Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Quarterly Statistics Report

1 October – 31 December 2018

oaic.gov.au

OAIC

Final report issued: 7/02/19

Contents

Key statistics

262
notifications

33%
human error

64%
malicious or criminal attacks

3%
system faults

About this report

This report captures notifications received by the Office of the Australian Information Commissioner (OAIC) under the Notifiable Data Breaches (NDB) scheme between 1 October 2018 and 31 December 2018 (referred to as 'data breaches').

The OAIC publishes quarterly statistical information about notifications received under the NDB scheme to assist entities and the public to understand the operation of the scheme.

Where data breaches affect multiple entities, the OAIC may receive multiple notifications relating to the same data breach. Notifications to the OAIC relating to the same data breach incident are counted as a single notification in this report.

The source of any given data 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 for statistical purposes. Source of data breach categories are defined in the glossary at the end of this report.

Notifications received from all sectors

Number of breaches reported — All sectors

Chart 1.1 — Number of breaches reported under the Notifiable Data Breaches scheme by month — All sectors

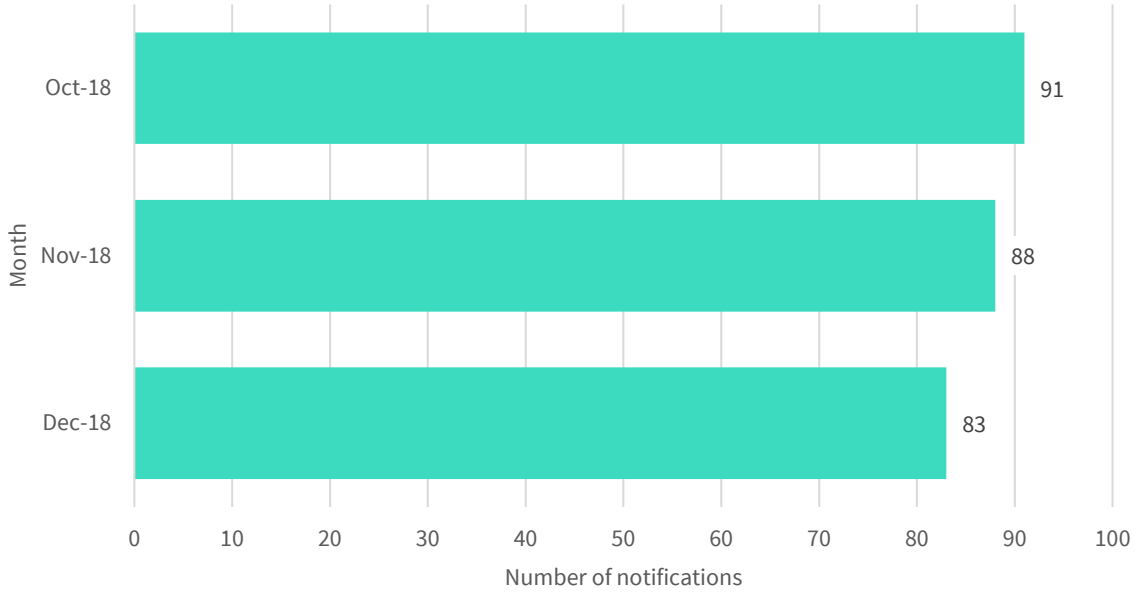
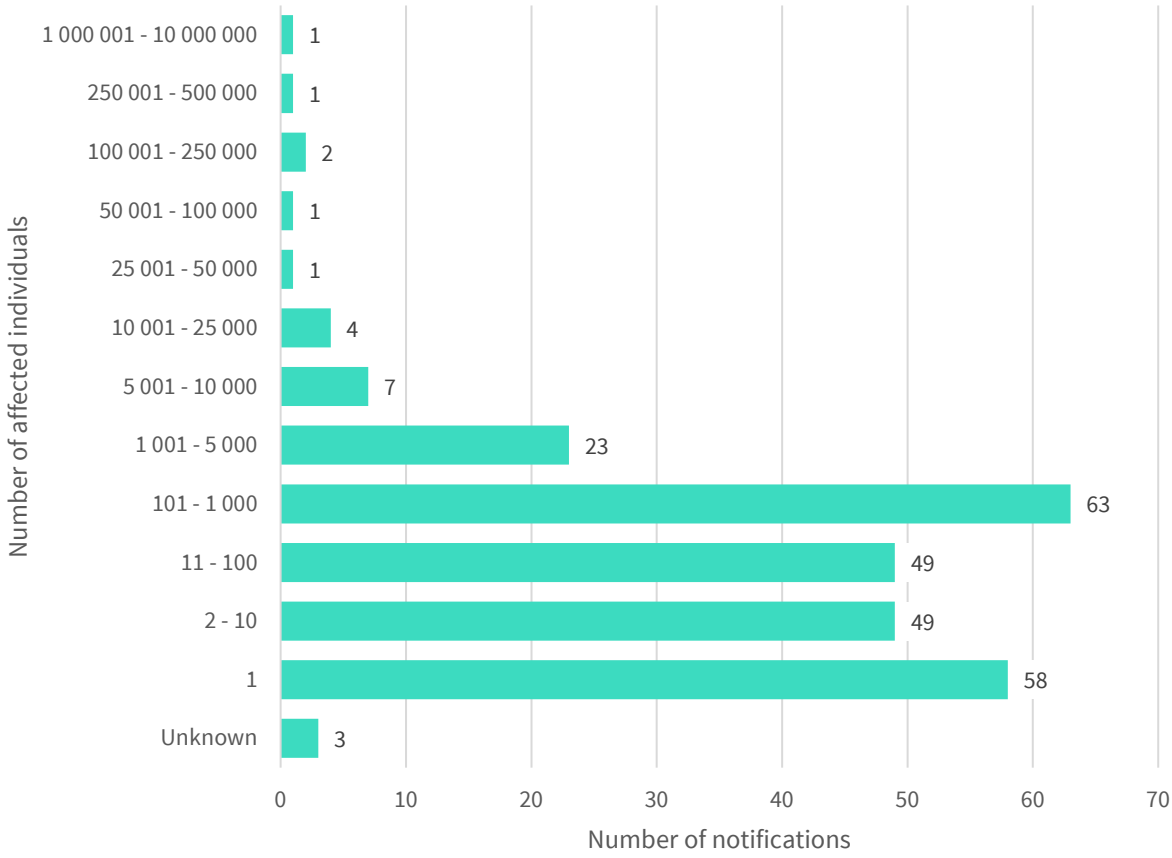


Table 1.A — Number of breaches reported under the Notifiable Data Breaches scheme by quarter —All sectors

Quarter	Total number of notifications
January to March 2018 * As the NDB scheme commenced on 22 February 2018, data is only available for part of the quarter	63
April to June 2018	242
July to September 2018	245
October to December 2018	262

Number of individuals affected by breaches — All sectors

Chart 1.2 — Number of individuals affected by breaches in the quarter — All sectors



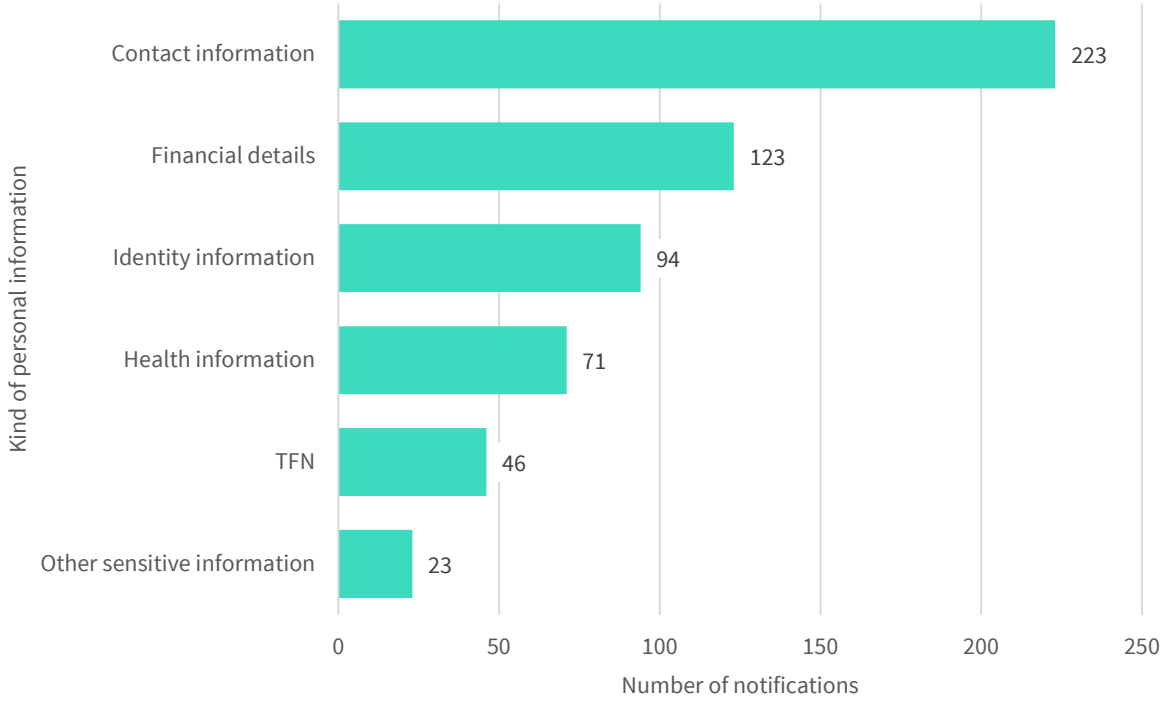
Note: Where bands are not shown (for example, 500 001 – 1 000 000), there were nil reports in the period. 'Unknown' includes notifications by entities whose investigations were ongoing at the time of this report.

The majority of data breaches in the period involved the personal information of 100 individuals or fewer (60 per cent of breaches).

Breaches impacting between 1 and 10 individuals comprised 41 per cent of the notifications.

Kinds of personal information involved in breaches — All sectors

Chart 1.3 — Kinds of personal information involved in breaches by number of notifications — All sectors



Note: Data breaches may involve one or more kinds of personal information.

Table 1.B — Kinds of personal information involved in breaches by percentage of notifications – All sectors

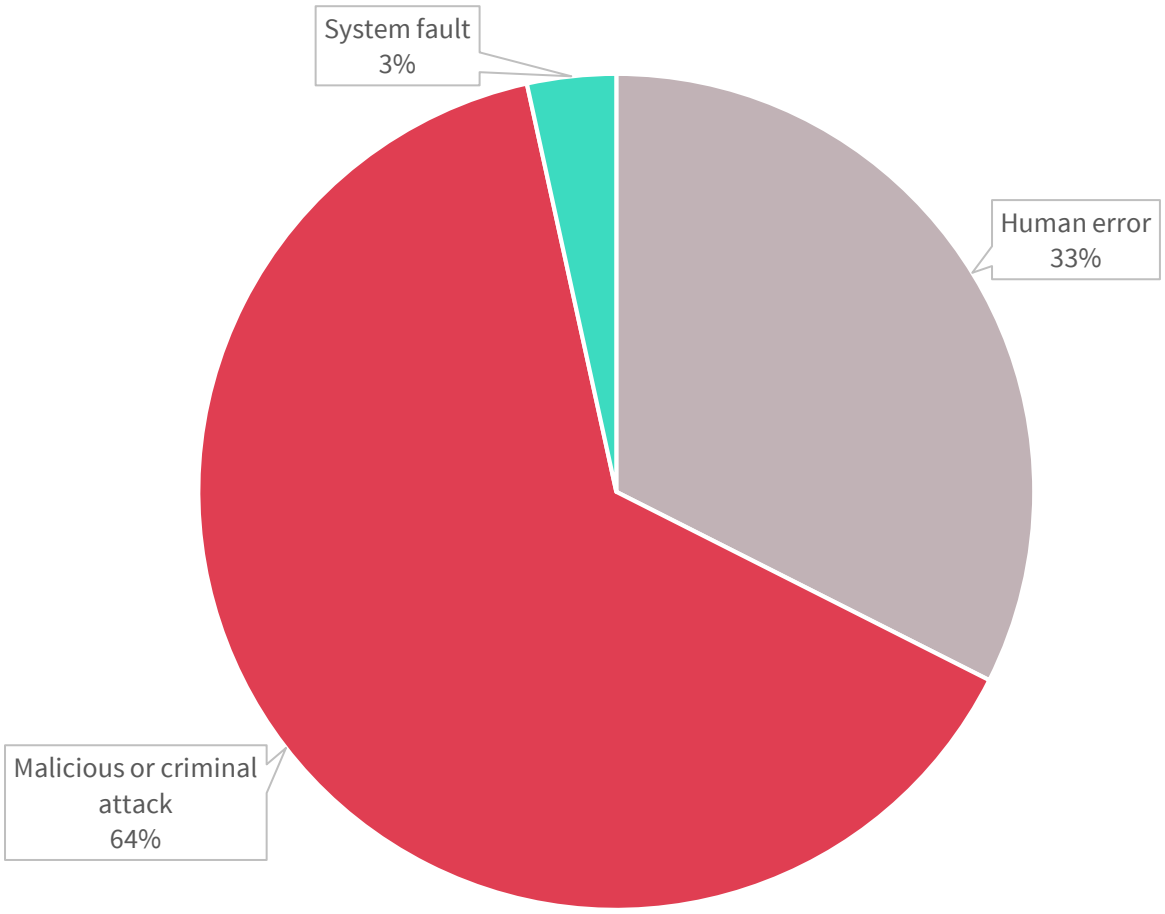
Kinds of personal information	% of NDBs received
Contact information	85%
Financial details	47%
Identity information	36%
Health information	27%
TFN	18%
Other sensitive information	9%

The definitions for the above kinds of personal information are contained in the Glossary.

Source of the breaches — All sectors

This chart breaks down the sources of data breaches as identified by notifying entities in all sectors in the quarter.

Chart 1.4 — Source of data breaches by percentage — All sectors



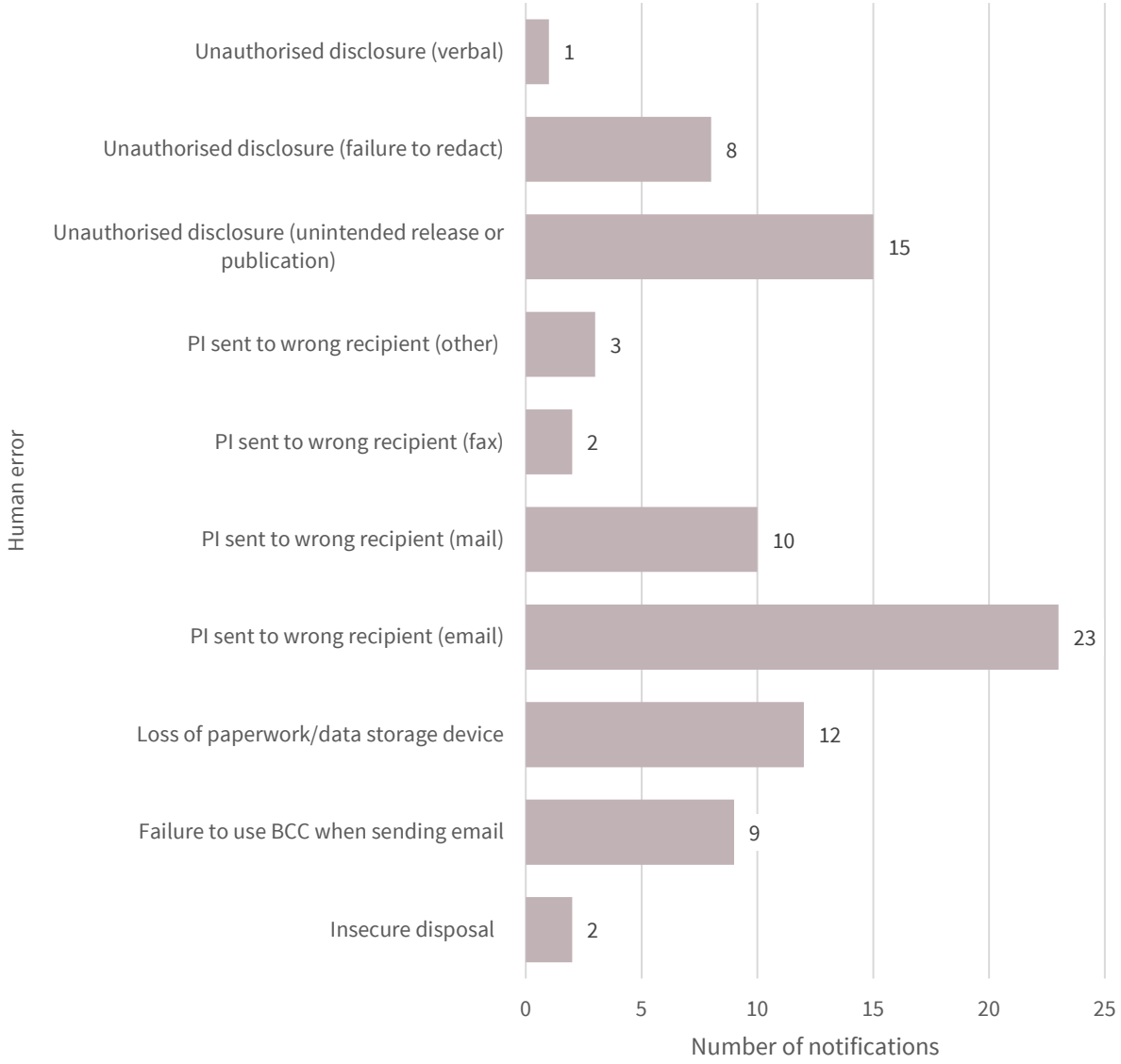
Malicious or criminal attacks accounted for 168 data breaches this quarter, while human error accounted for 85 data breaches. System faults accounted for nine data breaches.

Malicious or criminal attacks differ from human error breaches in that they are deliberately crafted to exploit known vulnerabilities for financial or other gain. Many cyber incidents in this quarter appear to have exploited vulnerabilities involving a human factor, such as clicking on a phishing email or disclosing passwords.

Human error breaches — All sectors

This chart breaks down the kinds of breaches identified as 'human error' in the quarter.

Chart 1.5 — Human error breakdown — All sectors



The second largest source of data breaches was human error, with examples including sending personal information to the wrong recipient via email (27 per cent) or mail (12 per cent) as well as unintended release or publication of personal information (18 per cent).

Certain kinds of breaches can affect larger numbers of people. For example, in this quarter data breaches involving human error resulting in the unintended release or publication of personal information impacted the largest numbers of people (an average of 17,746 affected individuals per breach). Failure to securely dispose of records of personal information impacted an average of 300 affected individuals per breach.

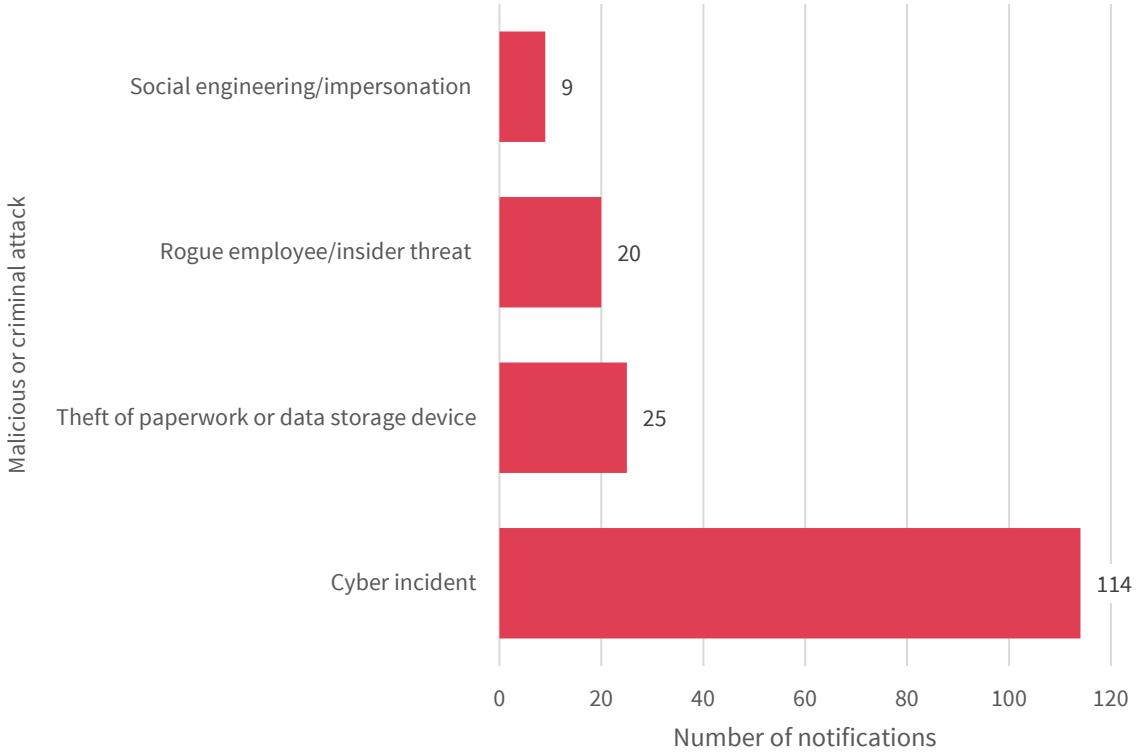
Table 1.C — Human error breakdown by average number of affected individuals — All sectors

Kinds of personal information	No. of NDBs received	Average no. of affected individuals
Unauthorised disclosure (unintended release or publication)	15	17,746
Insecure disposal	2	300
Failure to use BCC when sending email	9	234
PI sent to wrong recipient (other)	3	75
Loss of paperwork/data storage device	12	28
PI sent to wrong recipient (mail)	10	6
PI sent to wrong recipient (email)	23	3
Unauthorised disclosure (failure to redact)	8	2
Unauthorised disclosure (verbal)	1	1
PI sent to wrong recipient (fax)	2	1

Malicious or criminal attack breaches — All sectors

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack' in the quarter.

Chart 1.6 — Malicious or criminal attacks breakdown — All sectors



Malicious or criminal attacks were the largest source of data breaches this quarter, accounting for 64 per cent of all data breaches. Of these 168 data breaches, 68 per cent involved cyber incidents such as phishing, malware or ransomware, brute-force attacks, compromised or stolen credentials, and social engineering or impersonation.

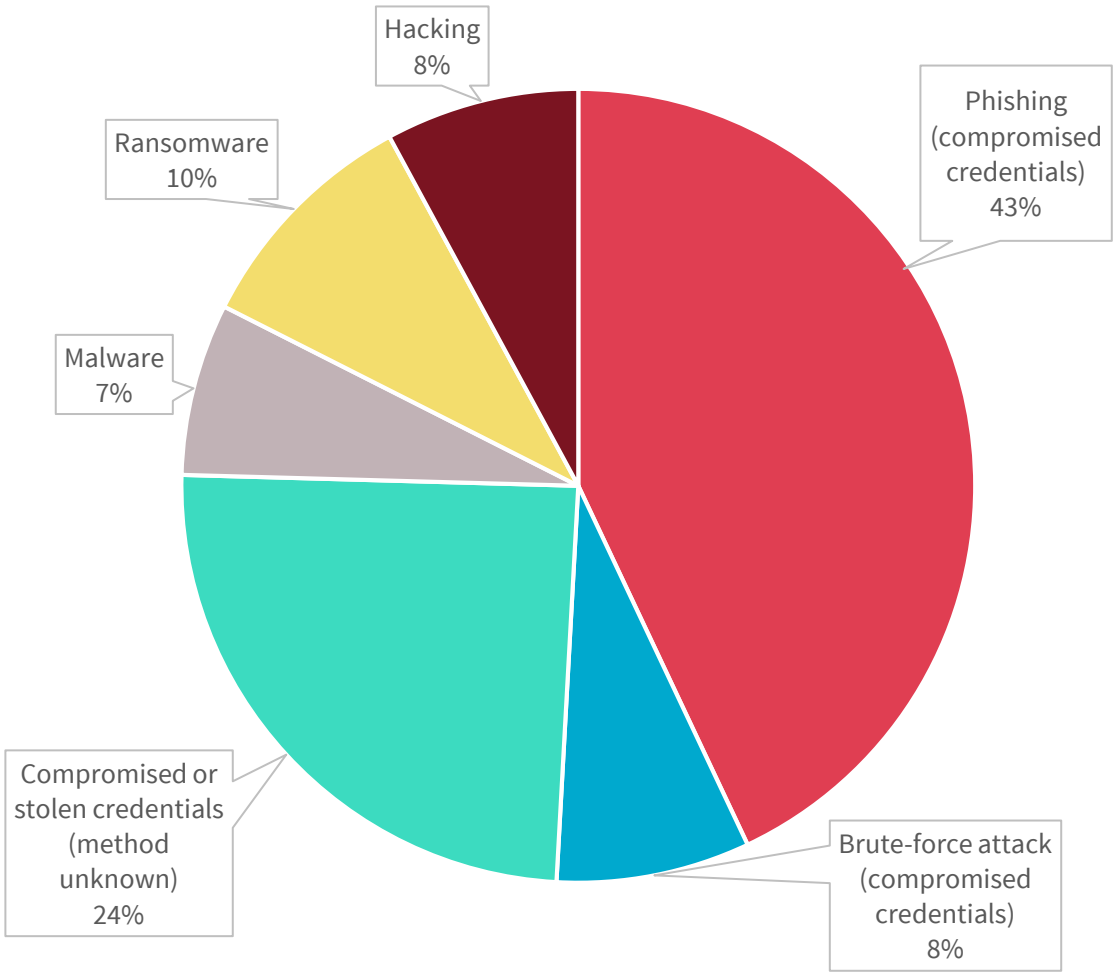
Many cyber incidents in this quarter appear to have exploited vulnerabilities involving a human factor, such as clicking on an attachment to a phishing email.

Theft of paperwork or data storage devices was also a significant source of malicious or criminal attacks (15 per cent). Other sources included actions taken by a rogue employee or insider threat (12 per cent), as well as social engineering or impersonation (5 per cent).

Cyber incident breaches — All sectors

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack - cyber incident' in the quarter.

Chart 1.7 — Cyber incident breakdown — All sectors

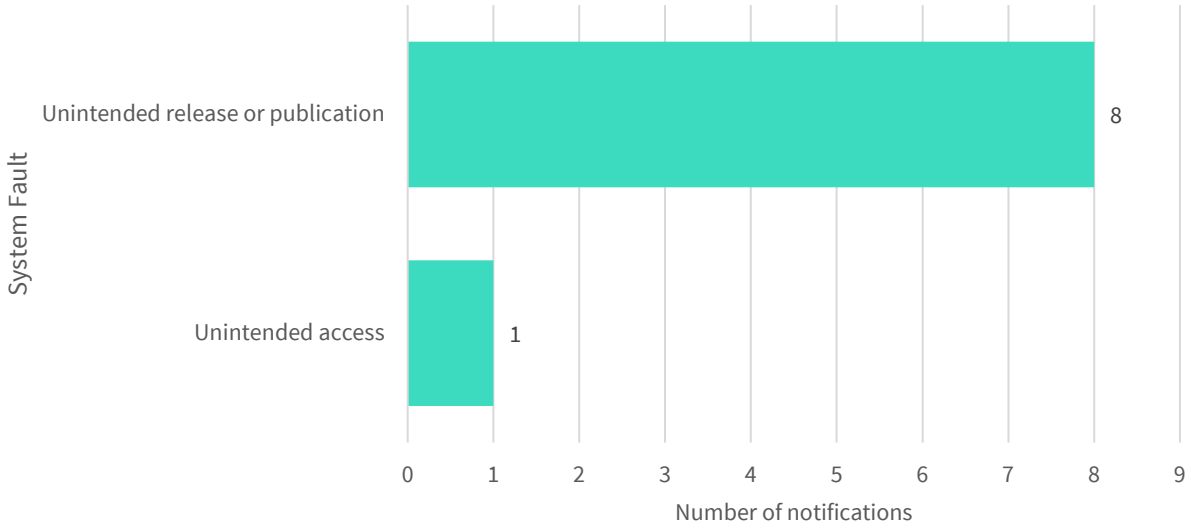


The majority of cyber incidents were linked to the compromise of credentials through phishing (49 notifications), by unknown methods (28 notifications), or by brute force attack (9 notifications).

System fault breaches — All sectors

This chart breaks down the kinds of breaches identified as 'system fault' in the quarter.

Chart 1.8 — System fault breakdown — All sectors



System faults accounted for 3 per cent of data breaches this quarter. The majority involved a system fault resulting in the unintended release or publication of personal information. This may include the disclosure of personal information on a website due to a bug in the web code, or a machine fault that results in a document containing personal information being sent to the wrong person.

Comparison of top five sectors that reported breaches in the quarter

This section compares notifications made under the Notifiable Data Breaches scheme by the five sectors that made the most notifications in the quarter (top five sectors).

Top five sectors

Table 2.A — Top five sectors by notifications in the quarter

Top five sectors	NDBs received
Health service providers [1]	54
Finance (incl. superannuation) [2]	40
Legal, accounting and management services	23
Education [3]	21
Mining and manufacturing	12

The NDB scheme applies to agencies and organisations that the Privacy Act requires to take reasonable steps to secure personal information. This includes Australian Government agencies, businesses and not-for-profit organisations with an annual turnover of $3 million or more, credit reporting bodies, health service providers, and TFN recipients, among others.

From October to December 2018, the top sector to report notifiable data breaches was the private health service provider sector (health sector) (21 per cent). The second largest source was the finance sector (15 per cent). This was followed by the legal, accounting and management services sector (9 per cent), the private education sector (education) (8 per cent), and the mining and manufacturing sector (5 per cent).

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

1 A health service provider includes any entity that provides a health service within the meaning of s 6FB of the Privacy Act, regardless of annual turnover.

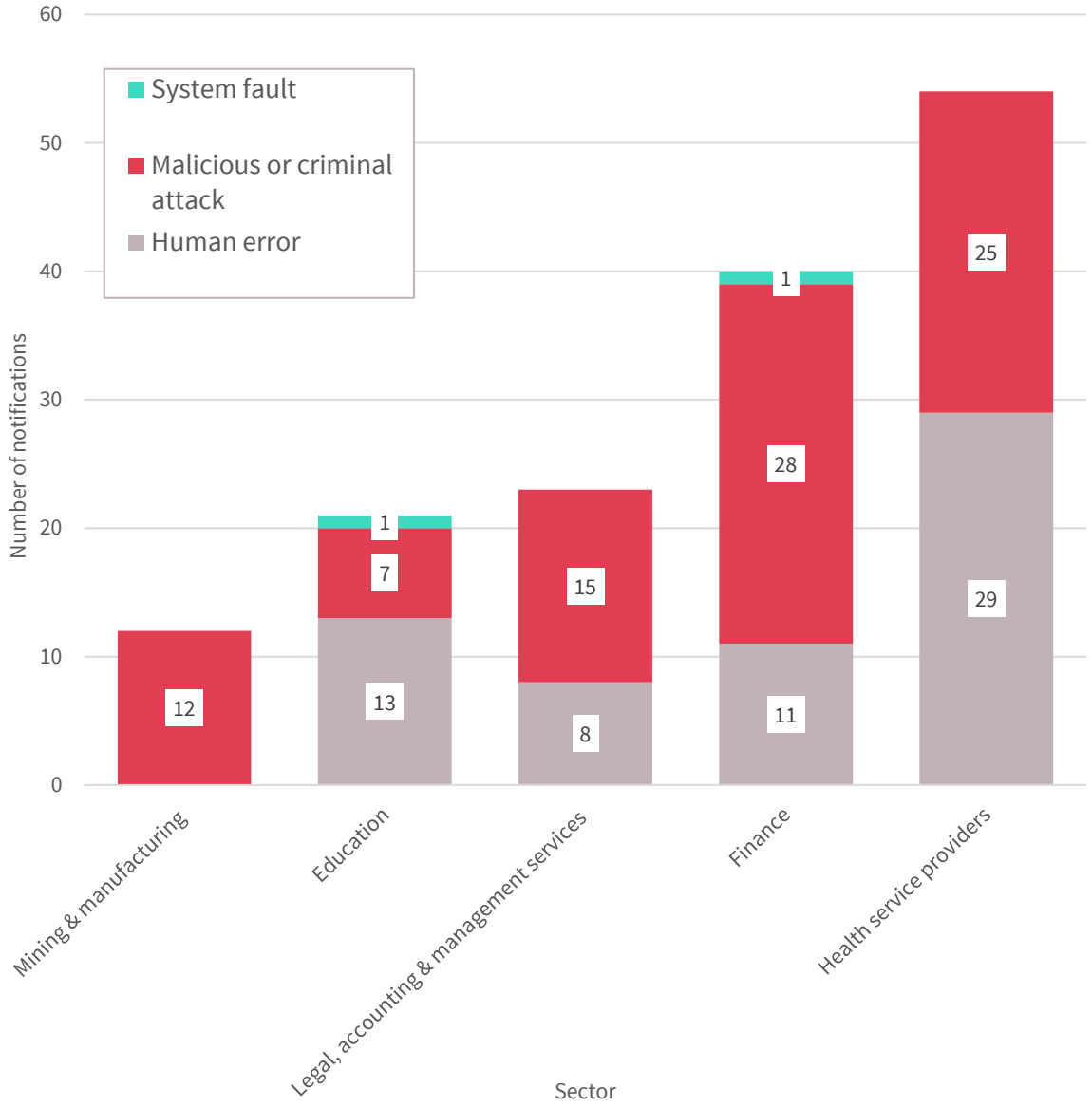
2 This sector includes banks, wealth managers, financial advisors, superannuation funds and consumer credit providers (regardless of annual turnover).

3 This sector includes private education providers only, as APP entities, and the Australian National University. Public sector education providers are bound by State and Territory privacy laws, as applicable.

Source of breaches — Top five sectors

This chart breaks down the sources of data breaches as identified by notifying entities in the top five sectors in the quarter.

Chart 2.1 — Source of data breaches — Top five sectors



The highest reporting sector this quarter was the health sector (54 notifications). Of those notifications, 54 per cent of reportable data breaches resulted from human error. In contrast, notifications from the second highest reporting sector, finance, indicated that 70 per cent of its data breaches resulted from malicious or criminal attacks.

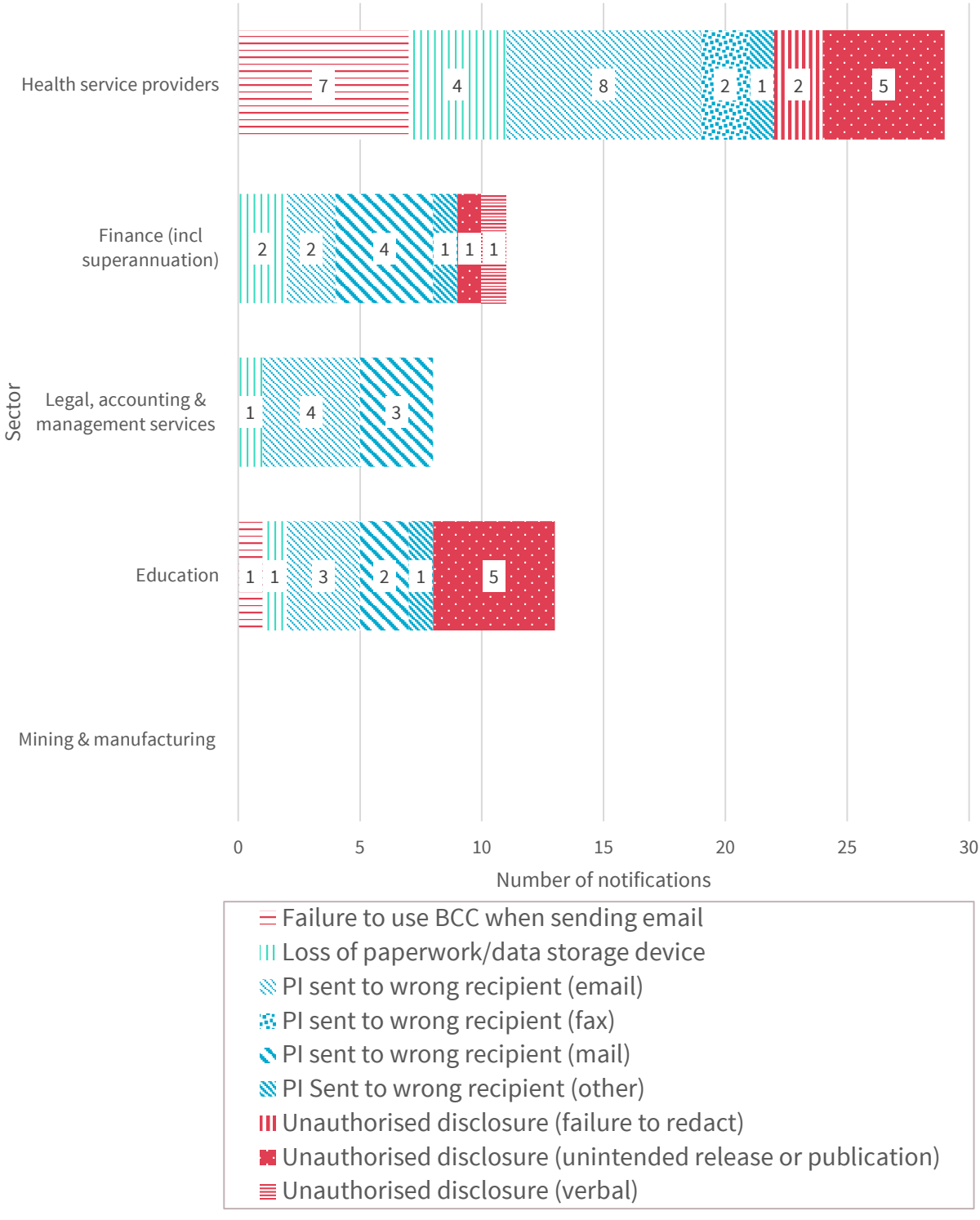
The legal, accounting and management services sector and the mining and manufacturing sector also reported the majority of breaches resulted from malicious or criminal attacks.

Of the top five sectors, only the finance and education sectors notified a data breach resulting from a system fault.

Human error breaches — Top five sectors

This chart breaks down the kinds of breaches identified as 'human error' by the top five sectors in the quarter.

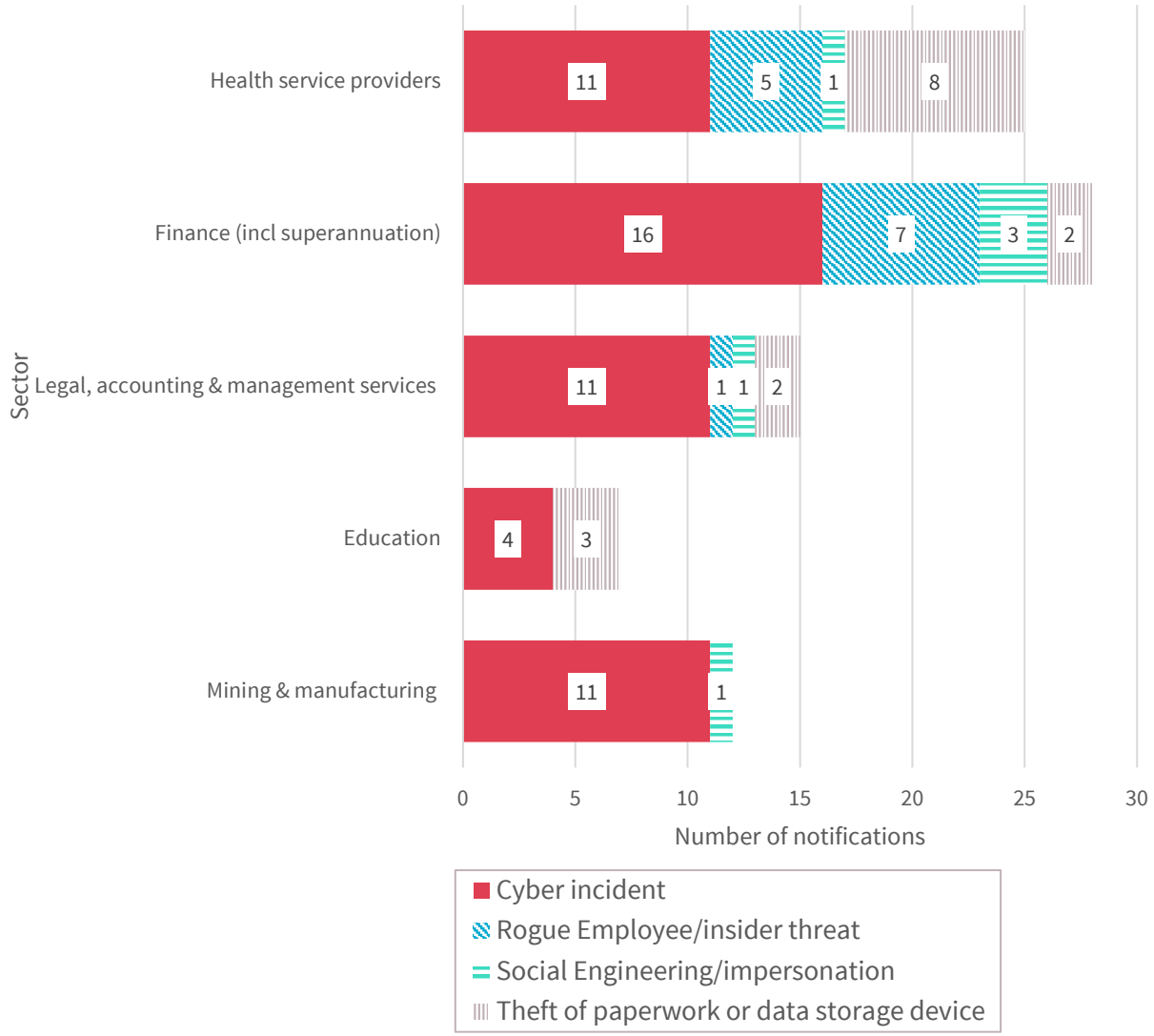
Chart 2.2 — Human error breakdown — Top five sectors



Malicious or criminal attack breaches — Top five sectors

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack' by the top five sectors in the quarter.

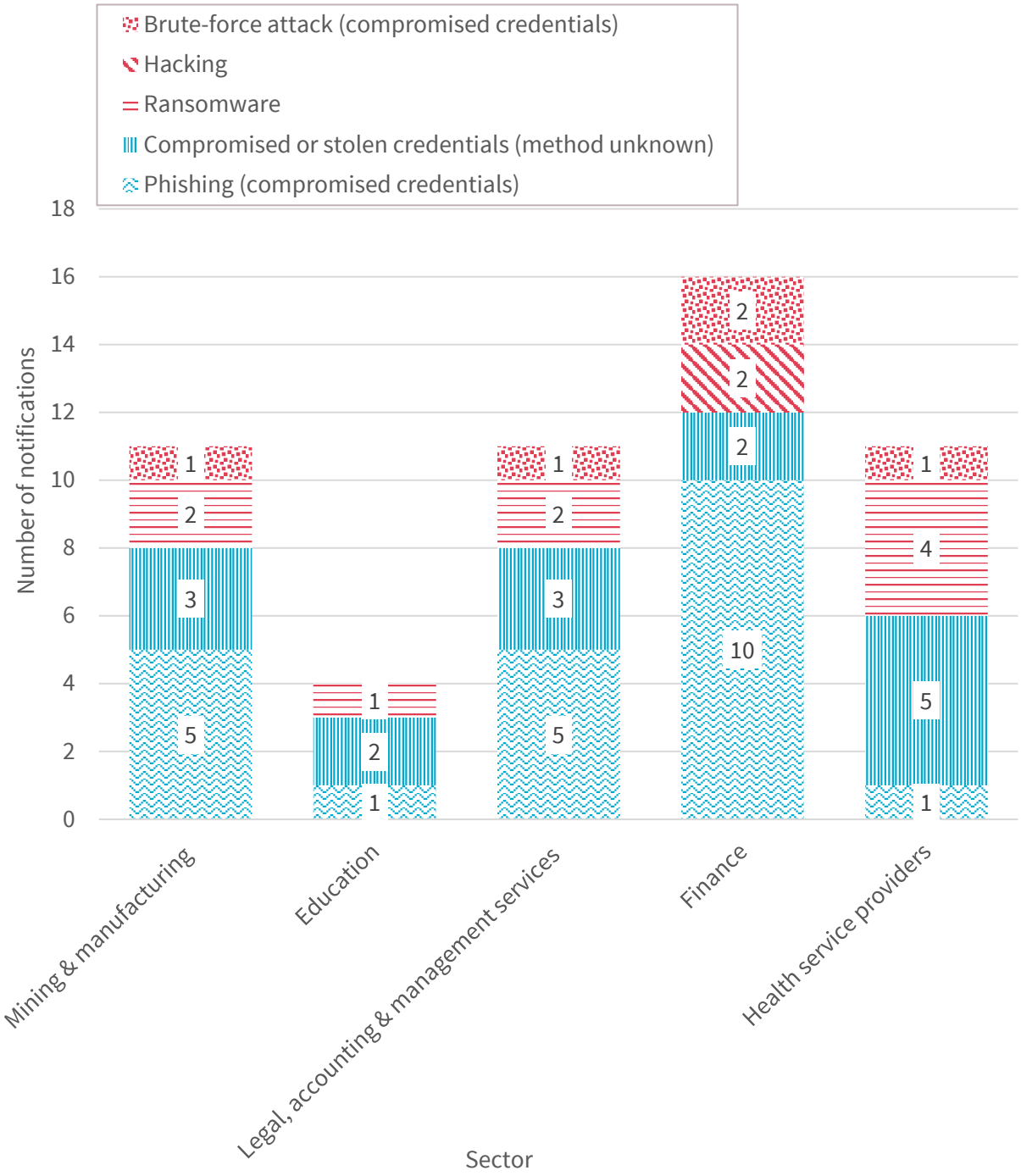
Chart 2.3 — Malicious or criminal attacks breakdown — Top five sectors



Cyber incident breaches — Top five sectors

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack - cyber incident' by the top five sectors in the quarter.

Chart 2.4 — Cyber incident breakdown — Top five sectors

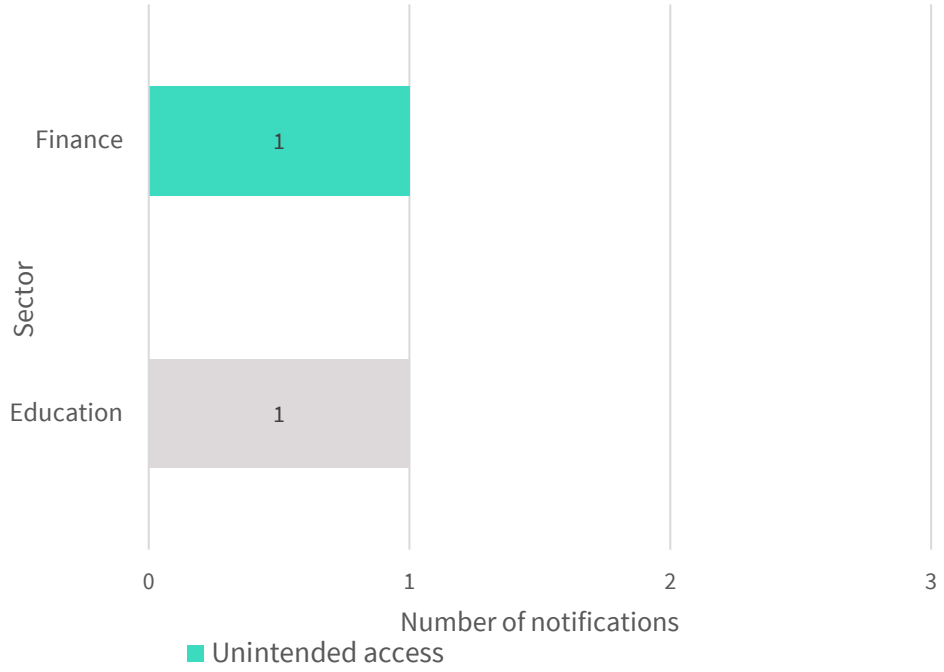


In line with the overall trend, the majority of cyber incidents reported by the top five sectors were linked to the compromise of credentials through phishing, brute force attacks, or by unknown methods.

System fault breaches — Top five sectors

This chart breaks down the kinds of breaches identified as 'system fault' by the top five sectors in the quarter.

Chart 2.5 — System fault breakdown — Top five sectors

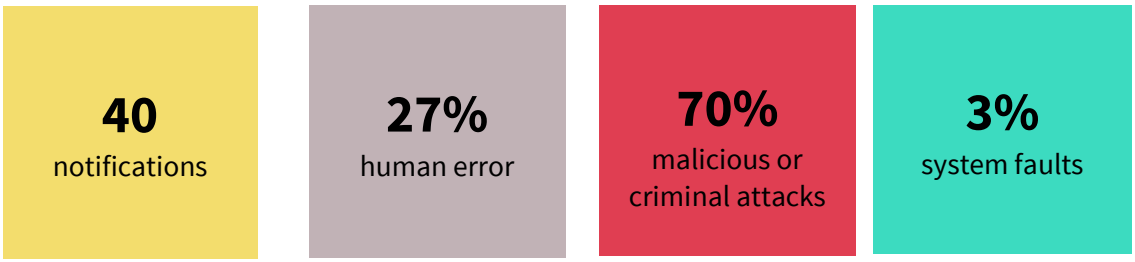


The health sector, the legal, accounting and management services sector and the mining and manufacturing sector did not report any data breaches resulting from a system fault.

Finance (including superannuation) sector report

This section captures notifications made under the NDB scheme by entities in the finance sector, such as banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

Summary — Finance sector



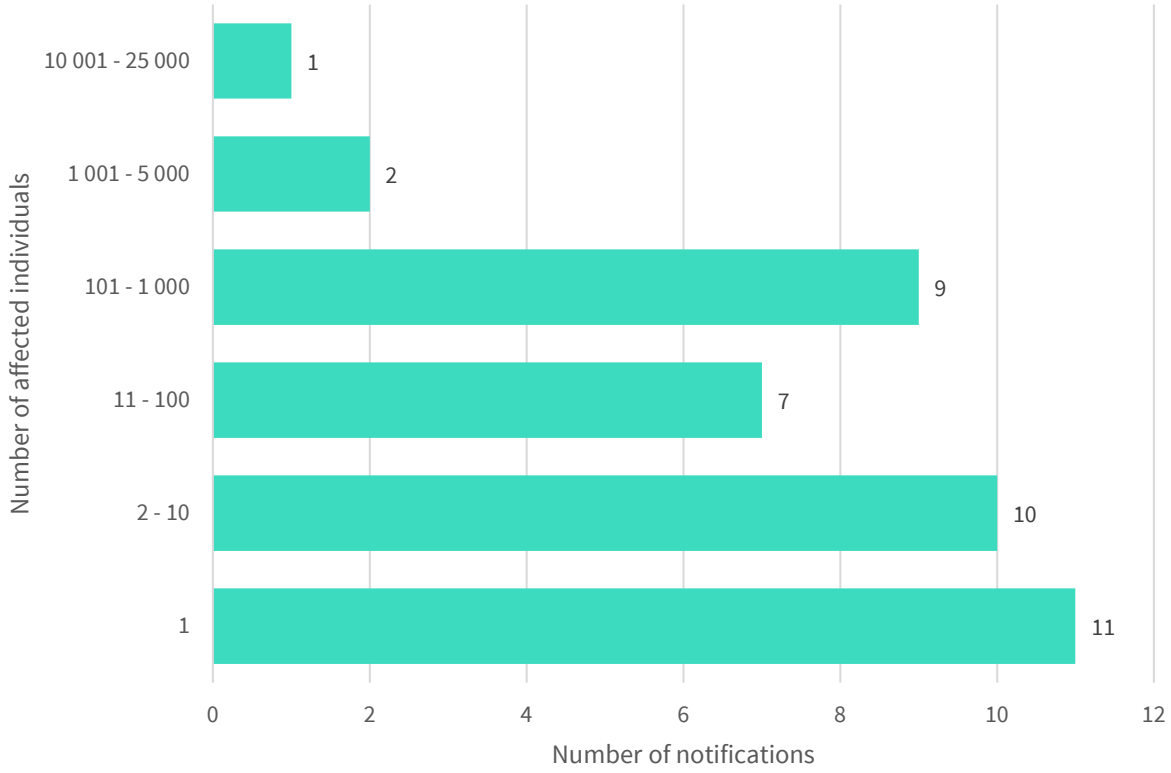
Number of breaches reported under the Notifiable Data Breaches Scheme — Finance sector

Table 3.A — Number of breaches reported under the Notifiable Data Breaches scheme by the finance sector by quarter

Quarter	Total number of notifications
January to March 2018 * As the NDB scheme commenced on 22 February 2018, data is only available for part of the quarter	8
April to June 2018	36
July to September 2018	35
October to December 2018	40

Number of individuals affected by breaches — Finance sector

Chart 3.1 — Number of individuals affected by breaches in the quarter — Finance sector

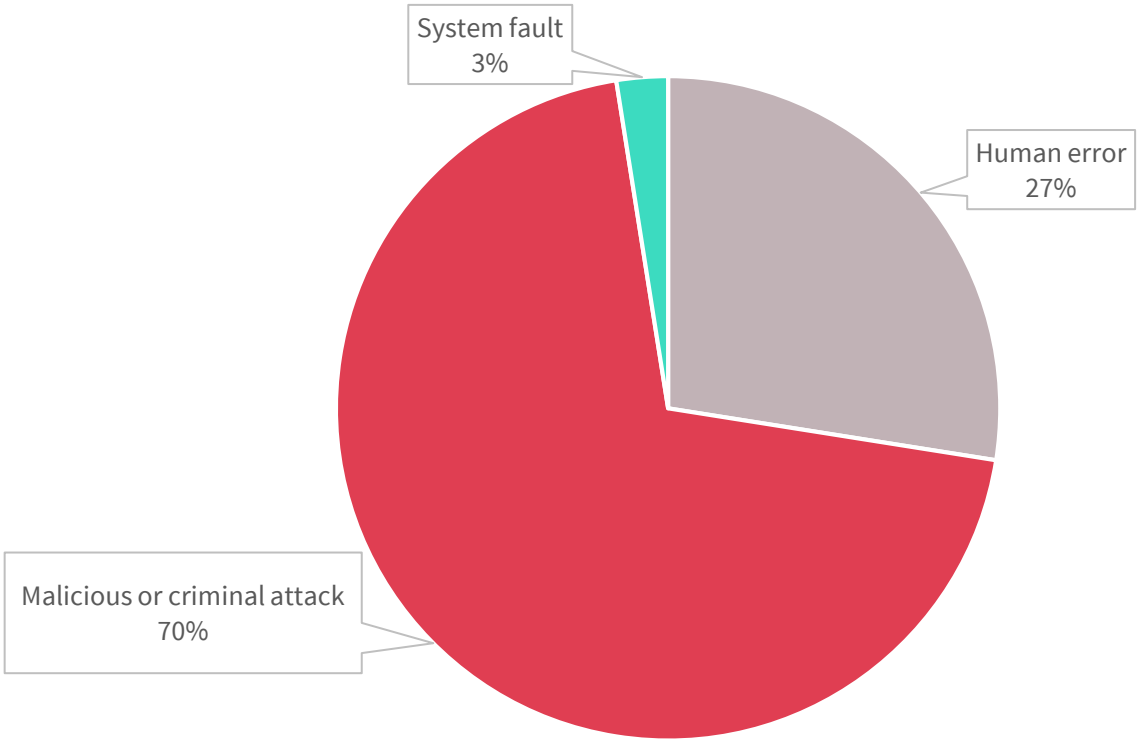


Note: Where bands are not shown, there were nil reports in the period.

Most finance sector notifications in the period involved the personal information of 100 individuals or fewer (70 per cent of breaches). Breaches affecting between one and ten individuals comprised 53 per cent of the notifications.

Source of the breaches — Finance sector

Chart 3.2 — Source of data breaches by percentage — Finance sector



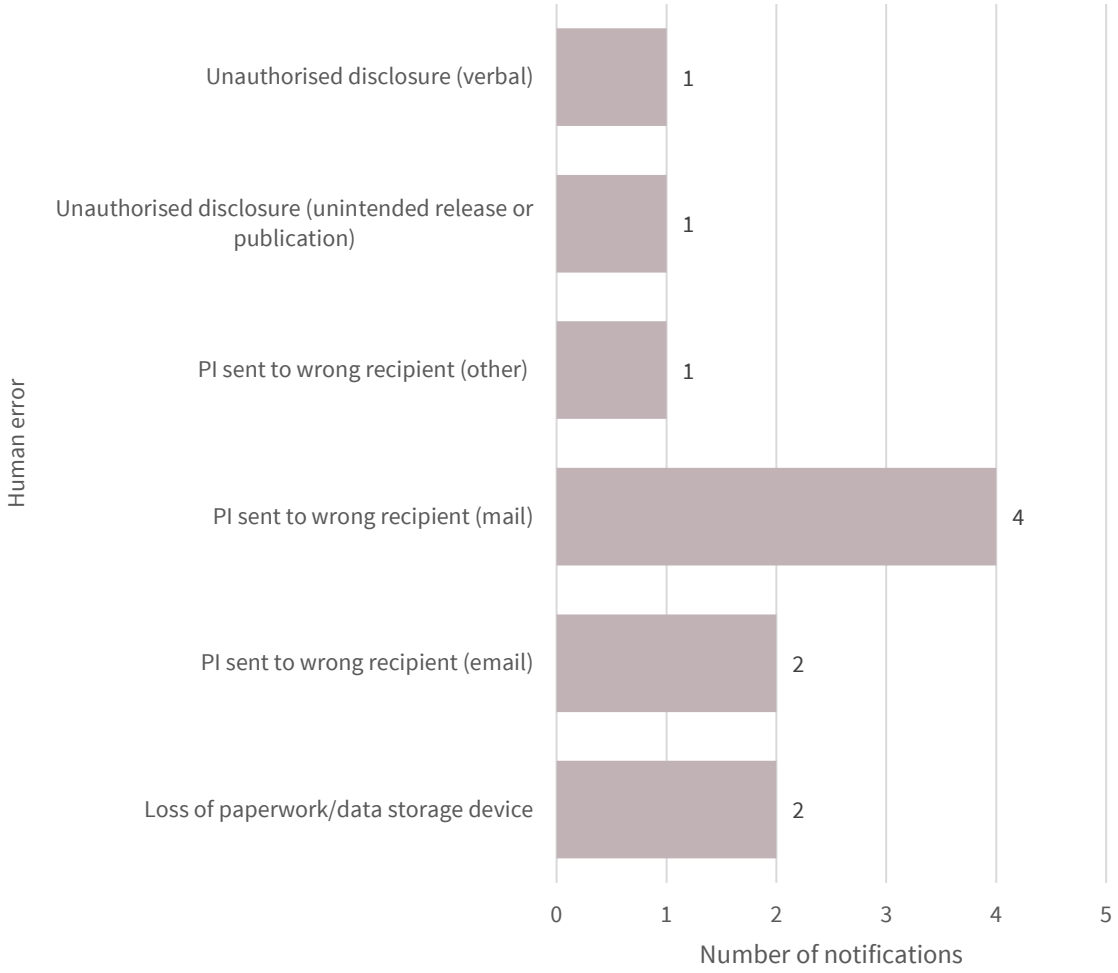
Malicious or criminal attacks was the source of most notifications from the finance sector this quarter (28 notifications). This may involve a cyber incident, such as a phishing email or malware attack, as well as the theft of paperwork or a data storage device.

Human error was the source of 11 notifications from the finance sector, such as communications sent to the wrong recipient, insecure disposal of personal information, or a failure to properly redact personal information.

Human error breaches — Finance sector

This chart breaks down the kinds of breaches identified as 'human error' by the finance sector in the quarter.

Chart 3.3 — Human error breakdown — Finance sector

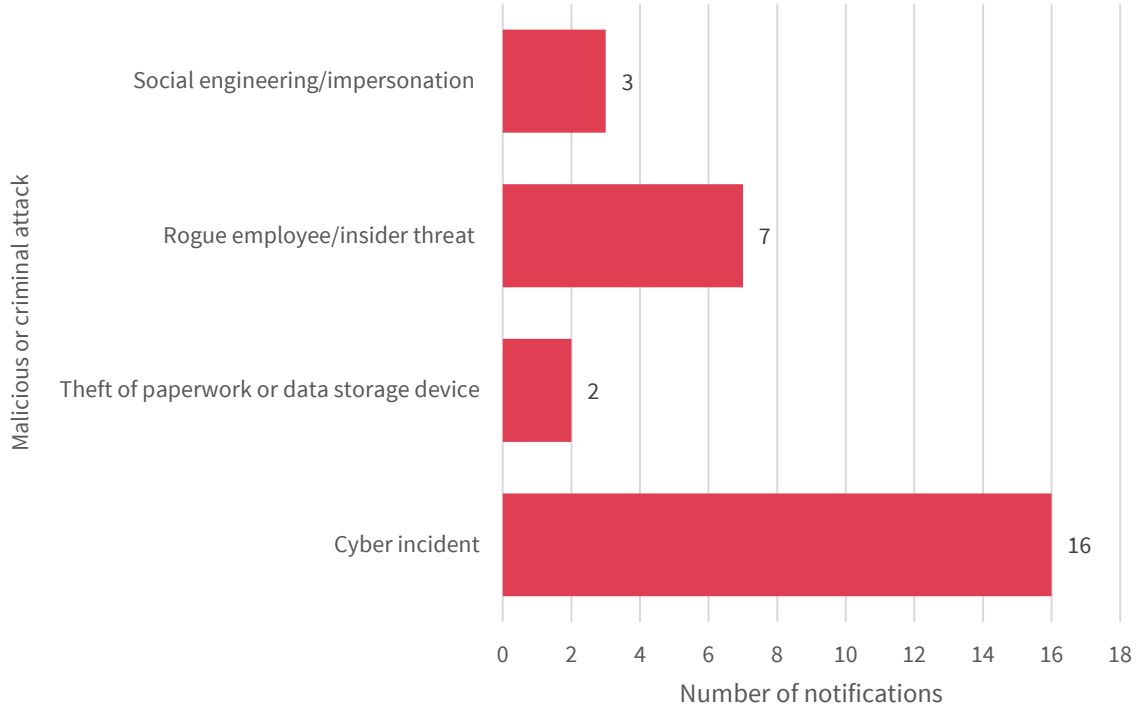


Human error was the second largest source of data breaches from the finance sector. Examples include sending correspondence containing personal information to the wrong recipient by mail (10 per cent of human error notification) or email (5 per cent), and loss of paperwork or data storage device (5 per cent).

Malicious or criminal attack breaches — Finance sector

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack' by the finance sector in the quarter.

Chart 3.4 — Malicious or criminal attacks breakdown — Finance sector

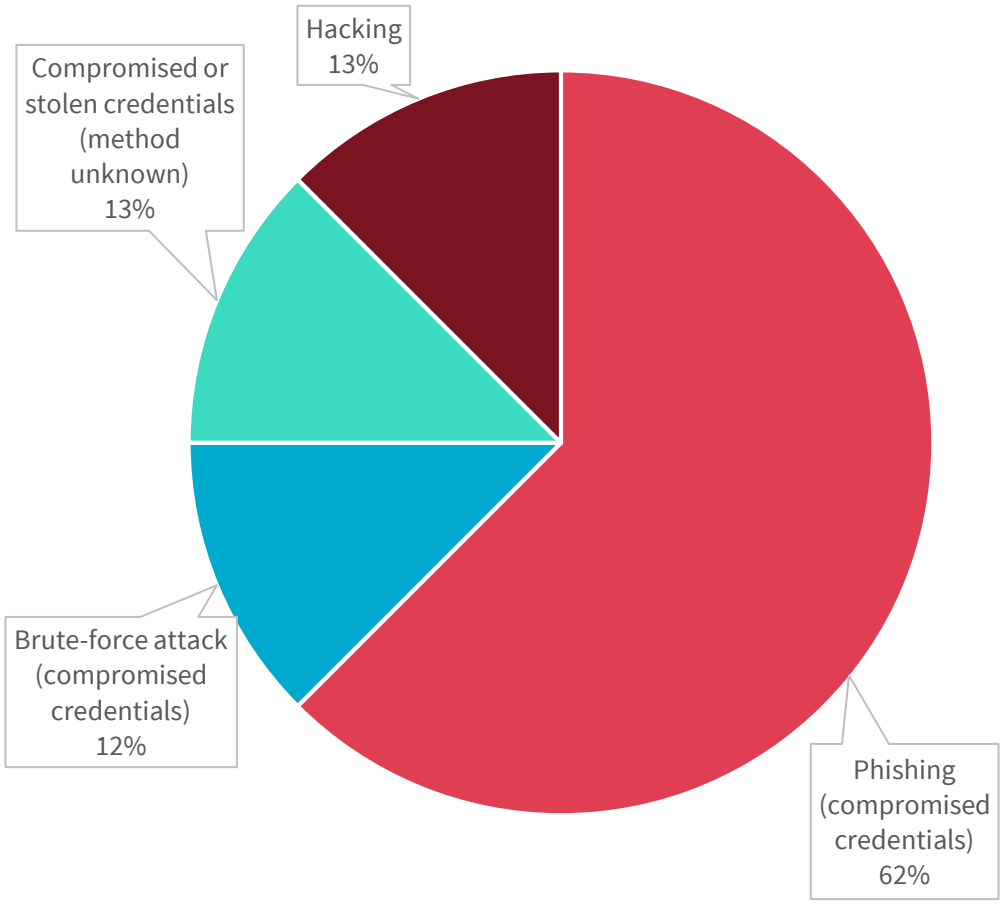


Malicious and criminal attacks was the leading source of data breaches notified by the finance sector (70 per cent). Of these, cyber incidents were the most common type of attack (57 per cent), followed by rogue employees or insider threats (25 per cent), social engineering/impersonation (11 per cent) and theft of paperwork or data storage device (7 per cent).

Cyber incident breaches — Finance sector

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack — cyber incident' by the finance sector in the quarter.

Chart 3.5 — Cyber incident breakdown — Finance sector



The majority of cyber incidents reported by the finance sector were related to compromised or stolen credentials, through phishing (10 notifications), brute-force attacks (2 notifications), and by unknown methods (2 notifications). Hacked websites or systems was the source for 2 notifications.

System fault breaches — Finance sector

One notification in the quarter identified the source of the data breach as a system fault leading to unauthorised access.

Health sector report

This section captures notifications made under the Notifiable Data Breaches scheme by entities in the health sector.

Summary — Health sector

54
notifications

54%
human error

46%
malicious or criminal attacks

0%
system faults

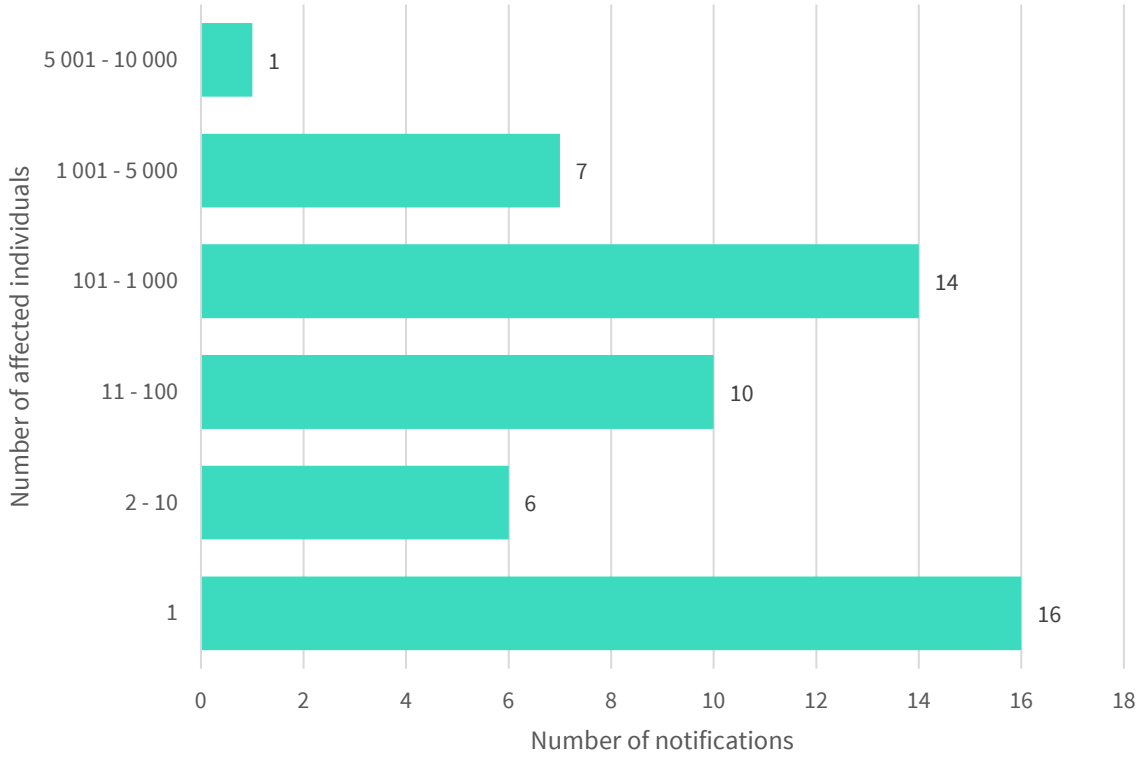
Number of breaches reported under the Notifiable Data Breaches scheme — Health sector

Table 4.A — Number of breaches reported under the Notifiable Data Breaches scheme by the health sector by quarter

Quarter	Total number of notifications
January to March 2018 * As the NDB scheme commenced on 22 February 2018, data is only available for part of the quarter	15
April to June 2018	49
July to September 2018	45
October to December 2018	54

Number of individuals affected by breaches — Health sector

Chart 4.1 — Number of individuals affected by breaches in the quarter — Health sector

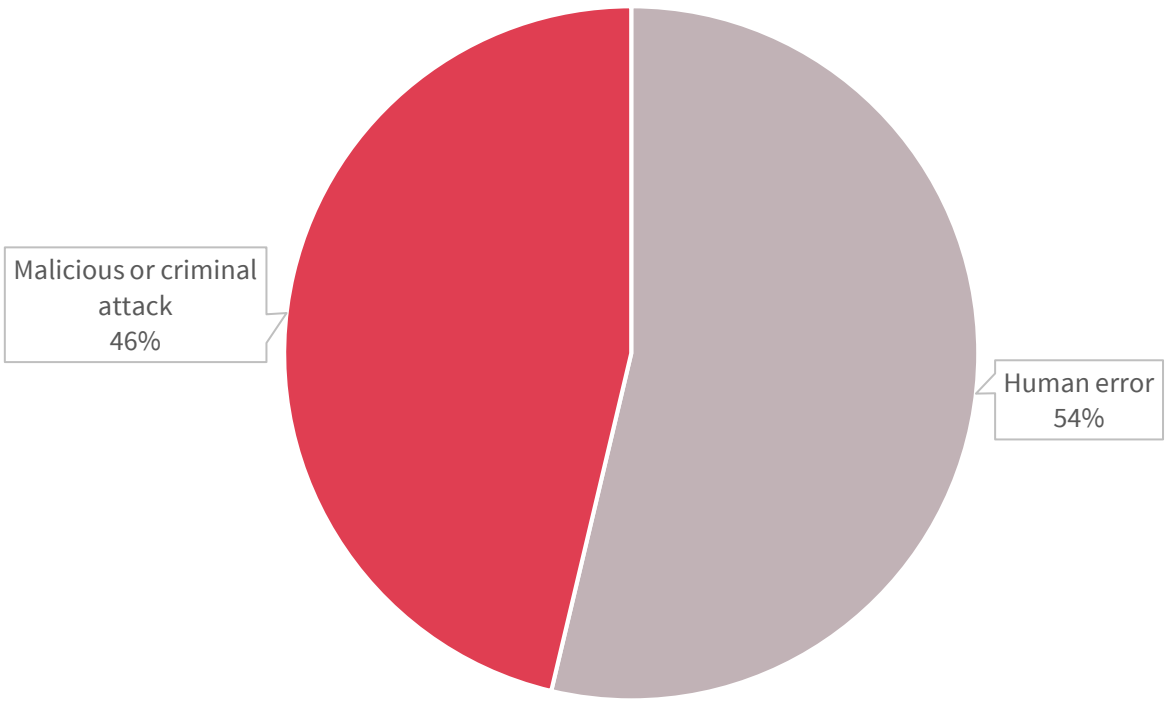


Note: Where bands are not shown, there were nil reports in the period.

Most health sector notifications in the period involved the personal information of 100 individuals or fewer (59 per cent of breaches). Breaches affecting between one and ten individuals comprised 41 per cent of the notifications.

Source of the breaches — Health sector

Chart 4.2 — Source of data breaches by percentage — Health sector



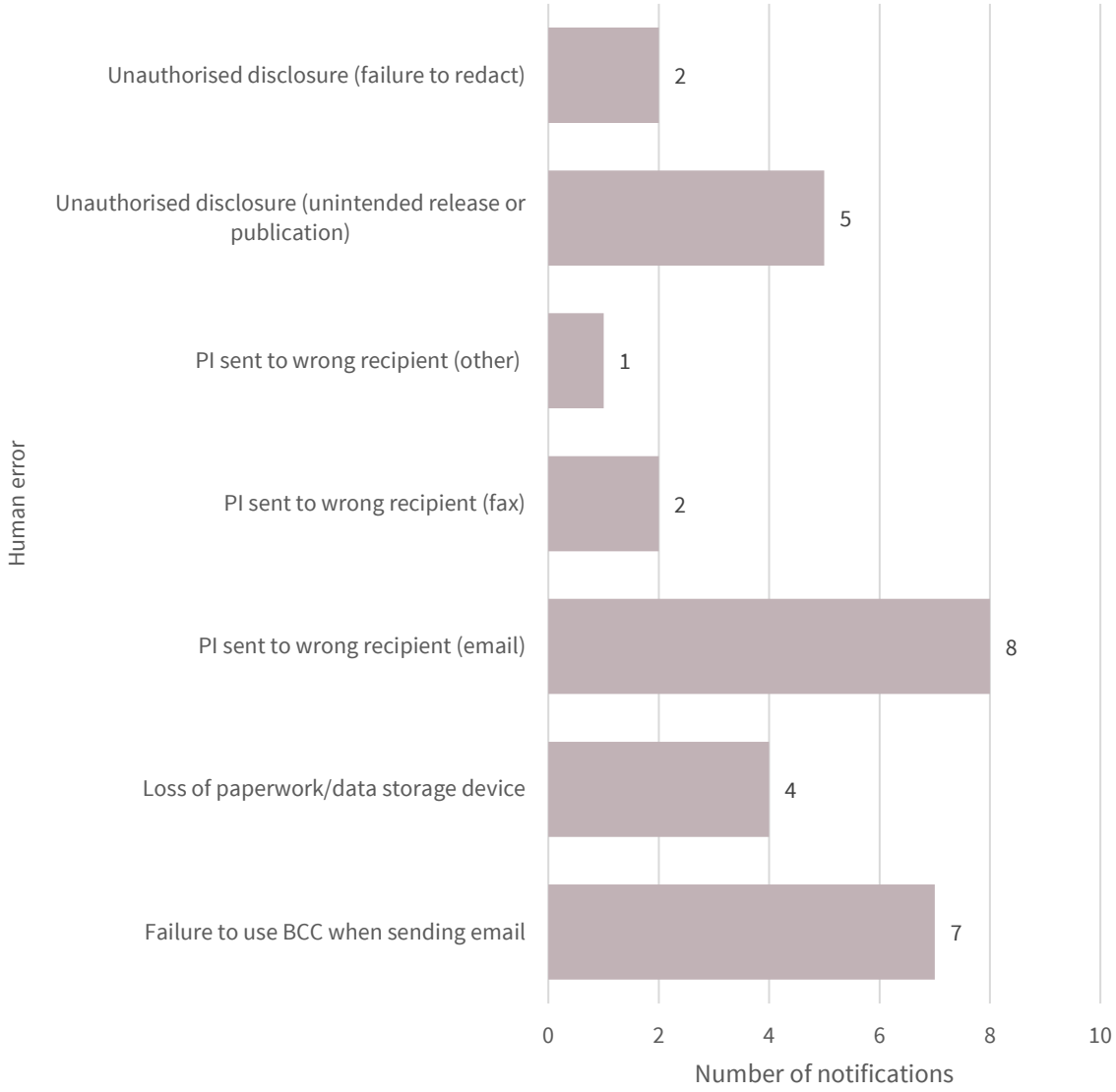
Human error was the leading source of notifications in the health sector (29 notifications). This includes incidents involving communications sent to the wrong recipient, insecure disposal of personal information, or loss of paperwork or a data storage device.

Malicious or criminal attacks was the source of the remaining 25 health sector data breaches.

Human error breaches — Health sector

This chart breaks down the kinds of breaches identified as 'human error' by the health sector in the quarter.

Chart 4.3 — Human error breakdown — Health sector

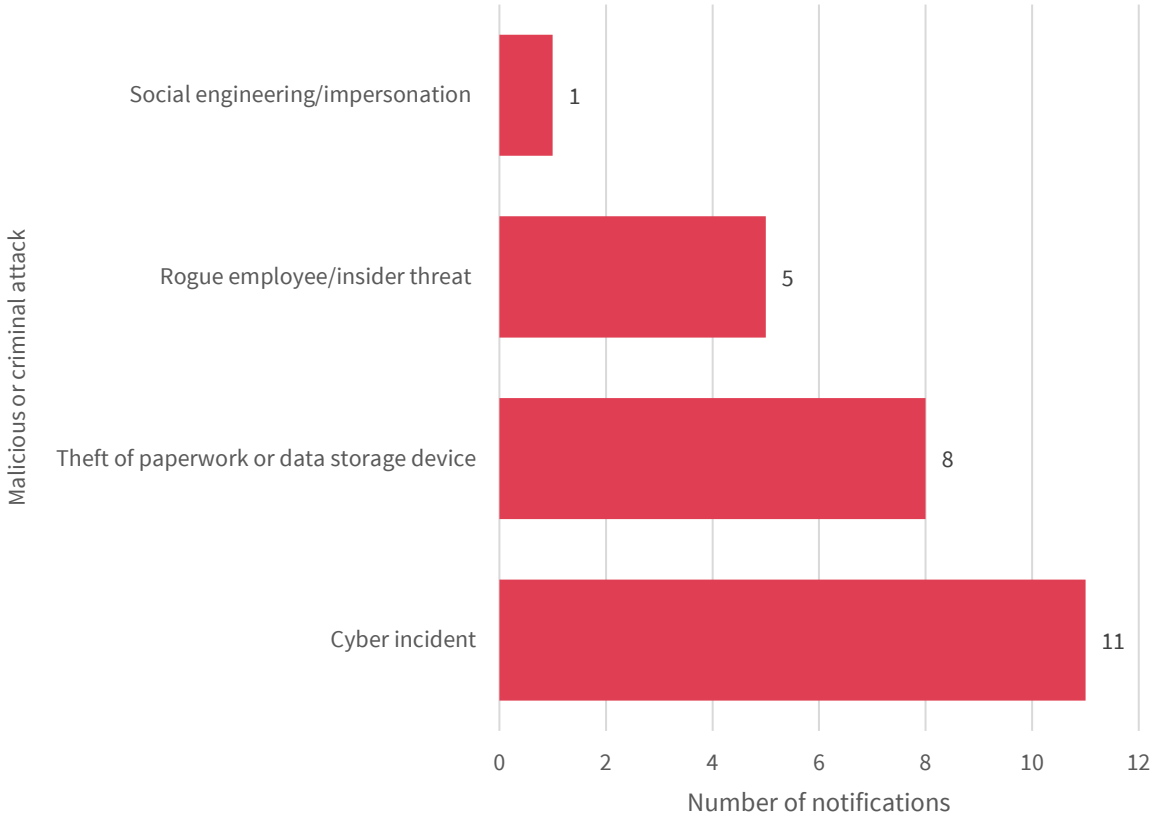


The largest source of data breaches from the health sector was human error (54 per cent), with examples including sending personal information to the wrong recipient by email (28 per cent of human error data breaches), failure to use the blind carbon copy (BCC) function when sending group emails (24 per cent), and unintended release or publication of personal information (17 per cent).

Malicious or criminal attack breaches — Health sector

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack' by the health sector in the quarter.

Chart 4.4 — Malicious or criminal attacks breakdown — Health sector

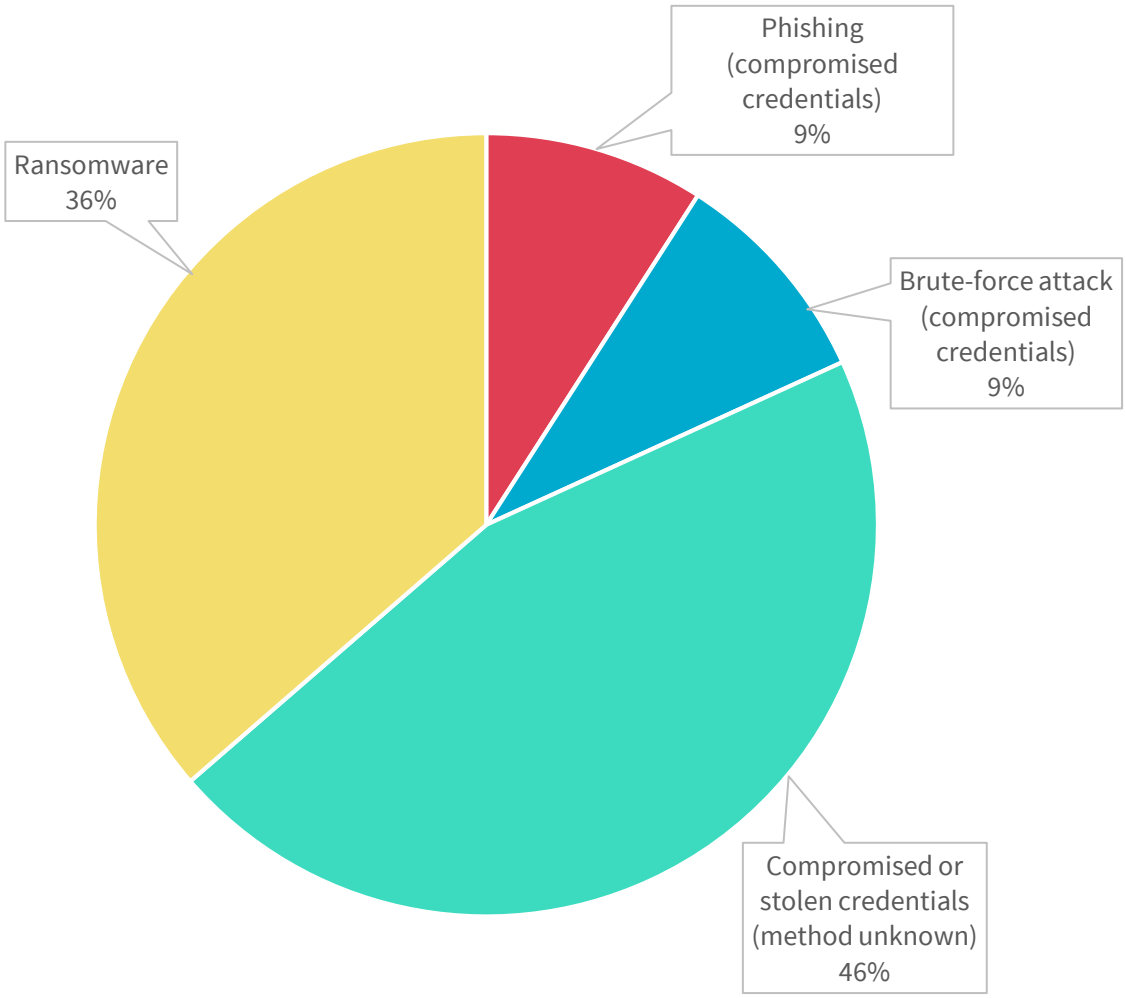


Malicious and criminal attacks was the second largest source of data breaches from the health sector. Cyber incidents were the most common type of attack, accounting for 44 per cent, while theft of paperwork or data storage device was the second most common type of attack (32 per cent).

Cyber incident breaches — Health sector

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack — cyber incident' by the health sector in the quarter.

Chart 4.5 — Cyber incident breakdown — Health sector



The health sector reported that 5 data breaches caused by cyber incidents were the result of compromised credentials through unknown methods. Ransomware (4 notifications), phishing (1 notification) and a brute-force attack (1 notification) account for the remaining cyber incidents.

System fault breaches — Health sector

In the quarter, system fault was not identified as the source of any breaches notified by the health sector.

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 misaddressed email or incorrect 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 fax number incorrectly entered or 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 transcribing error or wrong address on files.
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' or 'CC' 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(s) 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 without authorisation, verbally, 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.

Term	Definition
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.
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks, or personal computer devices.
Malware	Software which 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.
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[4]

Term	Definition/ examples
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, home address, phone number or email address.
Health information	As defined in section 6FA of the Privacy Act.
Other sensitive information	Sensitive information, other than health information, as defined in section 6(1) of the Privacy Act. For example, sexual orientation, political or religious views.

[4] OAIC's Notifiable Data Breach Form.