Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Report

July to December 2020

28 January 2021

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 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 July to 31 December 2020**.

Where data breaches affect multiple entities, the OAIC may receive multiple notifications relating to the same breach. 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.

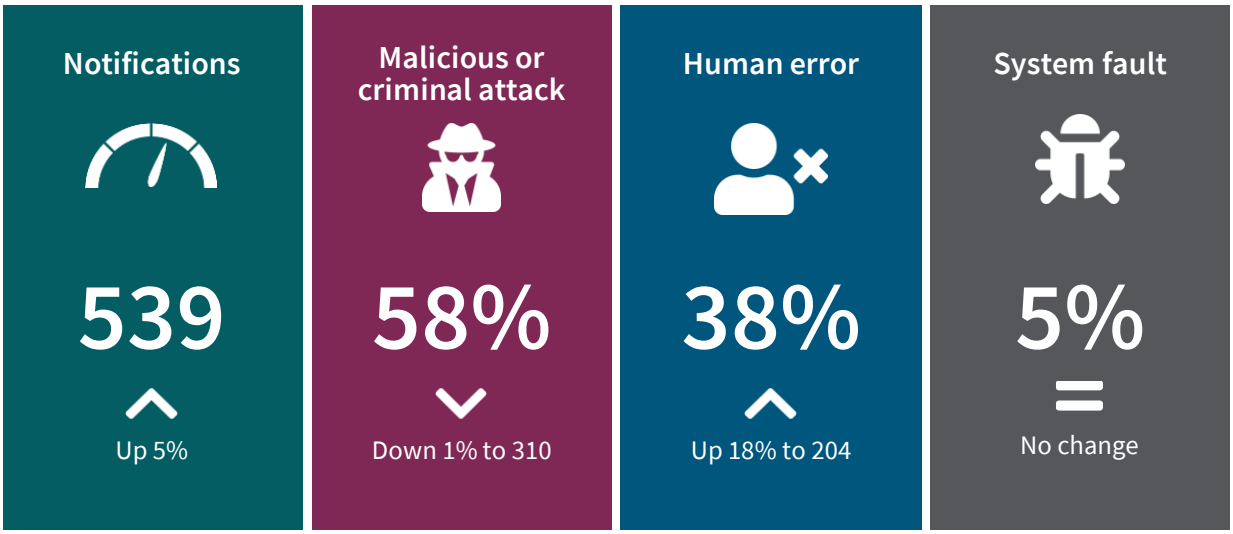
As with previous reports, notifications made under the *My Health Records Act 2012* are not included as they are subject to specific notification requirements set out in that Act.

NDB scheme statistics in this report are current as of 8 January 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 2020 that are published in future reports. Similarly, there may have been adjustments to statistics in previous NDB reports because of changes to the status or categorisation of individual notifications after publication. As a result, references to statistics from before July 2020 in this report may differ from references 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.

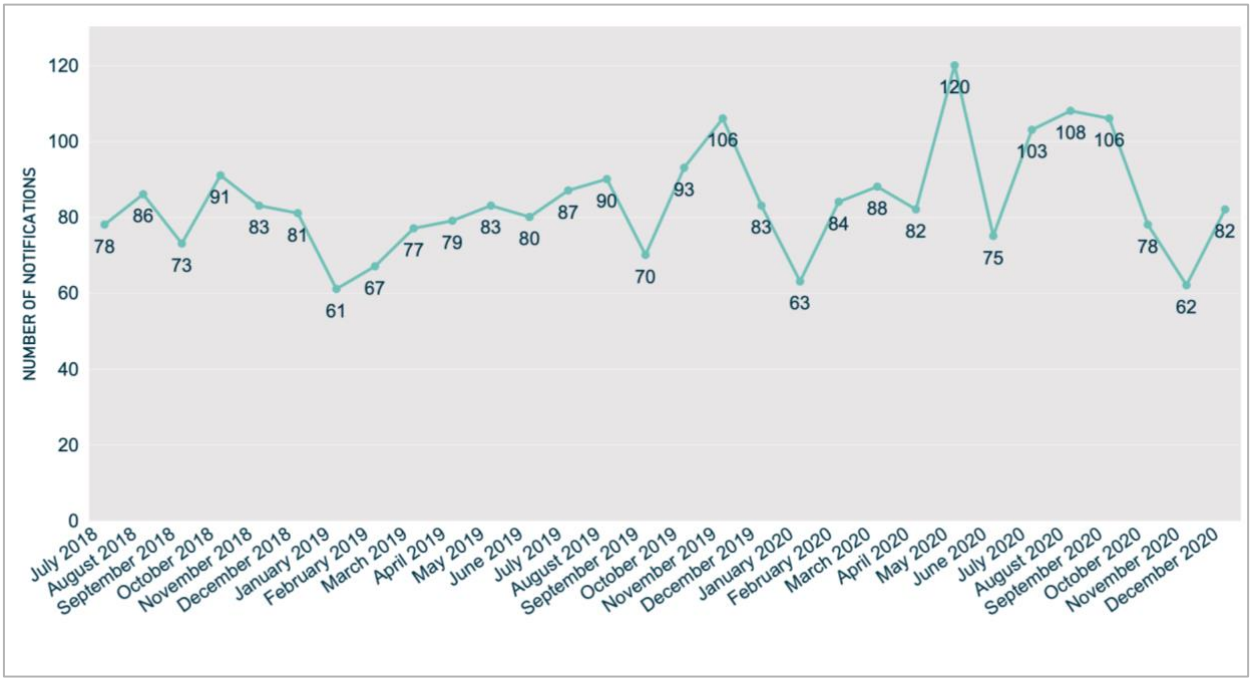


Comparisons are to the period from 1 January to 30 June 2020.
These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

Key findings for the July to December 2020 reporting period:

- 539 breaches were notified under the scheme, an increase of 5% from the 512 notifications received from January to June 2020.
- Malicious or criminal attacks (including cyber incidents) remain the leading source of data breaches, accounting for 58% of notifications.
- Data breaches resulting from human error accounted for 38% of notifications, up 18% from 173 notifications to 204.
- The health sector remains the highest reporting industry sector, notifying 23% of all breaches, followed by finance, which notified 15% of all breaches.
- The Australian Government entered the top 5 industry sectors to notify data breaches for the first time, notifying 6% of all breaches.
- 68% of data breaches affected 100 individuals or fewer.
- 78% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach.

Chart 1 — Data breach notifications under the NDB scheme



Notifications received July to December 2020

The OAIC received 539 notifications this reporting period. This is a 5% increase compared to the previous 6 months and a 2% increase compared to the same period in 2019.

There was significant variation in the number of notifications received each month of the reporting period. The OAIC received 62 notifications in November – the second lowest monthly total since the NDB scheme commenced in February 2018 – but more than 100 notifications in July, August and September.

This reporting period saw continuation of the trend towards a greater proportion of data breaches attributed to human error. Data breaches resulting from human error accounted for 38% of all notifications, compared to 34% the previous 6 months and 32% in the same period in 2019.

Table 1 – Notifications received in 2020 under the NDB scheme

Reporting period	Total no. of notifications
July to December 2020	539
January to June 2020	512
Total no. of notifications received in 2020	**1,051**

Top industry sectors to notify breaches

Health service providers[1] have consistently reported the most data breaches compared to other industry sectors since the NDB scheme began. The Australian Government[2] entered the top reporting industry sectors for the first time, replacing the insurance sector.

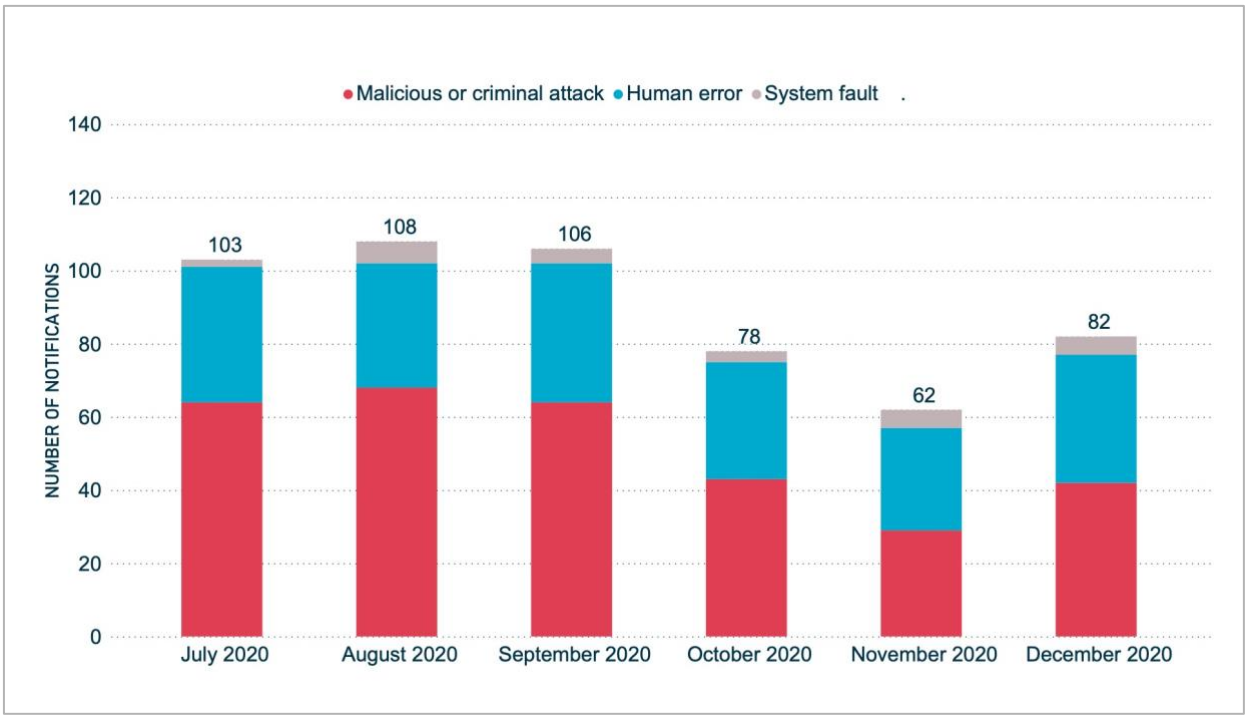
[1] A health service provider generally includes any private sector entity that provides a health service within the meaning of section 6FB of the Privacy Act, regardless of annual turnover. State or territory public hospitals and health services are generally not covered – they are bound by state and territory privacy laws, as applicable.

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

Table 2 – Top 5 industry sectors by notifications

Industry sector	Total no. of notifications
Health service providers	123
Finance (incl. superannuation)[3]	80
Education[4]	40
Legal, accounting & management services	38
Australian Government	33

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



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

[4] This sector includes private education providers only, as APP entities. Public sector education providers are bound by state and territory privacy laws, as applicable.

The impact of remote working arrangements resulting from COVID-19 restrictions

In early 2020, businesses across Australia introduced remote working arrangements in response to the COVID-19 pandemic. The OAIC has highlighted the privacy risks arising from these arrangements, recommending that entities consider undertaking privacy impact assessments to screen for unexpected privacy issues and to help mitigate any privacy risks associated with remote working arrangements.

Across the reporting period, the OAIC has closely monitored trends in NDB scheme notifications for any indications that remote working arrangements have either increased the risk of data breaches or impacted the capacity of notifying entities to meet their obligations under the Privacy Act.

Considering the public reporting on the increase in both COVID-19-themed fraud and the vulnerability of entities with remote working arrangements to cyber security incidents, it is noteworthy that there has only been a modest increase of 5% in the total number of notifications compared to the previous reporting period.

However, it is also notable that data breaches resulting from human error have significantly increased, both in terms of the total number received – up 18% – and proportionally – up from 34% to 38% of all notifications. While it is possible that this increase is linked to changed business and information handling practices resulting from remote working arrangements, the OAIC is yet to identify any information or incidents that conclusively prove a link.

Data breaches attributed to malicious or criminal attacks, including cyber incidents, have decreased both in terms of the total number received and proportionally, albeit only slightly. Breaches attributed to cyber security incidents decreased from 218 last reporting period to 212. This represents a decrease of 3%, roughly in line with the previous 6-monthly comparison.

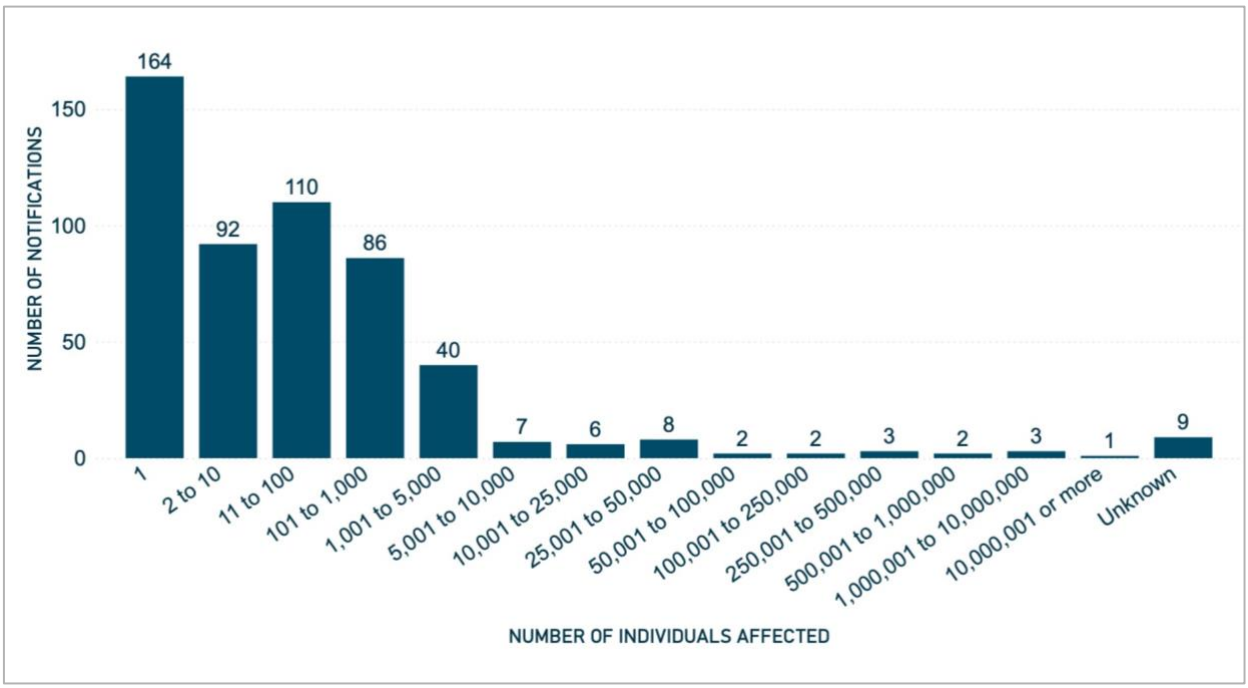
This downward trend, particularly in relation to data breaches arising from cyber incidents, followed the Australian Cyber Security Centre's 2019-20 Annual Cyber Threat Report highlighting an increase in reported spear phishing campaigns and COVID-19-themed malicious cyber activity during the pandemic. However, not all cyber security incidents reported to the Australian Cyber Security Centre constitute eligible data breaches under the NDB scheme.

The OAIC considers that more data and analysis are required before a view can be developed on the impact of remote working arrangements on the capacity of entities to securely manage personal information.

Number of individuals affected by breaches – All sectors

As with previous reporting periods, the majority of eligible data breaches (68%) involved the personal information of 100 individuals or fewer. Breaches affecting 10 individuals or fewer comprised 47% 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.

Data breaches involving managed service providers

The OAIC received a number of notifications during the reporting period that involved a managed service provider (MSP) hosting or holding data on behalf of one or more other entities.

As outlined in the OAIC's Data breach preparation and response guide, the NDB scheme recognises that entities often hold[5] personal information jointly. An entity may collect

[5] Under section 6(1) of the Privacy Act, an entity is taken to 'hold' personal information if it has possession or control of a record that contains personal information. This means that the term 'hold' extends beyond physical possession of a record to include a record that an entity has a right or power to deal with, even if it does not physically possess the record or own the medium on which it is stored.

personal information and retain legal control or ownership of the information, while an MSP may physically possess the information.

In these circumstances, an eligible data breach of one entity is considered an eligible data breach of other entities that hold the affected information. All have obligations under the NDB scheme.[6] In general, compliance by one entity will be taken as compliance by each of the entities that hold the information. As such, only one entity needs to take the steps required by the NDB scheme. The NDB scheme leaves it up to the entities to decide which of them should do so.

The OAIC has seen different responses by entities involved in multi-party breaches. In several instances, the MSP managed all aspects of the data breach response in consultation with its clients and coordinated the notification to the OAIC and individuals affected by the data breach.

In some other cases, MSPs notified their clients of the data breach but otherwise left to them the responsibility for meeting the assessment and notification requirements of the NDB scheme. This approach broadly corresponds with OAIC guidance that suggests the entity with the most direct relationship with the individuals affected by the data breach should generally carry out the notification. However, it is not without risk and may result in entities falling short of their obligations under the NDB scheme.

For example, the OAIC received notifications from multiple entities that experienced a data breach resulting from a single compromise of an MSP they all used. However, the OAIC had grounds to believe the compromise had also affected several other entities that did not notify the OAIC of the data breach. Here, both the MSP and the MSP's clients that did not notify the OAIC may have failed to meet their obligations under the Privacy Act.

A failure by both the MSP and its clients to notify the OAIC and individuals at risk of serious harm from a data breach will represent a breach of the provisions of Part IIIC of the Privacy Act, and will likely constitute an interference with privacy by all.

Kinds of personal information involved in breaches – All sectors

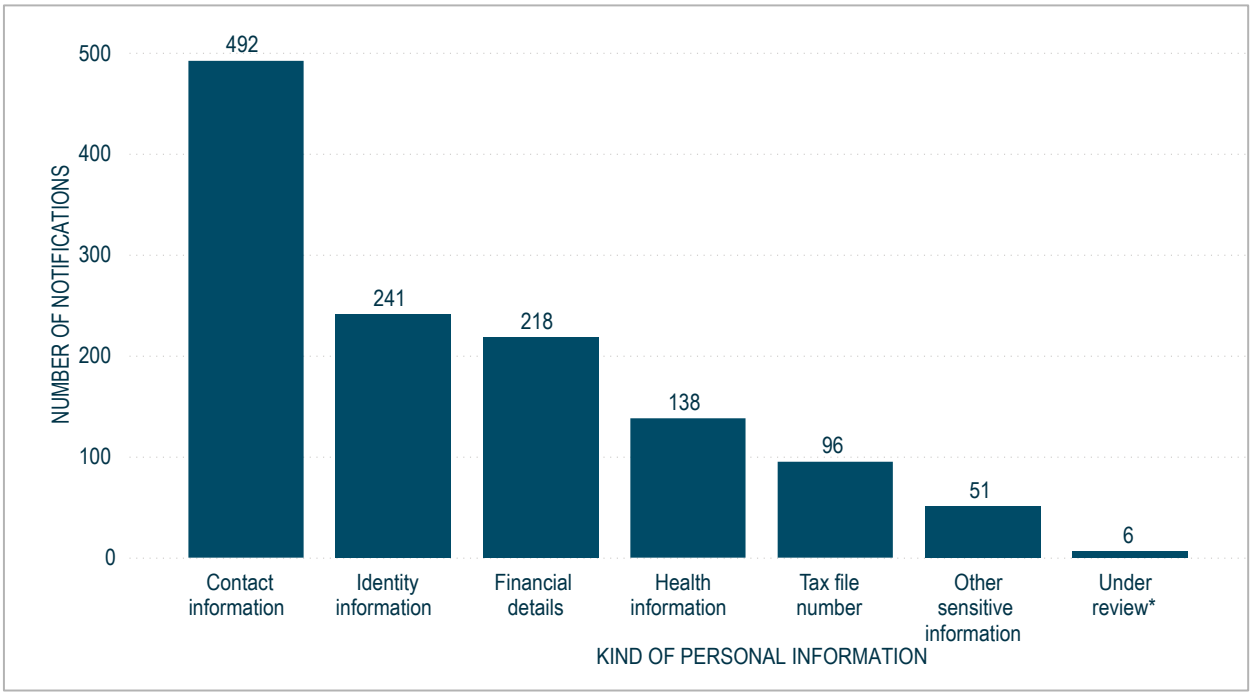
Most data breaches (91%) notified under the NDB scheme from July to December 2020 involved 'contact information', such as an individual's home address, phone number or email address. This is distinct from 'identity information', which refers to information that is used to confirm an individual's identity, such as a passport number or driver's licence number. Identity information was exposed in 45% of data breaches notified during the period.

Data breaches notified in the period also involved financial details, such as bank account or credit card numbers (40%), health information (26%) and tax file numbers (18%). 'Other sensitive

[6] Notifications relating to the same data breach incident are counted as a single notification in this report.

information' (9%) refers to categories of sensitive information as set out in section 6 of the Privacy Act, other than health information as defined in section 6FA.

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



Note: Eligible data breaches may involve more than one kind of personal information.
* For breaches listed against this category, the notifying entity was still conducting its assessment of the breach, including which categories of personal information had been disclosed or accessed, at the time it notified the OAIC.

The importance of timely assessment and notification

The OAIC has seen significant variation in the time taken by entities to identify, assess and investigate breaches and then notify affected individuals.

Most entities took all reasonable steps to conduct an assessment of the incident suspected to be an eligible data breach within 30 days – as required by section 26WH of the Privacy Act – and then moved promptly to notify both the OAIC and affected individuals. An example of good practice is provided later in this report.

However, increasingly the OAIC is seeing instances of organisations taking much longer than 30 days to complete their assessments, with further significant delays before they notify affected individuals. Additional time taken to assess a breach must be reasonable and justified in the circumstances, with notification to individuals to occur as soon as practicable.

Some data breaches are complex and may affect entire networks or enterprise environments. In certain instances, it may take the affected entity a significant amount of time to identify the extent of the data breach and all affected individuals.

The Privacy Act is clear that an entity responding to a data breach should not only take all reasonable steps to complete its assessment of whether an incident constituted an eligible data breach within 30 days, but also notify the OAIC and affected individuals as soon as practicable after confirming that there are reasonable grounds to believe an eligible data breach occurred.

Section 26WL(2) of the Privacy Act provides 3 ways by which individuals affected by a data breach may be notified. An entity may notify each individual whose personal information has been involved in the eligible data breach, or notify only individuals who are at risk of serious harm. If neither of these options are practicable, an entity may publish a statement on the eligible data breach on its website and publicise the statement.

In determining the appropriate course, entities should have regard to the need to conduct a thorough assessment, the need to provide information that assists individuals to mitigate harm and the need to provide timely notification to affected individuals.

Unnecessarily delayed notifications undermine the NDB scheme by denying affected individuals the ability to take timely steps to protect themselves from harm.

Time taken to identify breaches – All sectors

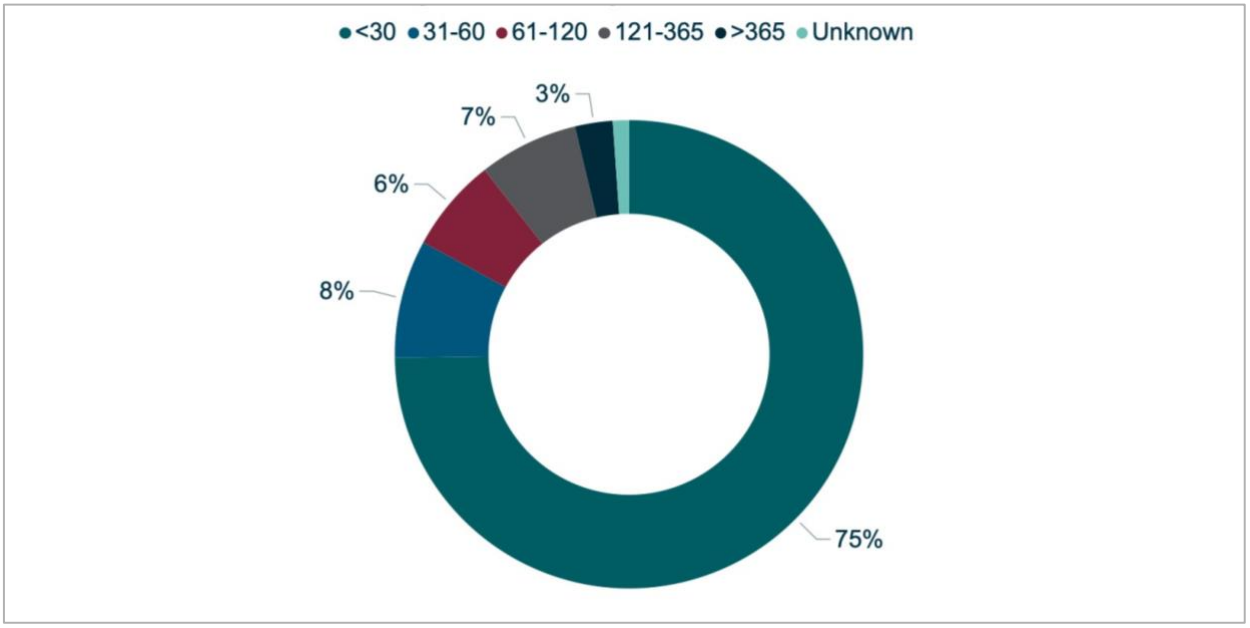
As part of complying with Australian Privacy Principle 11, entities should take reasonable steps to ensure that data breaches can be detected in a timely manner.

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.[7]

For 75% of notifications, entities identified that an incident that may constitute an eligible data breach had occurred within 30 days of it taking place.

[7] 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 that 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.

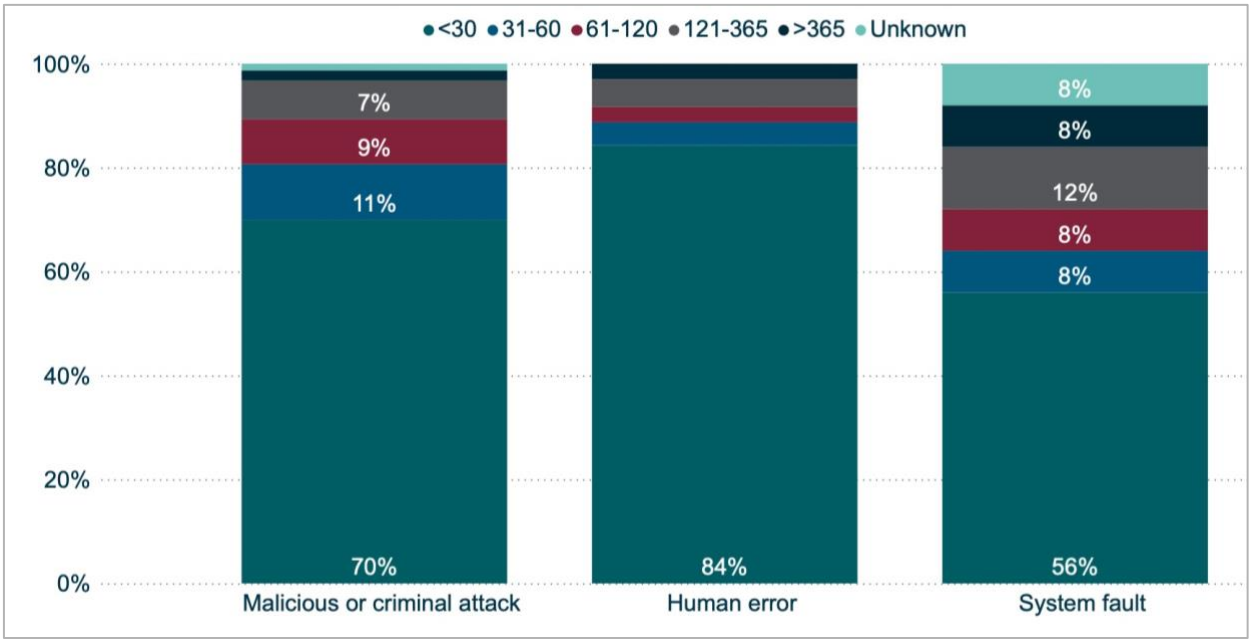
Chart 5 – Days taken to identify breaches – All sectors



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

The time taken to identify a data breach varied significantly depending on the source of the breach. For human error breaches, 84% of entities identified the incident within 30 days of it occurring. However, only 56% of entities identified an incident resulting from a system fault within 30 days.

Chart 6 – Days taken to identify 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. For notifications in the 'Unknown' category, the notifying entity was unable to identify the date the breach occurred.

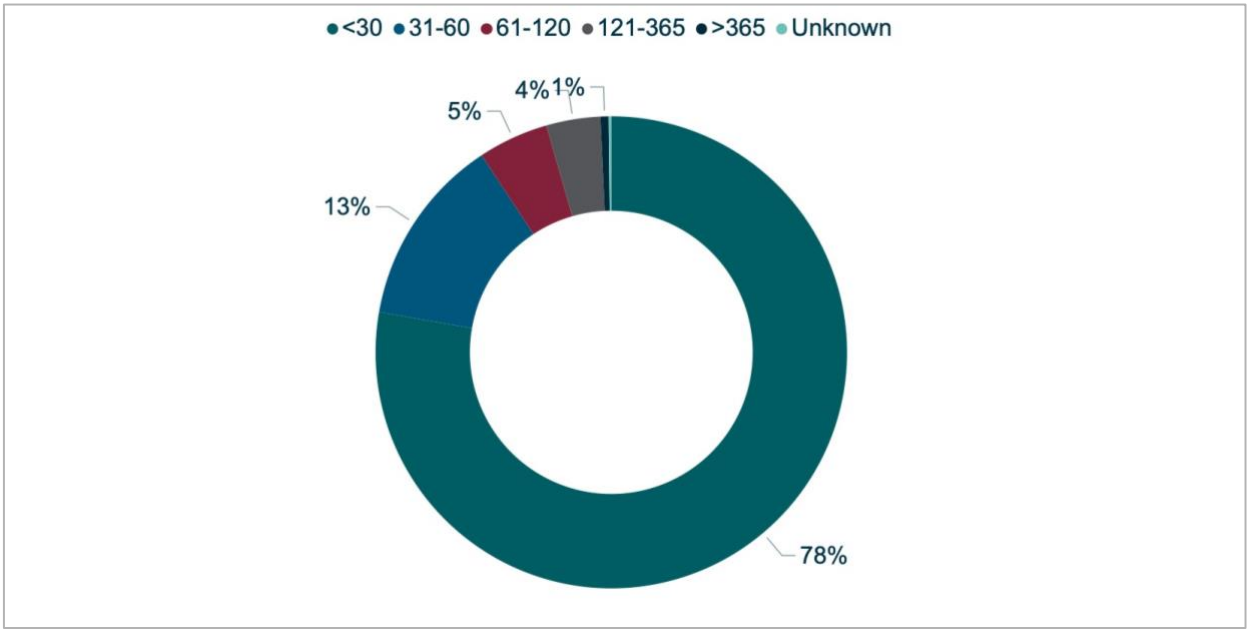
Time taken to notify the OAIC of breaches – All sectors

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 opportunities that individuals have to take steps to prevent harm resulting from a data breach.

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.[8]

From July to December 2020, 78% of entities notified the OAIC within 30 days of becoming aware of an incident that was subsequently assessed to be an eligible data breach. However, 23 entities took longer than 120 days after 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, individuals were notified some time after the OAIC.

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



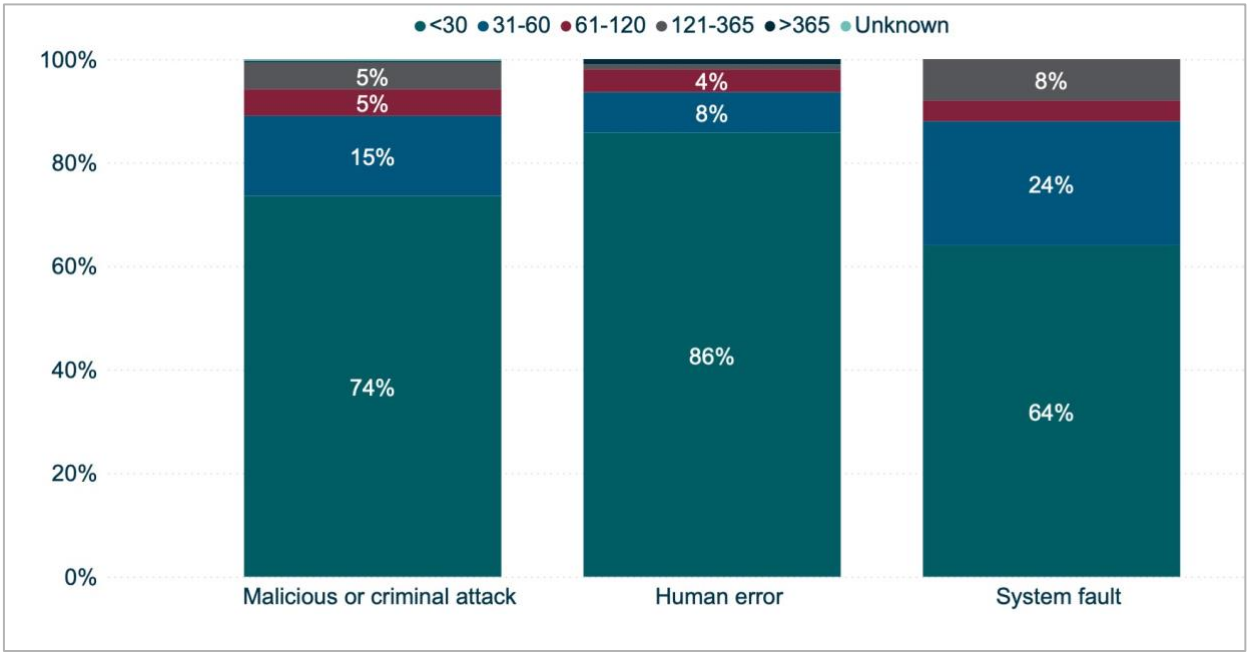
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category. For notifications in the 'Unknown' category, the notifying entity was unable to identify the date the breach occurred.

The source of the breach influenced the time entities took to notify the OAIC after the incident was identified. In the case of human error breaches, 86% of entities notified the OAIC within 30 days of identifying the breach.

[8] 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 that 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.

However, this figure dropped to 74% for data breaches that resulted from malicious or criminal attacks, and 64% for breaches that resulted from system faults.

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

Requirements for notifications to individuals

During the reporting period, there were multiple instances where entities' notifications to individuals were deficient. In these instances, the OAIC required that the notifications be revised and reissued.

Entities must provide the following information to the OAIC as soon as practicable after becoming aware that there are reasonable grounds to believe there has been an eligible data breach:

- the identity of the entity and their contact details
- a description of the eligible data breach
- the kind or kinds of information involved in the data breach
- recommendations about the steps that individuals should take in response.

The entity must also provide a notification to individuals affected by the breach that reflects the content of the statement provided to the OAIC, and it must do so as soon as practicable.

These requirements ensure individuals affected by a data breach can make informed decisions about how to best mitigate harm.

The OAIC has identified instances where entities have provided individuals affected by a data breach with relatively generic advice that their 'personal details' may have been exposed. In these instances, the entities did not clarify the kind or kinds of information involved in the data breaches, which included bank account details, credit card details, tax file numbers, Medicare numbers and identity numbers.

The OAIC required these entities to send an updated notification to the affected individuals that:

- specified all the kinds of personal information involved in the data breach
- included corresponding recommendations about the steps individuals should take in response to the breach.

In other instances, notifying entities did not provide affected individuals with sufficient information regarding the data breach to understand the risk arising from it.

For example, an entity notified the OAIC of a data breach caused by social engineering where a staff member of the entity was deceived by a malicious actor into disclosing personal information about other individuals. However, the entity only advised individuals affected by the data breach that it involved a disclosure of their personal information to an 'unintended recipient'. In response to the OAIC's inquiries, the entity acknowledged that it had incorrectly paraphrased the description of the eligible data breach and reissued the notification to clarify that it involved a malicious actor.

Examples such as these may not only fall short of reporting obligations but also adversely affect an individual's ability to make an informed decision about how to best mitigate harm.

Entities' data breach notifications must balance timeliness and thoroughness to meet the requirements of the Privacy Act.

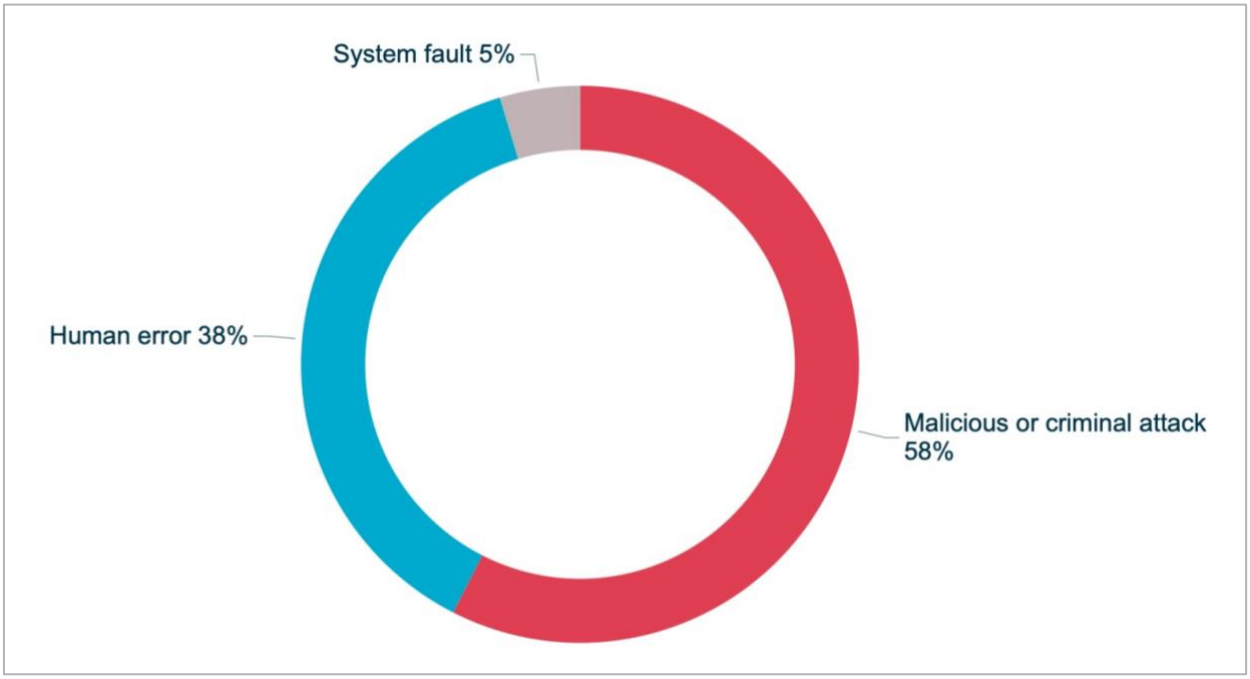
Source of breaches – All sectors

Malicious or criminal attacks were the largest source of data breaches notified to the OAIC from July to December 2020, accounting for 310 breaches. Malicious or criminal attacks are defined as attacks that are deliberately crafted to exploit known vulnerabilities for financial or other gain.

Attacks included cyber incidents such as phishing and malware, data breaches caused by social engineering or impersonation, theft of paperwork or storage devices, and actions taken by a rogue employee or insider threat.

Human error remained a major source of breaches, accounting for 204 notifications. This was a notable increase from the 173 notifications attributed to human error in the previous period. System faults accounted for the remaining 25 breaches notified.

Chart 9 – Source of data 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.

Malicious or criminal attack breaches – All sectors

Malicious or criminal attacks remain the leading source of data breaches, accounting for 58% of notifications. However, the number of these breaches is holding steady – down only 1% from 312 notifications last reporting period to 310.

The majority of breaches (68%) in the malicious or criminal attack category involved cyber incidents. The OAIC received 212 notifications of cyber incidents, a slight decrease from the 218 notifications received during the previous period. Cyber incidents were responsible for 39% of all data breaches, with phishing, compromised or stolen credentials, and ransomware the main sources of the data breaches in this category.

Data breaches resulting from social engineering or impersonation accounted for 34 notifications. This represented a decrease from the 48 notifications received in the previous period. Actions taken by a rogue employee or insider threat accounted for 35 notifications, up from 23. Theft of paperwork or storage devices resulted in 29 notifications.

Chart 10 – Breaches resulting from malicious or criminal attacks – All sectors

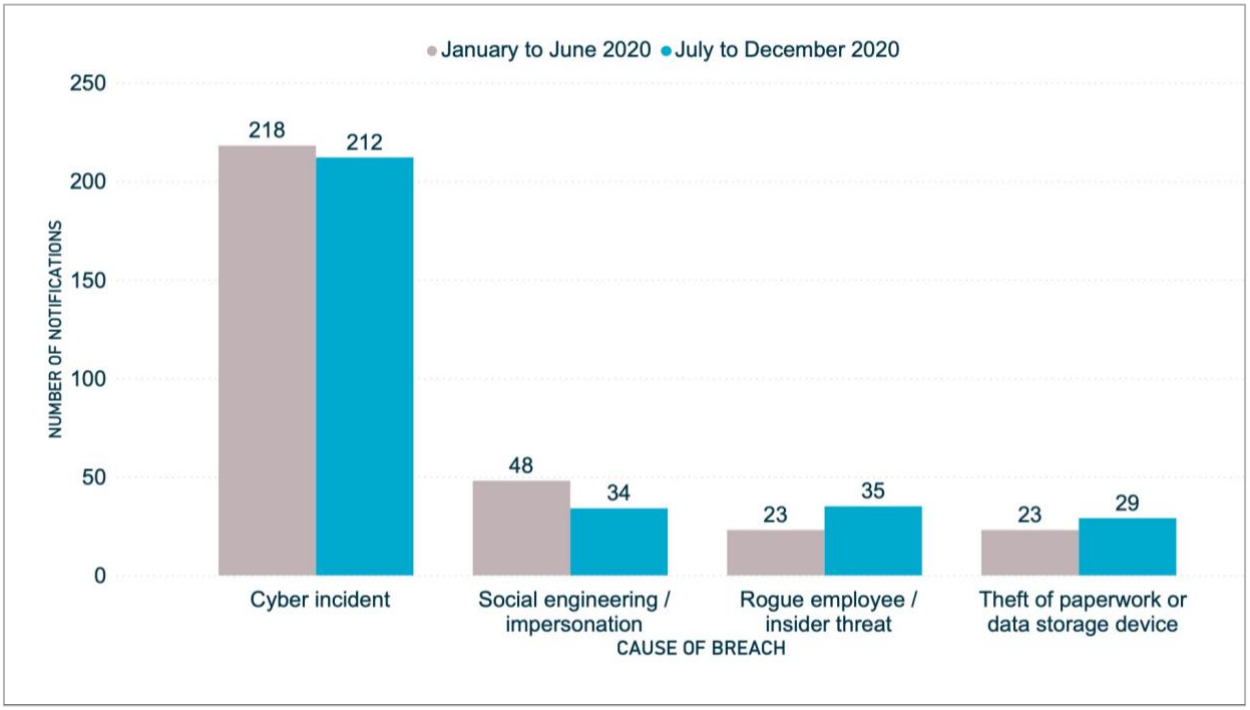
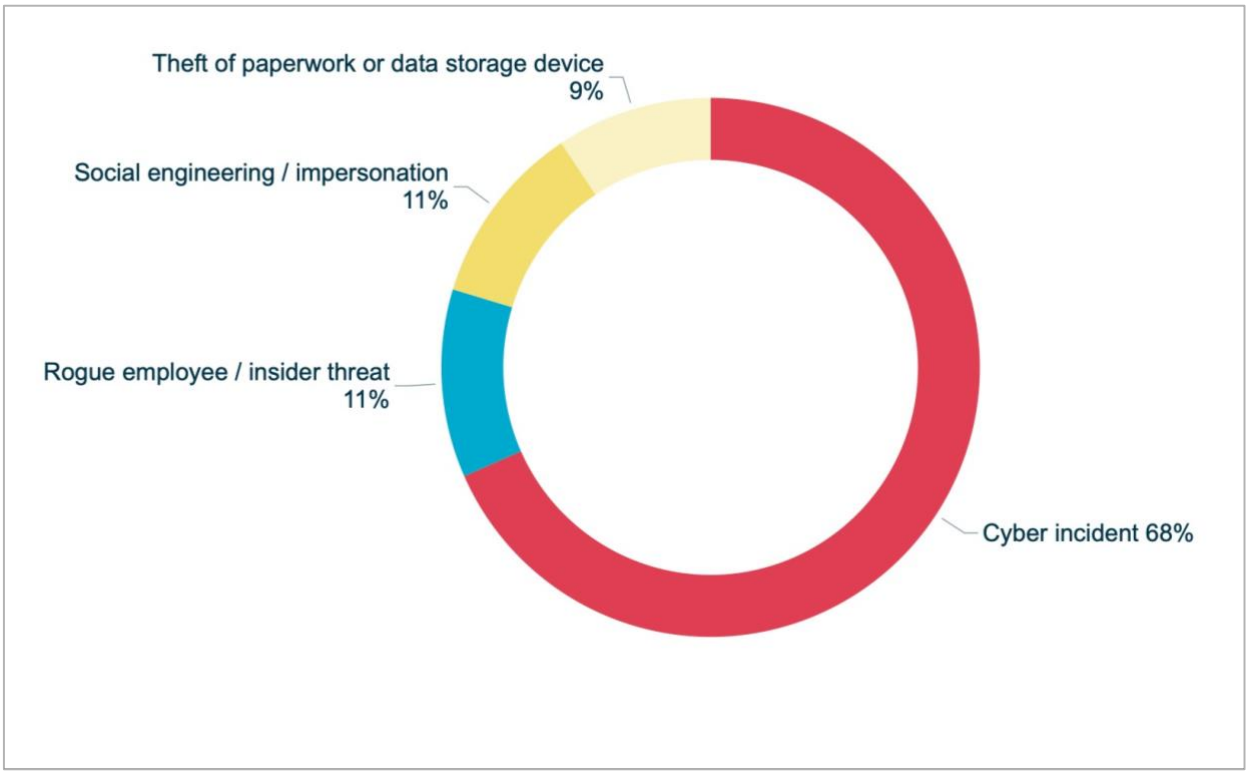


Chart 11 – Malicious or criminal attacks – All sectors



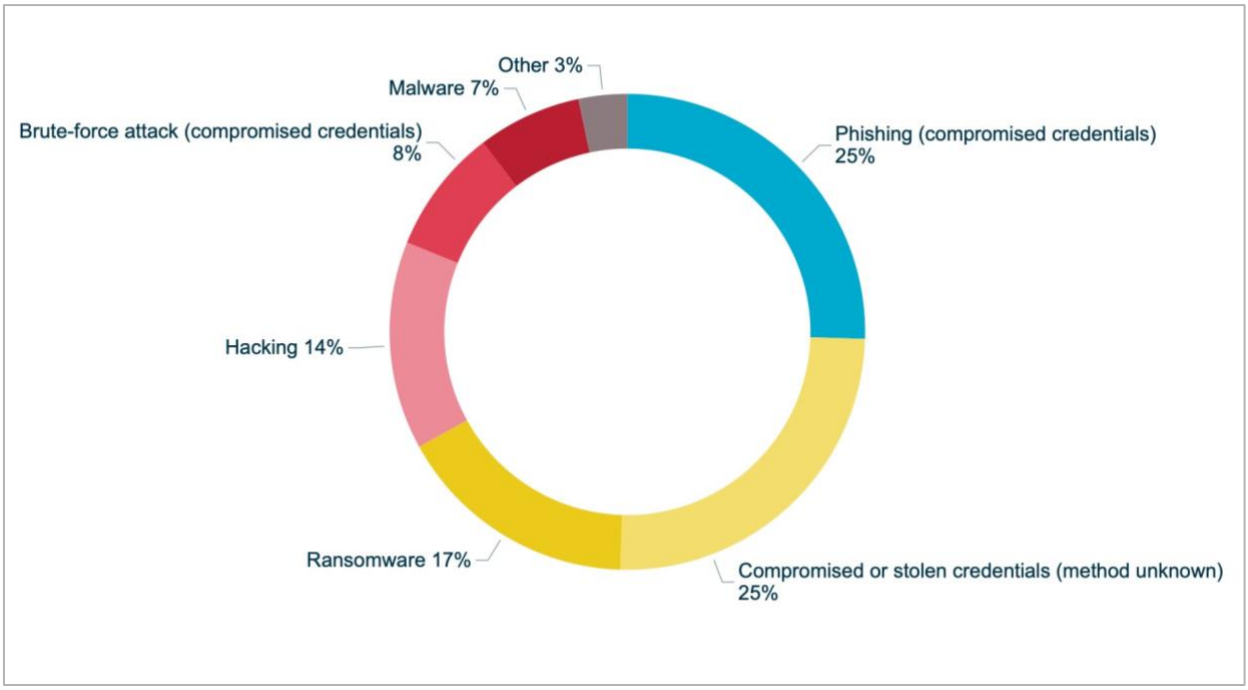
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

Cyber incident breaches – All sectors

More than half of all cyber incidents – and 23% of all notifications – during the reporting period involved malicious actors gaining access to accounts using compromised or stolen credentials.

The most common method used by malicious actors to obtain compromised credentials was email-based phishing (54 notifications). This confirms that email-based vulnerability is one of the greatest risks to information security facing organisations. The human factor is an important element in an organisation's overall information and cyber security posture, given these attacks rely on a person clicking on a phishing link.

Chart 12 – Cyber incident breakdown – All sectors



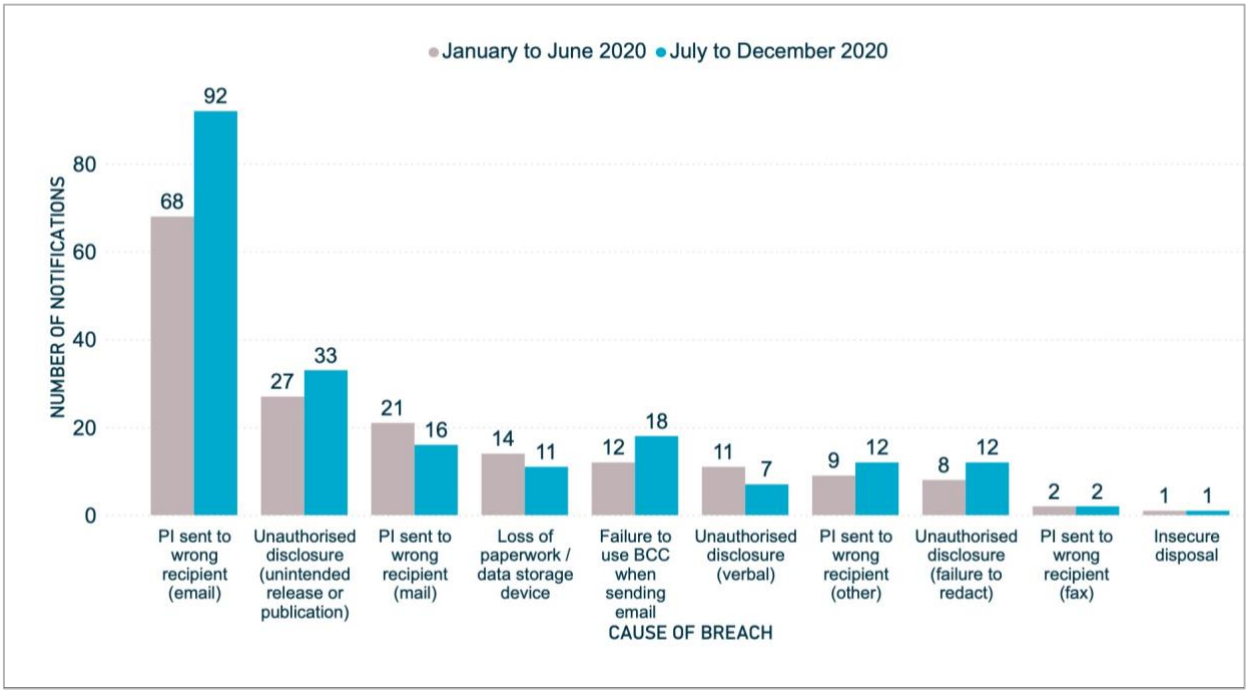
Note: These figures do not add up to a total of 100% due to the rounding up or down of the percentages for each category.

Human error breaches – All sectors

The second largest source of data breaches was human error. The number of breaches attributed to human error has increased overall – up 18% from 173 notifications last reporting period to 204 – and proportionally – up from 34% of all data breaches to 38%.

Common examples of human error breaches include sending personal information to the wrong recipient via email (45% of human error breaches), unintended release or publication of personal information (16%), and failure to use the 'blind carbon copy' (BCC) function when sending group emails.

Chart 13 – Human error breakdown – All sectors



Certain human error breaches affect larger numbers of individuals. Unauthorised disclosure (unintended release or publication) affected the largest number of individuals per breach in this category, with an average of 20,117 individuals affected per breach. Failure to use the BCC function when sending group emails affected an average of 19,163 individuals per breach.

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)	92	29
Unauthorised disclosure (unintended release or publication)	33	20,117
Failure to use BCC when sending email	18	19,163
PI sent to wrong recipient (mail)	16	1
PI sent to wrong recipient (other)	12	5
Unauthorised disclosure (failure to redact)	12	2
Loss of paperwork/data storage device	11	24

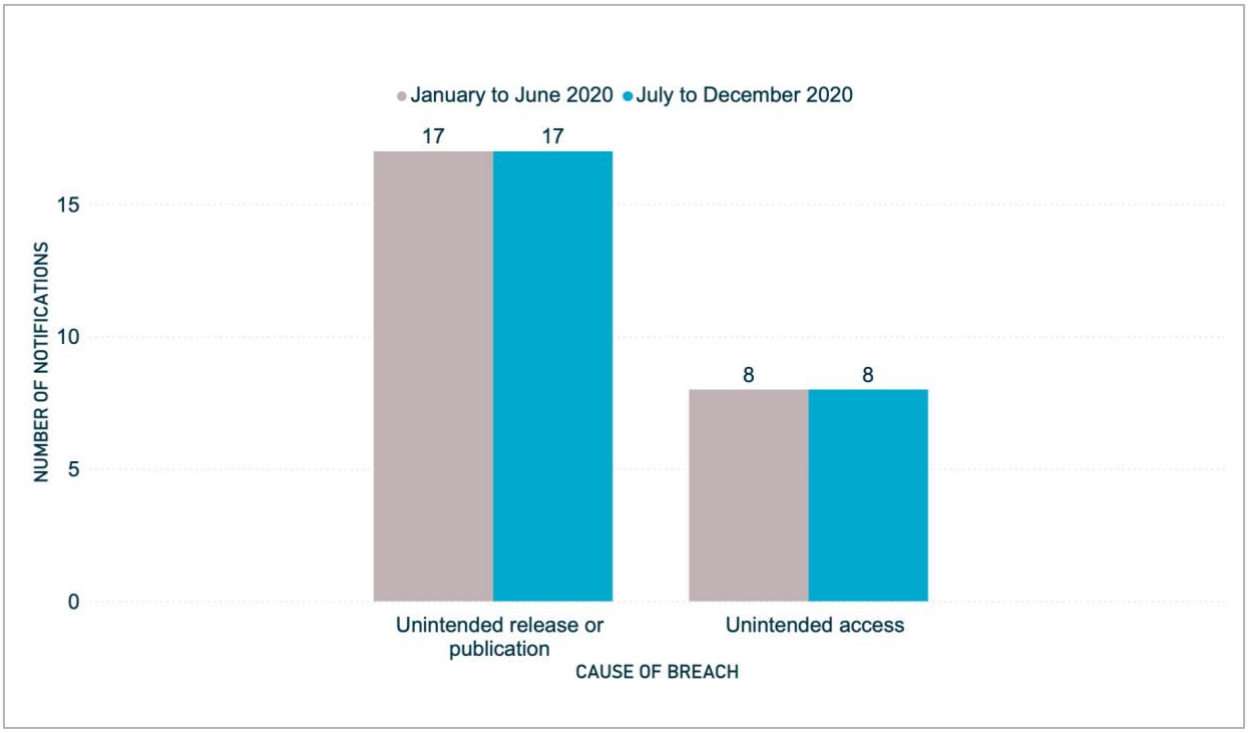
Source of breach	No. of notifications received	Average no. of affected individuals
Unauthorised disclosure (verbal)	7	1
PI sent to wrong recipient (fax)	2	1
Insecure disposal	1	185

System fault breaches – All sectors

System faults accounted for 5% of data breaches – the same proportion as the last reporting period. System fault breaches include data breaches that occur due to a business or technology process error.

Unintended release or publication of personal information due to a system fault caused 17 data breaches, while unintended access to personal information as a result of a system fault caused 8 data breaches.

Chart 14 – System fault breakdown – All sectors



Good data breach response and assessment

Across the reporting period, the OAIC saw several examples of good data breach response and assessment practices.

A notable example involved a business email compromise attack, where an entity's staff member received several suspicious emails requesting payment of falsified invoices.

- The entity immediately locked down the affected staff member's email account and commenced an internal investigation.
- Within 2 days, the entity commissioned an external IT security incident response company to conduct a forensic investigation of its network.
- Eight days after the original suspicious email was identified, the entity received preliminary findings from the IT security incident response company and concluded that an eligible data breach had occurred. Investigations identified over 1,000 employees whose personal information had been exposed and around 100 external individuals who were potentially at risk of serious harm.
- By day 10, the entity notified all staff of the breach, providing them with guidance on IT security best practice and the details of potentially compromised personal information.
- The entity continued its forensic investigation into the incident. Through this process, it confirmed the extent of access obtained by the malicious actor, clarified the data that had been viewed or exfiltrated from its network, and continued its assessment of the serious harm caused to each individual (internal and external) whose personal information had potentially been exposed.
- As part of its assessment process, the entity categorised exposed personal information into 6 categories, against which it weighed the risk of serious harm.
- The entity commissioned a third party to provide support to affected individuals.
- By day 35, the entity had concluded its forensic investigation and provided a final, tailored notification to the OAIC, and to all internal and external individuals it had identified as at risk of serious harm from the breach.
- Given the breach resulted in the exposure of Australian Government identifiers such as tax file numbers and Medicare numbers, the entity also contacted the relevant agencies regarding the breach.

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.

From July to December 2020, health service providers reported 123 data breaches, or 23% of the total.

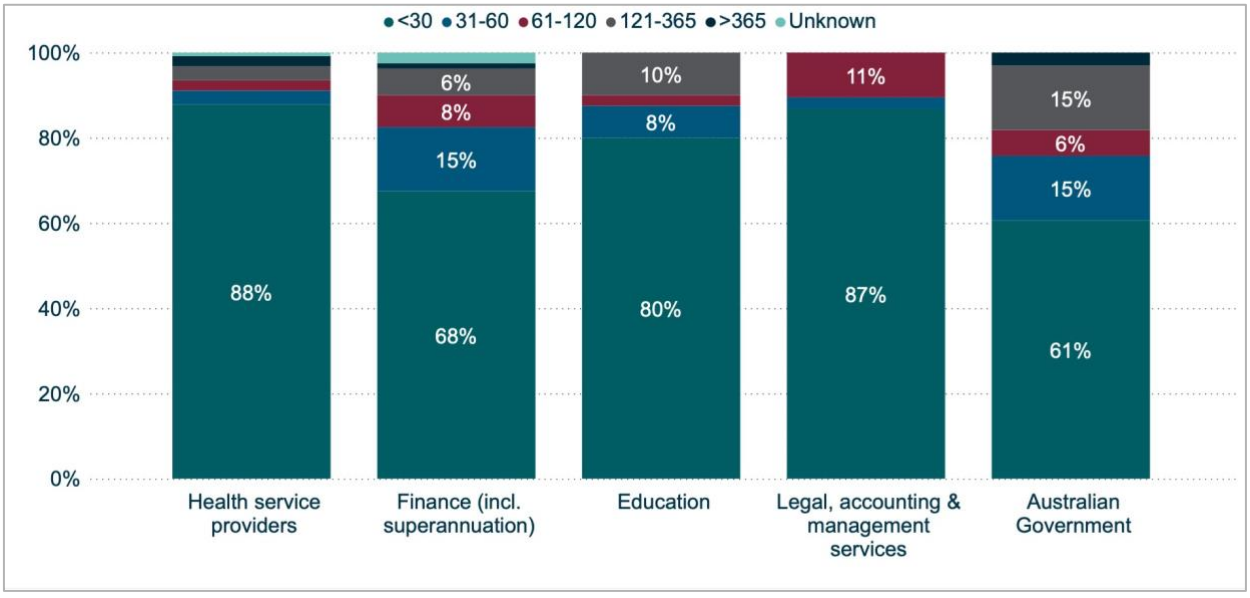
The second largest source of notifications was the finance sector (15%), followed by education (7%), legal, accounting and management services (7%), and the Australian Government (6%). This is the first report where the Australian Government has been among the top 5 industry sectors to notify data breaches.

Time taken to identify breaches – Top 5 industry sectors

The time taken by entities to identify incidents that were subsequently assessed to be eligible data breaches varied by industry sector. [9]

In the reporting period, 88% of health service providers and 87% of entities in the legal, accounting and management services sector identified the incident within 30 days of it occurring. This figure was 68% for the finance sector and 61% for Australian Government entities.

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

[9] 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.

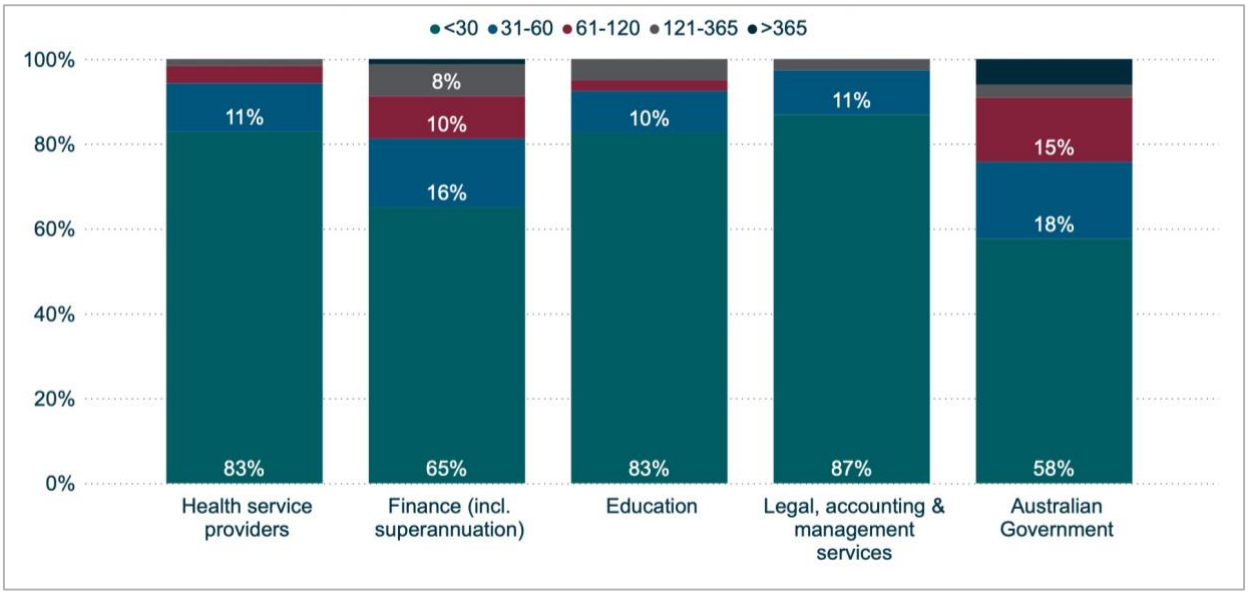
Time taken to notify the OAIC of data breaches – Top 5 industry sectors

The time taken by entities to notify the OAIC of a data breach[10] varied by industry sector.

Eighty-seven per cent of notifications from the legal, accounting and management services sector, and 83% of notifications from the health and education sectors, were made within 30 days of the entity becoming aware of the incident.

Sixty-five per cent of notifications from the finance sector and 58% of notifications from the Australian Government were made to the OAIC within 30 days of the entity becoming aware of the incident.

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.

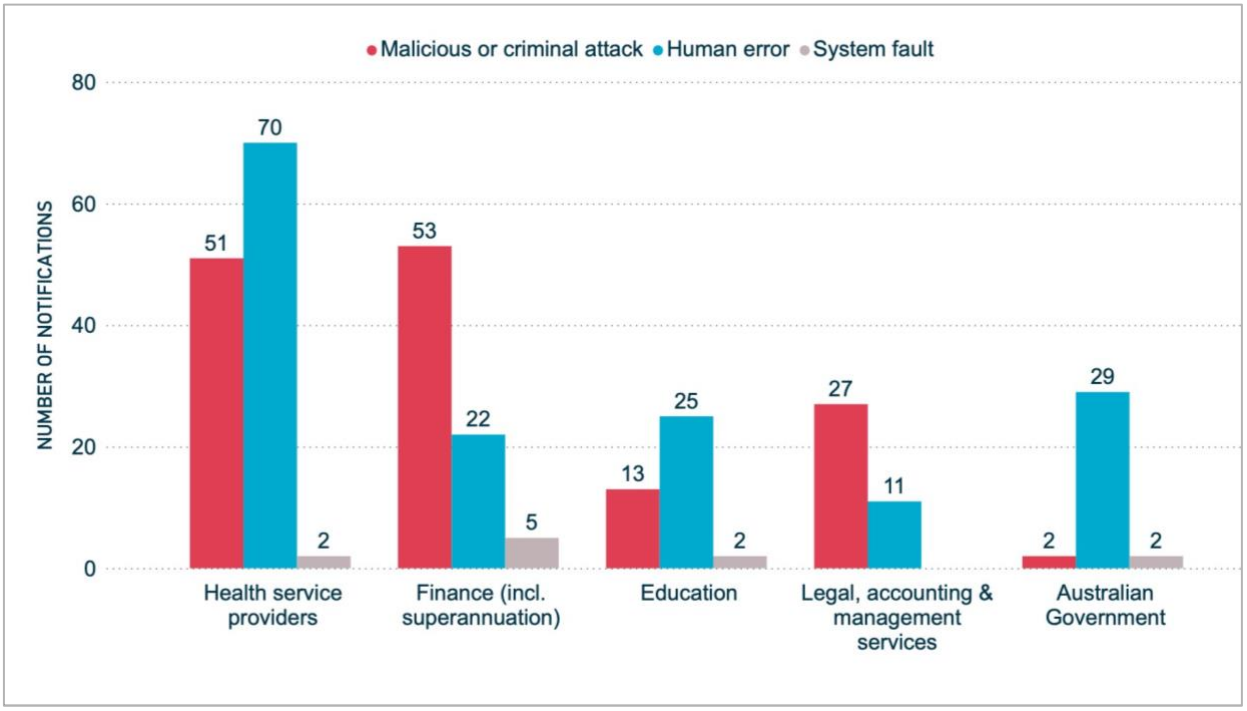
Source of breaches – Top 5 industry sectors

Consistent with previous reports, human error remained the most common source of data breaches within the health sector, accounting for 57% of data breaches reported by the sector. Malicious or criminal attacks caused 41% of data breaches reported by the health sector.

In comparison, malicious or criminal attacks were the most common source of data breaches within the finance sector, comprising 66% of data breaches reported by the sector. Human error was the source of 28% of data breaches within the finance sector.

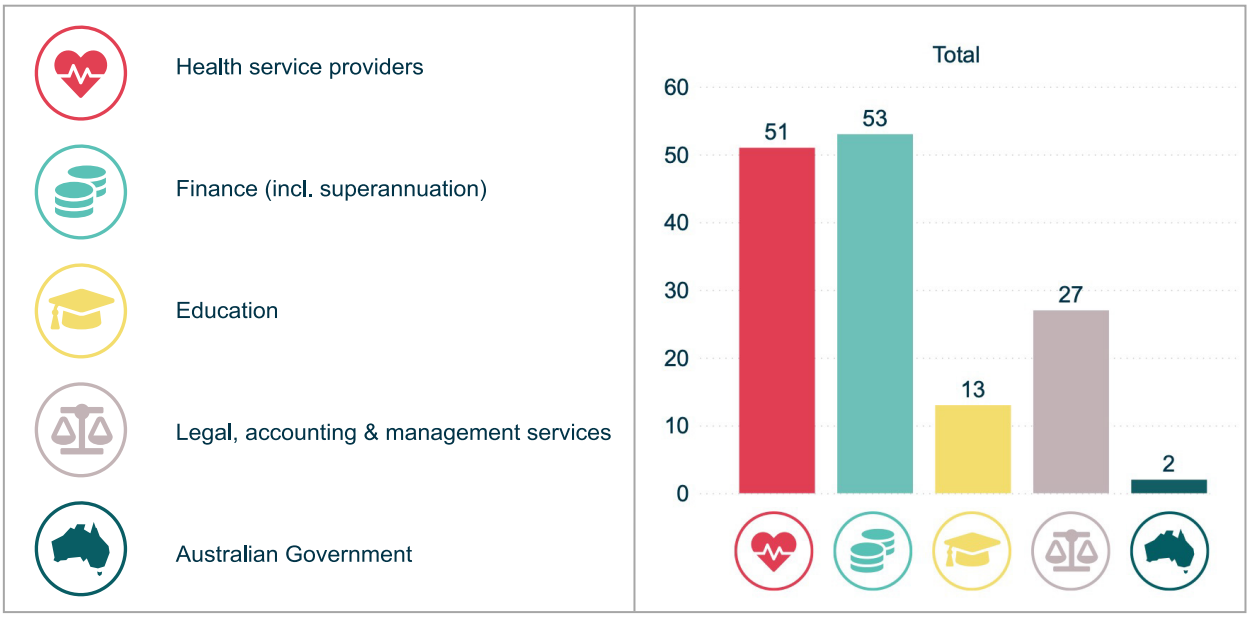
[10] The figures in this section relate to the time between when an entity became aware of an incident and when they notified the OAIC. They do not relate to the time between when the entity determined the incident to be an eligible data breach and when they notified the OAIC.

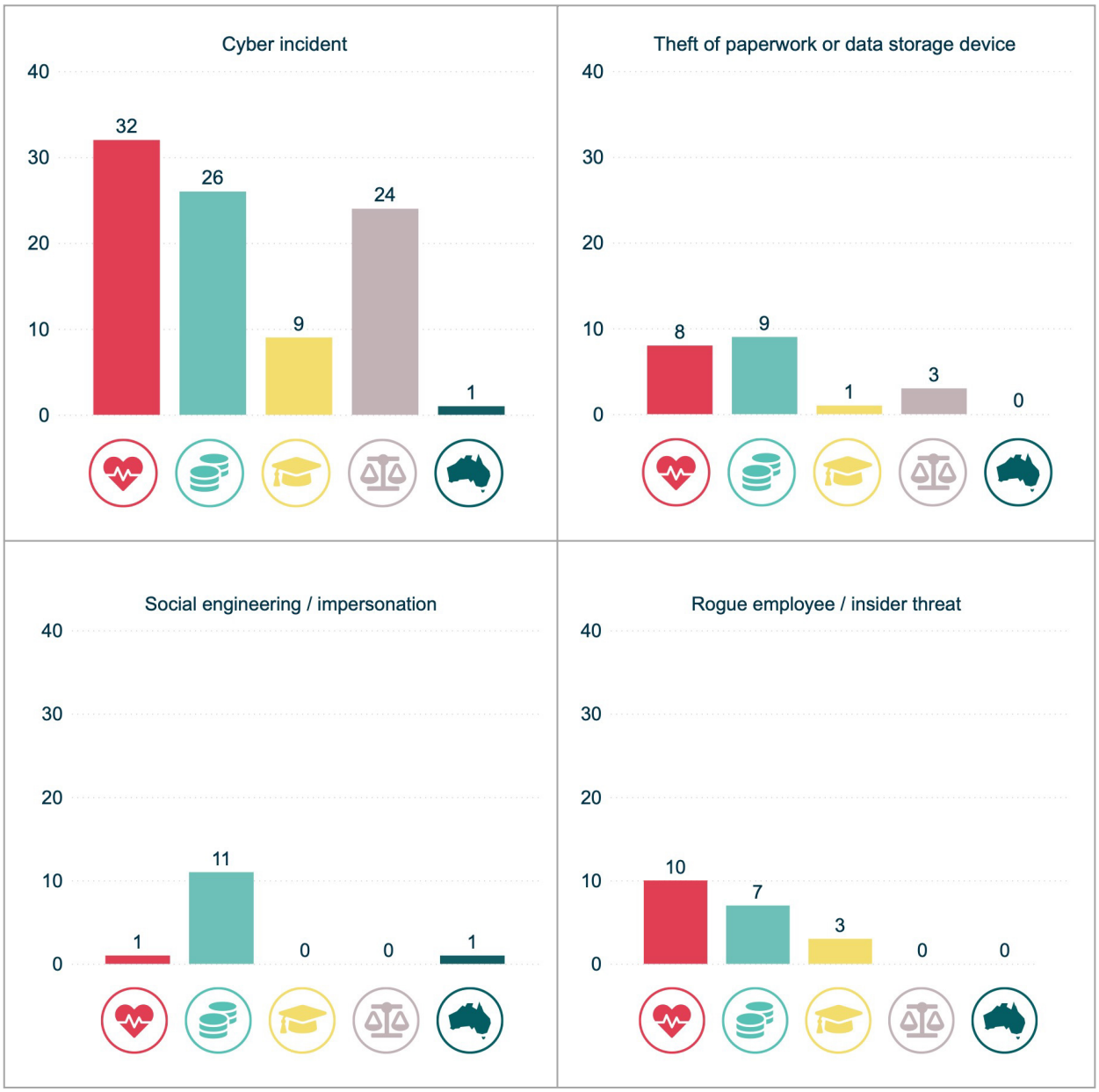
Chart 17 – Source of data breaches – Top 5 industry sectors



Malicious or criminal attack breaches – Top 5 industry sectors

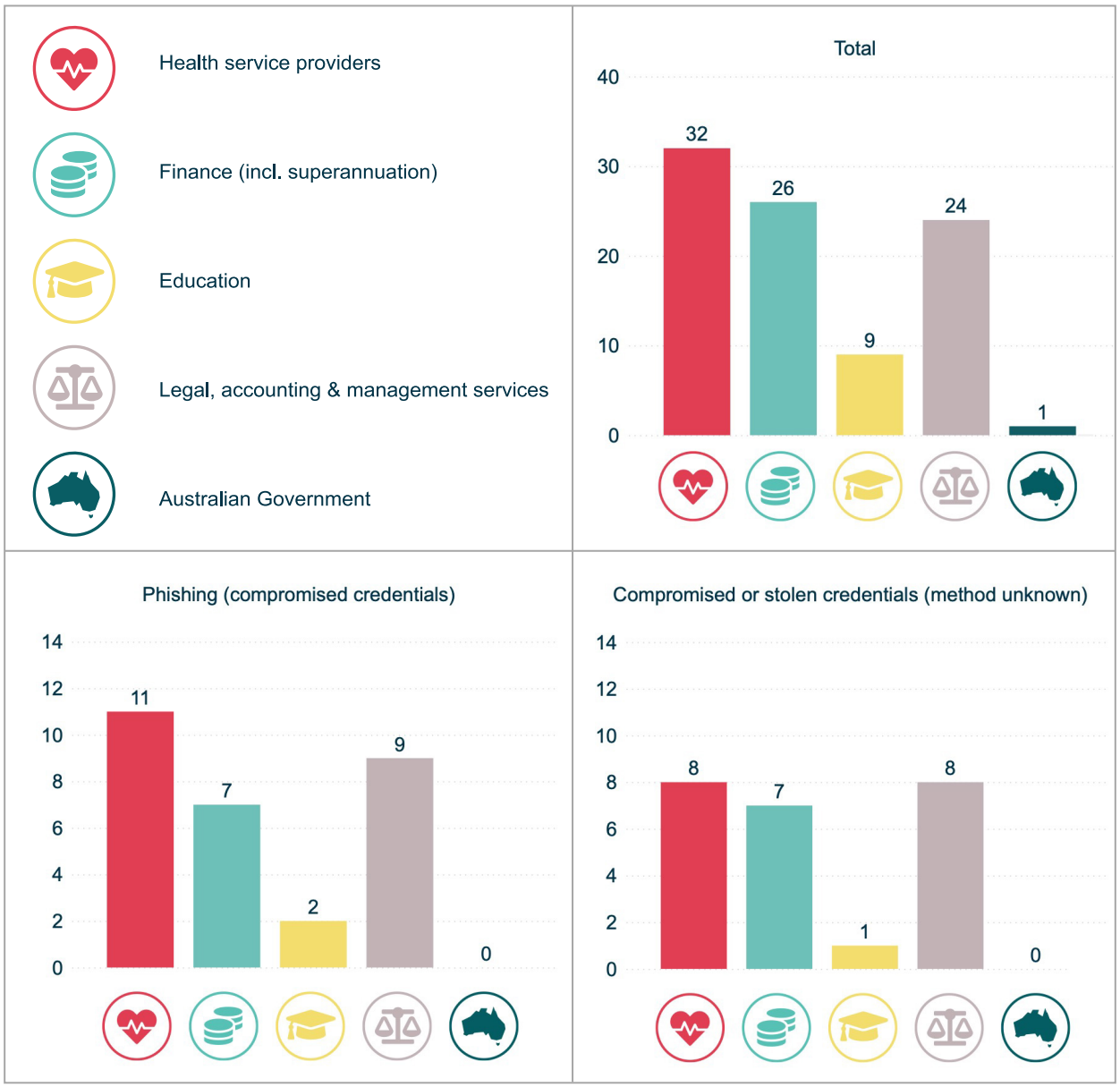
Chart 18 – Malicious or criminal attacks breakdown – Top 5 industry sectors




Cyber incident
40
30
20
10
0
32
26
9
24
1
Theft of paperwork or data storage device
40
30
20
10
0
8
9
1
3
0
Social engineering / impersonation
40
30
20
10
0
1
11
0
0
1
Rogue employee / insider threat
40
30
20
10
0
10
7
3
0
0

Cyber incident breaches – Top 5 industry sectors

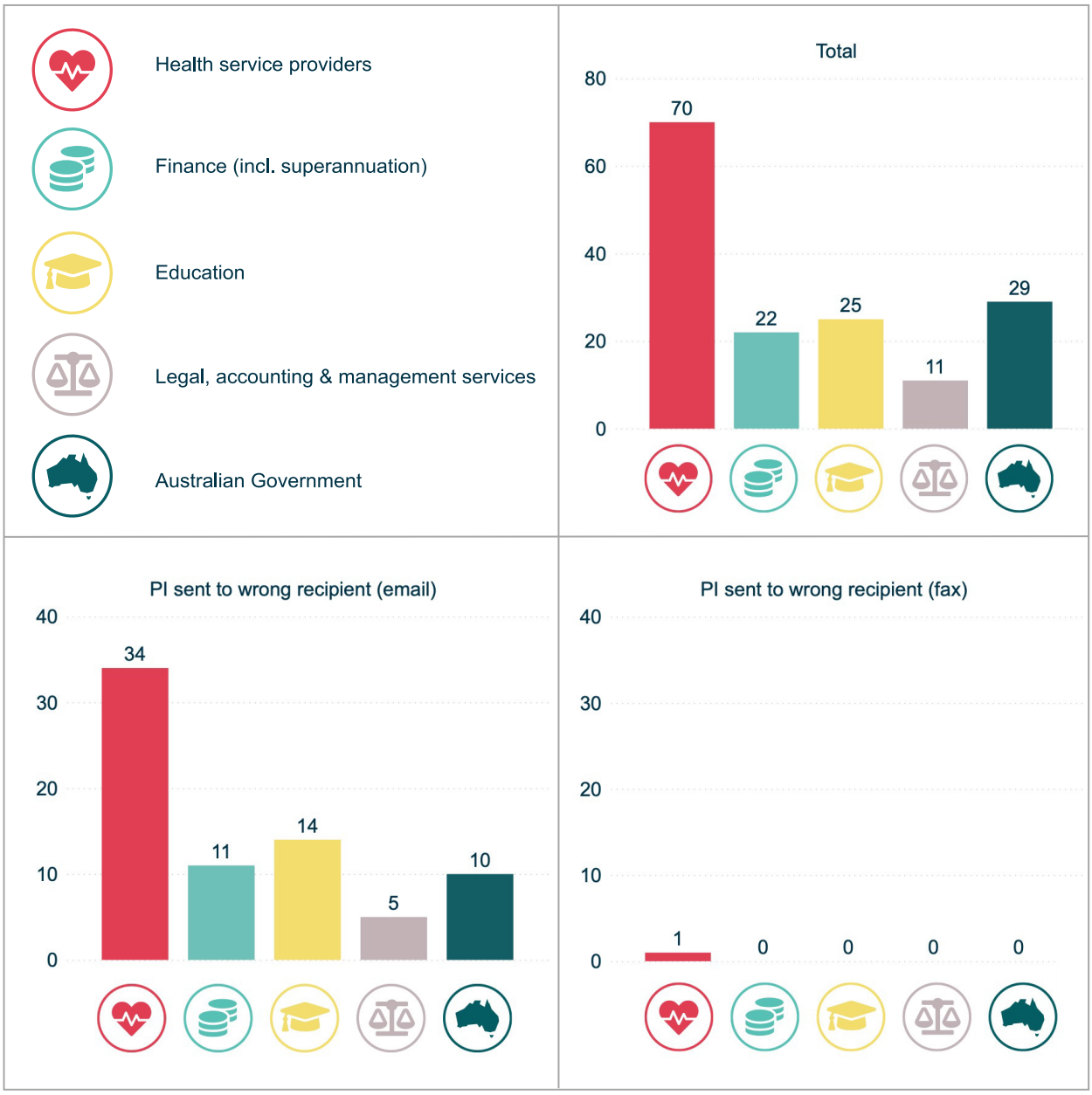
Chart 19 – Cyber incident breakdown – Top 5 industry sectors

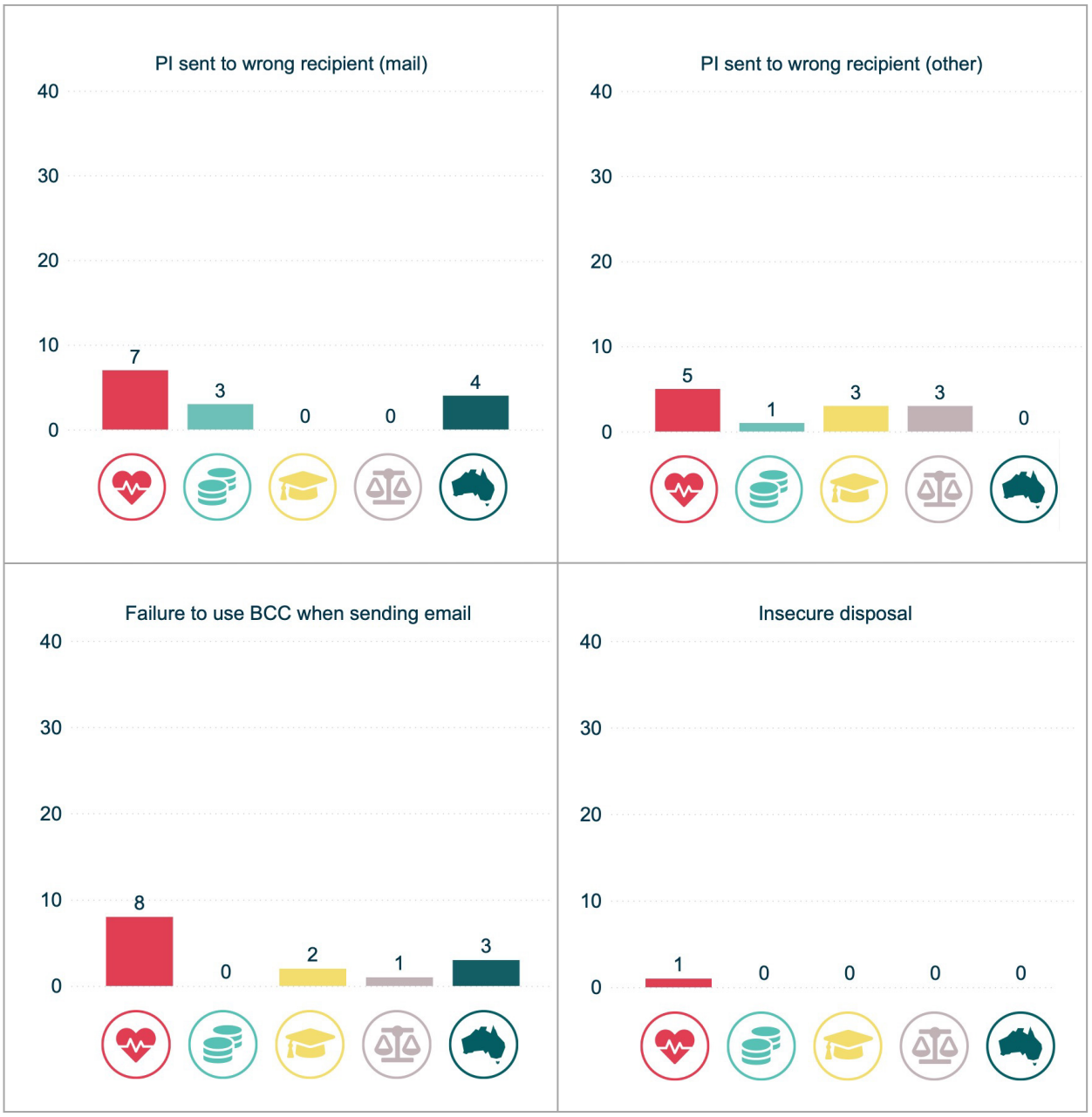


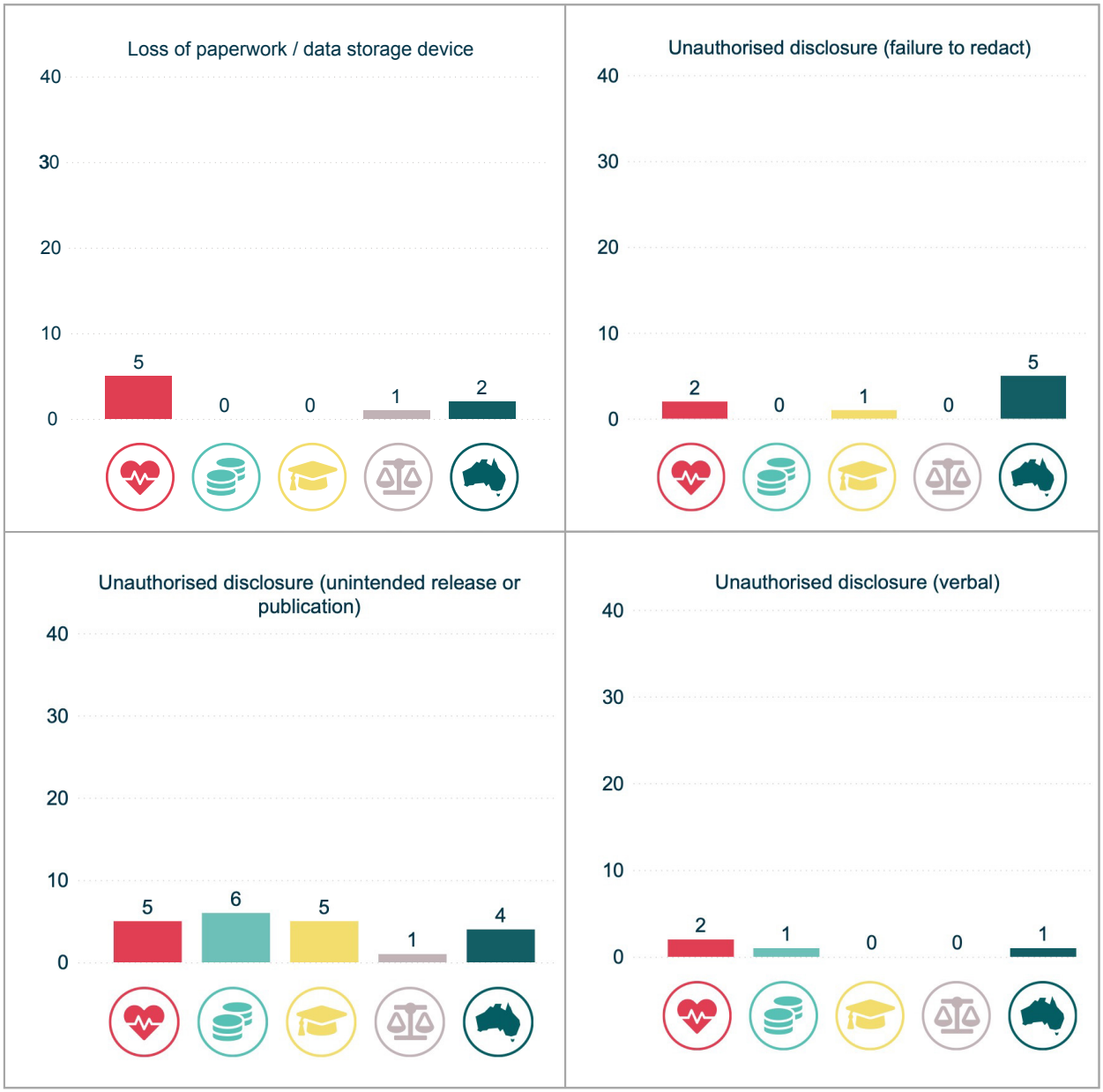
Note: Cyber incidents categorised as 'Other' are included in the total.

Human error breaches – Top 5 industry sectors

Chart 20 – Human error breakdown – Top 5 industry sectors




PI sent to wrong recipient (mail)
40
30
20
10
0
7
3
0
0
4
PI sent to wrong recipient (other)
40
30
20
10
0
5
1
3
3
0
Failure to use BCC when sending email
40
30
20
10
0
8
0
2
1
3
Insecure disposal
40
30
20
10
0
1
0
0
0
0

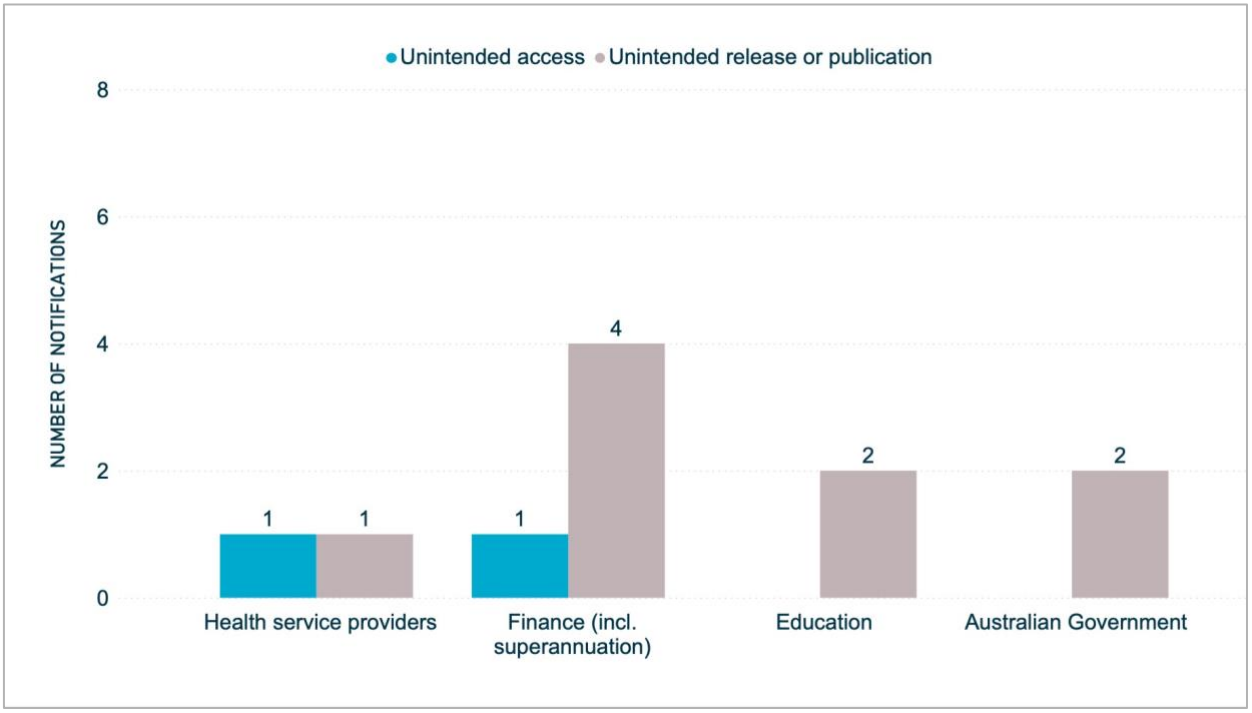

Loss of paperwork / data storage device
40
30
20
10
0
5
0
0
1
2
Unauthorised disclosure (failure to redact)
40
30
20
10
0
2
0
1
0
5
Unauthorised disclosure (unintended release or publication)
40
30
20
10
0
5
6
5
1
4
Unauthorised disclosure (verbal)
40
30
20
10
0
2
1
0
0
1

System fault breaches – Top 5 industry sectors

Four of the top 5 industry sectors notified breaches resulting from a system fault.

The majority of system fault breaches reported by the top 5 industry sectors involved the unintended release or publication of personal information (9 notifications). Of the top 5 industry sectors, the finance sector reported the most data breaches resulting from system faults.

Chart 21 – System fault breakdown – Top 5 industry sectors



Note: The legal, accounting and management services sector did not report any breaches caused by a system fault.

Glossary

Breach categories

Term	Definition
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
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

Term	Definition
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
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
Malware	Software that is specifically designed to disrupt, damage, or gain unauthorised access to a computer system
Ransomware	A type of malicious software designed to block access to data or a computer system until a sum of money is paid or other conditions are met
Phishing (compromised credentials)	An attack in which the target is contacted by email or text message by someone posing as a legitimate institution to lure individuals into providing personal information, sensitive information or passwords
Brute-force attack (compromised credentials)	Automated software is used to generate a large number of consecutive guesses as to the value of the desired data, for example passwords
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown
Hacking (other means)	Exploiting a software or security weakness to gain access to a system or network, other than by way of phishing, brute-force attack or malware
Business email compromise	Business email compromise is a scam where a criminal sends an email message that appears to come from a known source making legitimate request, such as request for payment of invoice or bank transfer
System fault	A business or technology process error not caused by direct human error

Other terminology used in this report and in the NDB Form[11]

Term	Definition/ examples
Personal information (PI)	Information or an opinion about an identified individual, or an individual who is reasonably identifiable
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

[11] OAIC's Notifiable Data Breach Form