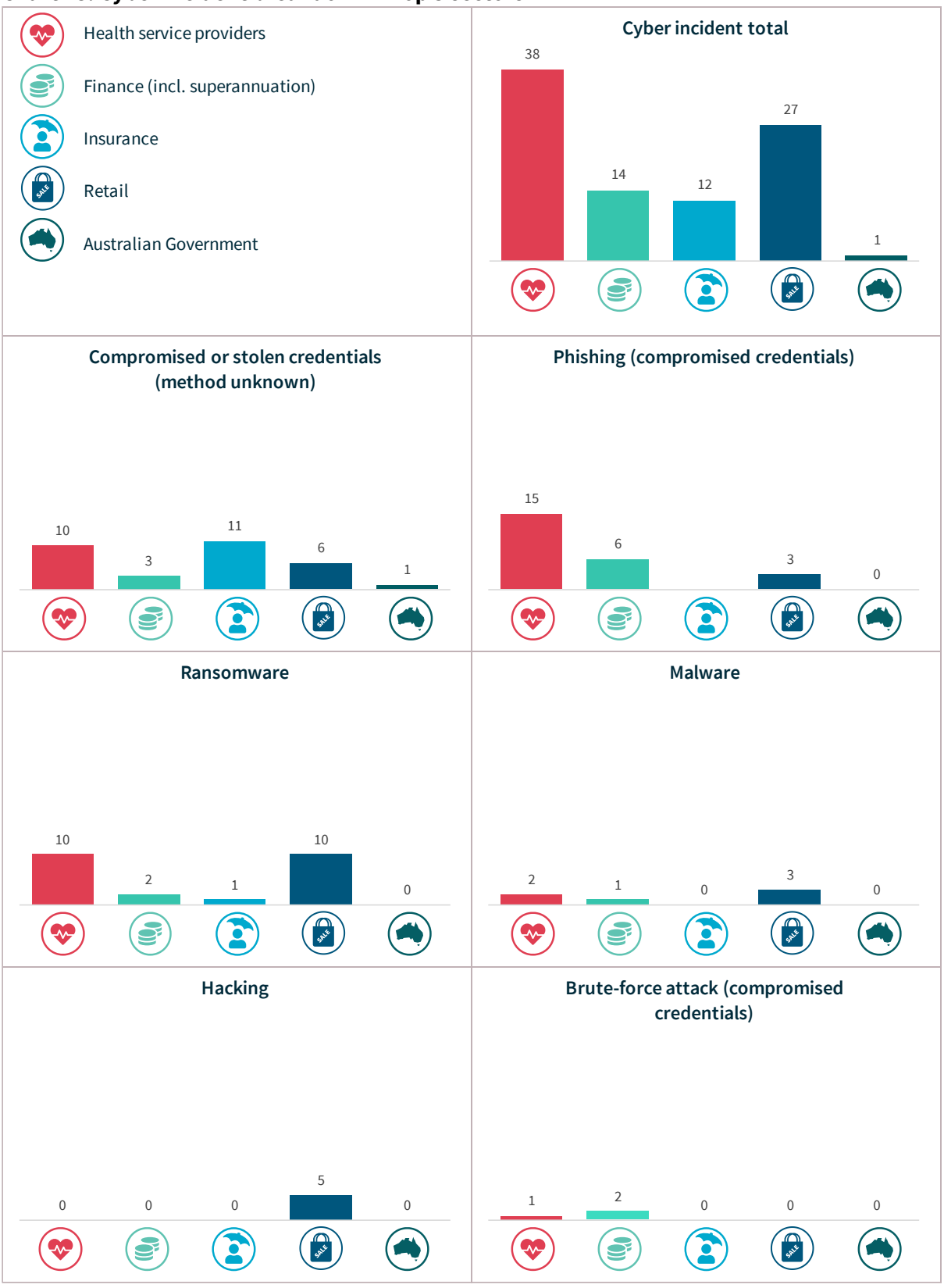
Malicious or criminal attack breaches – Top 5 sectors

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



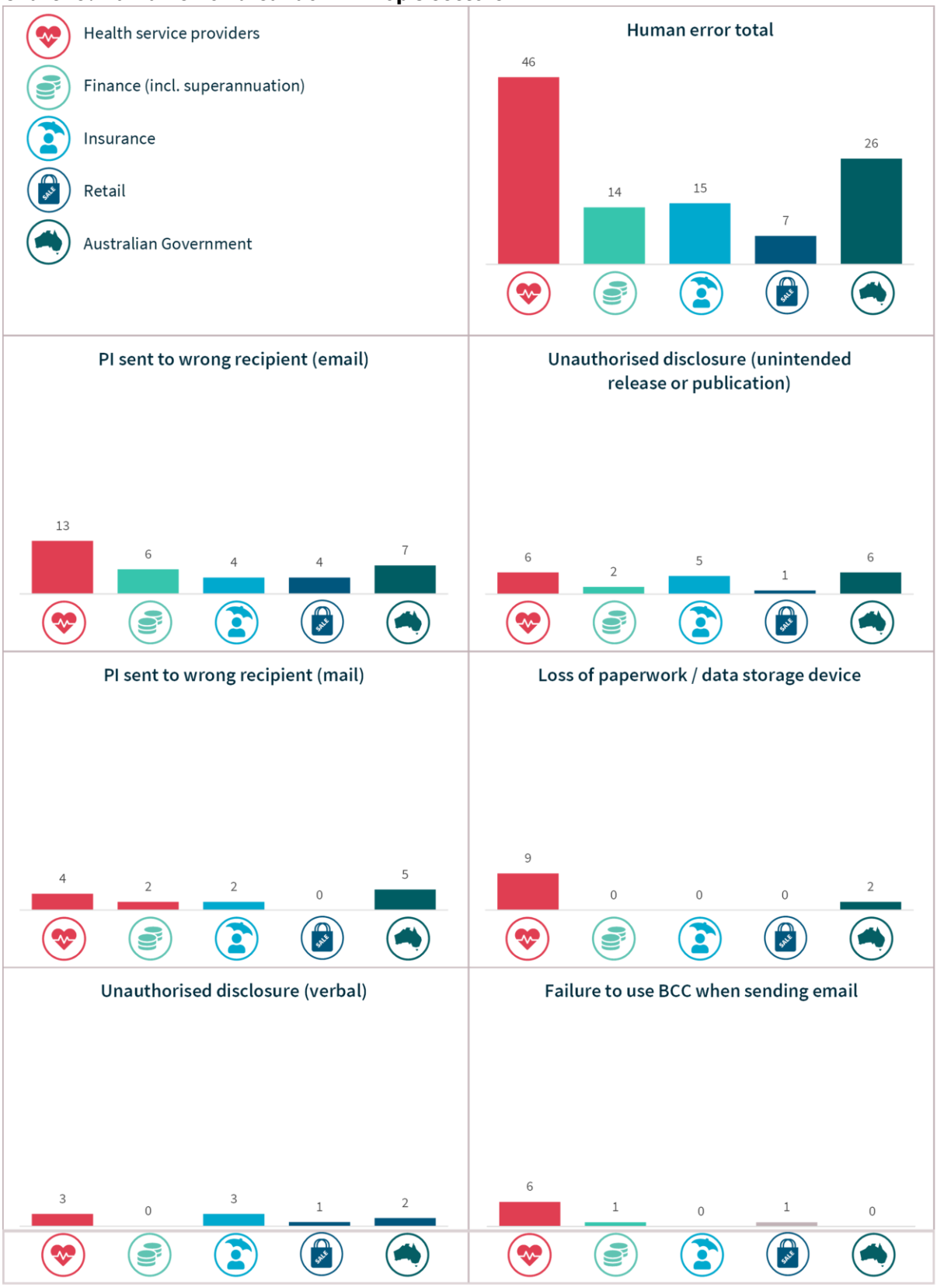
Cyber incident breaches – Top 5 sectors

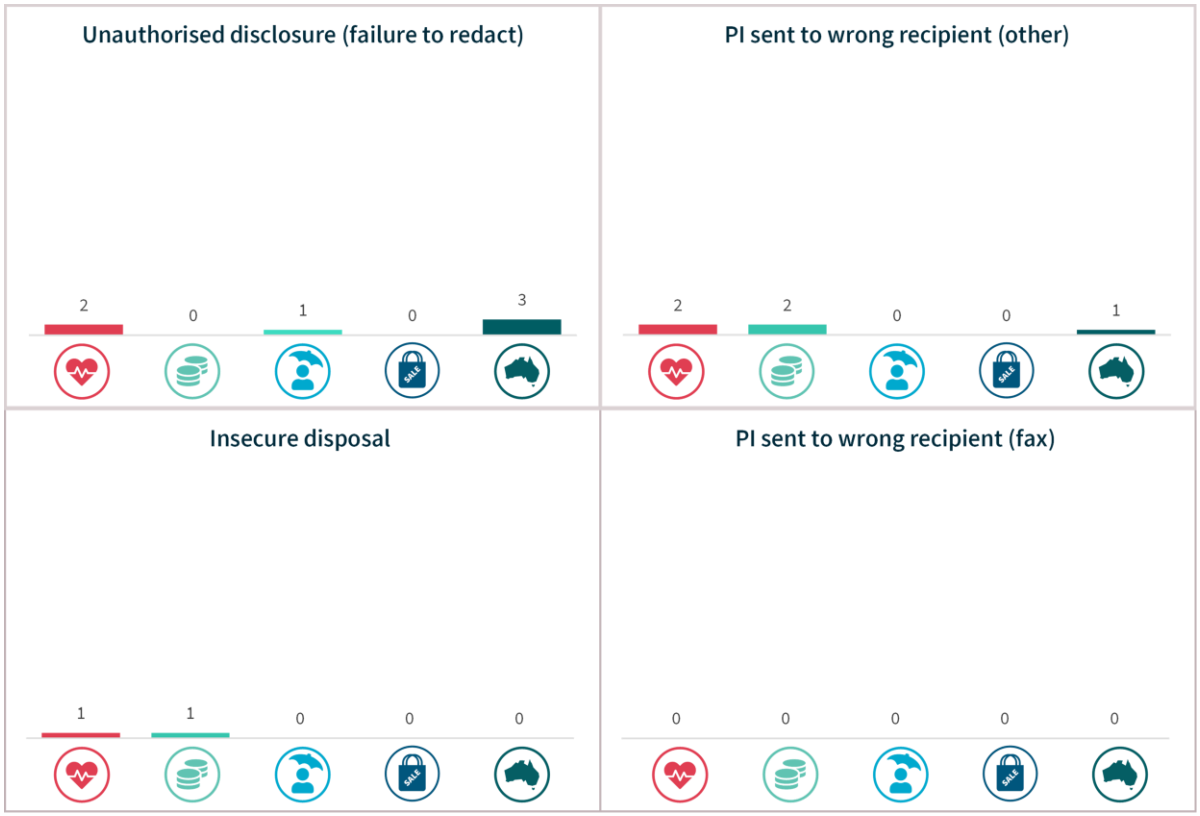
Chart 18: Cyber incident breakdown – Top 5 sectors



Human error breaches – Top 5 sectors

Chart 19: Human error breakdown – Top 5 sectors

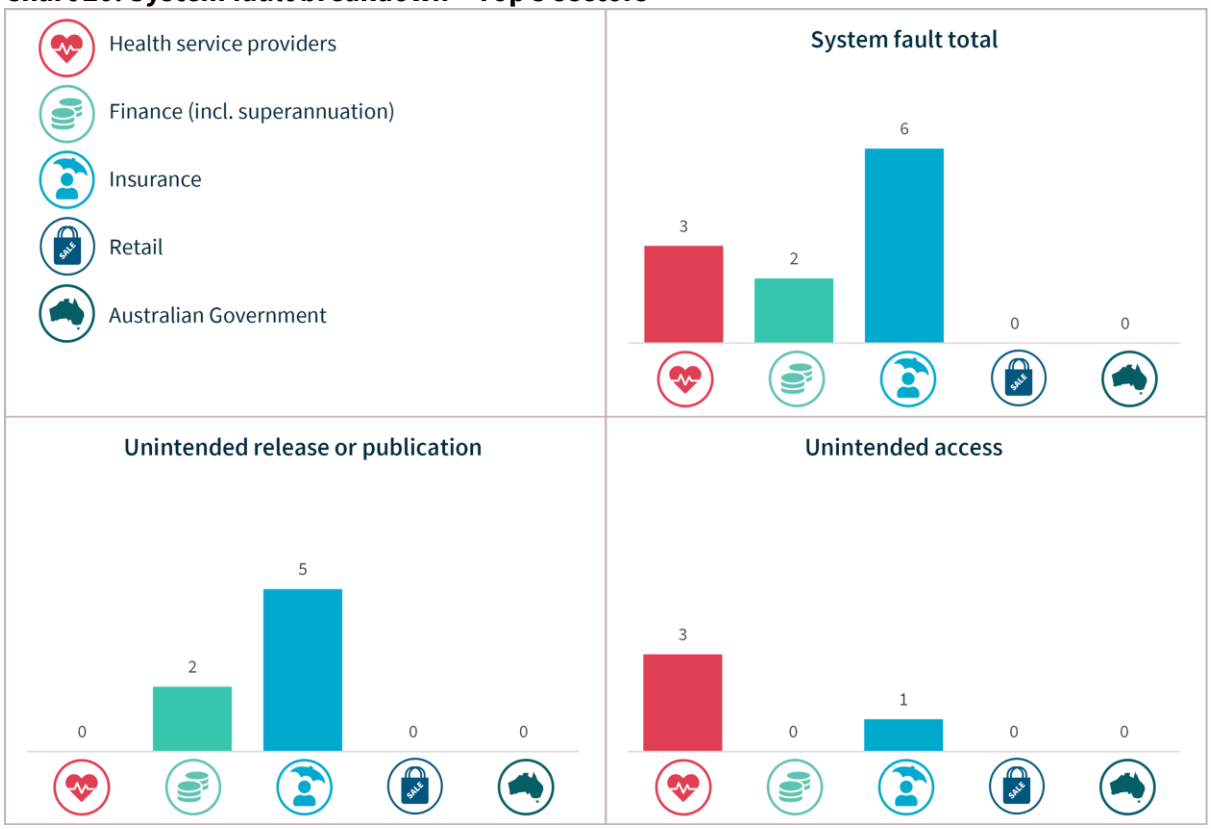



Unauthorised disclosure (failure to redact)
2
0
1
0
3
PI sent to wrong recipient (other)
2
2
0
0
1
Insecure disposal
1
1
0
0
0
PI sent to wrong recipient (fax)
0
0
0
0
0

System fault breaches – Top 5 sectors

Only 3 of the top 5 sectors – health service providers, 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 malicious actor collects and uses compromised credentials, often obtained in other data breaches or from the dark web, to access other systems and accounts without authorisation. A malicious actor may automate logins for many 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