Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Report

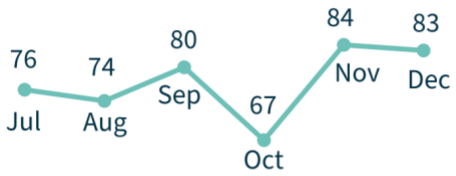
July to December 2021

22 February 2022

OAIC

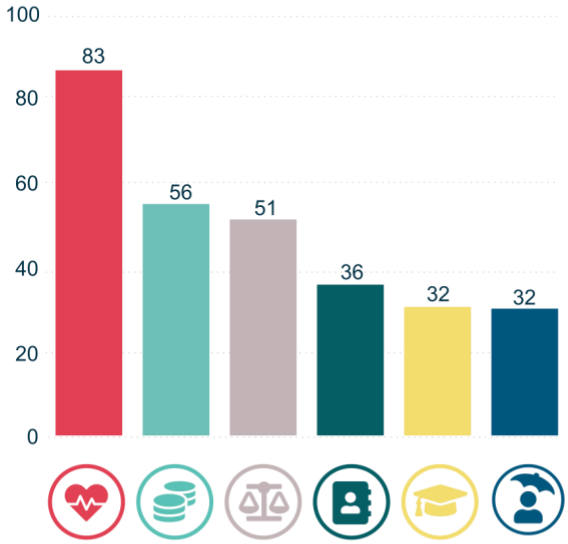
Snapshot

464
notifications
Up 6%



Top industry sectors to notify data breaches

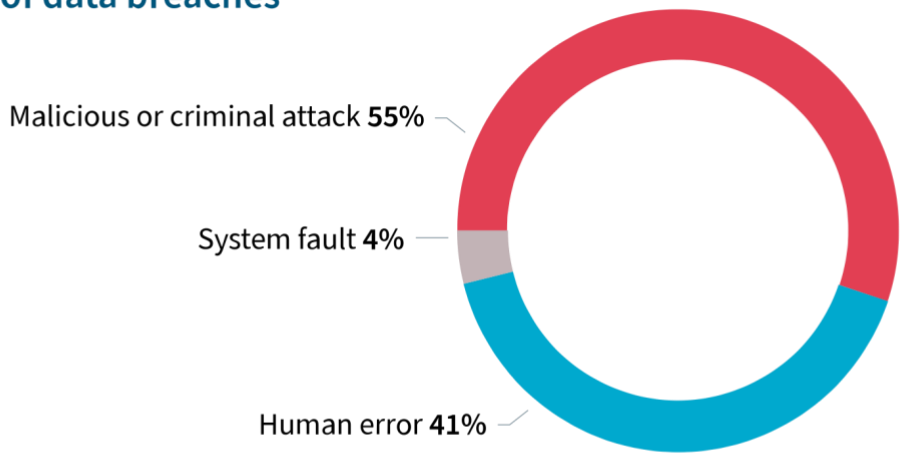
- Health service providers
- Finance
- Legal, accounting & management services
- Personal services
- Education
- Insurance



71%

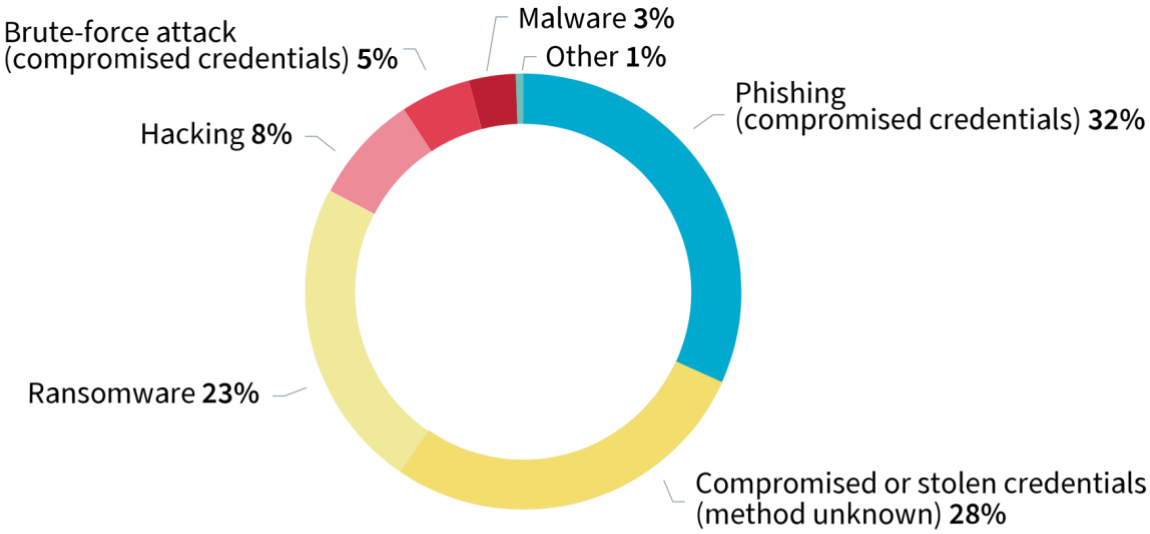
of data breaches affected 100 people or fewer

Sources of data breaches



37% of all data breaches resulted from cyber security incidents (173 notifications)

Cyber incident breakdown



Top causes of human error breaches

- Personal information emailed to wrong recipient **43%**
- Unintended release or publication **21%**
- Loss of paperwork or data storage device **8%**

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 the operation of the scheme. This report captures notifications made under the NDB scheme from **1 July to 31 December 2021**.

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

Figures in charts may not add up to a total of 100% due to the rounding up or down of the percentages for each category.

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.

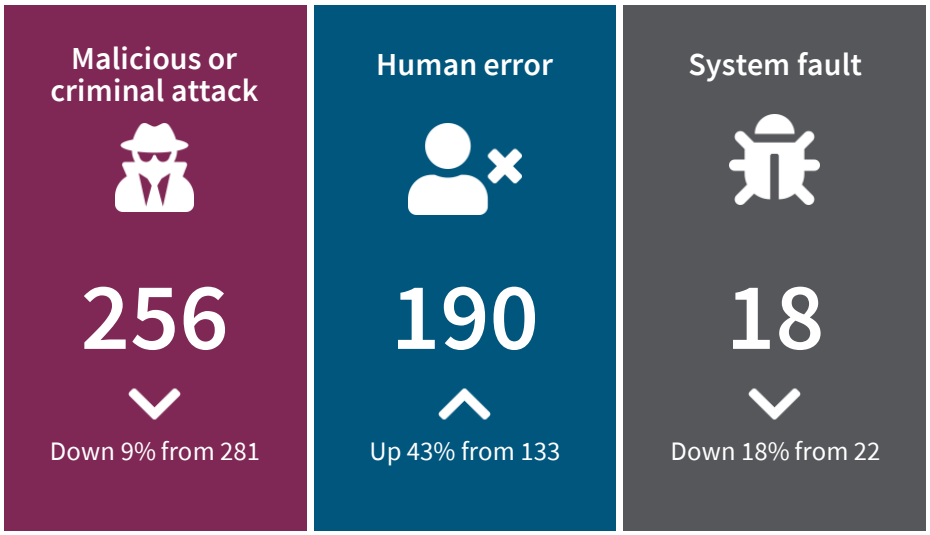
Notifications made under the *My Health Records Act 2012* are not included as they are subject to specific notification requirements set out in that Act.

NDB scheme statistics in this report are current as of 24 January 2022. However, a number of notifications included in these statistics are 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 July 2021 in this report may differ from statistics in previous NDB 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 highlight emerging issues and areas for ongoing attention by regulated entities.



Key findings for the July to December 2021 reporting period:

- 464 breaches were notified under the scheme, an increase of 6% compared with 436 notifications in January to June 2021.
- Malicious or criminal attacks remain the leading source of breaches, accounting for 256 notifications (55% of the total), down 9% in number from 281.
- Data breaches resulting from human error accounted for 190 notifications (41% of the total), up 43% in number from 133.
- The health sector remains the highest reporting industry sector notifying 18% of all breaches, followed by finance (12%).
- Contact information remains the most common type of personal information involved in breaches.
- 96% of breaches affected 5,000 individuals or fewer, while 71% affected 100 people or fewer.
- 75% of entities notified the OAIC within 30 days of becoming aware of an incident.

Notifications received July to December 2021 – All sectors

The OAIC received 464 notifications this reporting period. This is a 6% increase compared with the previous 6 months.

There was less variation from month to month in the number of notifications received compared with the previous reporting period. The lowest monthly total was 67 notifications in October and the highest was 84 notifications in November.

Table 1 – Notifications received in 2021

Reporting period	Total no. of notifications
January to June 2021	436
July to December 2021	464
2021	**900**

Chart 1 – Notifications received by month from January 2020 to December 2021

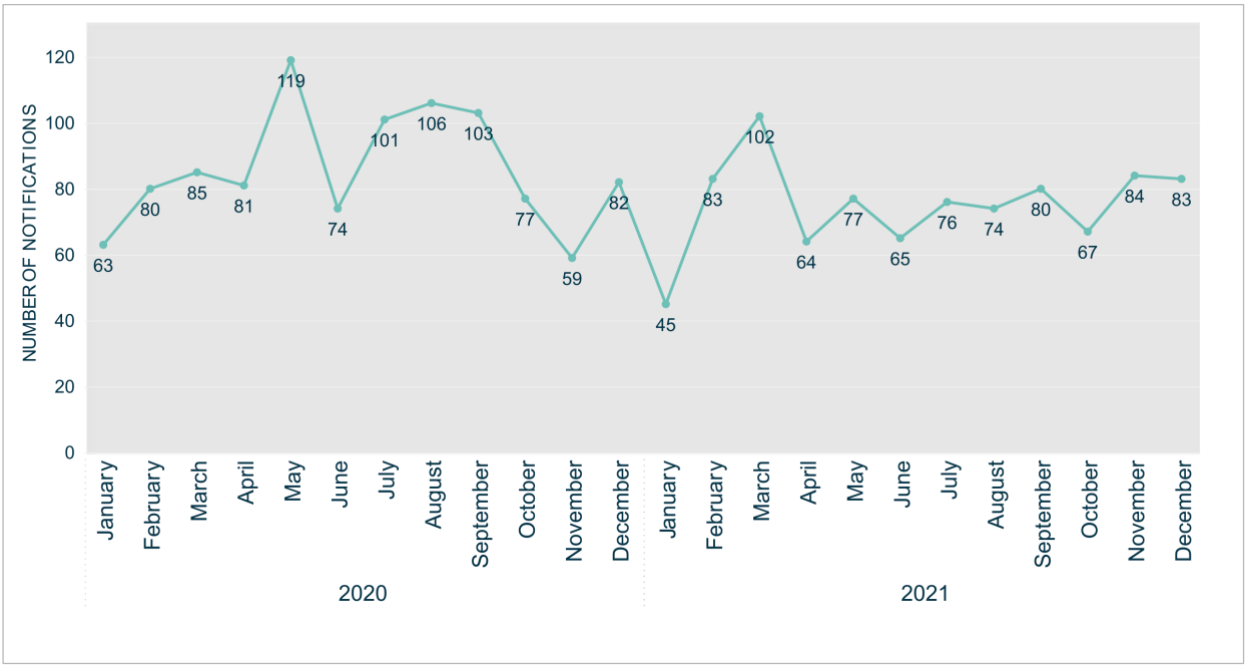
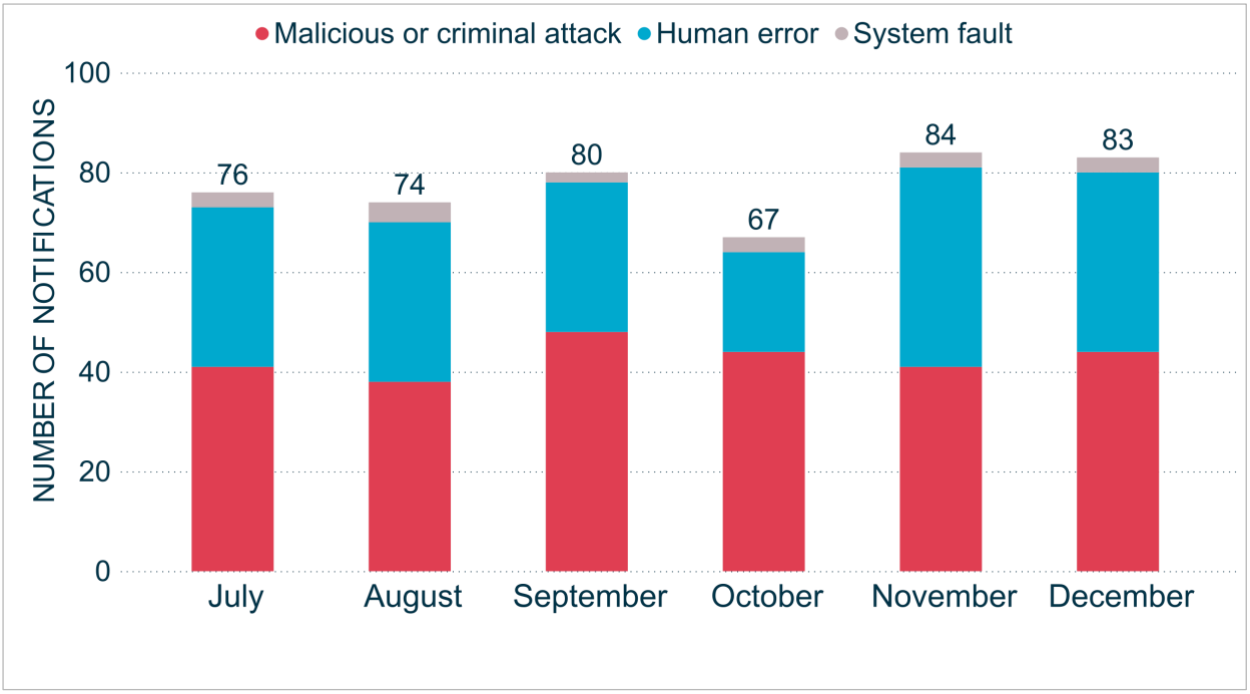


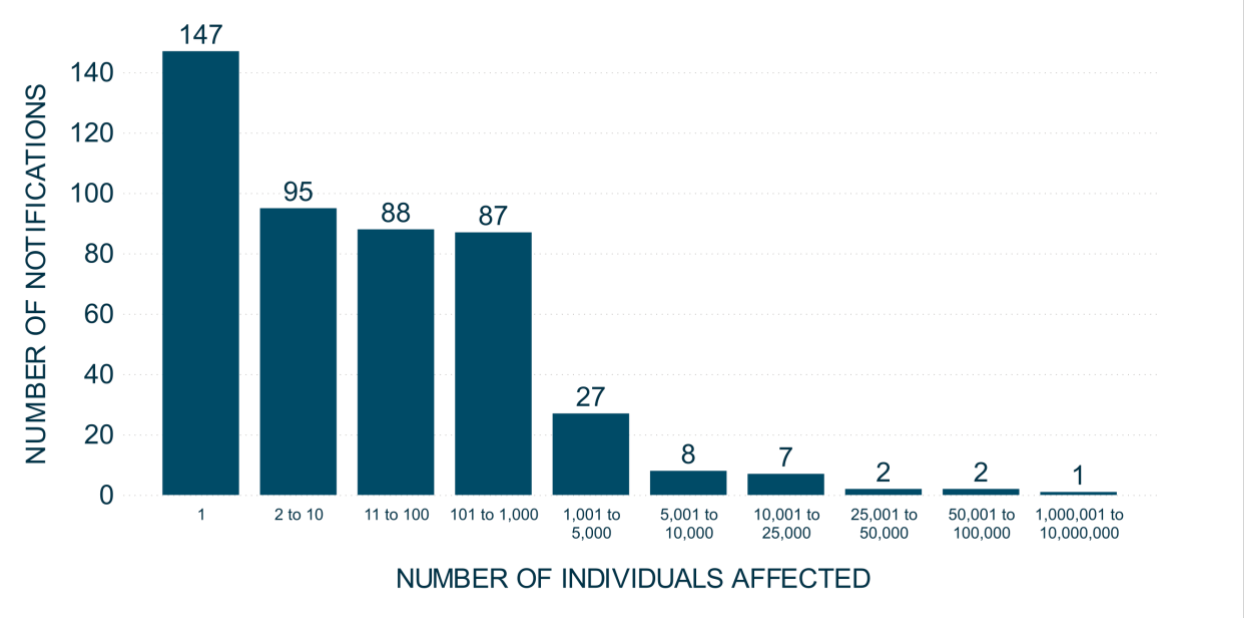
Chart 2 – Notifications received by month showing the sources of breaches



Number of individuals affected by breaches

Consistent with previous reports, most data breaches (96%) involved the personal information of 5,000 individuals or fewer. Breaches affecting 100 individuals or fewer comprised 71% of notifications and breaches affecting between 1 and 10 individuals accounted for 52% of notifications.

Chart 3 – Number of individuals affected by breaches



Note: These figures reflect the number of individuals worldwide whose personal information was compromised in these data breaches, as estimated by the notifying entities.

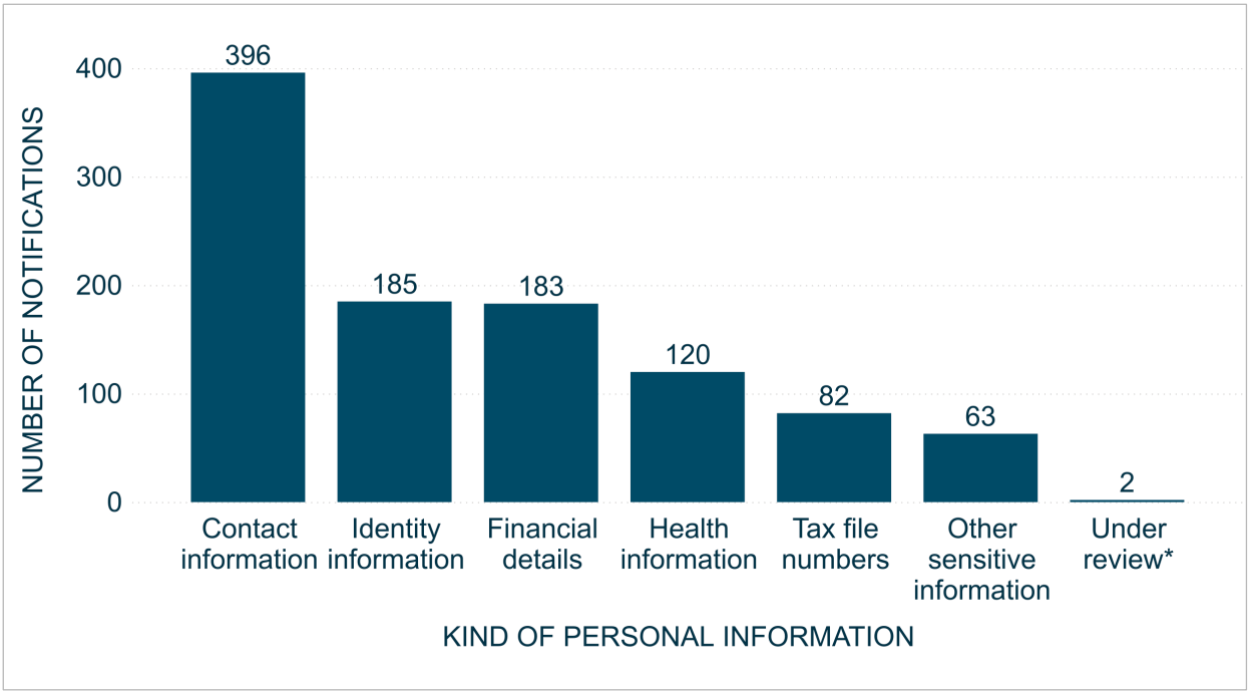
Kinds of personal information involved in breaches

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

Most breaches (85%) 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 40% 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 39% of breaches.

Chart 4 – Kinds of personal information involved in breaches



Note: Data breaches may involve more than one kind of personal information.
* The notifying entity was still conducting its assessment of the breach, including the kinds of personal information involved, at the time it notified the OAIC.

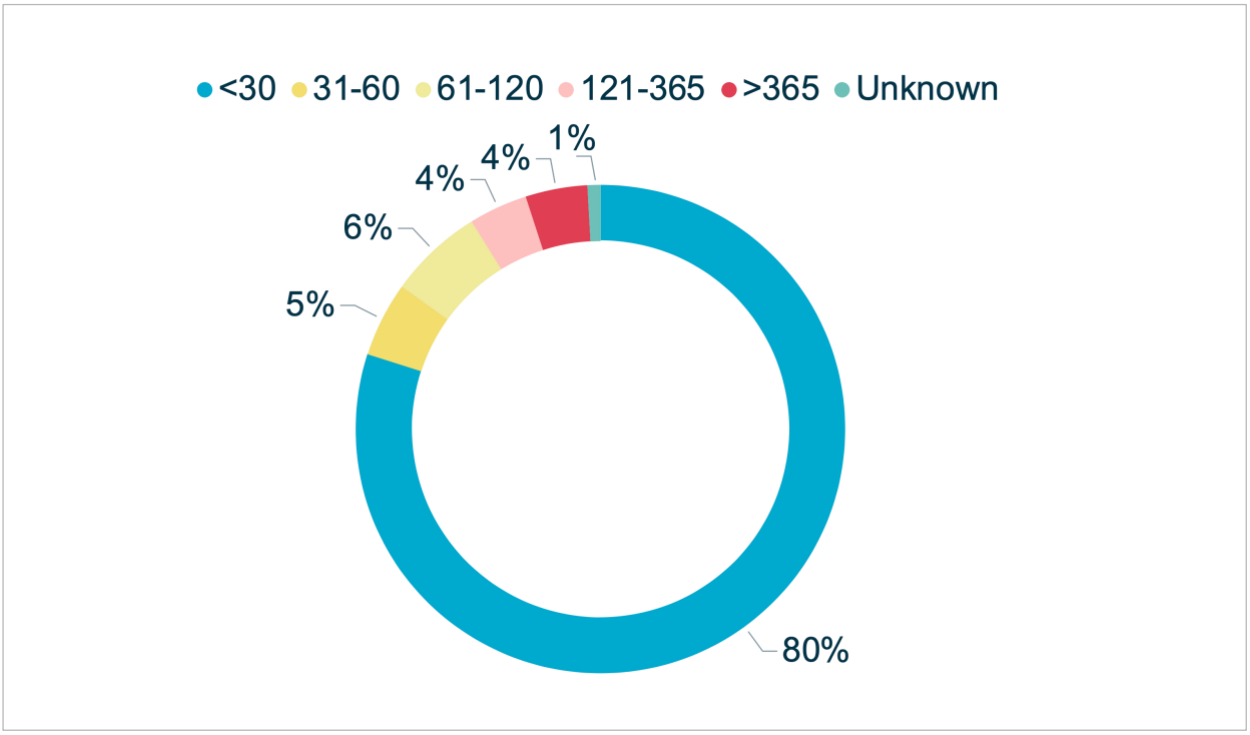
Time taken to identify breaches

As part of complying with Australian Privacy Principle 11, entities should take reasonable steps to ensure they detect data breaches 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.[1]

In the reporting period, 80% of breaches were identified by the entity within 30 days of it occurring, compared with 81% in January to June 2021.

Chart 5 – Days taken to identify breaches

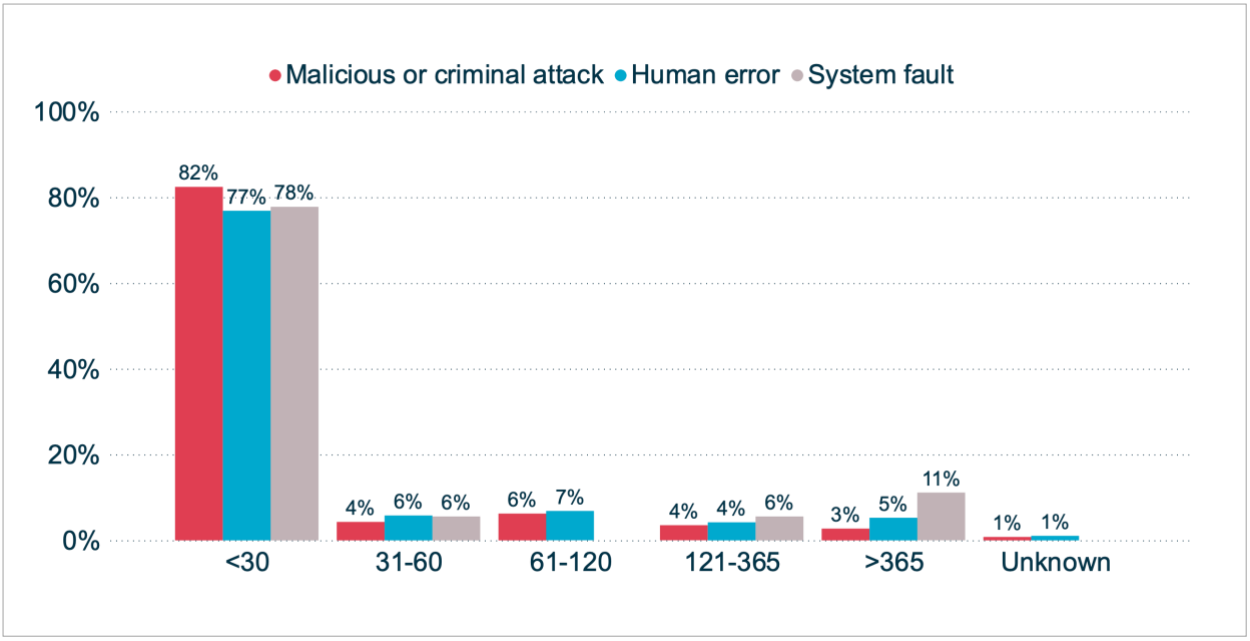


Note: For notifications in the 'Unknown' category, the notifying entity was unable to identify the date the breach occurred.

The time it takes entities to identify data breaches has tended to vary significantly depending on the source of the breach. There was less variation this reporting period, however a notable proportion of entities that experienced system faults (11%) did not become aware of the incident for over a year.

[1] 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



Note: 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

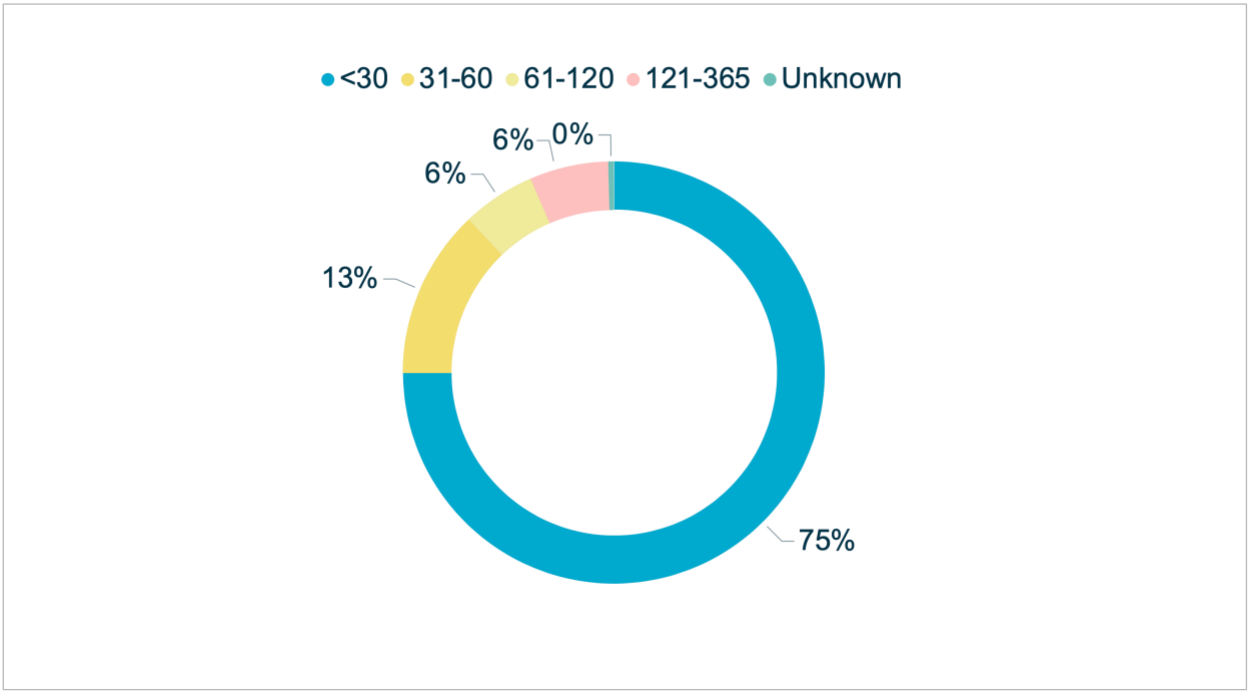
A key objective of the NDB scheme is to protect individuals by enabling them to respond quickly to a data breach to mitigate the risk of harm. Delays in assessment and notification reduce the opportunities for an individual to take steps to prevent harm.

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, 75% of entities notified the OAIC within 30 days of becoming aware of an incident, compared with 72% in the previous period. Twenty-eight 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. This approach gives individuals the ability to take timely steps to protect themselves from harm. In others, there was a delay between when the entity notified the OAIC and when they notified individuals.

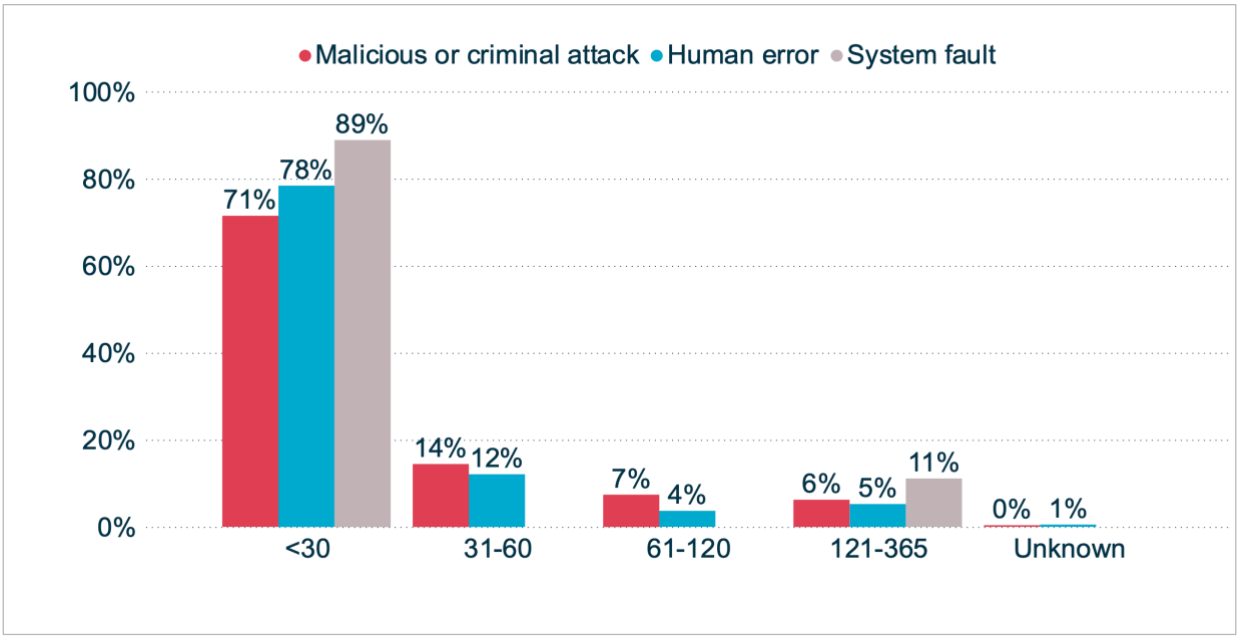
Chart 7 – Days taken to notify the OAIC of breaches



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

There was some variance by source of breach in the time taken to notify the OAIC after an incident was identified. For system fault breaches, 89% of entities notified the OAIC within 30 days compared with 78% for human error breaches and 71% for breaches caused by malicious or criminal attacks.

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



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

Delayed and partial notifications

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

- take all reasonable steps to complete its assessment of whether an incident amounts to an eligible data breach within 30 calendar days
- notify the OAIC and affected individuals as soon as practicable after confirming there are reasonable grounds to believe an eligible data breach occurred.

As the risk of serious harm to individuals often increases with time, the OAIC expects that, where possible, entities treat the 30 days as a maximum time limit and try to complete the assessment in a much shorter timeframe.

Where an entity has taken over 30 days to complete its assessment, the entity should be able to provide an explanation to the OAIC for the delay.

The NDB scheme does not require entities to notify the OAIC of a data breach incident on a preliminary basis. Notifying the OAIC on a preliminary basis without having undertaken an appropriate assessment does not discharge an entity's obligation to take steps to ensure the assessment is completed within 30 days.

The scheme provides 3 options for notification to individuals. An entity may:

- notify each individual whose personal information has been involved in the eligible data breach
- notify only individuals who are at risk of serious harm
- if neither of these options are practicable, publish a statement on the eligible data breach on its website and publicise the statement.

Notifications must contain recommendations about steps individuals should take in response to the breach. The entity can tailor the recommended steps in its notification to individuals or provide general recommendations that apply to all individuals. The OAIC does not consider that tailoring notifications justifies delay in notifying affected individuals.

Scenario

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

The entity's preliminary review of the contents of the compromised email account indicated that the account contained a large quantity of personal information, ranging from contact information to clients' bank account details and picture copies of their driver licences and/or passports.

As the mailbox contained a large amount of documents, the entity determined it would take over 5 months to conduct a manual review of all documents contained in the mailbox to identify and tailor notifications to each individual at risk of serious harm.

On this basis, rather than taking additional time to tailor its notifications, the entity proceeded to promptly notify all affected individuals, providing general recommendations that applied to everyone whose personal information was contained in the mailbox.

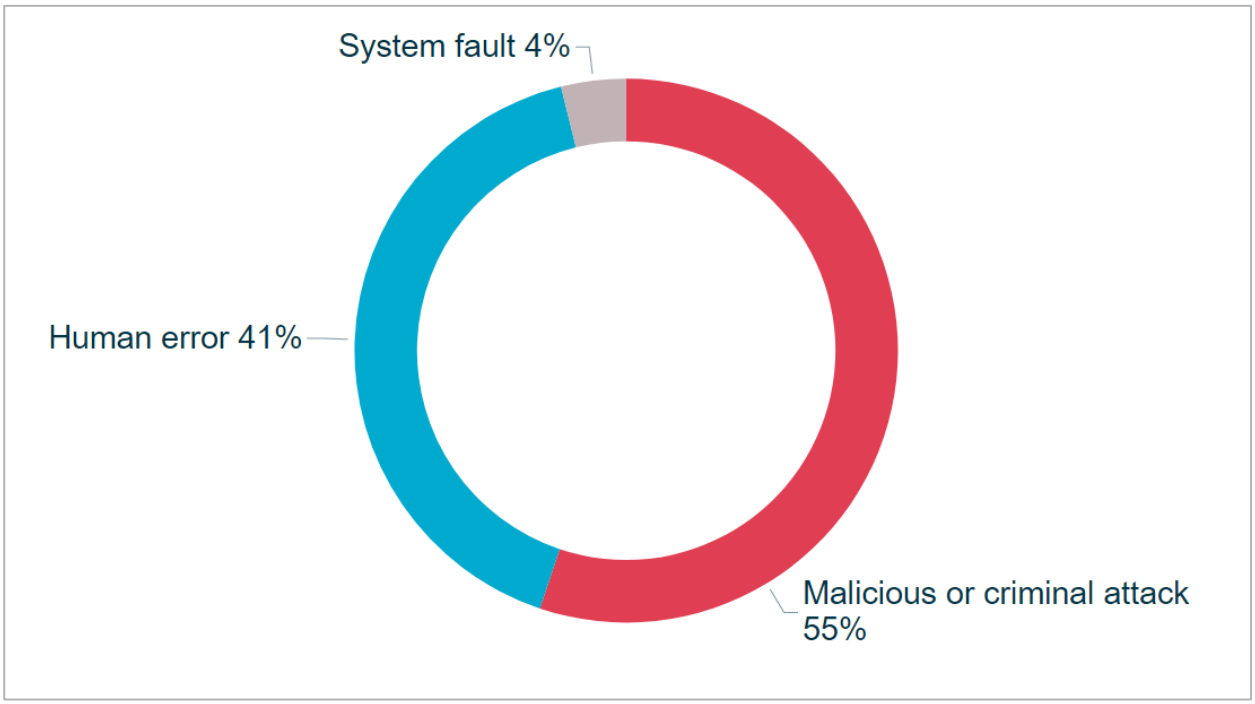
Source of breaches

Consistent with previous reports, malicious or criminal attacks were the largest source of data breaches notified to the OAIC, accounting for 256 breaches.

Human error remained a major source of breaches, accounting for 190 notifications, up from 133 notifications in the previous period.

System faults accounted for the remaining 18 breaches, down from 22.

Chart 9 – Source of data breaches



Malicious or criminal attack breaches

The number of breaches attributed to a malicious or criminal attack decreased by 9% from 281 notifications to 256, while the proportion of total breaches caused by malicious or criminal attack decreased from 64% to 55%.

The majority of breaches (68%) in this category involved cyber incidents (173 notifications). The remaining 32% of breaches resulted from social engineering or impersonation (30 notifications), theft of paperwork or data storage device (27 notifications) and actions taken by a rogue employee or insider threat (26 notifications).

Chart 10 – Malicious or criminal attacks

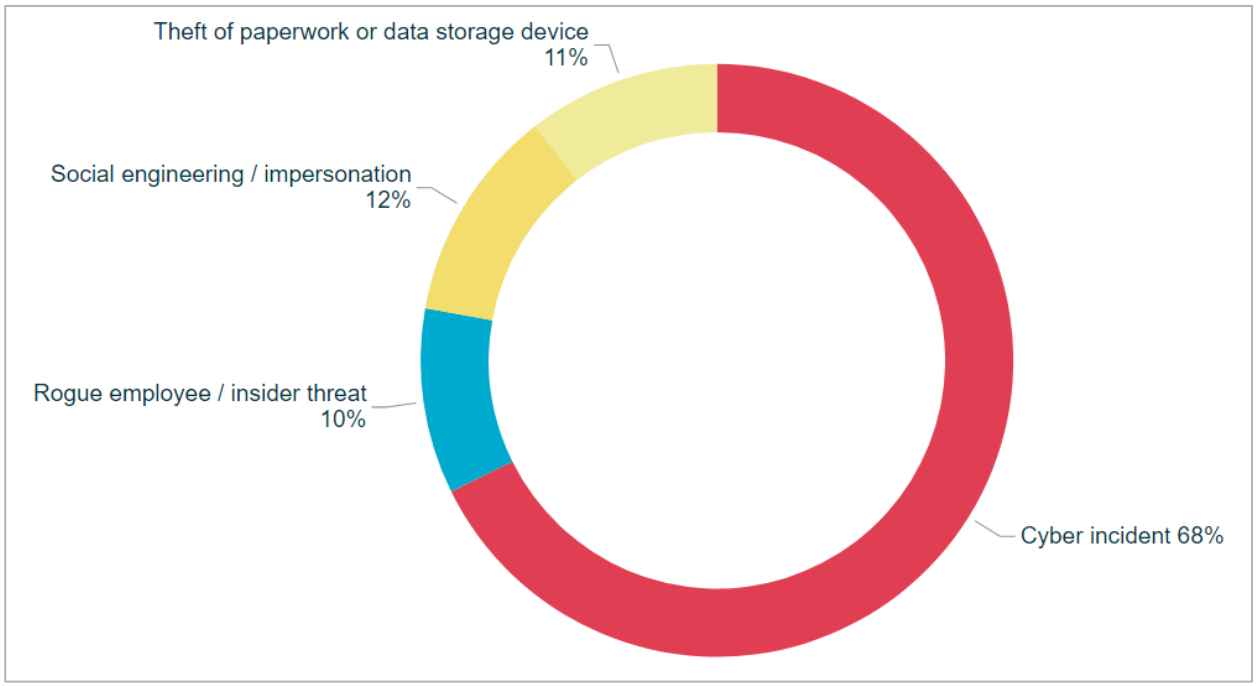
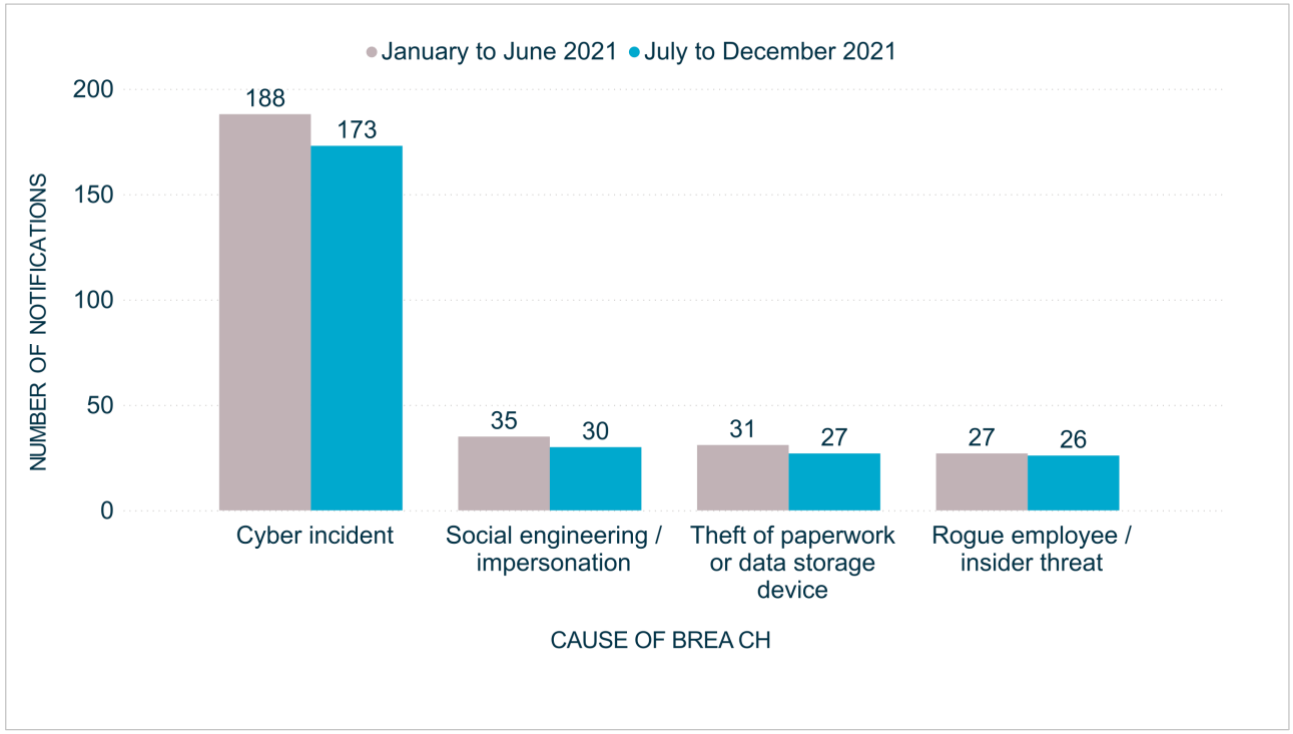


Chart 11 – Breaches resulting from malicious or criminal attacks



Assessing the risk of serious harm

The question of whether 'serious harm' has occurred is central to the NDB scheme.

There is no strict definition of serious harm, however the Privacy Act outlines a range of factors to consider in assessing whether an incident is likely to result in serious harm.

Serious harm may include serious physical, psychological, emotional, financial or reputational harm.

Entities must assess the risk of serious harm holistically and take into account the likelihood of the harm occurring for individuals whose personal information was part of the data breach, as well as the range of factors outlined in section 26WG, including the nature of the harm.

Scenario

A malicious actor gained access to an email account of an organisation after an employee inadvertently entered their login credentials into a fraudulent website.

On investigation, the organisation discovered the malicious actor had used the employee's email account in order to send invoices with fraudulent bank account details to the organisation's clients. This resulted in one client making a payment to a fraudulent bank account.

The organisation's review of the contents of the compromised email account indicated it contained clients' bank account details and picture copies of driver licences and/or passports.

Through undertaking a holistic assessment, the organisation concluded that the data breach would be likely to result in serious harm to an individual whose personal information was contained in the email account, not only the client who made the payment or the clients who received fraudulent invoices, based on:

- the malicious nature of the attack
- the personal information contained in the email account and risk of identity theft or fraud to clients
- the financial impact to at least one of its clients and the likelihood of further financial harm to other clients.

Cyber incident breaches

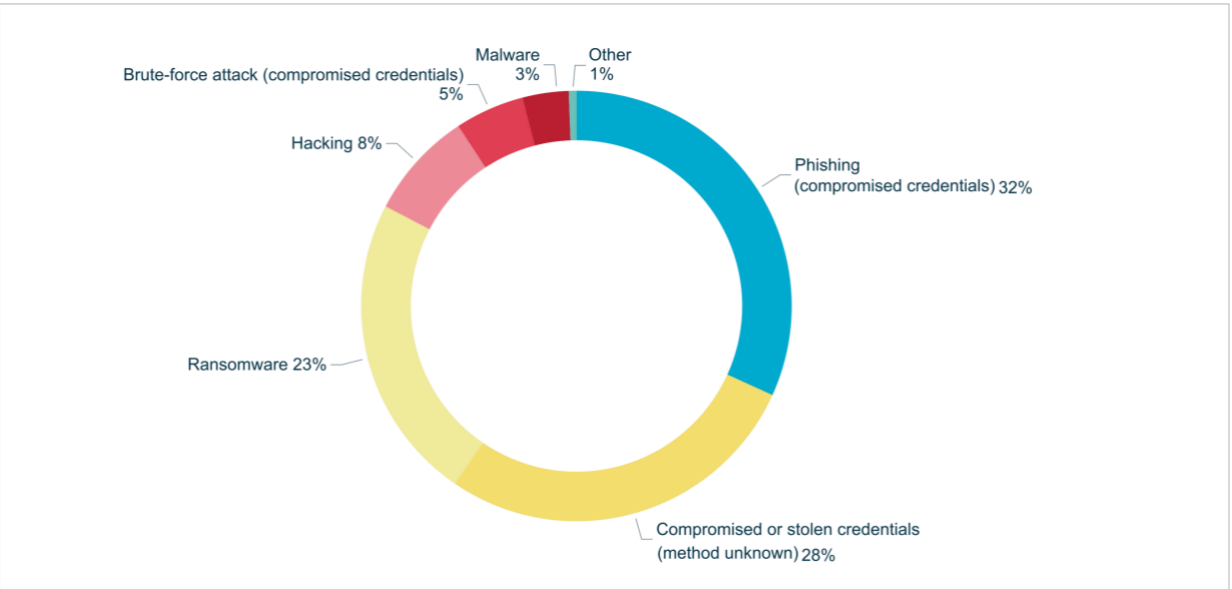
In this reporting period, 37% of all breaches (173 notifications) resulted from cyber security incidents.

The top sources of cyber incidents were phishing (55 notifications), compromised or stolen credentials (method unknown) (48 notifications) and ransomware (40 notifications).

Almost two-thirds (65%) of cyber incidents involved malicious actors gaining access to accounts using compromised or stolen credentials.

Ransomware incidents accounted for 40 notifications, down 11% from 45.

Chart 12 – Cyber incident breakdown

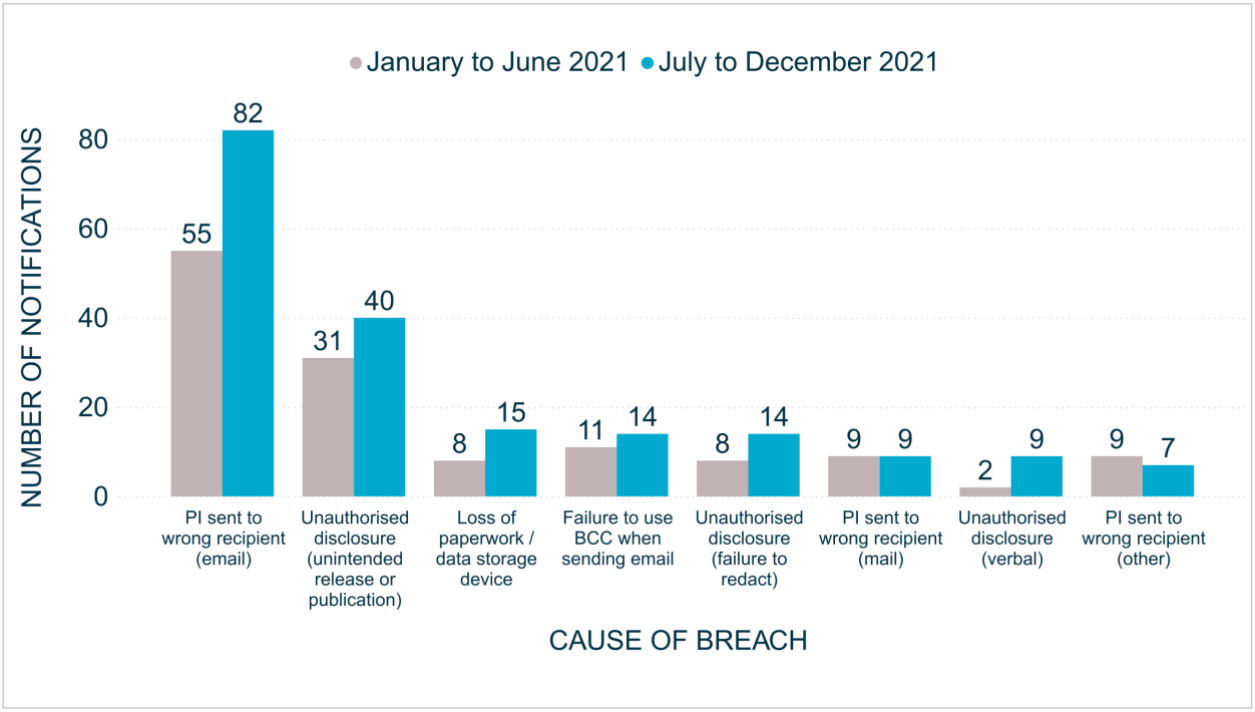


Human error breaches

The reporting period saw a significant increase in human error breaches both in terms of the total number of notifications received – up 43% from 133 to 190 – and proportionally – up from 31% to 41%.

Common examples of human error breaches include emailing personal information to the wrong recipient (43% of human error breaches), unintended release or publication of personal information (21%) and loss of paperwork or data storage device (8%).

Chart 13 – Human error breakdown



Certain human error breaches affect larger numbers of individuals. This reporting period, unintended release or publication affected an average 745 people per breach, while verbal disclosure affected one person on average per breach.

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

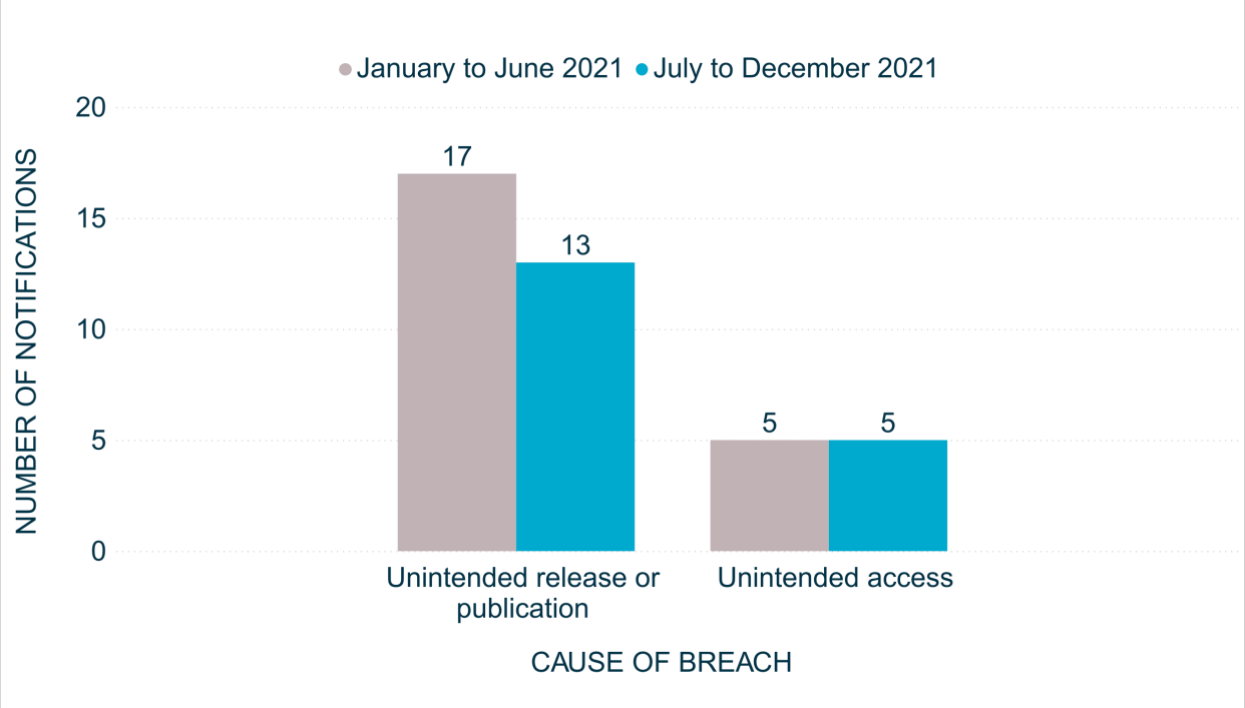
Source of breach	No. of notifications received	Average no. of affected individuals
Unauthorised disclosure (unintended release or publication)	40	745
Failure to use BCC when sending email	14	492
PI sent to wrong recipient (email)	82	196
Loss of paperwork/data storage device	15	12
PI sent to wrong recipient (mail)	9	6
PI sent to wrong recipient (other)	7	3
Unauthorised disclosure (failure to redact)	14	3
Unauthorised disclosure (verbal)	9	1

System fault breaches

System fault breaches include incidents that occur due to a business or technology process error and accounted for 4% 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 13 breaches, while unintended access to personal information because of a system fault caused 5 breaches.

Chart 14 – System fault breakdown



Comparison of top industry sectors

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

Health service providers reported 83 data breaches, or 18% of the total. The second largest source of notifications was the finance sector (12%).

This period saw personal services (8%) and education (7%) return to the top industry sectors by notifications.

Table 3 – Top industry sectors by notifications

Industry sector	Total no. of notifications
Health service providers[2]	83
Finance[3]	56
Legal, accounting & management services	51
Personal services[4]	36
Insurance	32
Education[5]	32

This section compares notifications made under the NDB scheme by these sectors, which accounted for 63% of all notifications.

Time taken to identify breaches – Top industry sectors

Consistent with previous reports, there was some variation by industry sector in the time taken by entities to identify incidents.

In the reporting period, 91% of education providers identified the incident within 30 days of it occurring. This figure was 66% for the insurance sector.

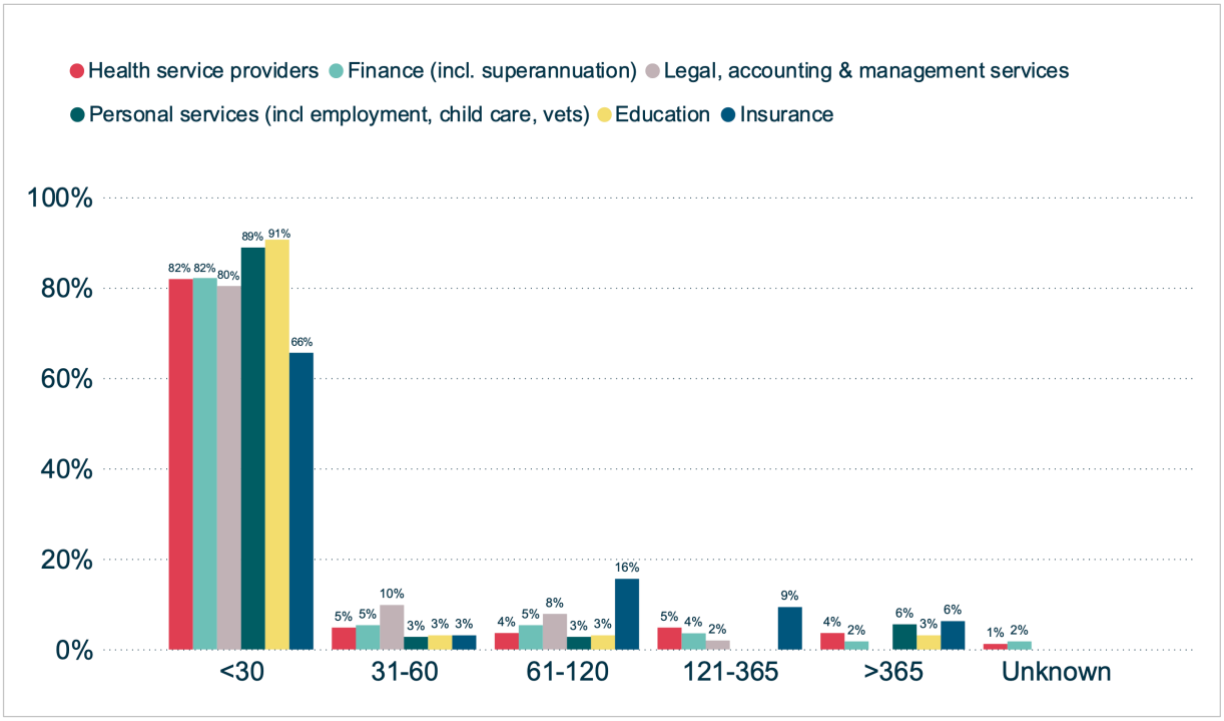
[2] A health service provider generally includes any private sector entity that provides a health service within the meaning of section 6FB of the Privacy Act, regardless of annual turnover.

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

[4] This sector includes employment, training and recruitment agencies, childcare centres, vets and community services.

[5] This sector includes private education providers only.

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



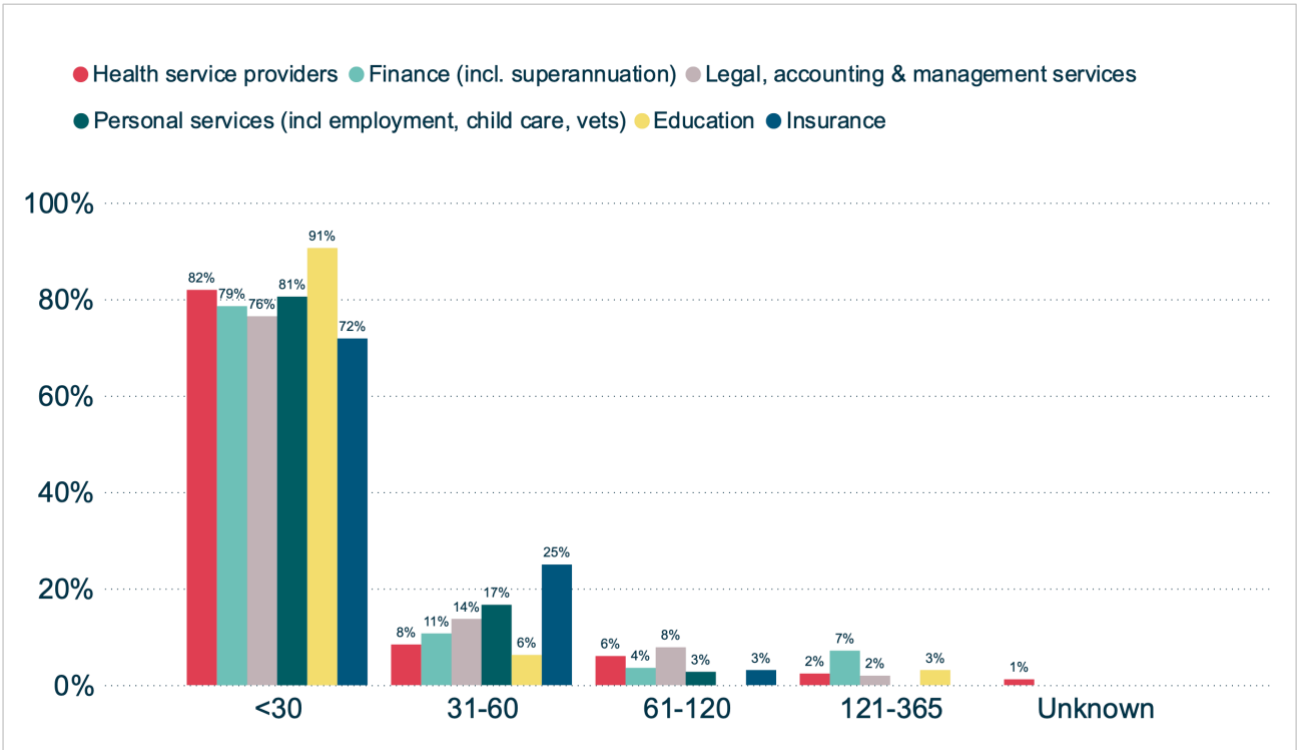
Note: For notifications in the 'Unknown' category, the notifying entity was unable to identify the date the breach occurred.

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

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

Ninety-one per cent of notifications from education providers were made within 30 days of the entity becoming aware of the incident. This figure was 72% for the insurance sector.

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



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

Source of breaches – Top industry sectors

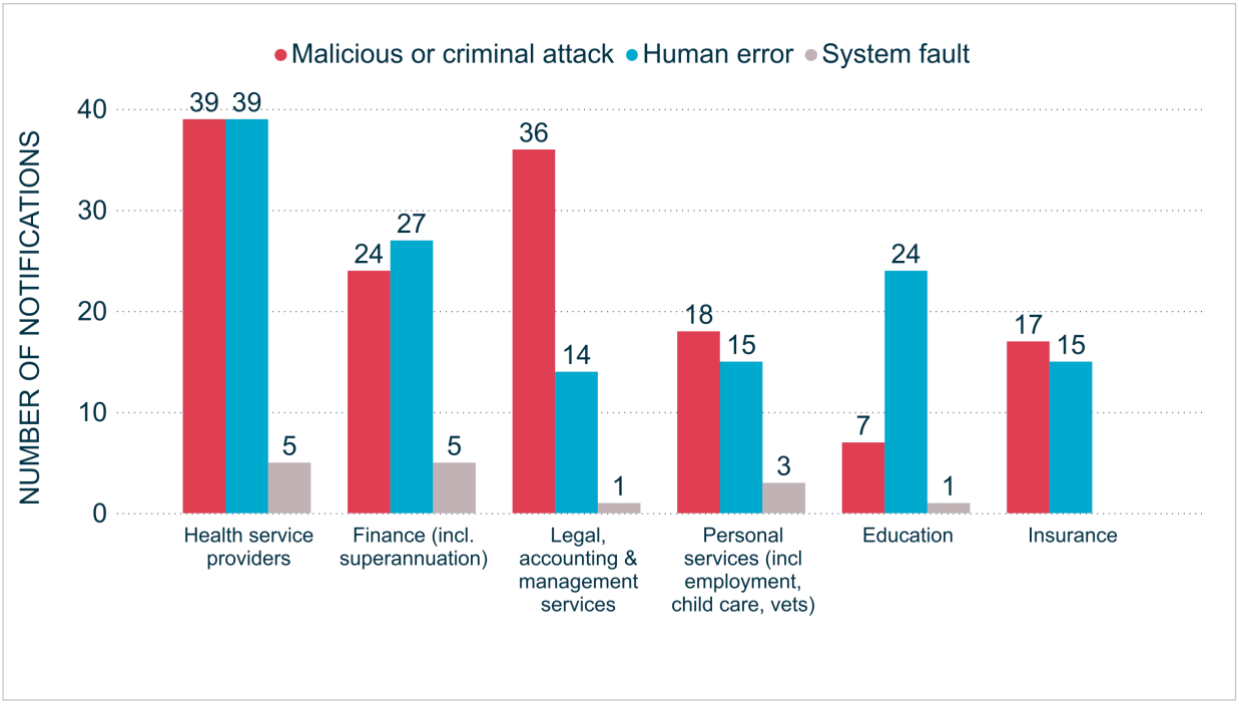
The most common source of data breaches varied for the top industry sectors.

Malicious or criminal attacks were the leading source of breaches for legal, accounting and management services (71%), insurance (53%) and personal services (50%).

Health service providers reported an equal number of breaches resulting from malicious or criminal attack and human error (47% each).

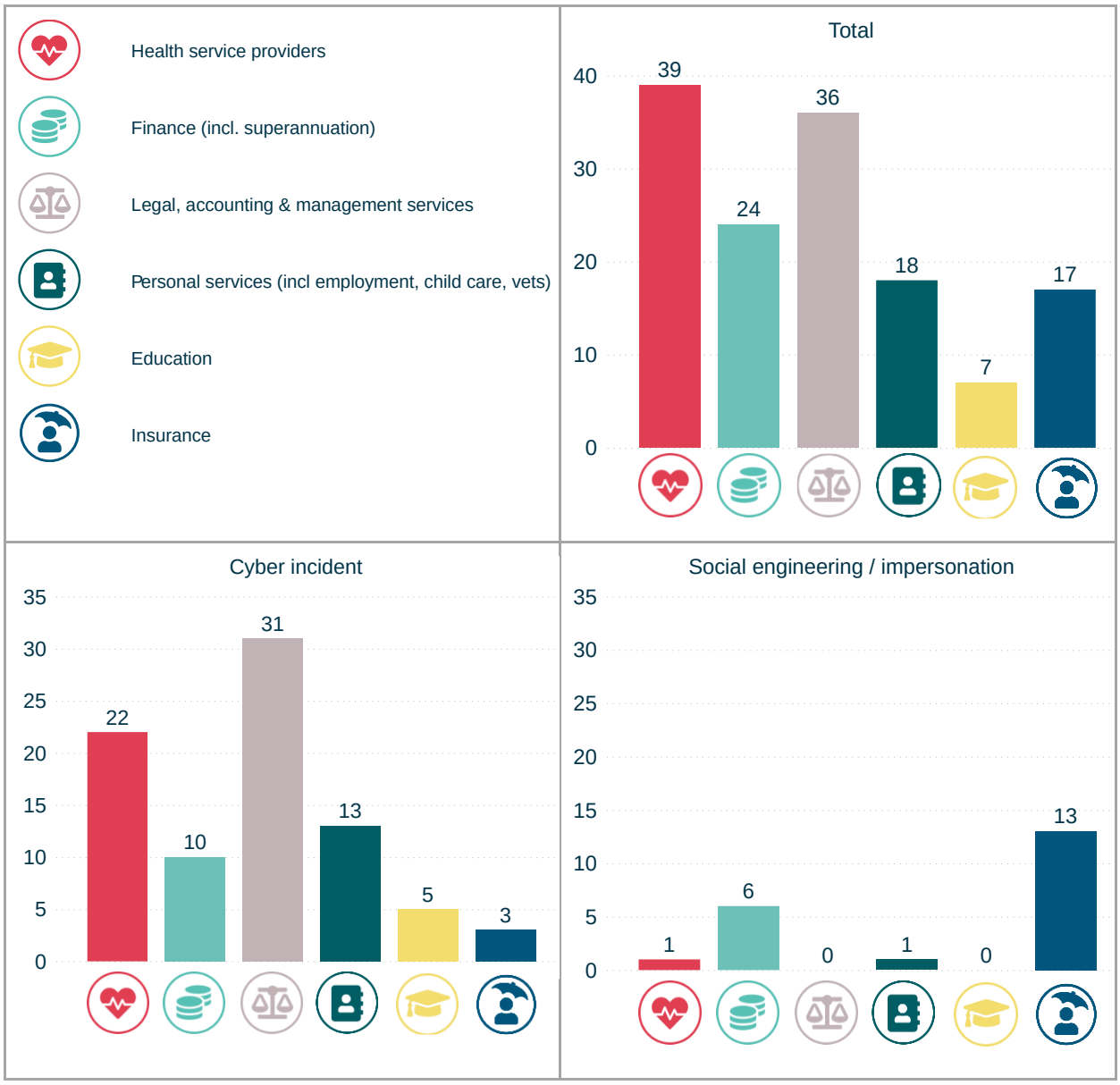
Unlike previous reports, human error was the leading source of breaches for the finance sector (48%). Human error also caused the majority of breaches experienced by education providers (75%).

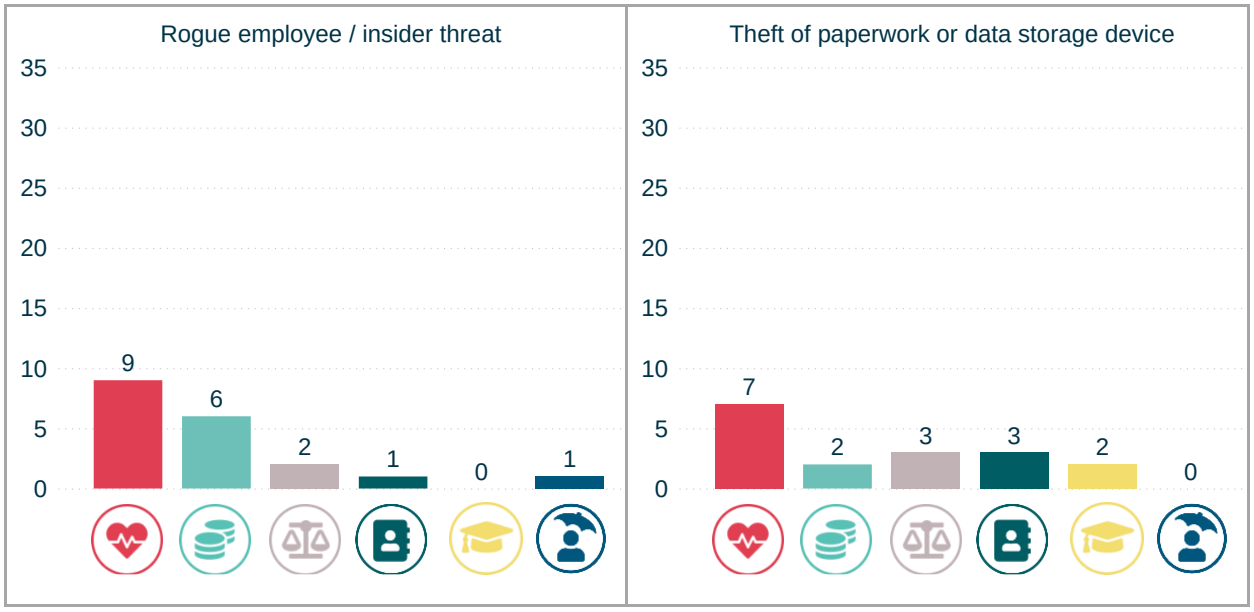
Chart 17 – Source of data breaches – Top industry sectors



Malicious or criminal attack breaches – Top industry sectors

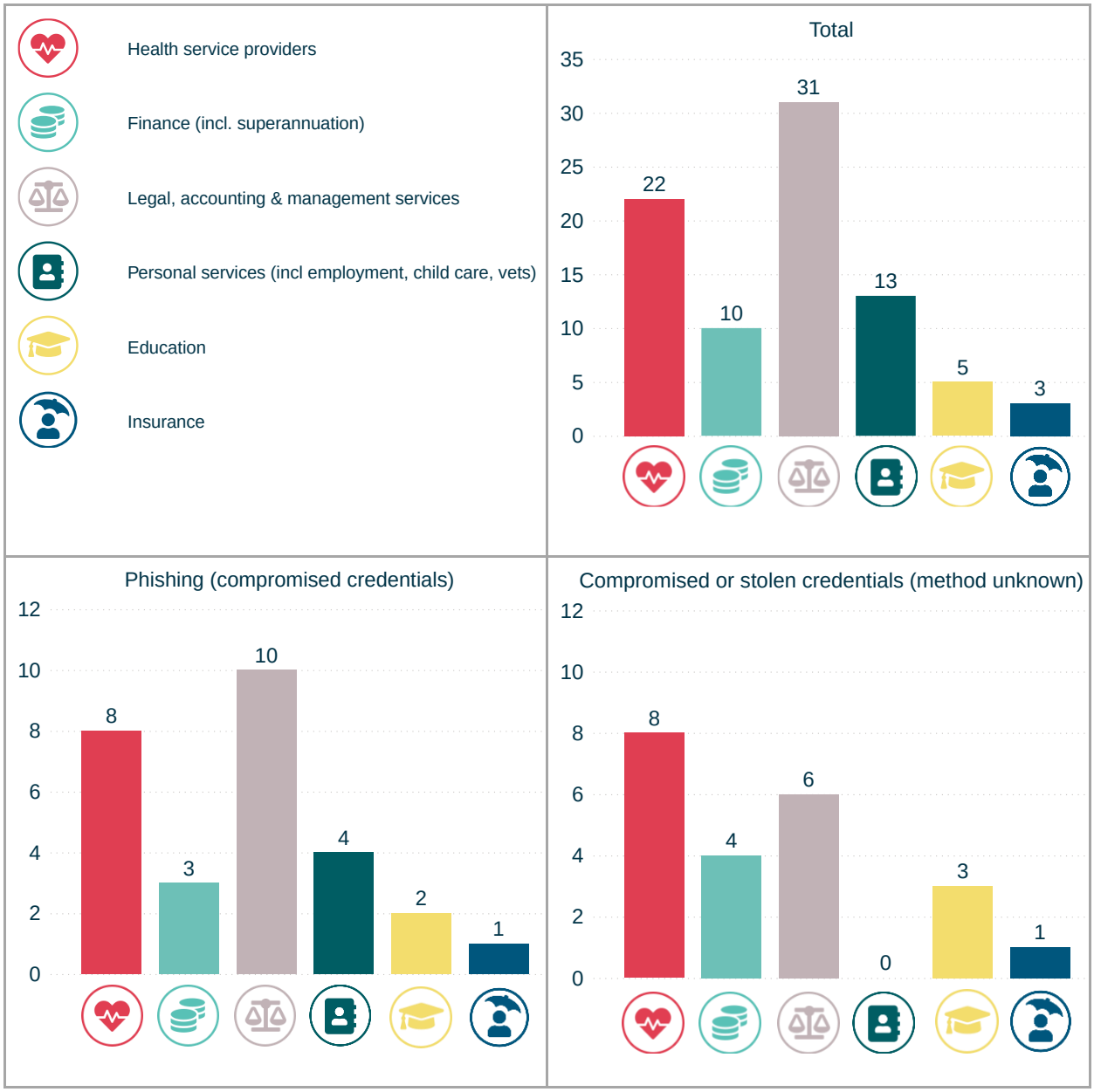
Chart 18 – Malicious or criminal attacks breakdown – Top industry sectors

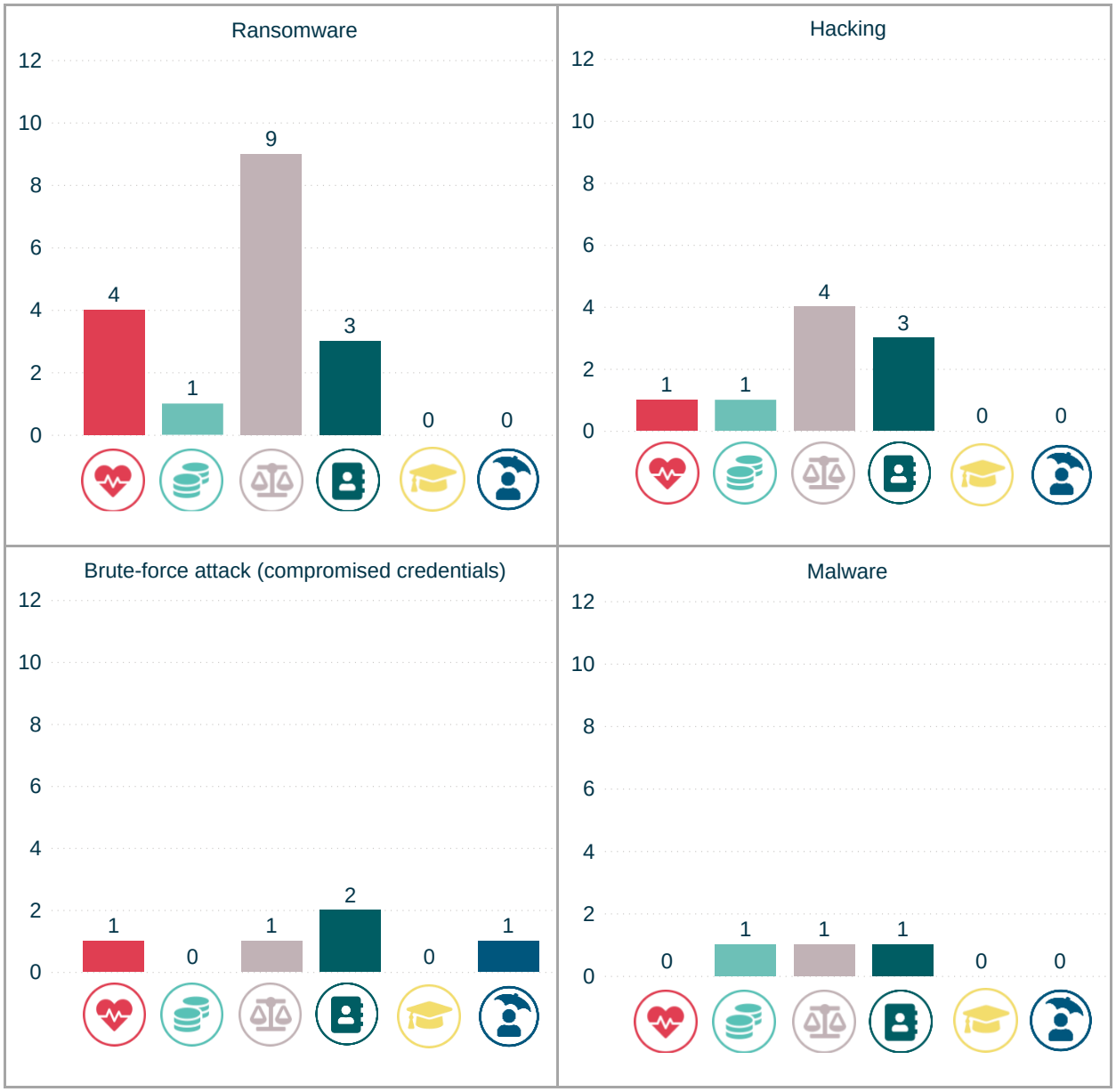



Rogue employee / insider threat
35
30
25
20
15
10
5
0
9
6
2
1
0
1
Theft of paperwork or data storage device
35
30
25
20
15
10
5
0
7
2
3
3
2
0

Cyber incident breaches – Top industry sectors

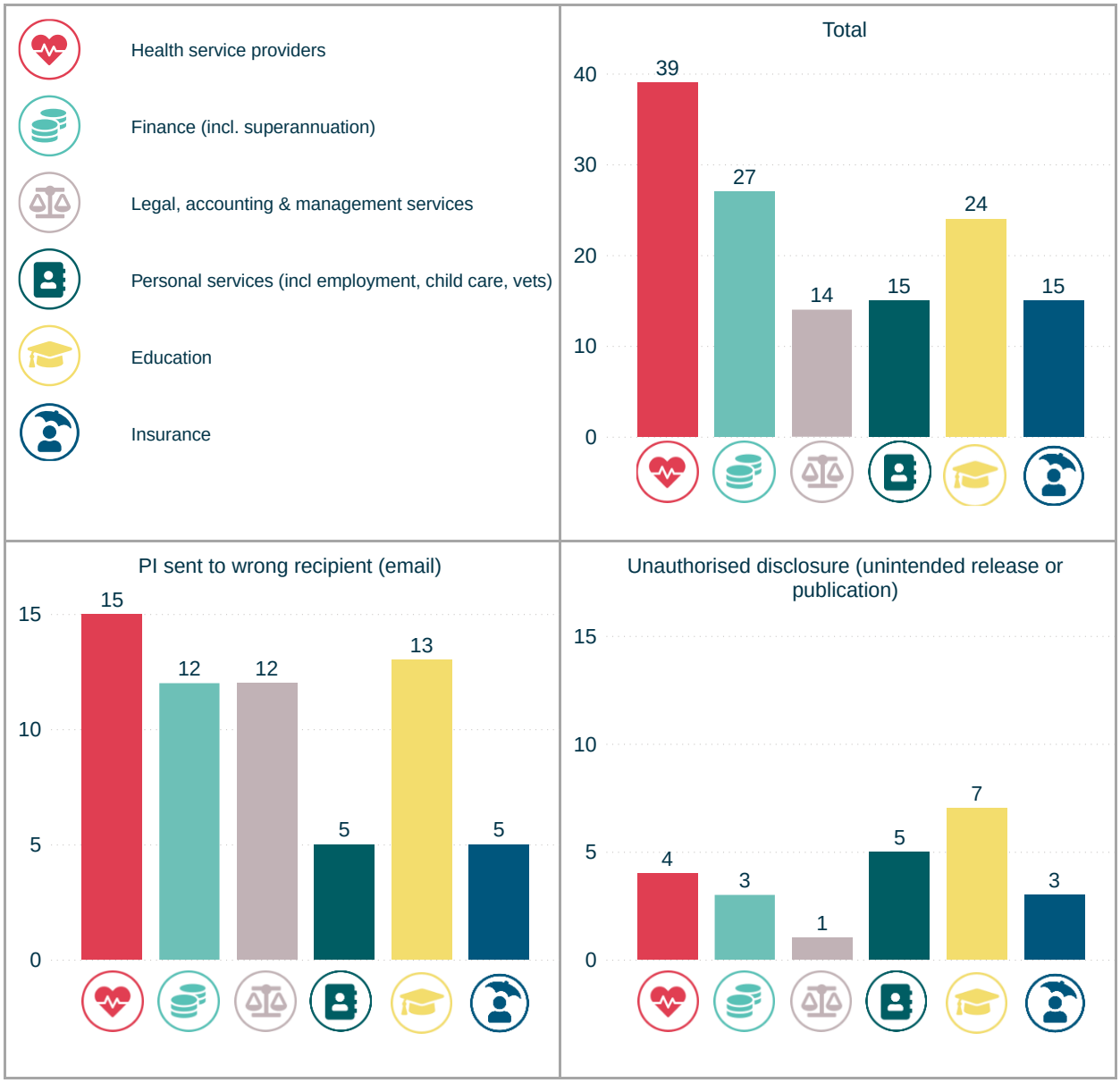
Chart 19 – Cyber incident breakdown – Top industry sectors

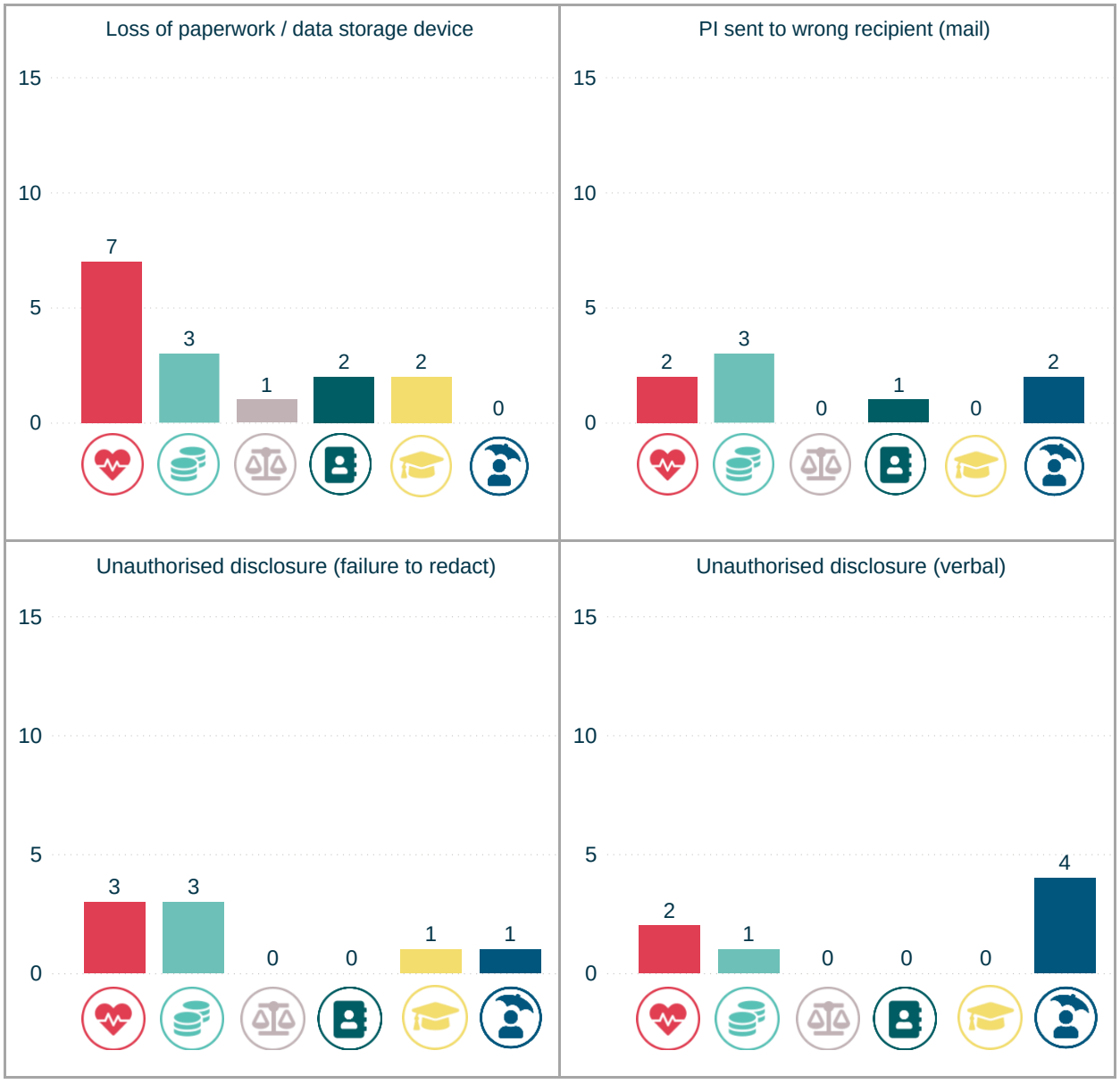


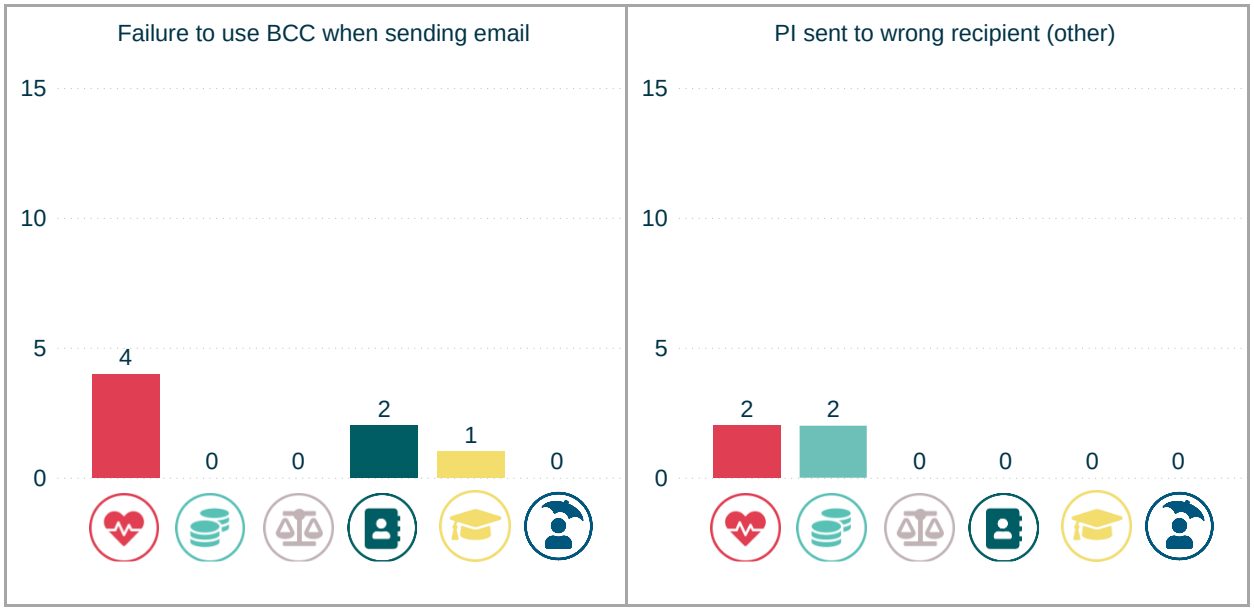

Ransomware
12
10
8
6
4
2
0
4
1
9
3
0
0
Hacking
1
1
4
3
0
0
Brute-force attack (compromised credentials)
1
0
1
2
0
1
Malware
0
1
1
1
0
0

Human error breaches – Top industry sectors

Chart 20 – Human error breakdown – Top industry sectors




Loss of paperwork / data storage device
15
10
5
0
7
3
1
2
2
0
PI sent to wrong recipient (mail)
15
10
5
0
2
3
0
1
0
2
Unauthorised disclosure (failure to redact)
15
10
5
0
3
3
0
0
1
1
Unauthorised disclosure (verbal)
15
10
5
0
2
1
0
0
0
4

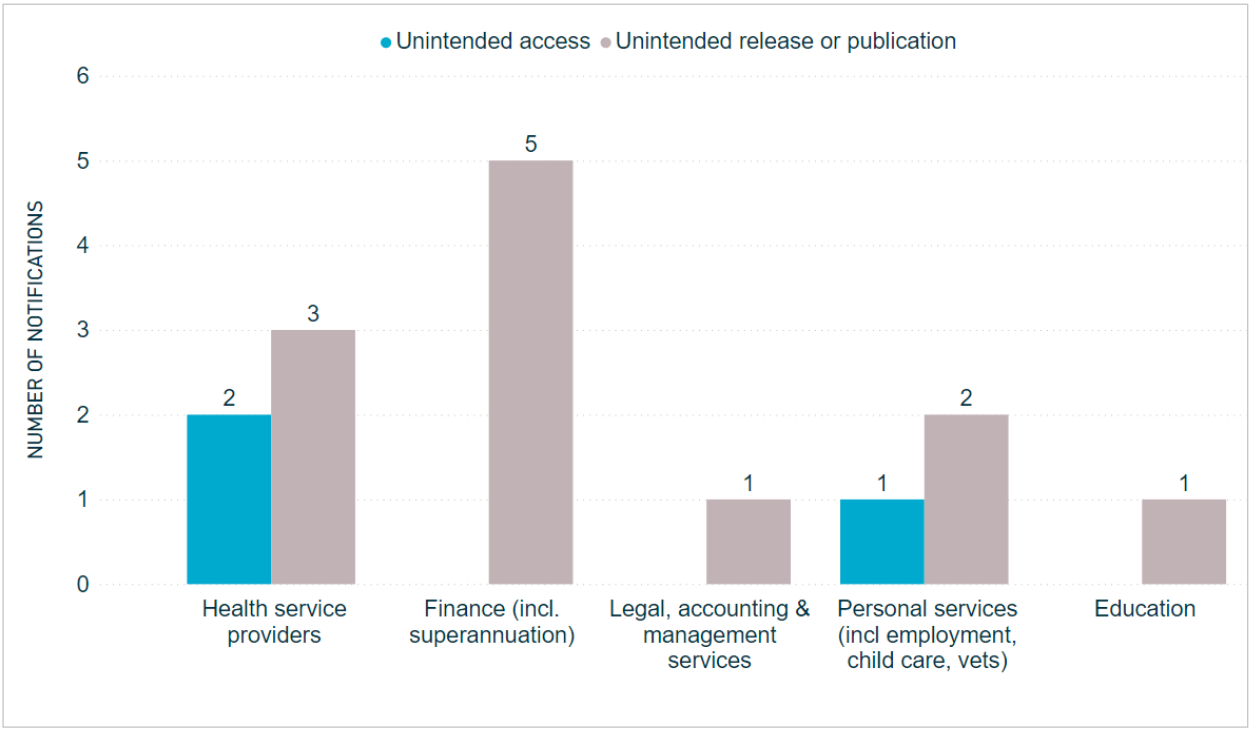


System fault breaches – Top industry sectors

Of the top industry sectors, all except insurance notified data breaches resulting from a system fault.

Most system fault breaches involved the unintended release or publication of personal information, such as automated messages sent to incorrect recipients or online forms or profiles automatically populated with incorrect personal information.

Chart 21 – System fault breakdown – Top industry sectors



Note: Insurance 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 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
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