Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Report

January to June 2021

23 August 2021

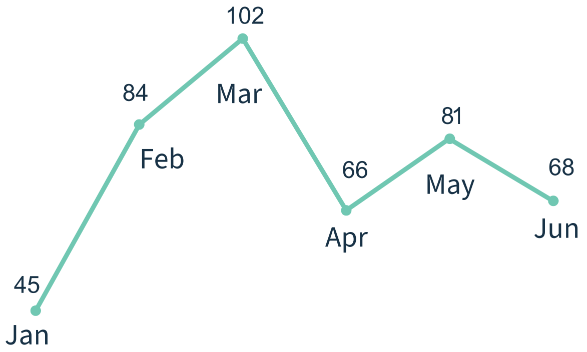
OAIC

Snapshot

446

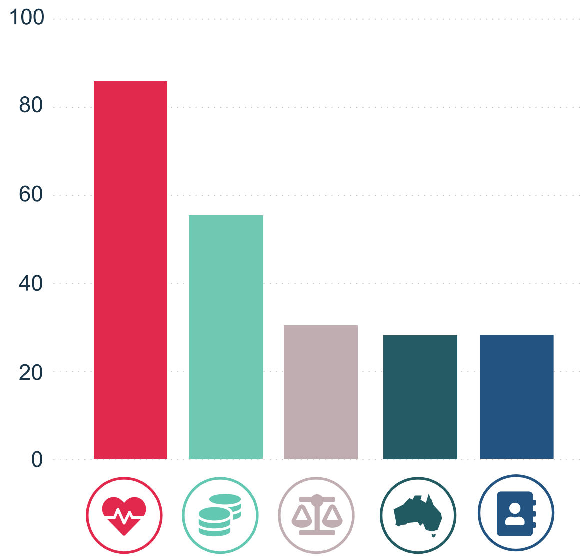
notifications

Down 16%



Top 5 industry sectors to notify data breaches

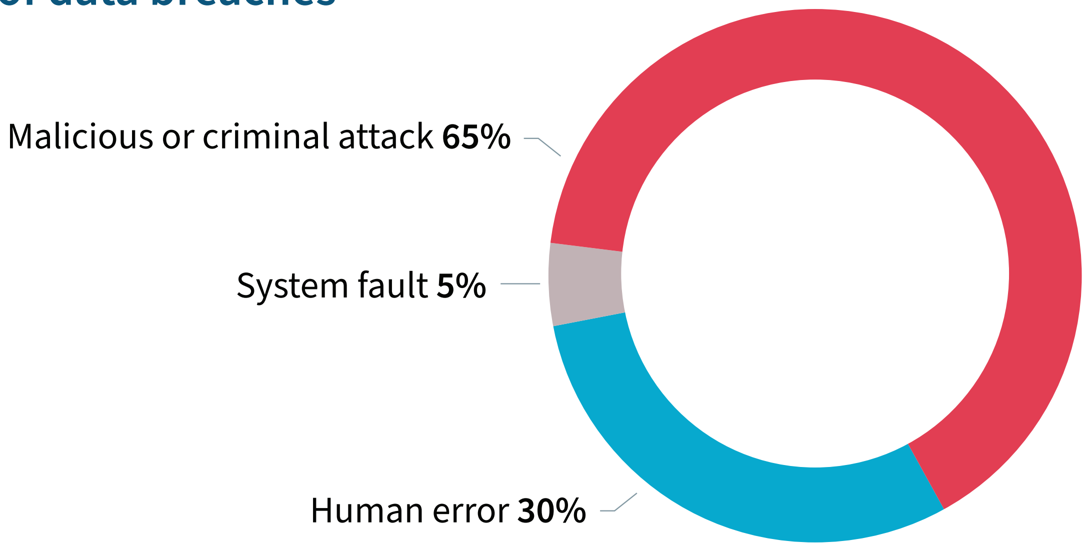
- Health service providers
- Finance (incl. superannuation)
- Legal, accounting & management services
- Australian Government
- Insurance



65%

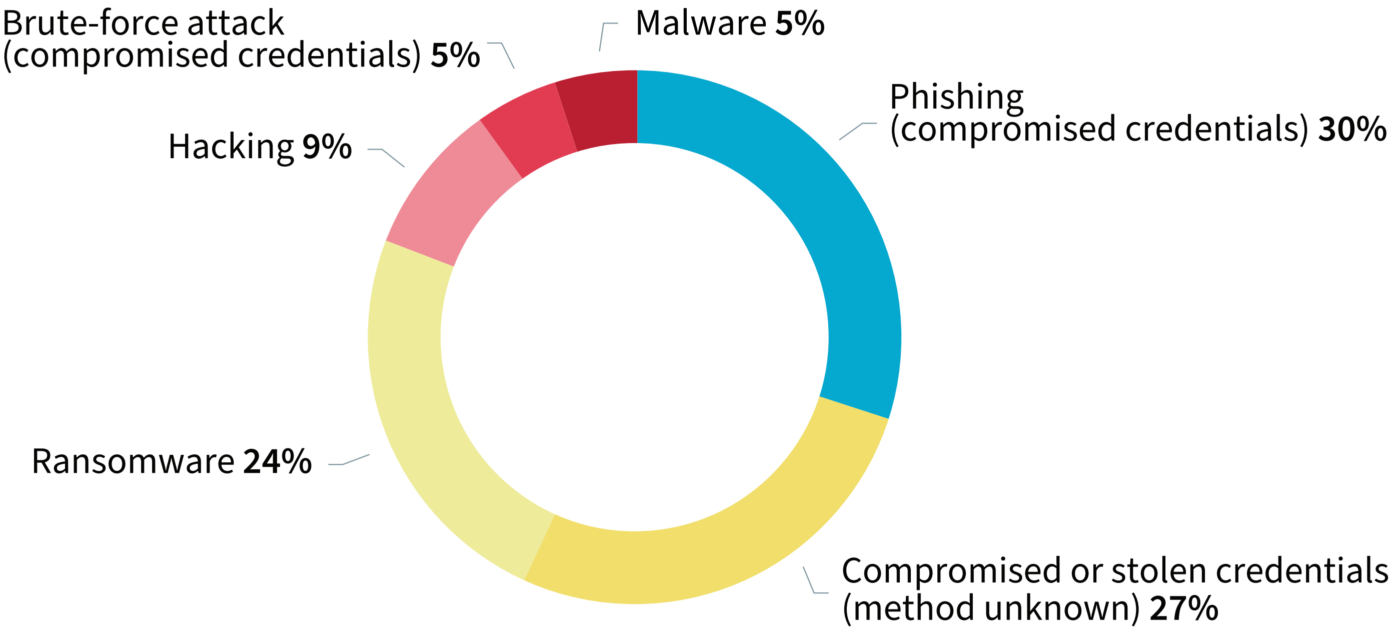
of data breaches affected 100 people or fewer

Sources of data breaches



43% of all data breaches (192 notifications) resulted from cyber security incidents

Cyber incident breakdown



Top causes of human error breaches

Personal information emailed to wrong recipient **40%**

Unintended release or publication **23%**

Failure to use BCC when sending email **8%**

Personal information sent to wrong recipient (other means) **7%**

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 assist entities and the public to understand the operation of the scheme. This report captures notifications made under the NDB scheme for the period from **1 January to 30 June 2021**.

Statistical comparisons are to the previous 6-month period, unless otherwise indicated.

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.

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.

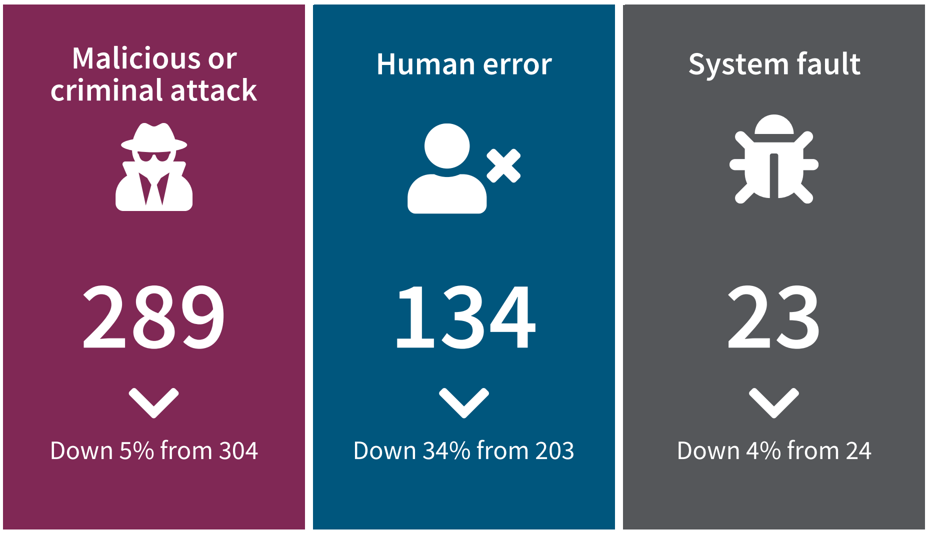
As with previous reports, notifications made under the *My Health Records Act 2012* are not included as they are subject to specific notification requirements set out in that Act.

NDB scheme statistics in this report are current as of 7 July 2021. However, a number of notifications included in these statistics are still under assessment and their status and categorisation are subject to change. This may affect statistics for the period July to December 2021 that are published in future reports. Similarly, there may have been adjustments to statistics provided in previous NDB reports because of changes to the status or categorisation of individual notifications after publication. As a result, statistics from before January 2021 in this report may differ to statistics in earlier published reports.

Executive summary

The NDB scheme was established in February 2018 to improve consumer protection and drive better security standards for protecting personal information. Under the scheme, any organisation or government agency covered by the *Privacy Act 1988* must notify individuals affected and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.

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



Key findings for the January to June 2021 reporting period:

- 446 breaches were notified under the scheme, a decrease of 16% compared to 530 notifications from July to December 2020.
- Malicious or criminal attacks remain the leading source of data breaches, accounting for 289 notifications (65% of the total), down 5% in number from 304.
- Data breaches resulting from human error accounted for 134 notifications (30% of the total), down 34% in number from 203.
- The health sector remains the highest reporting industry sector, notifying 19% of all breaches, followed by finance, which notified 13% of all breaches.
- Contact information remains the most common type of personal information involved in data breaches.
- 93% of data breaches affected 5,000 individuals or fewer, while 65% affected 100 people or fewer.
- 72% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach.

Notifications received January to June 2021

The OAIC received 446 notifications this reporting period. This is a 16% decrease compared to the previous 6 months and an 11% decrease compared to January to June 2020.

There was significant variation in the number of notifications received each month of the reporting period. The OAIC received 45 notifications in January – the lowest monthly total since the NDB scheme commenced – and 102 notifications in March – the fourth highest monthly total.

Table 1 – Notifications received under the NDB scheme

Reporting period	Total no. of notifications
January to June 2021	446
July to December 2020	530
2020–21 financial year	976

Chart 1 — Data breach notifications under the NDB scheme

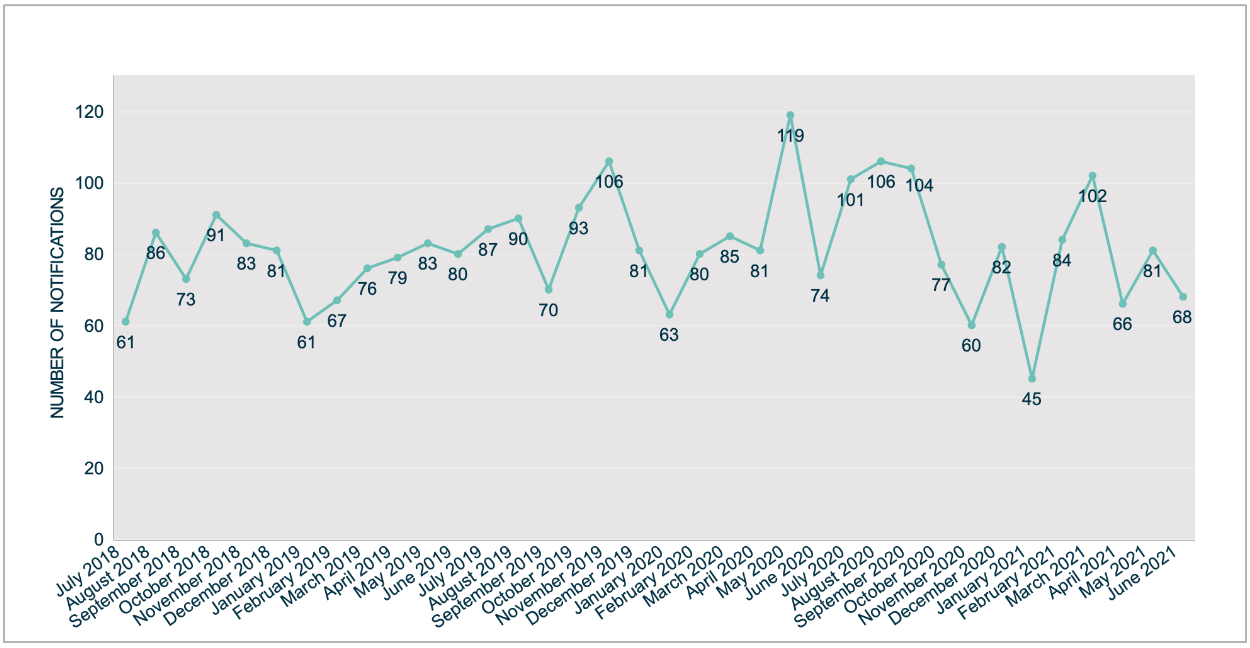
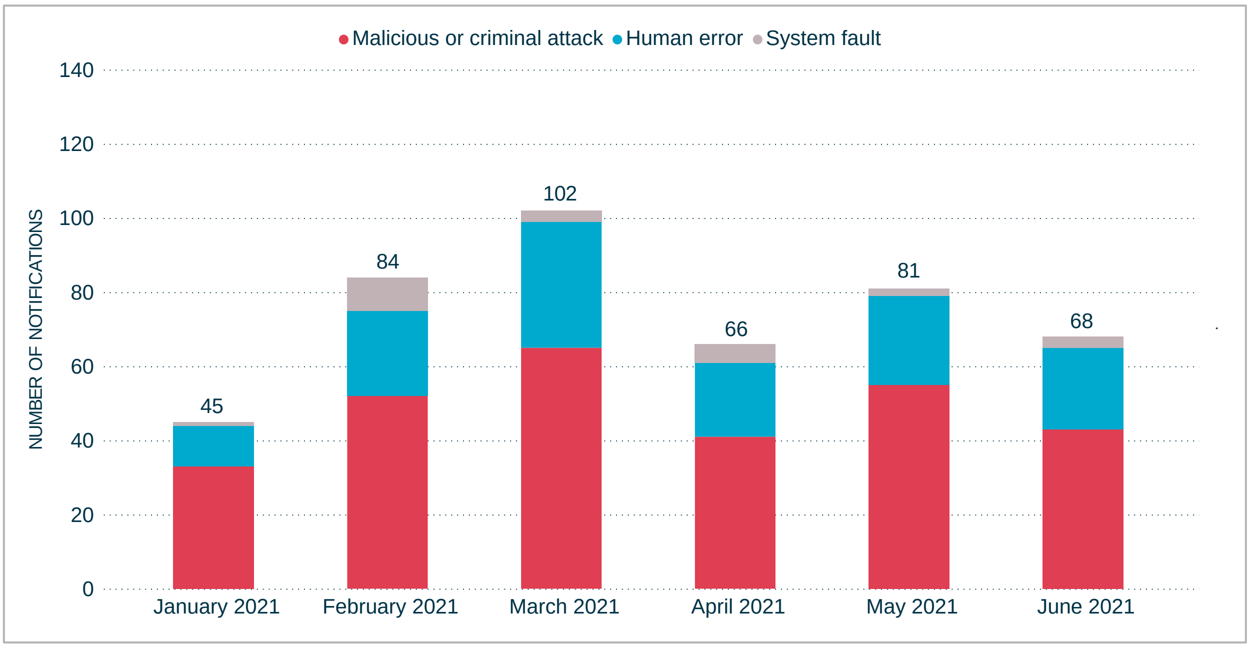


Chart 2 – Number of breaches reported under the NDB scheme – All sectors



Top industry sectors to notify breaches

Health service providers and the finance industry have consistently reported the most data breaches compared to other industry sectors since the NDB scheme began.

Health service providers reported 85 data breaches, or 19% of the total. The second largest source of notifications was the finance sector (13%).

Table 2 – Top 5 industry sectors by notifications

Industry sector	Total no. of notifications
Health service providers[1]	85
Finance (including superannuation)[2]	57
Legal, accounting & management services	35
Australian Government[3]	34
Insurance	34

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

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

[3] The Privacy Act covers most Australian Government agencies. It does not cover a number of intelligence and national security agencies. It also does not cover state, territory and local government agencies, public hospitals and public schools.

Preventing serious harm with remedial action

Under the NDB scheme, a breach is not an eligible data breach if:

- an entity takes action in relation to the loss, unauthorised access to or unauthorised disclosure of personal information before it results in serious harm to an individual, and
- a reasonable person who is properly informed based on the information immediately available would conclude that the action makes it unlikely that serious harm would be suffered by any of the affected individuals.

In these circumstances, a breach is not subject to the notification requirements of the Privacy Act.

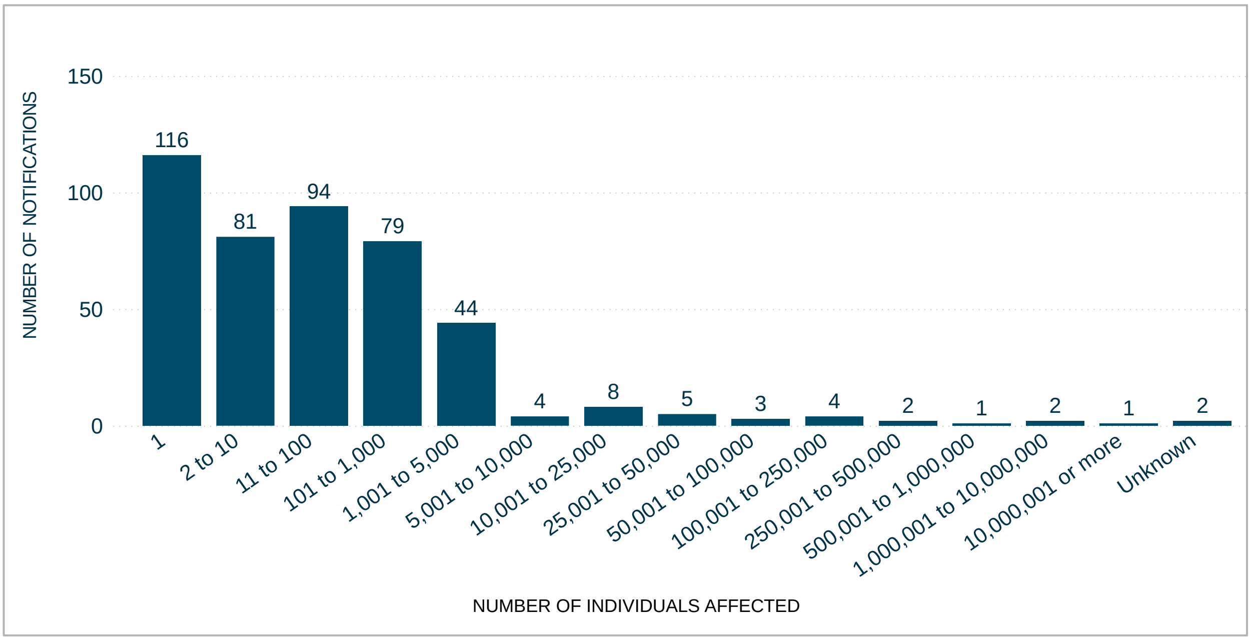
The following case study is an example of a data breach where the steps taken by the entity were insufficient to prevent the likelihood of serious harm.

> A staff member from an entity inadvertently sent a spreadsheet containing personal information to individuals in its database. The spreadsheet contained a range personal information including names, addresses, dates of birth, health and other sensitive information, belonging to hundreds of individuals.
>
> The entity advised the OAIC it did not consider this to be an eligible data breach because:
>
> - it had contacted each recipient within a few minutes of sending the email advising that it had been sent in error
> - it had requested that the email be deleted
> - most recipients advised they had deleted and not shared the email.
>
> While the entity moved quickly to respond to the breach, the actions taken in these circumstances did not remove the likelihood of serious harm. The risk of harm to individuals was increased because the breach disclosed a range of personal information, including sensitive information. The entity was also unable to confirm that all recipients deleted the email and it had not been accessed or shared.
>
> The OAIC closed the matter after the entity notified individuals of the data breach as required by the NDB scheme.

Number of individuals affected by breaches – All sectors

Consistent with previous NDB statistics reports, most data breaches (93%) involved the personal information of 5,000 individuals or fewer. Breaches affecting 100 individuals or fewer comprised 65% of notifications and breaches affecting between 1 and 10 individuals accounted for 44% of notifications.

Chart 3 – Number of individuals affected by breaches – All sectors



Note: 'Unknown' includes notifications by entities with ongoing investigations at the time of this report.
These figures reflect the number of individuals worldwide whose personal information was compromised in these data breaches, as estimated by the notifying entities.

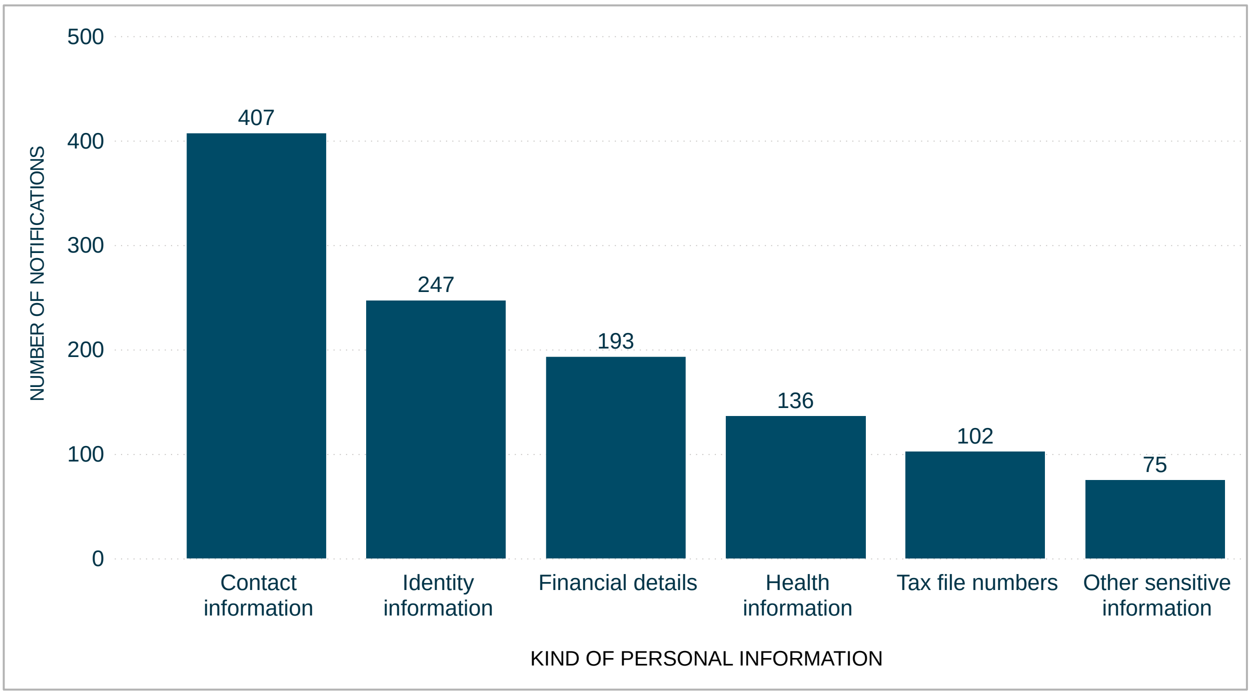
Kinds of personal information involved in breaches – All sectors

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

Most data breaches (91%) notified under the NDB scheme involved 'contact information', such as an individual's name, home address, phone number or email address.

This is distinct from 'identity information', which was exposed in 55% of data breaches and includes an individual's date of birth, passport details and driver licence details. Financial details, such as bank account and credit card numbers, were involved in 43% of breaches.

Chart 4 – Kinds of personal information involved in breaches – All sectors



Note: Eligible data breaches may involve more than one kind of personal information.

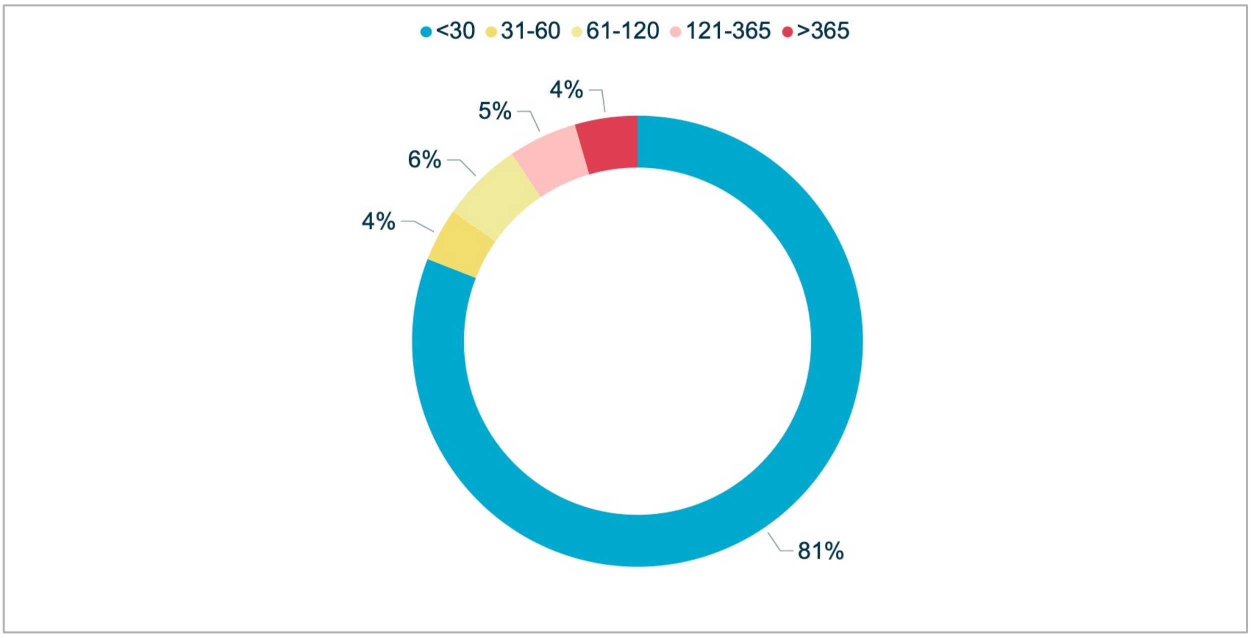
Time taken to identify breaches – All sectors

As part of complying with Australian Privacy Principle 11, entities must take reasonable steps to ensure that data breaches can be detected in a timely manner.

The figures in this section relate to the time between an incident occurring and the entity becoming aware of it. They do not relate to the time taken by the entity to assess whether an incident qualified as an eligible data breach.[4]

In the reporting period, 81% of breaches were identified by the entity within 30 days of it occurring, up from 75%.

Chart 5 – Days taken to identify breaches – All sectors

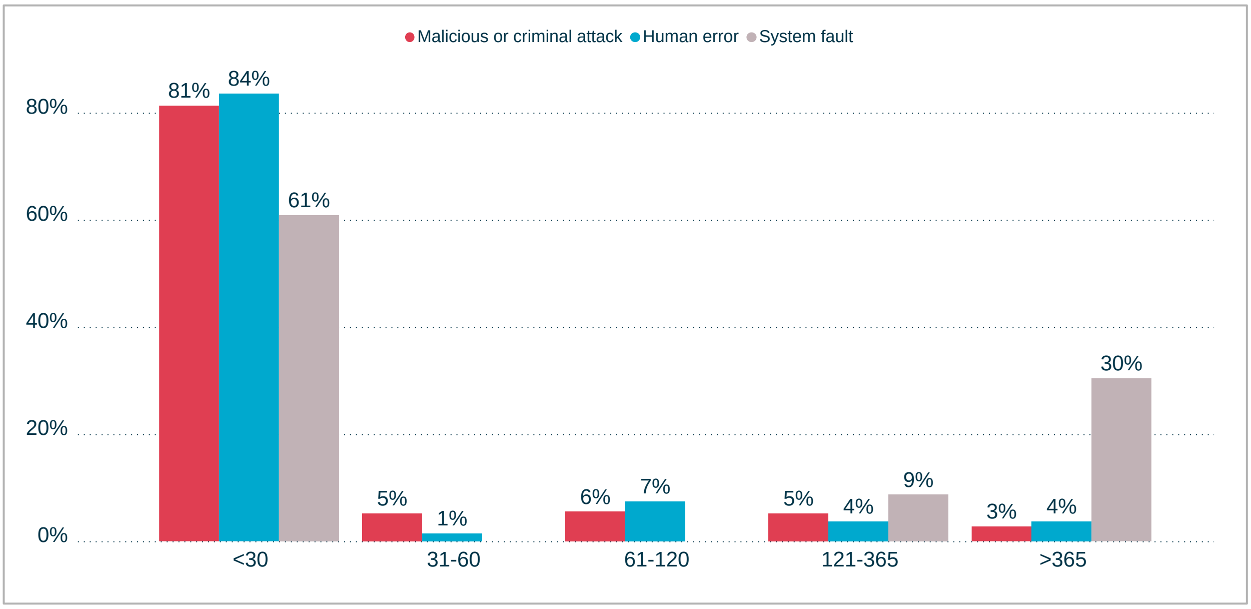


The time it took entities to identify data breaches varied significantly depending on the source of the breach.

For data breaches caused by malicious or criminal attack or human error, more than 80% of entities identified the incident within 30 days of it occurring. Where entities experienced a data breach resulting from a system fault, only 61% identified the incident within 30 days, and 30% did not become aware of the incident for over a year.

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

Chart 6 – Days taken to identify breaches by source of breach – All sectors



Time taken to notify the OAIC of breaches – All sectors

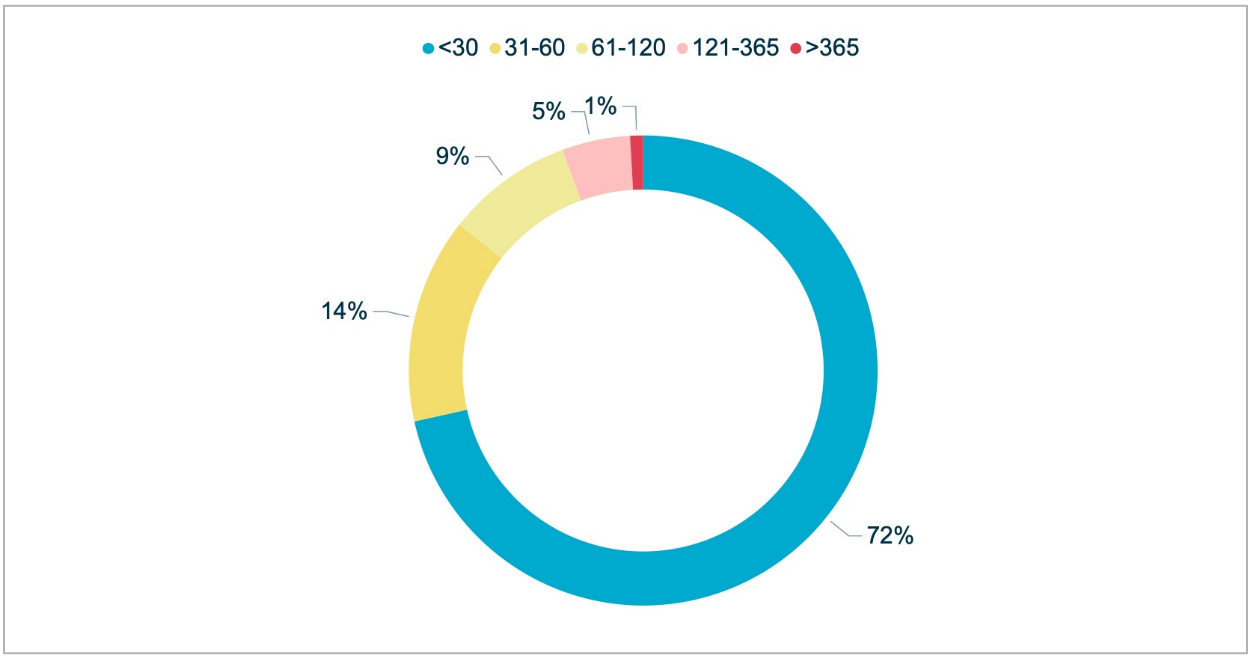
A key objective of the NDB scheme is to ensure that an entity that experiences a data breach provides timely notification to individuals at risk of serious harm from the breach. Delays in assessment and notification reduce the opportunity for an individual to take steps to prevent harm.

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

In the reporting period, 72% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach, compared to 78% in the previous period. Twenty-seven entities took longer than 120 days from when they became aware of an incident to notify the OAIC.

In a number of instances, individuals were notified at the same time as or shortly after the OAIC. However, in others, there was a delay between when the entity notified the OAIC and when they notified individuals.

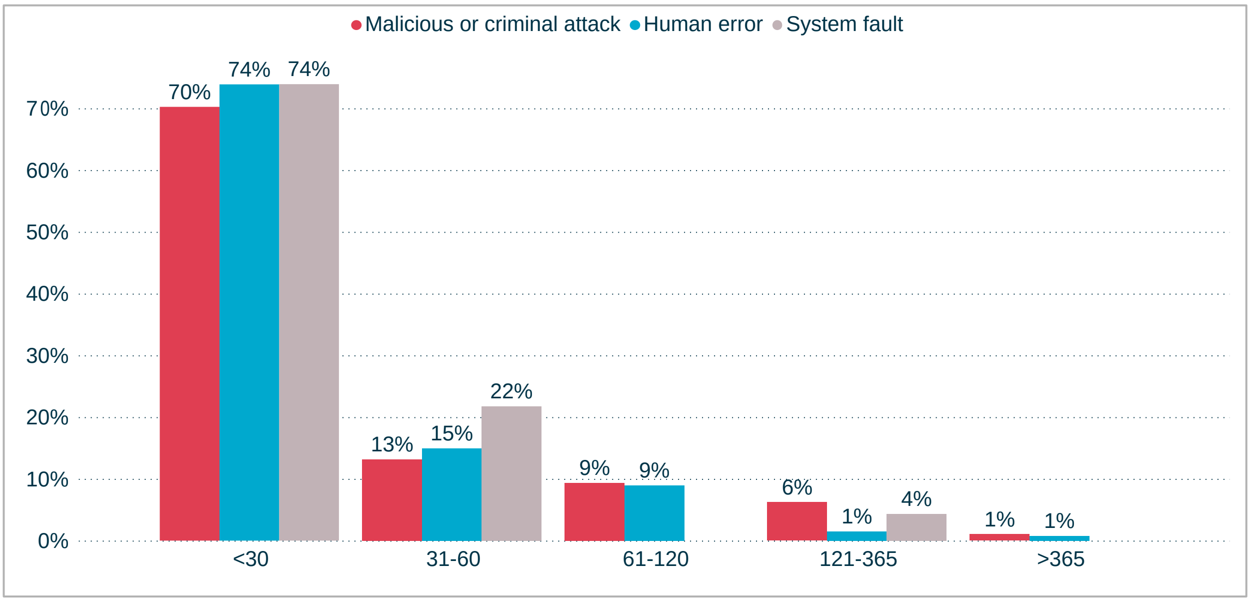
Chart 7 – Days taken to notify the OAIC of breaches – All sectors



Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

The source of the breach did not significantly influence the time it took entities to notify the OAIC after the incident was identified.

Chart 8 – Days taken to notify the OAIC of breaches by source of breach – All sectors



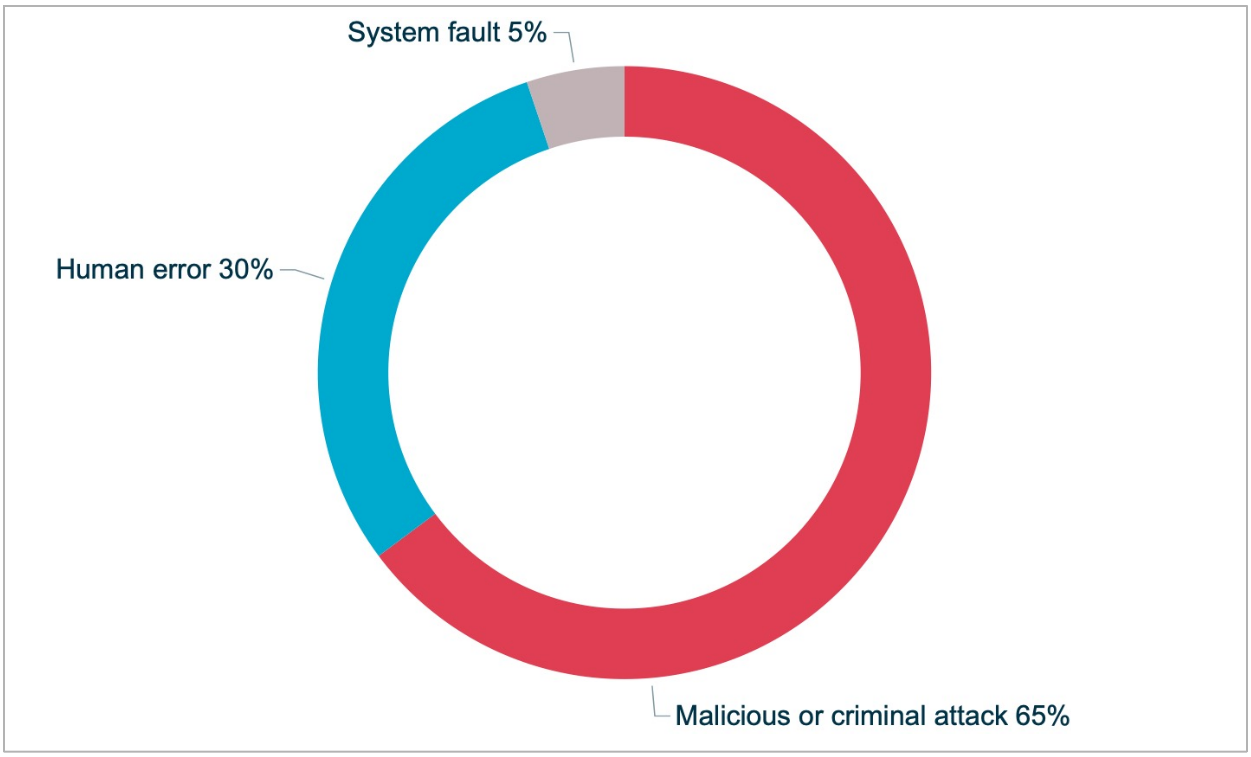
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

Source of breaches – All sectors

Malicious or criminal attacks were the largest source of data breaches notified to the OAIC, accounting for 289 breaches.

Human error remained a major source of breaches, accounting for 134 notifications. This was a notable decrease from the 203 notifications attributed to human error in the previous period. System faults accounted for the remaining 23 breaches, compared to 24 notifications in the previous period.

Chart 9 – Source of data breaches – All sectors



Malicious or criminal attack breaches – All sectors

Malicious or criminal attacks remain the leading source of data breaches, accounting for 65% of notifications. The number of these breaches has decreased by 5% from 304 notifications in the last reporting period to 289, while the proportion of total breaches caused by malicious or criminal attack has increased from 57% to 65%.

The majority of breaches (66%) in the malicious or criminal attack category involved cyber incidents. The OAIC was notified of 192 data breaches resulting from cyber incidents – 43% of all notifications.

The remaining 34% of breaches caused by malicious or criminal attack resulted from social engineering or impersonation (35 notifications), actions taken by a rogue employee or insider threat (28 notifications) and theft of paperwork or storage devices (34 notifications).

Chart 10 – Malicious or criminal attacks – All sectors

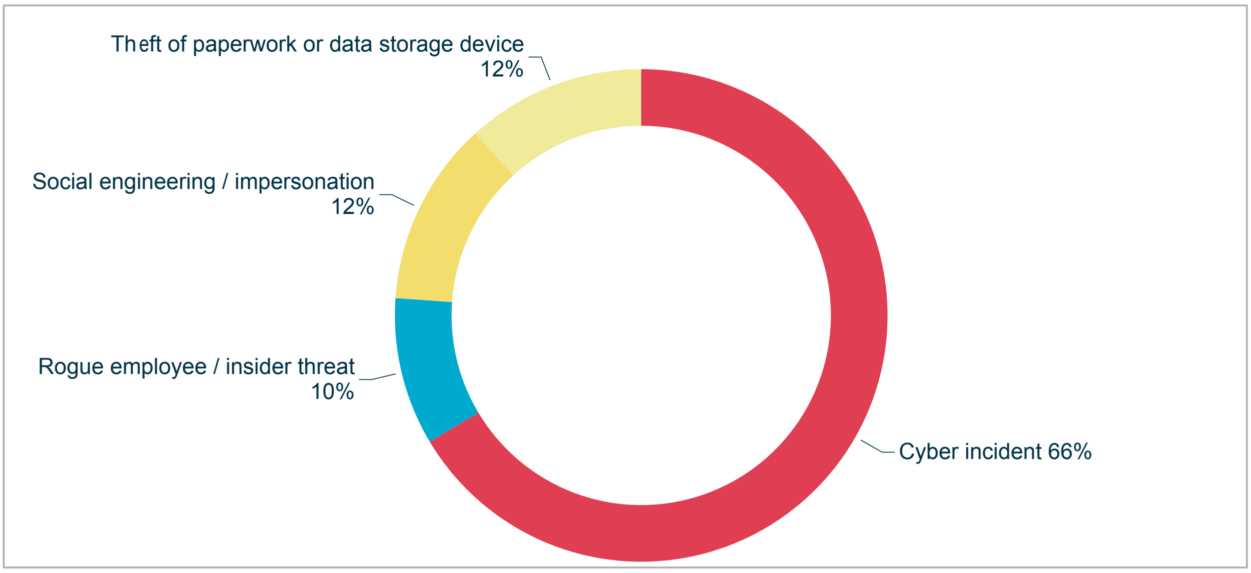
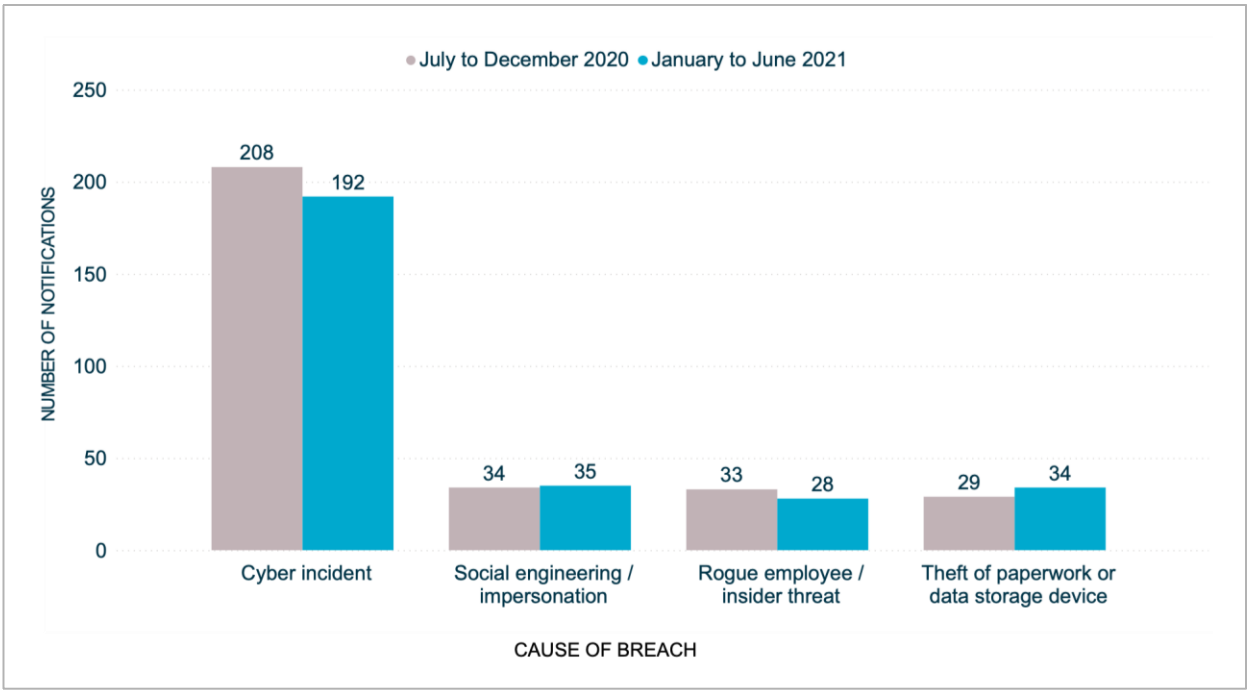


Chart 11 – Breaches resulting from malicious or criminal attacks – All sectors



Impersonation fraud and the NDB scheme

During the reporting period, there were a number of data breaches resulting from impersonation fraud. Impersonation fraud involves a malicious actor impersonating another individual to gain access to an account, system, network or physical location.

Entities should have controls and identity verification processes in place to minimise the risk of impersonation fraud. However, the growth of data on the dark web has meant that malicious actors increasingly hold sufficient personal information to circumvent these controls and processes and successfully impersonate an account holder.

The OAIC has been advised of data breaches resulting from a malicious actor calling a service provider's customer helpline or contact centre, impersonating a customer, and passing the organisation's verification processes. The impersonator is then able to login to online accounts, update the customer's personal information, make fraudulent transactions, and potentially obtain additional personal information that enables them to commit further impersonation fraud.

The OAIC generally considers impersonation fraud to be an eligible data breach under the NDB scheme where the personal information the entity holds is accessed by a third party and results in a likely risk of serious harm. This satisfies the test of an unauthorised disclosure, even when the malicious actor already held some of the personal information.

Entities should regularly review their security measures to minimise the risk of impersonation fraud and consider:

- having robust identity verification processes in place and adapting them to emerging impersonation fraud threats
- training staff in identity verification processes as well as how to report and escalate fraud
- implementing multifactor authentication
- automatically notifying customers when changes are made to their account or there are failed authentication attempts.

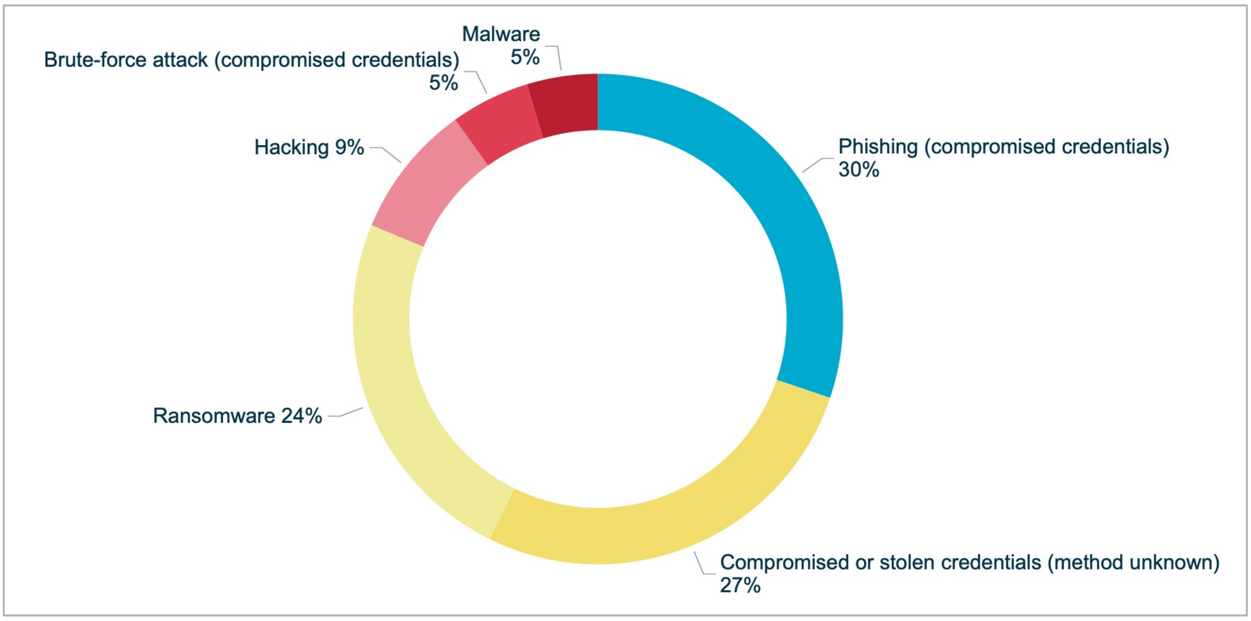
Cyber incident breaches – All sectors

The top sources of cyber incidents during the reporting period were phishing, compromised or stolen credentials (method unknown), and ransomware.

More than half of cyber incidents (62%) during the reporting period involved malicious actors gaining access to accounts using compromised or stolen credentials. In line with the previous reporting period, the most common method used by malicious actors to obtain compromised credentials was email-based phishing (58 notifications).

Ransomware incidents increased by 24%, up from 37 in the last reporting period to 46.

Chart 12 – Cyber incident breakdown – All sectors



Assessing suspected data breaches involving ransomware

During this reporting period, a number of entities assessed that a ransomware attack did not constitute an eligible data breach due to a 'lack of evidence' that access to or exfiltration of data had occurred.

An assessment of a suspected data breach under section 26WH of the Privacy Act is required if there are reasonable grounds to suspect that there *may have been* an eligible data breach, even if there are insufficient reasonable grounds to believe that an eligible data breach *has occurred*.

It is insufficient for an entity to rely on the absence of evidence of access to or exfiltration of data to conclusively determine that an eligible data breach has not occurred. Where an entity cannot confirm whether a malicious actor has accessed, viewed or exfiltrated data stored within the compromised network, there will generally be reasonable grounds to believe that an eligible data breach may have occurred and an assessment under section 26WH will be required.

Given the prevalence of ransomware attacks, the OAIC expects entities to have appropriate internal practices, procedures, and systems in place to undertake a meaningful assessment under section 26WH. As best practice, entities should:

- have appropriate audit and access logs
- use a backup system that is routinely tested for data integrity
- have an appropriate incident response plan
- consider engaging a cyber security expert at an early stage to conduct a forensic analysis if a ransomware attack occurs.

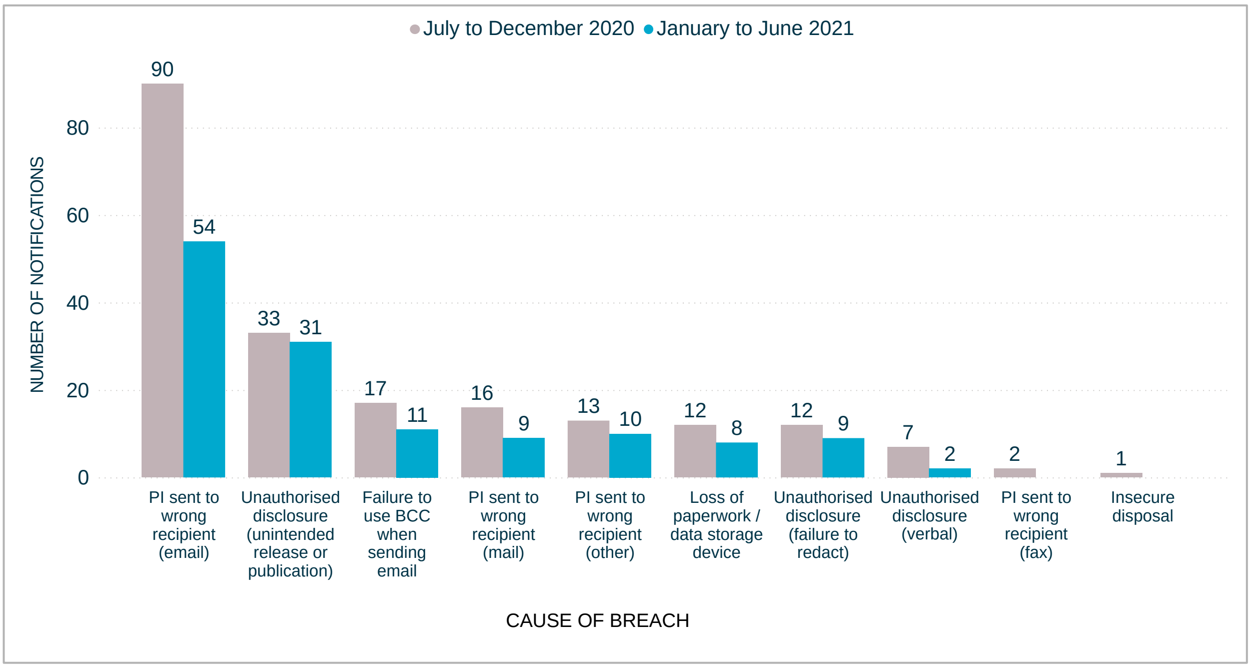
Protective measures can prevent ransomware from occurring in the first place. The Australian Cyber Security Centre has advice on how to protect your organisation against ransomware attacks.

Human error breaches – All sectors

The second largest source of data breaches between January and June 2021 was human error. The number of breaches attributed to human error decreased overall – down 34% from 203 notifications in the last reporting period to 134 – and proportionally – down from 38% to 30% of all notifications.

Common examples of human error breaches include sending personal information to the wrong recipient via email (40% of human error breaches), unintended release or publication of personal information (23%), and failure to use the 'blind carbon copy' function when sending group emails (8%). This is consistent with the top 3 human error categories in the last reporting period.

Chart 13 – Human error breakdown – All sectors



Certain human error breaches affect larger numbers of individuals. This reporting period, unauthorised disclosure (unintended release or publication) affected an average 523,998 people per breach. This is significantly higher than previous reports due to a data breach that affected an estimated 15.7 million individuals globally, including 186,000 Australians.

Table 3 – Human error breakdown by average number of affected individuals – All sectors

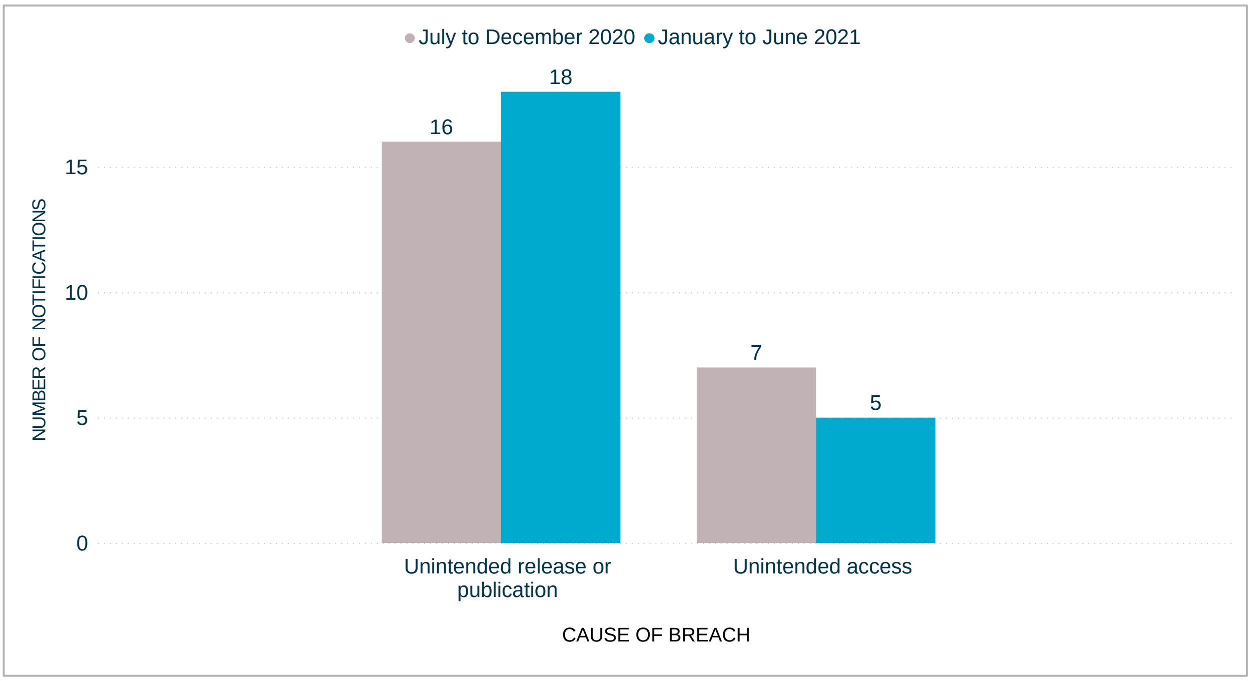
Source of breach	No. of notifications received	Average no. of affected individuals
PI sent to wrong recipient (email)	54	91
Unauthorised disclosure (unintended release or publication)	31	523,998
Failure to use BCC when sending email	11	103
PI sent to wrong recipient (other)	10	2
PI sent to wrong recipient (mail)	9	18
Unauthorised disclosure (failure to redact)	9	2
Loss of paperwork/data storage device	8	14
Unauthorised disclosure (verbal)	2	1

System fault breaches – All sectors

System fault breaches include incidents that occur due to a business or technology process error and accounted for 5% of notifications. The proportion of breaches attributed to system faults has been consistent since the NDB scheme began.

Unintended release or publication of personal information due to a system fault caused 18 data breaches, while unintended access to personal information because of a system fault caused 5 breaches.

Chart 14 – System fault breakdown – All sectors



Comparison of top 5 industry sectors

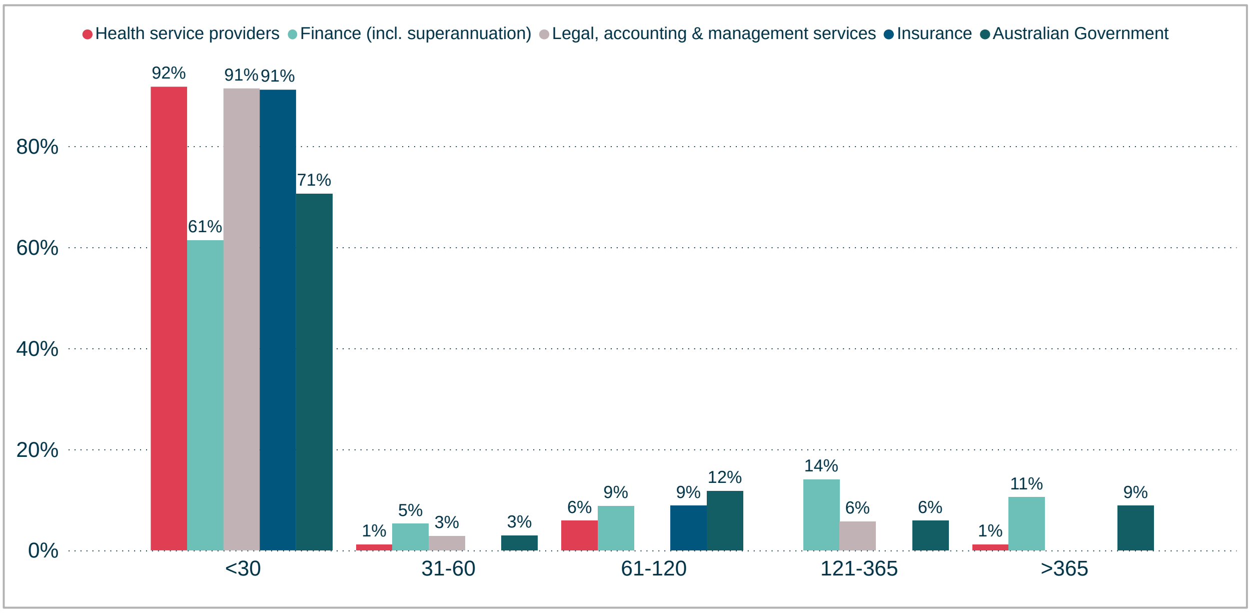
This section compares notifications made under the NDB scheme by the 5 industry sectors that made the most notifications in the reporting period. These sectors accounted for 55% of all notifications.

Time taken to identify breaches – Top 5 industry sectors

Consistent with the last report, the time taken by entities to identify incidents that were subsequently assessed to be eligible data breaches varied by industry sector.

In the reporting period, 92% of health service providers and 91% of entities in the legal, accounting and management services and insurance sectors identified the incident within 30 days of it occurring. This figure was 71% for Australian Government agencies and 61% for the finance sector.

Chart 15 – Days taken to identify breaches – Top 5 industry sectors



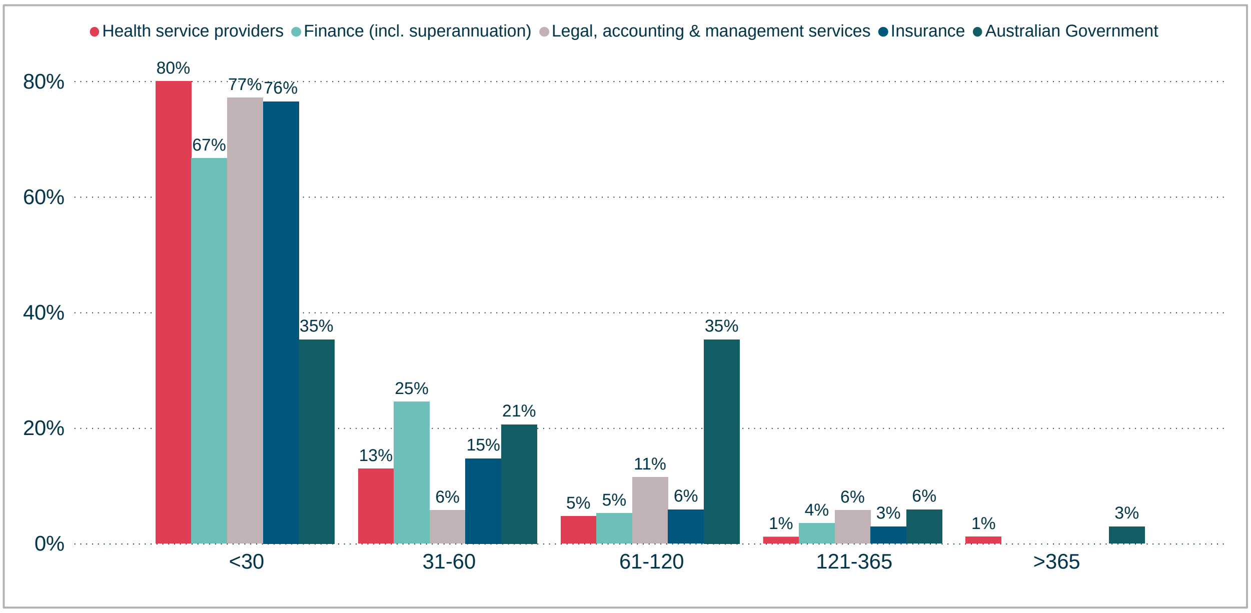
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

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

The time taken by entities to notify the OAIC of a data breach also varied by industry sector.

Over 75% of notifications from health service providers, the insurance sector, and legal, accounting and management services were made within 30 days of the entity becoming aware of the incident. This figure was 67% for the finance sector and 35% for Australian Government agencies.

Chart 16 – Days taken to notify the OAIC of data breaches – Top 5 industry sectors



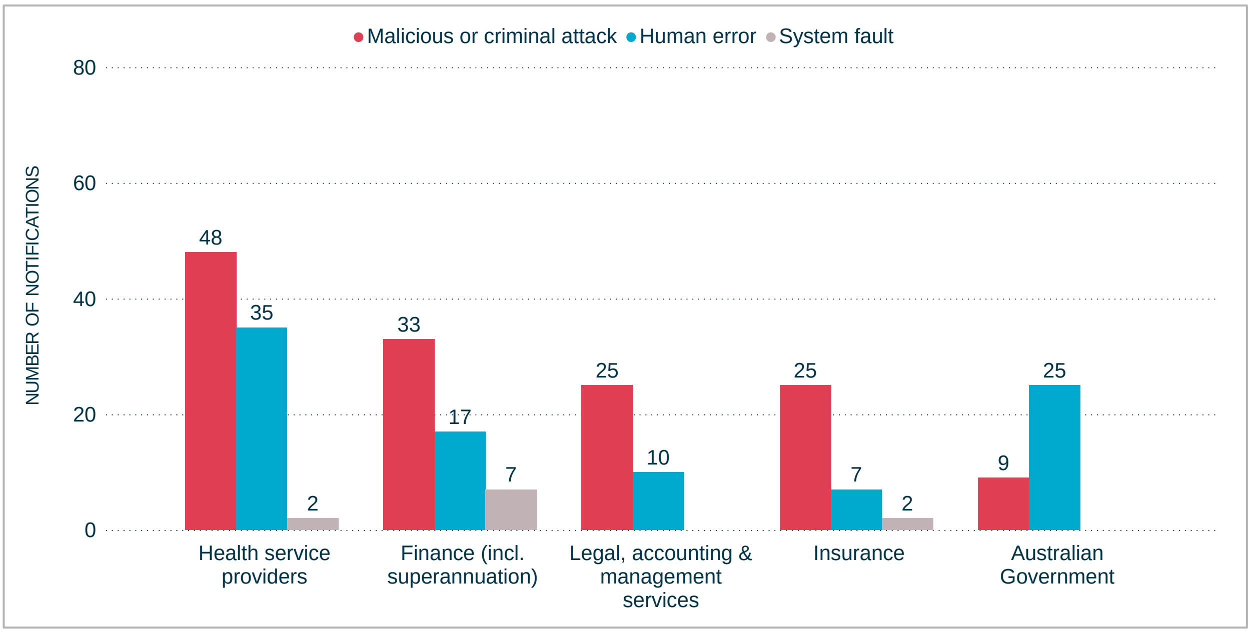
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

Source of breaches – Top 5 industry sectors

Malicious or criminal attacks were the leading source of data breaches for all top 5 industry sectors except the Australian Government. This category accounted for 56% of data breaches notified by health service providers, marking a significant shift from previous reports where human error was consistently the main cause of data breaches in this sector.

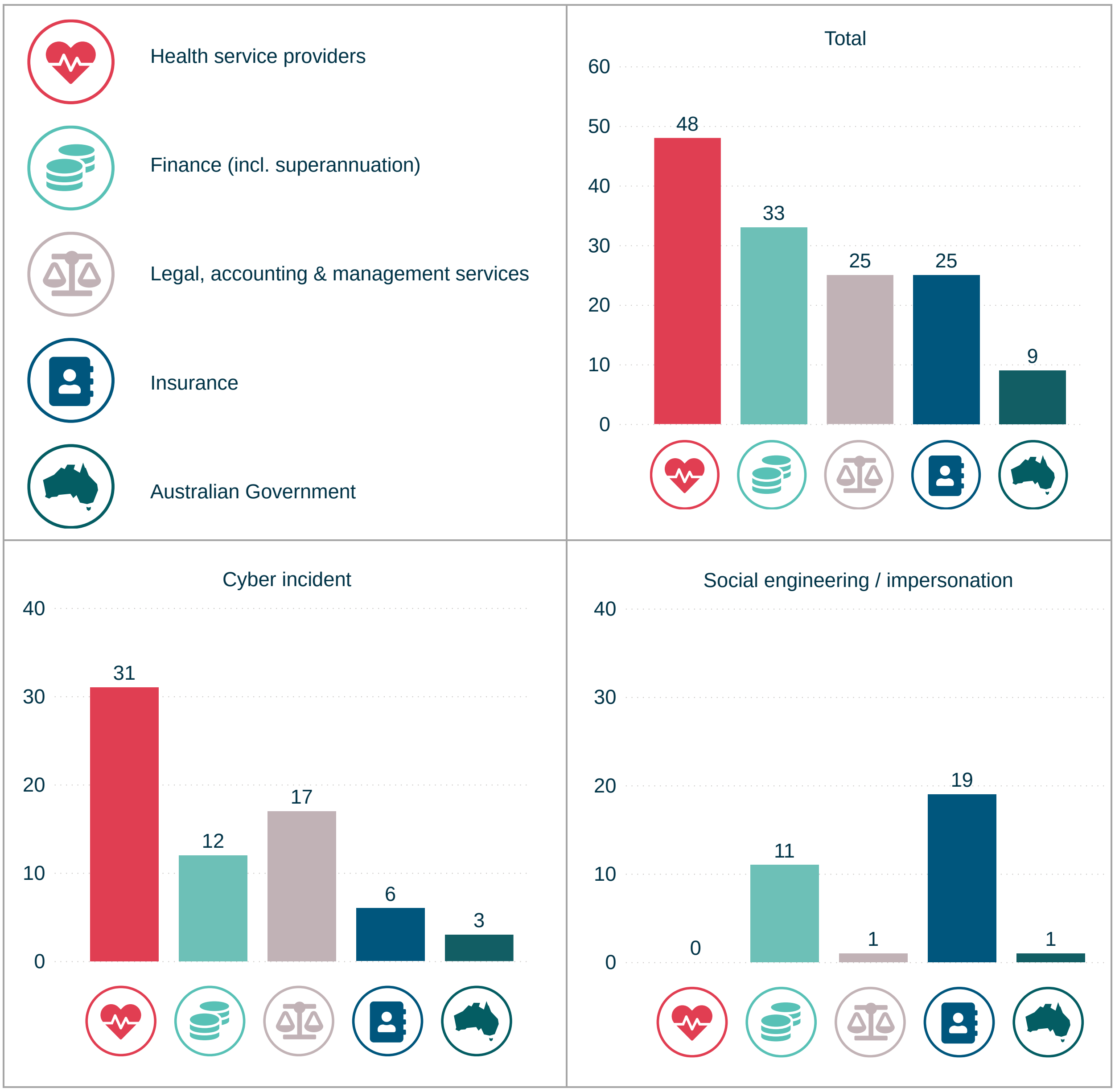
In comparison, human error was the cause of 74% of data breaches notified by the Australian Government.

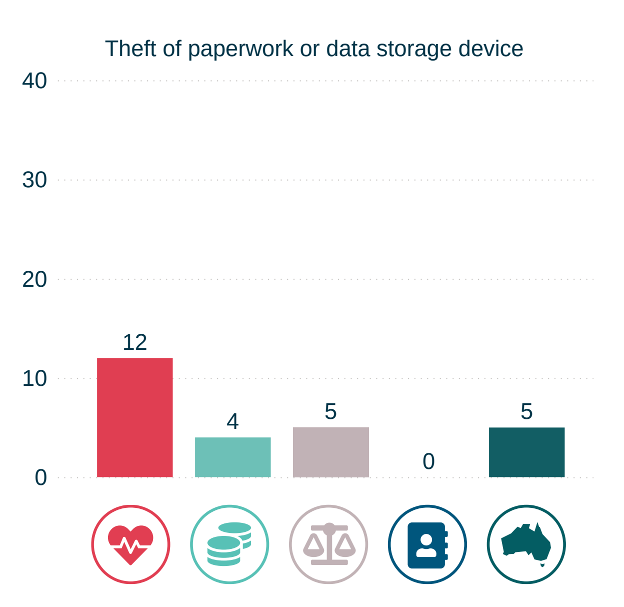
Chart 17 – Source of data breaches – Top 5 industry sectors

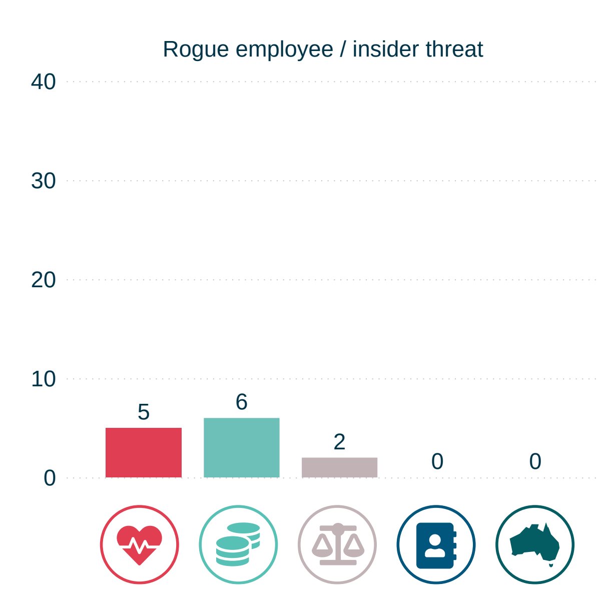


Malicious or criminal attack breaches – Top 5 industry sectors

Chart 18 – Malicious or criminal attacks breakdown – Top 5 industry sectors

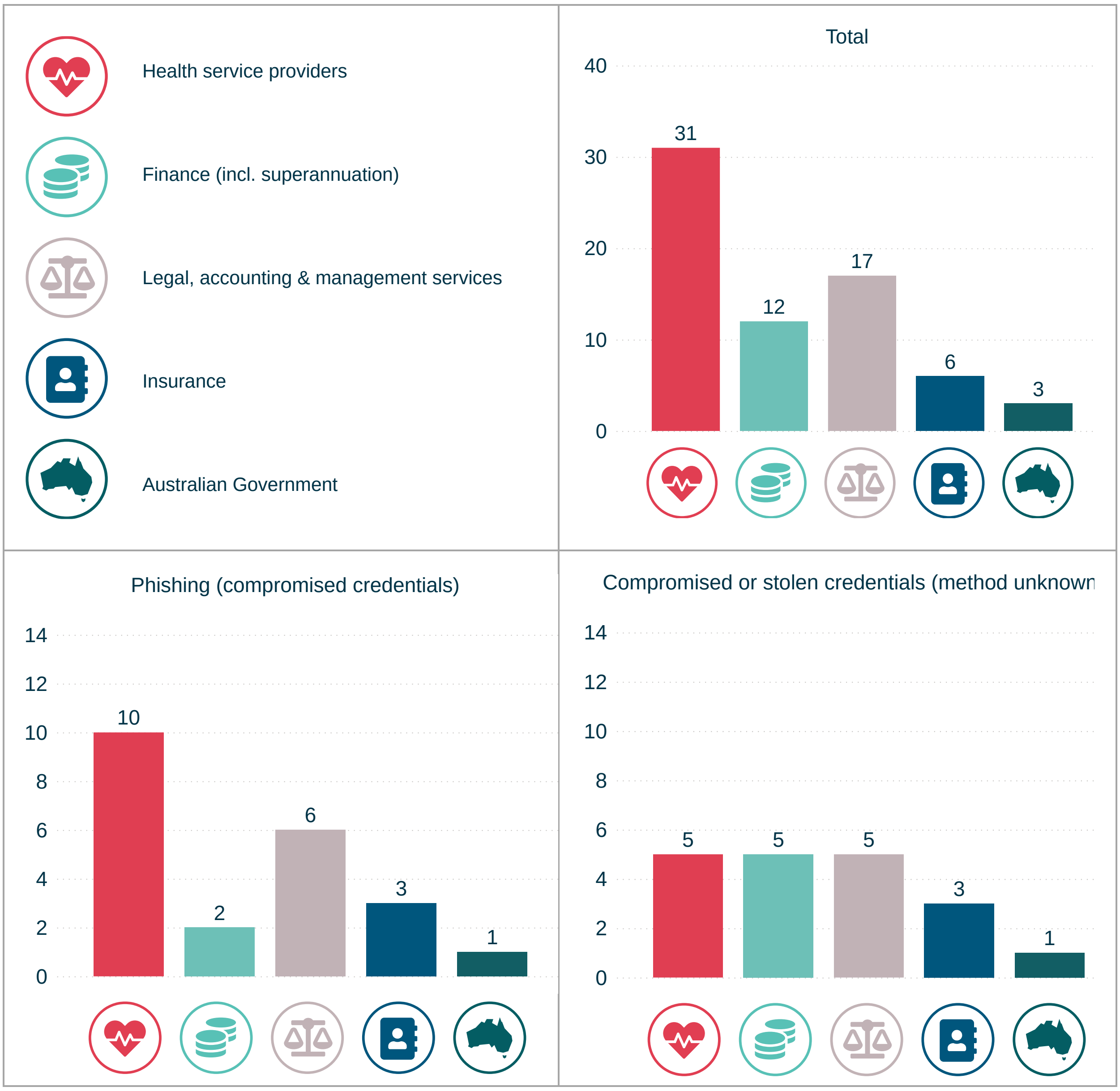



Theft of paperwork or data storage device
40
30
20
10
0
12
4
5
0
5

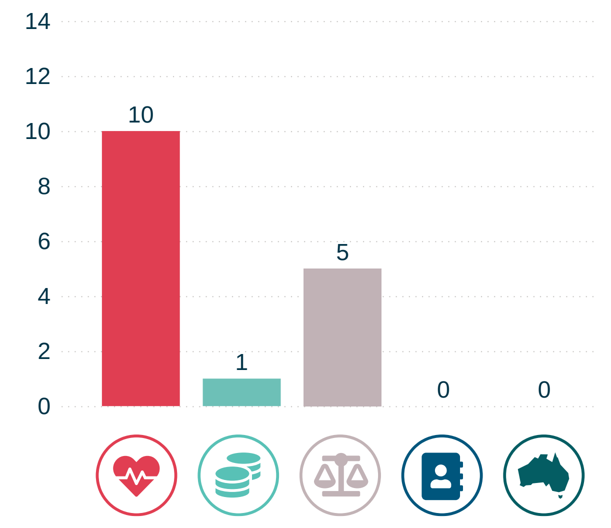

Rogue employee / insider threat
40
30
20
10
0
5
6
2
0
0

Cyber incident breaches – Top 5 industry sectors

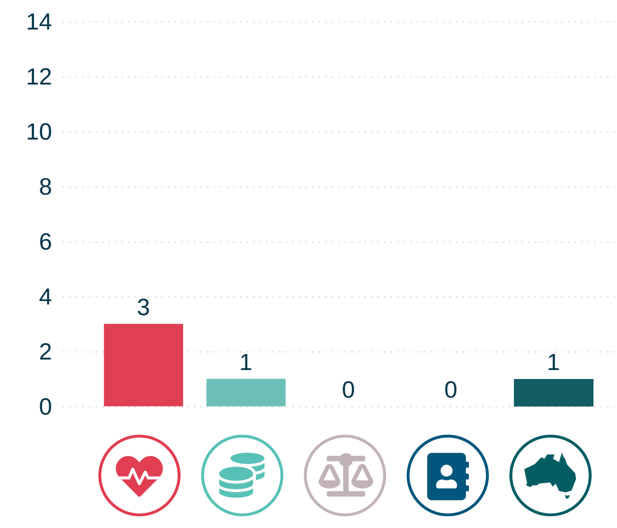
Chart 19 – Cyber incident breakdown – Top 5 industry sectors



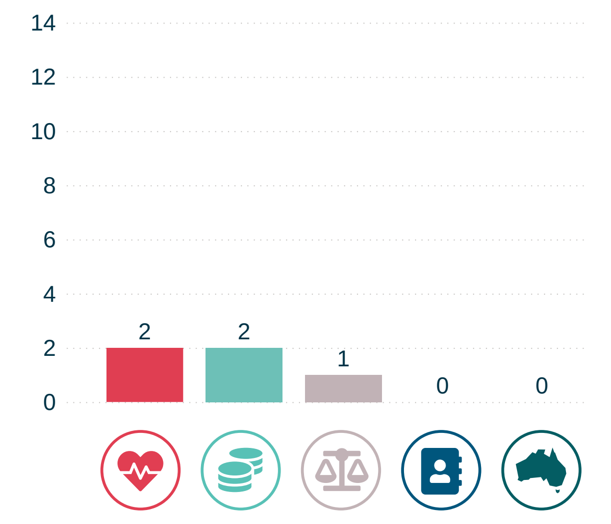
Ransomware



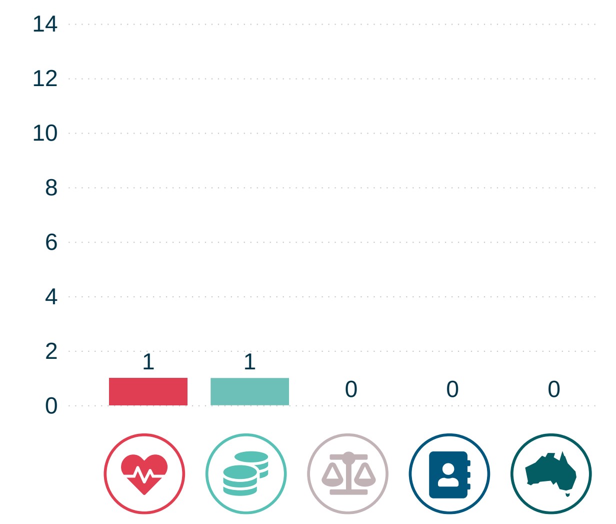
Hacking



Malware

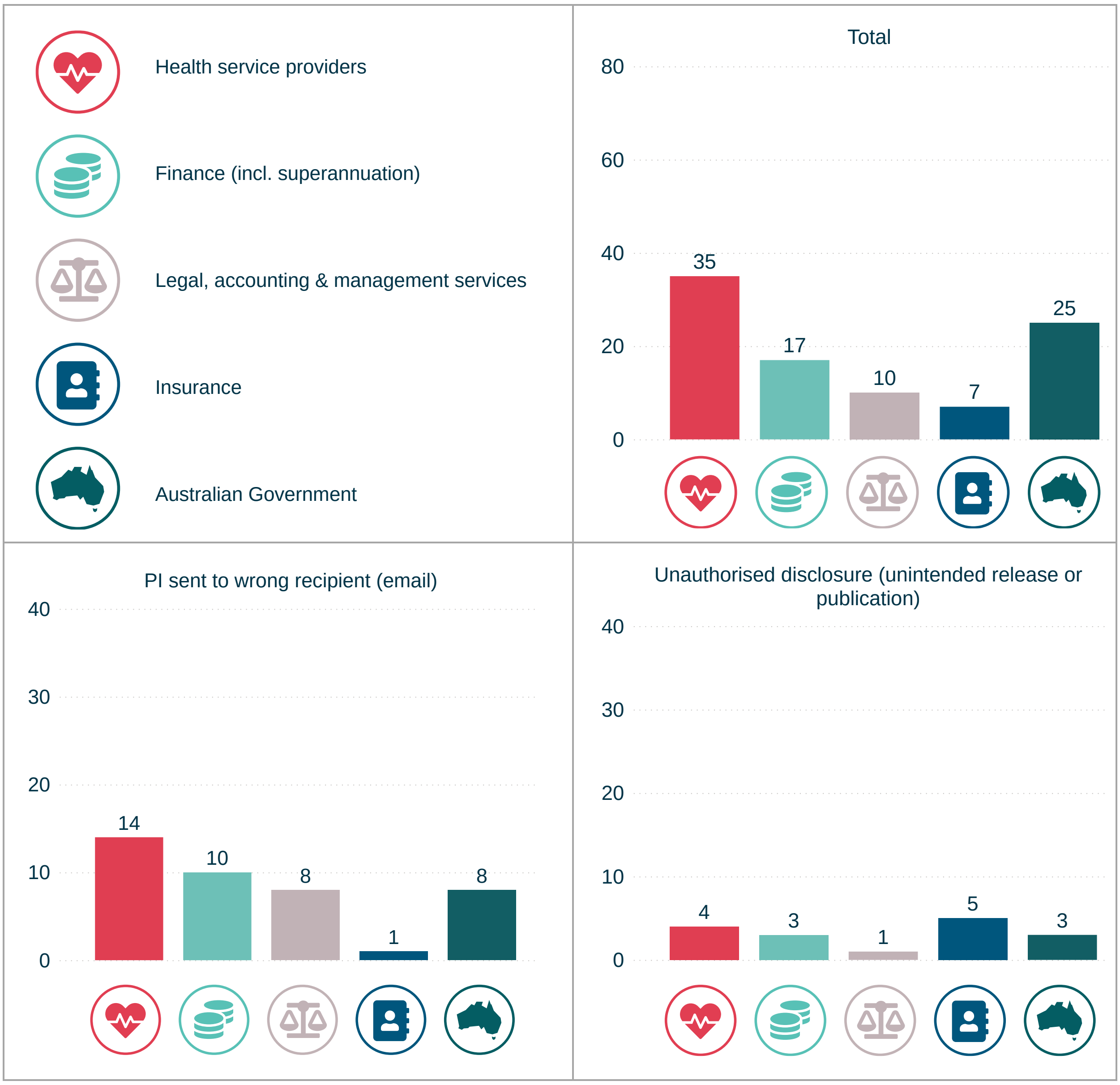


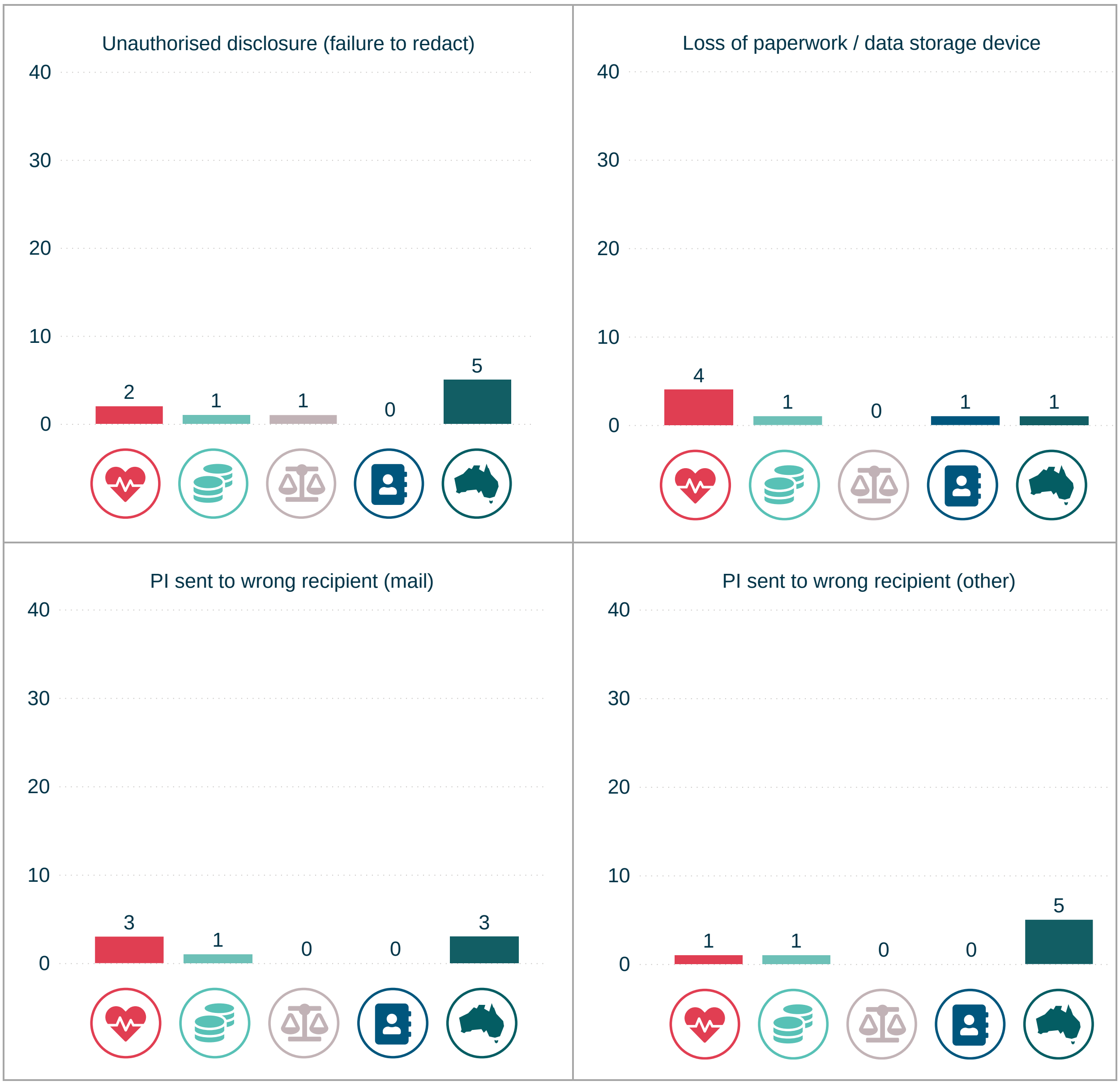
Brute-force attack (compromised credentials)

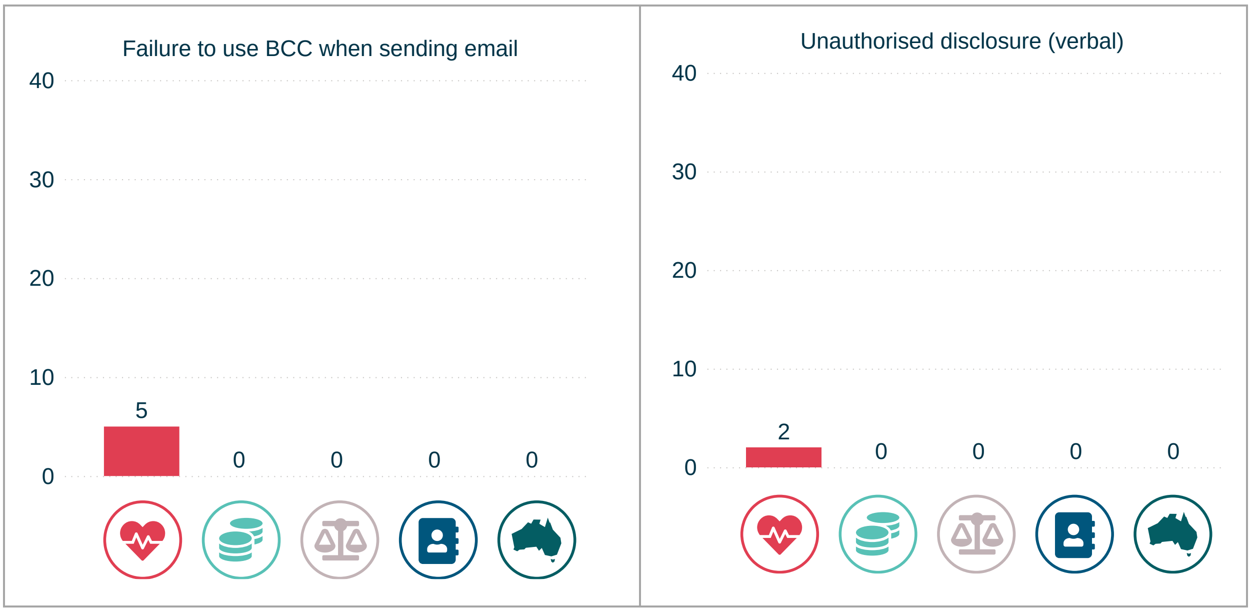


Human error breaches – Top 5 industry sectors

Chart 20 – Human error breakdown – Top 5 industry sectors




Unauthorised disclosure (failure to redact)
40
30
20
10
0
2
1
1
0
5
Loss of paperwork / data storage device
40
30
20
10
0
4
1
0
1
1
PI sent to wrong recipient (mail)
40
30
20
10
0
3
1
0
0
3
PI sent to wrong recipient (other)
40
30
20
10
0
1
1
0
0
5

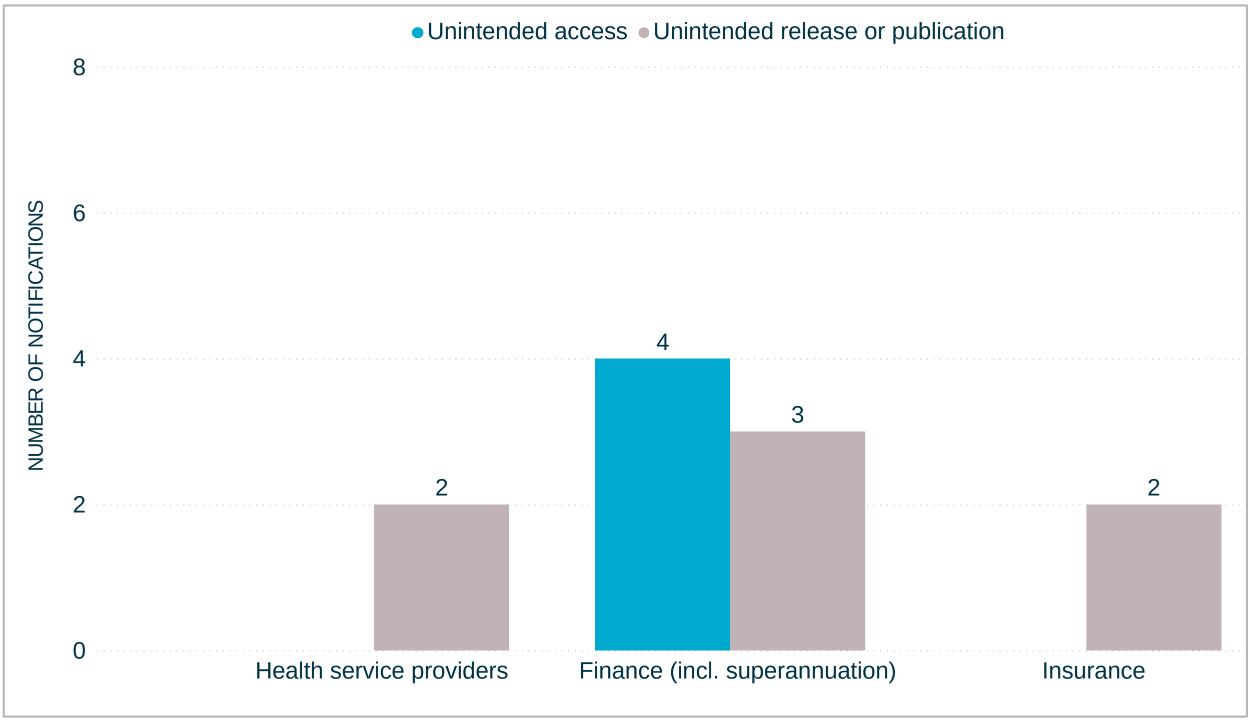


System fault breaches – Top 5 industry sectors

Three of the top 5 industry sectors notified data breaches resulting from a system fault, including finance, which made 7 notifications in this category.

Most system fault breaches involved the unintended release or publication of personal information (7 notifications).

Chart 21 – System fault breakdown – Top 5 industry sectors



Note: Legal, accounting and management services and the Australian Government did not report any system faults.

Glossary

Term	Definition
Personal information (PI)	Information or an opinion about an identified individual, or an individual who is reasonably identifiable
Sensitive information	Sensitive information is personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations • religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information some aspects of biometric information.
Financial details	Information relating to an individual's finances, for example, bank account or credit card numbers
Tax file number (TFN)	An individual's personal reference number in the tax and superannuation systems, issued by the Australian Taxation Office
Identity information	Information that is used to confirm an individual's identity, such as a passport number, driver's licence number or other government identifier
Contact information	Information that is used to contact an individual, for example, a home address, phone number or email address
Health information	As defined in section 6 of the Privacy Act
Other sensitive information	Sensitive information, other than health information, as defined in section 6 of the Privacy Act. For example, sexual orientation, political or religious views
APP entity	An agency or organisation that is subject to the Privacy Act
Managed service provider (MSP)	A managed service provider (MSP) is a business that delivers services relating to IT infrastructure or end user systems to customers
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

Term	Definition
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
Failure to use BCC when sending email	Sending an email to a group by including all recipient emails addresses in the 'To' field, thereby disclosing all recipient email address to all recipients
Insecure disposal	Disposing of personal information in a manner that could lead to its unauthorised disclosure, for example, using a public rubbish bin to dispose of customer records instead of a secure document disposal bin
Loss of paperwork/data storage device	Loss of a physical asset containing personal information, for example, leaving a folder or a laptop on a bus
Unauthorised disclosure (failure to redact)	Failure to effectively remove or de-identify personal information from a record before disclosing it
Unauthorised disclosure (verbal)	Disclosing personal information verbally without authorisation, for example, calling it out in a waiting room
Unauthorised disclosure (unintended release or publication)	Unauthorised disclosure of personal information in a written format, including paper documents or online
Malicious or criminal attack	A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain
Theft of paperwork or data storage device	Theft of paperwork or data storage device
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
Rogue employee/insider threat	An attack by an employee or insider acting against the interests of their employer or other entity

Term	Definition
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
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
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
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
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
Business email compromise	A form of cybercrime that uses email fraud to attack business, government and non-profit organisations to achieve a specific outcome that negatively impacts the target organisation
System fault	A business or technology process error not caused by direct human error