Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Quarterly Statistics Report

1 January to 31 March 2019

oaic.gov.au

OAIC

Final report issued: 13/05/19

Contents

Key statistics

215
notifications

35%
human error

61%
malicious or criminal attacks

4%
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 January 2019 and 31 March 2019 (referred to as 'data breaches').

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

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.

Please note, from July 2019 the OAIC will report every six months on notifications received under the NDB scheme.

Notifications received from all sectors

Number of data breaches reported — All sectors

Chart 1.1 — Number of data breaches reported under the NDB scheme by month — All sectors

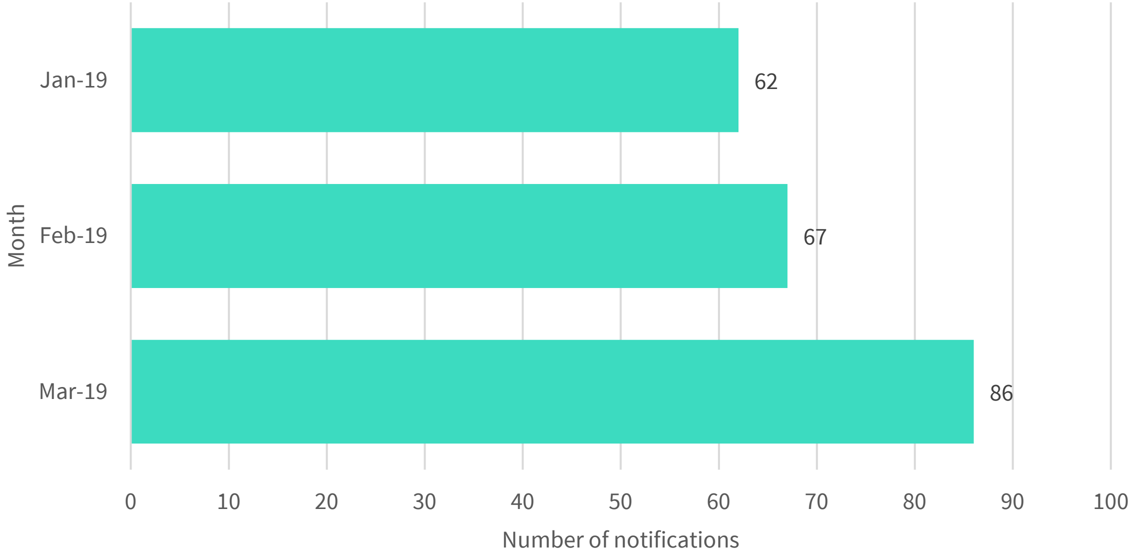
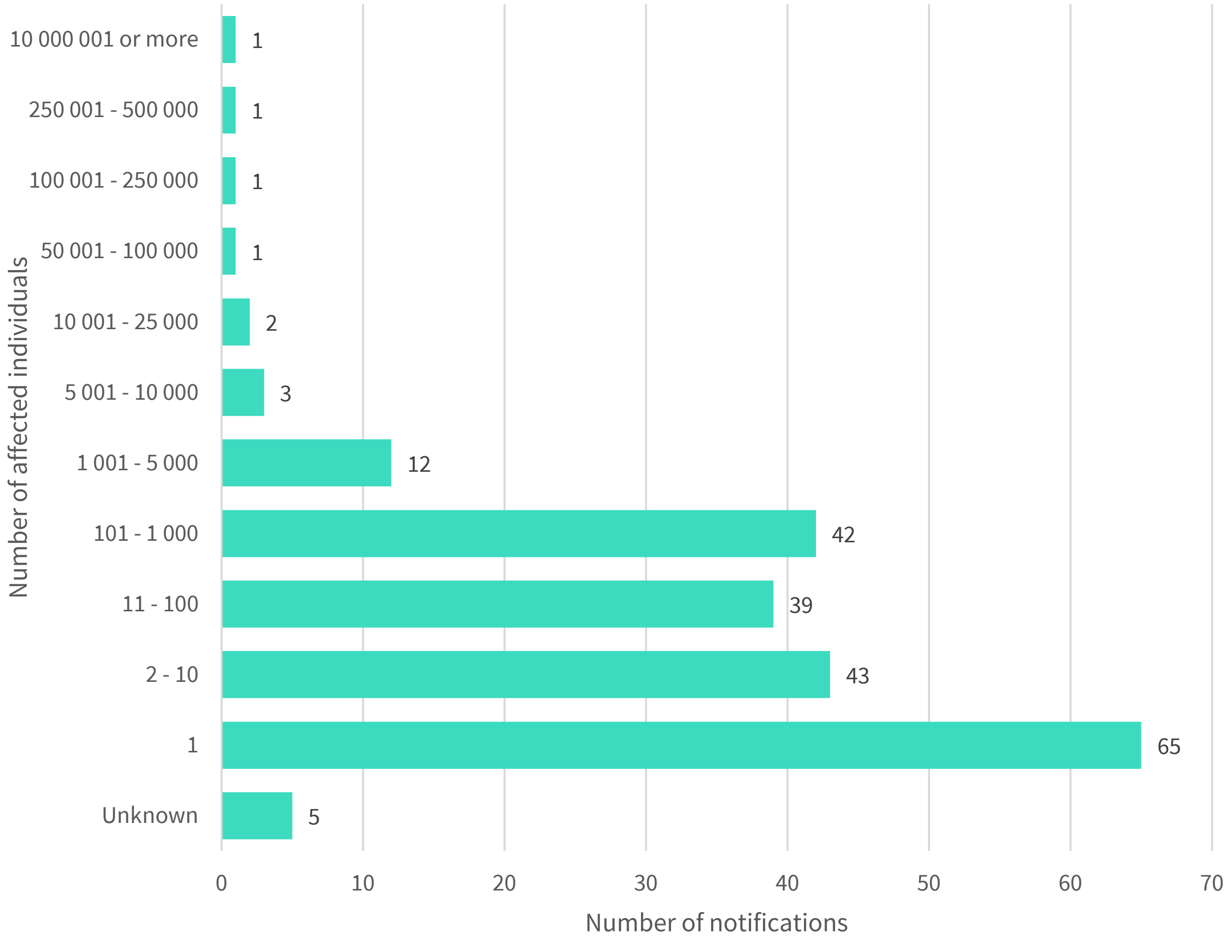


Table 1.A — Number of data breaches reported under the NDB scheme by quarter — All sectors

Quarter	Total number of notifications
April to June 2018	242
July to September 2018	245
October to December 2018	262
January to March 2019	215

Number of individuals affected by data breaches — All sectors

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



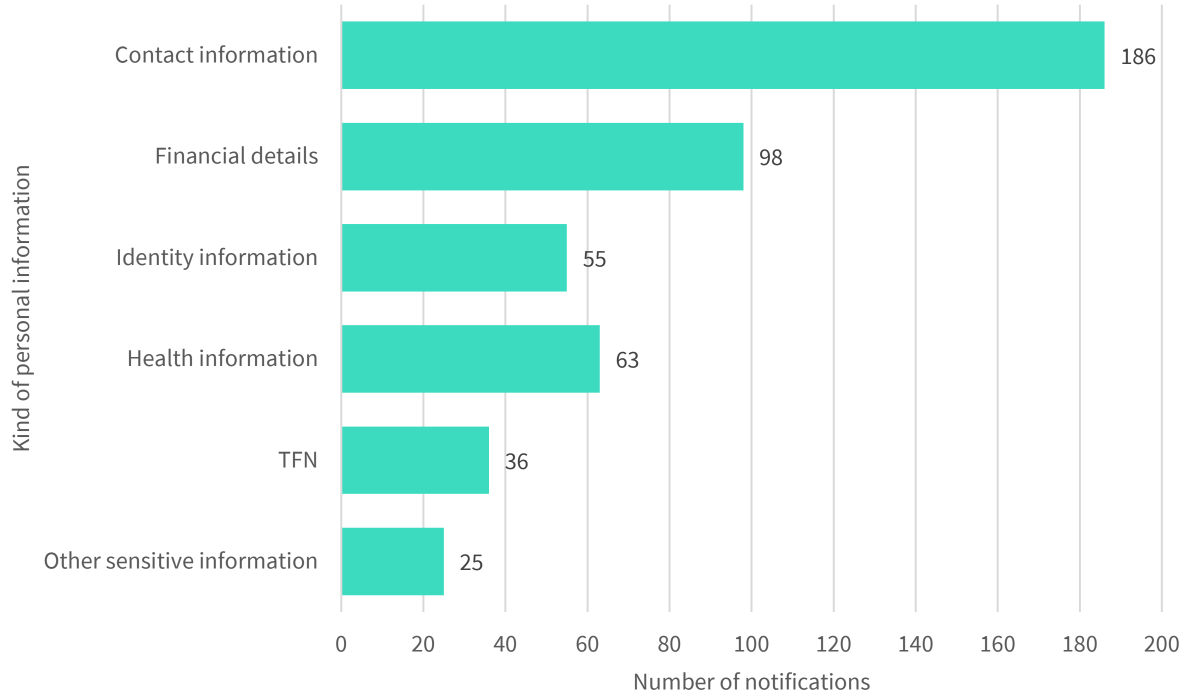
Note: Where bands are not shown (for example, 500 001 – 1 000 000) there were nil reports in the period. ‘Unknown’ includes notifications by entities whose investigations were ongoing at the time of this report.

The majority of data breaches in the period involved the personal information of 100 individuals or fewer (68 per cent of data breaches).

Data breaches impacting between one and 10 individuals comprised 50 per cent of the notifications.

Kind of personal information involved in data breaches — All sectors

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



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

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

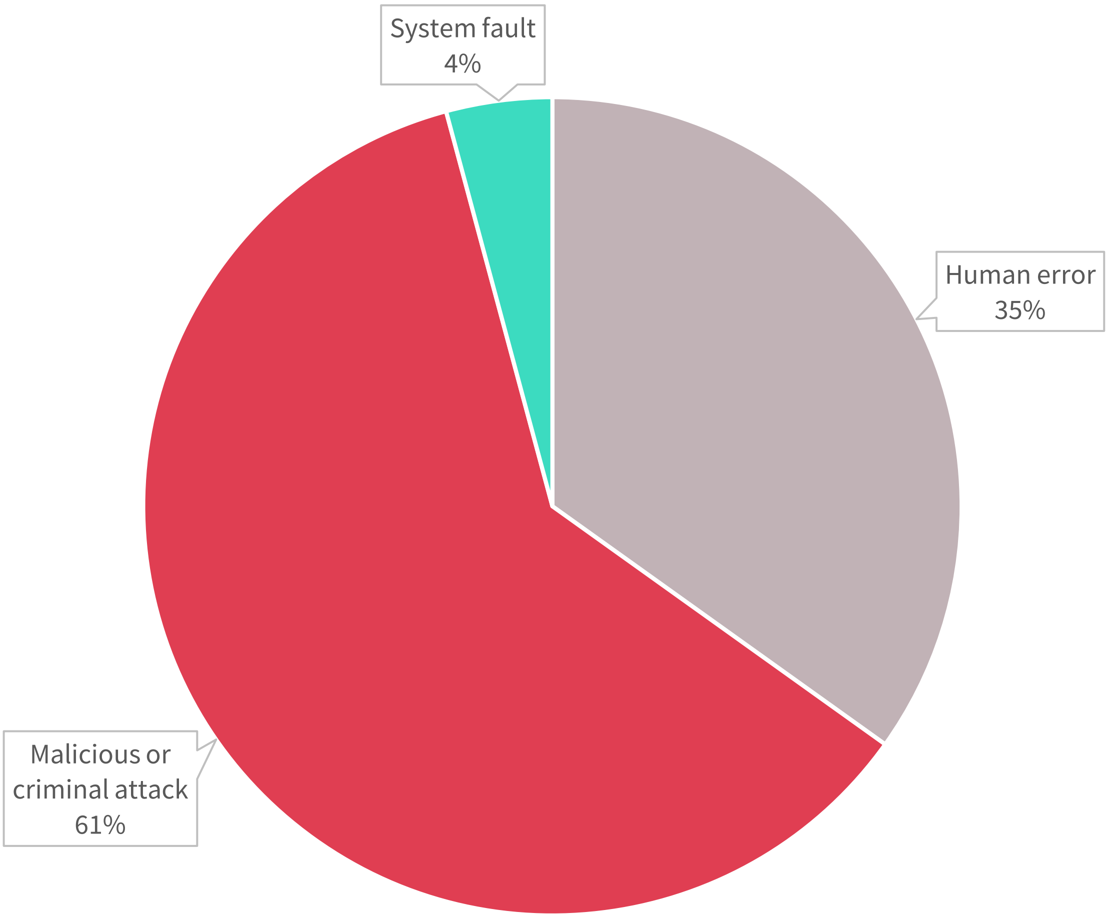
Kind of personal information	NDBs received (%)
Contact information	87
Financial details	46
Identity information	26
Health information	29
TFN	17
Other sensitive information	12

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

Source of data breaches — All sectors

This chart breaks down the sources of data breaches as identified by notifying entities.

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



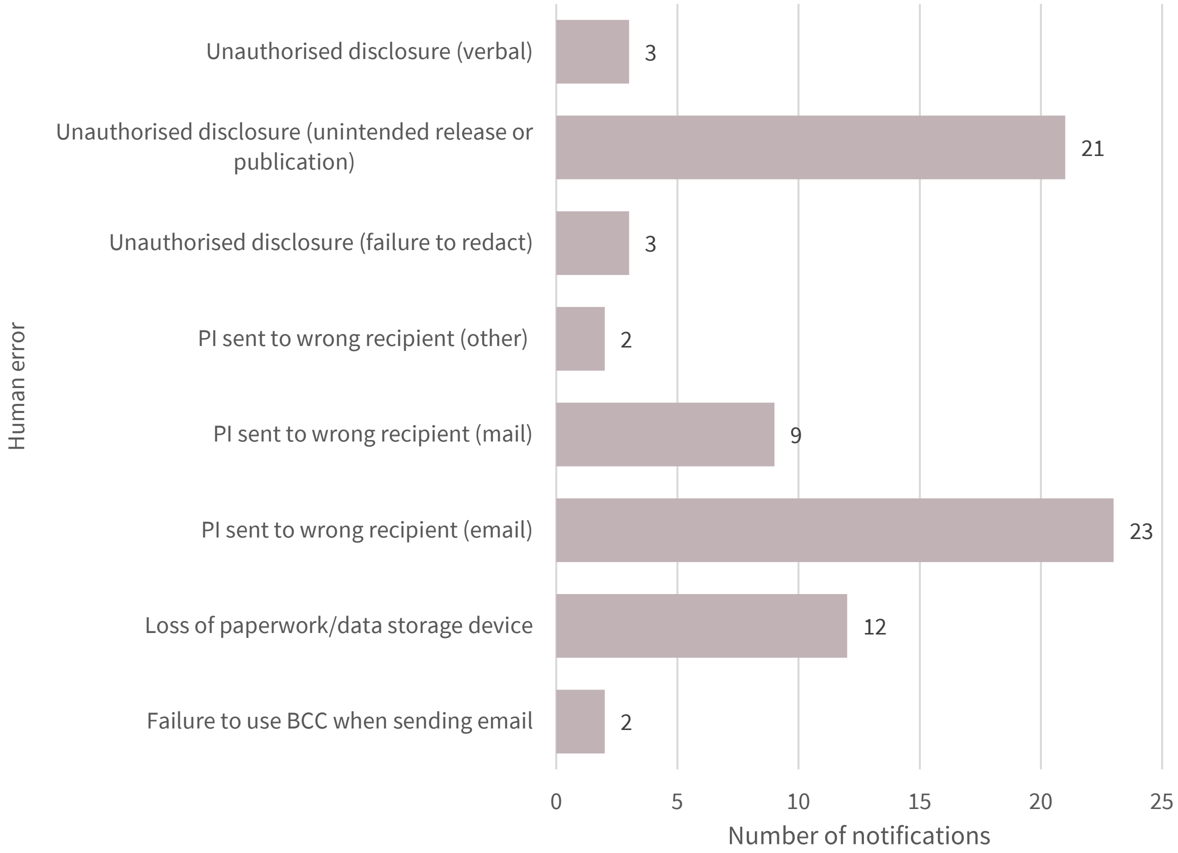
Malicious or criminal attacks accounted for 131 data breaches this quarter, while human error accounted for 75 data breaches. System faults accounted for nine data breaches.

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 incidents in this quarter appear to have exploited vulnerabilities involving a human factor, such as clicking on a phishing email or by using social engineering or impersonation to obtain access to personal information fraudulently.

Human error data breaches — All sectors

This chart shows the types of data breaches identified as 'human error' during the quarter.

Chart 1.5 — Human error breakdown — All sectors



The second largest source of data breaches was human error, such as sending personal information to the wrong recipient via email (31 per cent), loss of paperwork or storage device (16 per cent) as well as the unintended release or publication of personal information (28 per cent).

Certain kinds of data 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 36,993 affected individuals per data breach). This is consistent with the previous quarterly trend. Failure to use BCC when sending emails impacted an average of 432 individuals per data breach.

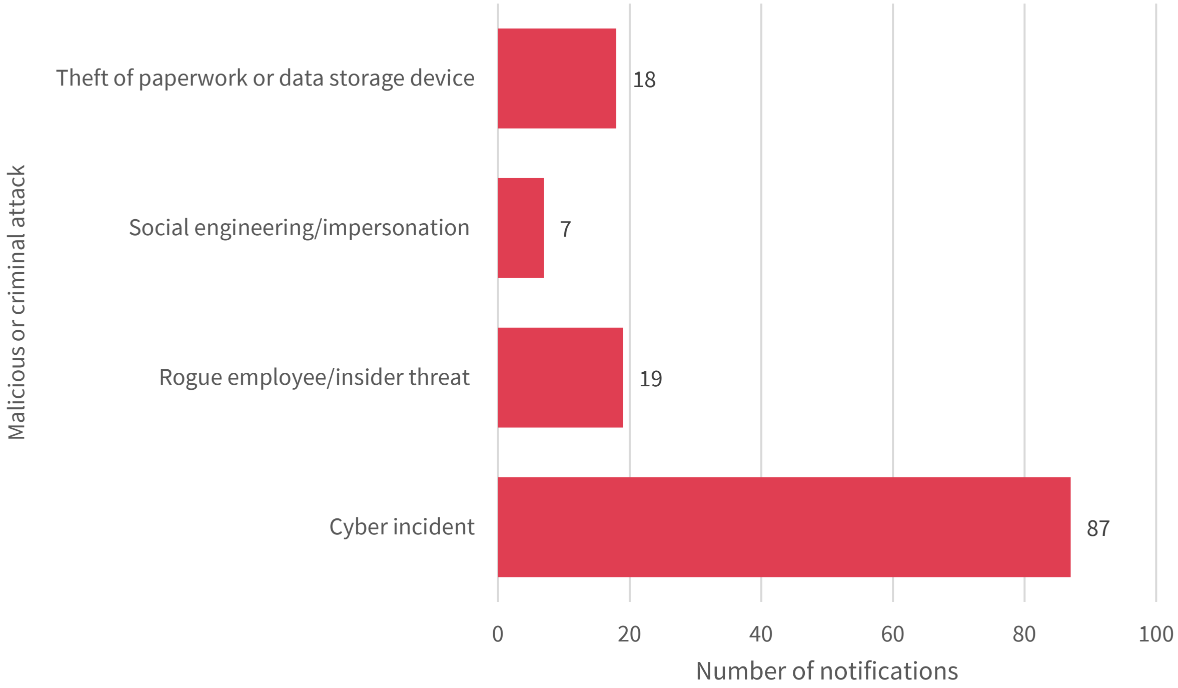
Table 1.C — Human error breakdown by average number of affected individuals — All sectors

Type of data breach	NDBs received	Average number of affected individuals
Unauthorised disclosure (unintended release or publication)	21	36,993
Failure to use BCC when sending email	2	432
PI sent to wrong recipient (other)	2	69
Unauthorised disclosure (failure to redact)	3	24
Loss of paperwork/data storage device	12	19
PI sent to wrong recipient (email)	23	13
PI sent to wrong recipient (mail)	9	5
Unauthorised disclosure (verbal)	3	1

Malicious or criminal attack data breaches — All sectors

This chart shows the types of data breaches identified as 'malicious or criminal attack' during the quarter.

Chart 1.6 — Malicious or criminal attacks breakdown — All sectors



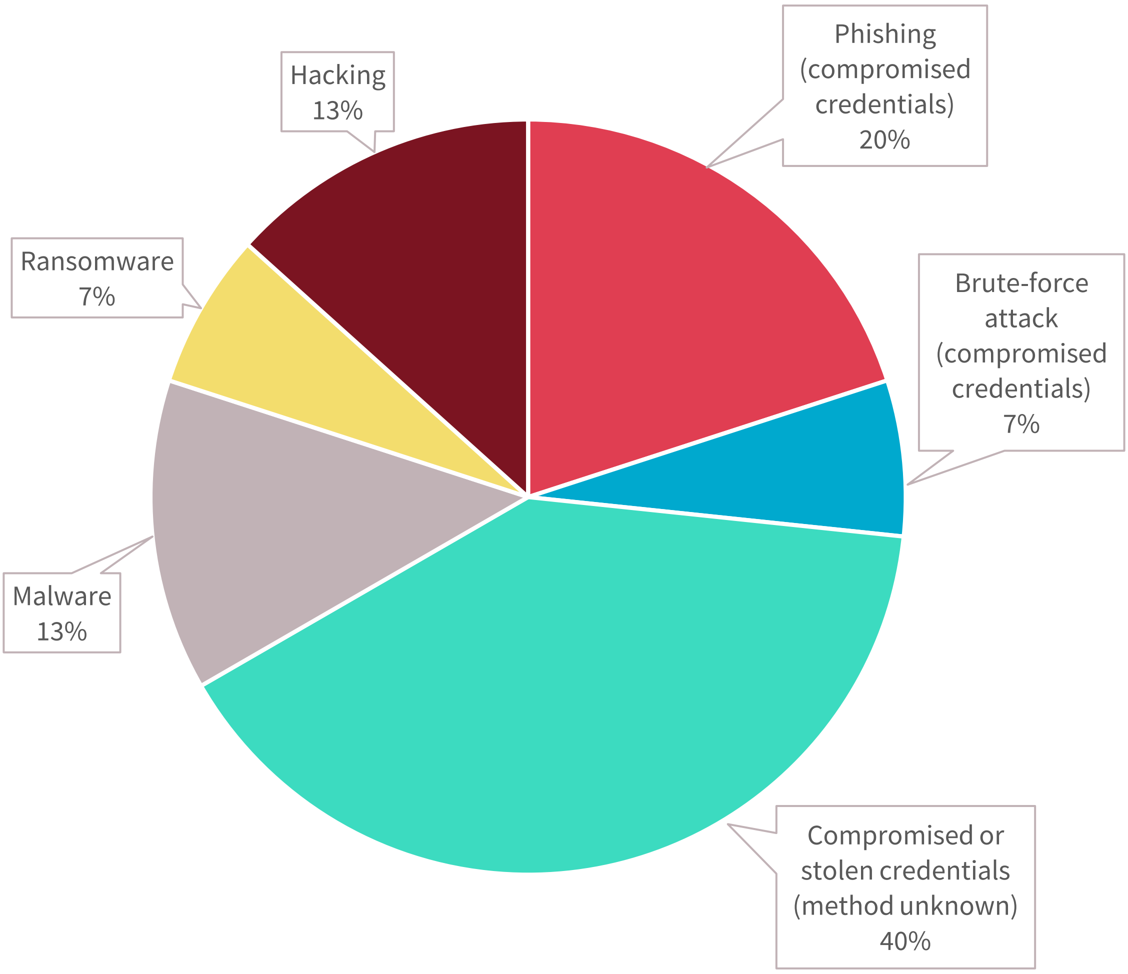
Malicious or criminal attacks were the largest source of data breaches this quarter, accounting for 61 per cent of all data breaches. Of these 131 data breaches, 66 per cent involved cyber incidents such as phishing, malware or ransomware, brute-force attacks, compromised or stolen credentials.

Theft of paperwork or data storage devices was another source of malicious or criminal attacks (14 per cent). Other sources included actions taken by a rogue employee or insider threat (15 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' during the quarter.

Chart 1.7 — Cyber incident breakdown — All sectors

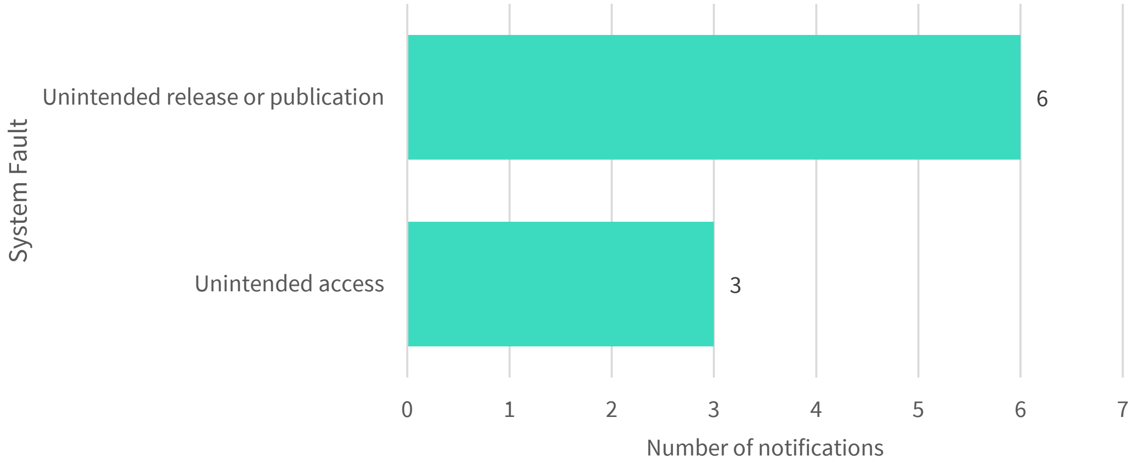


The majority of cyber incidents were linked to the compromise of credentials through phishing (28 notifications), unknown methods (33 notifications) or by brute-force attack (six notifications).

System fault data breaches — All sectors

This chart shows the types of breaches identified as 'system fault' during the quarter.

Chart 1.8 — System fault breakdown — All sectors



System faults accounted for four 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 data breaches in the quarter

This section compares notifications made under the NDB scheme by the five sectors that made the most notifications during 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]	58
Finance (including superannuation) [2]	27
Legal, accounting and management services	23
Education [3]	19
Retail	11

The NDB scheme applies to agencies and organisations that the *Privacy Act 1988* (Cth) (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 tax file number (TFN) recipients, among others.

From January to March 2019, the top sector to report data breaches under the NDB scheme was the private health service provider sector (health sector) (27 per cent). The second largest source of NDBs was the finance sector (13 per cent). This was followed by the legal, accounting and management services sector (11 per cent), the private education sector (education) (9 per cent), and the retail 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.

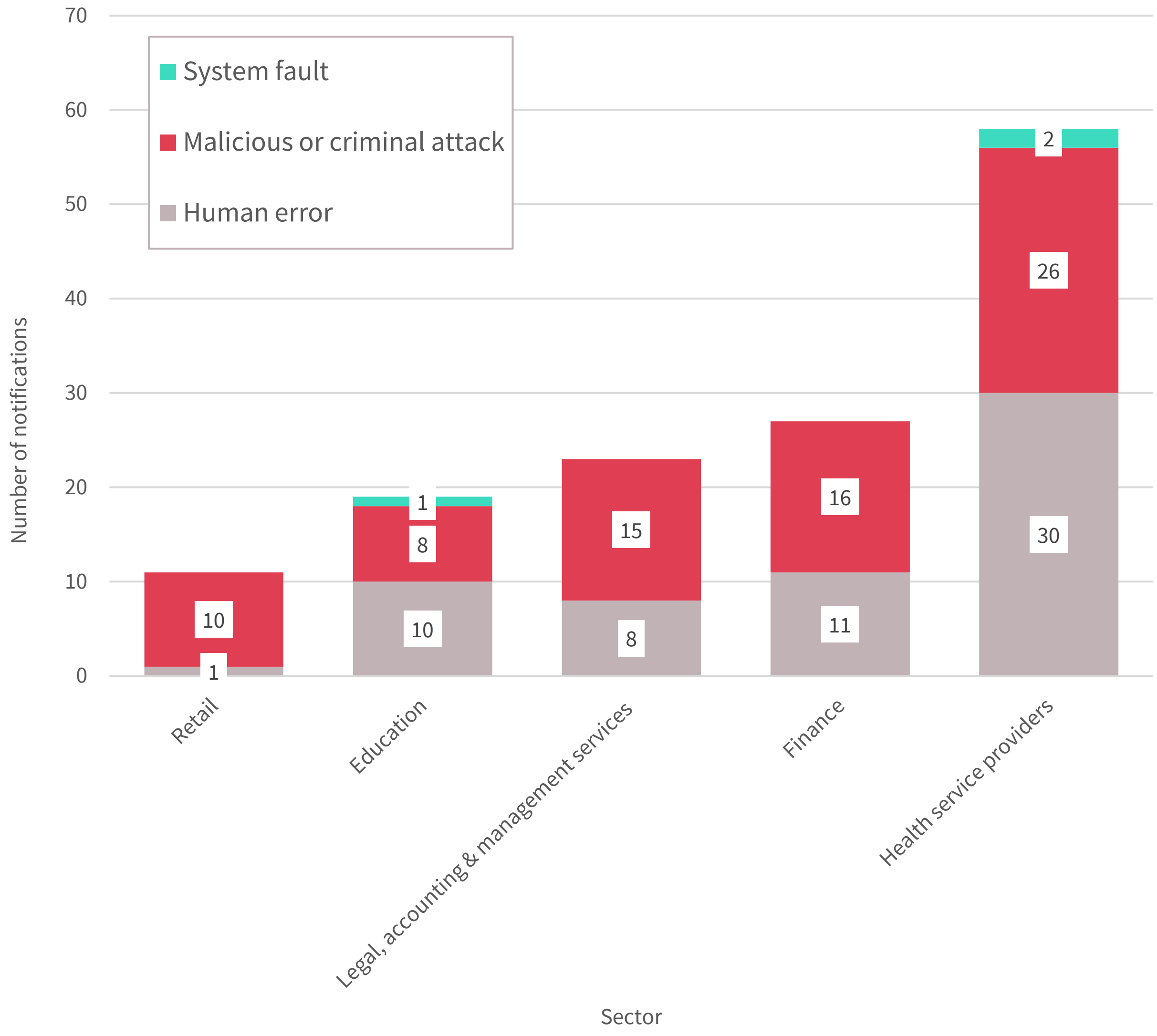
[2] This sector includes banks, wealth managers, financial advisors, superannuation funds and consumer credit providers (regardless of annual turnover).

[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 data breaches — Top five sectors

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

Chart 2.1 — Source of data breaches — Top five sectors



The highest reporting sector this quarter was the health sector (58 notifications). Of those notifications, 52 per cent of data breaches resulted from human error. In contrast, notifications from the second highest reporting sector, finance, indicated that 59 per cent of its data breaches resulted from malicious or criminal attacks.

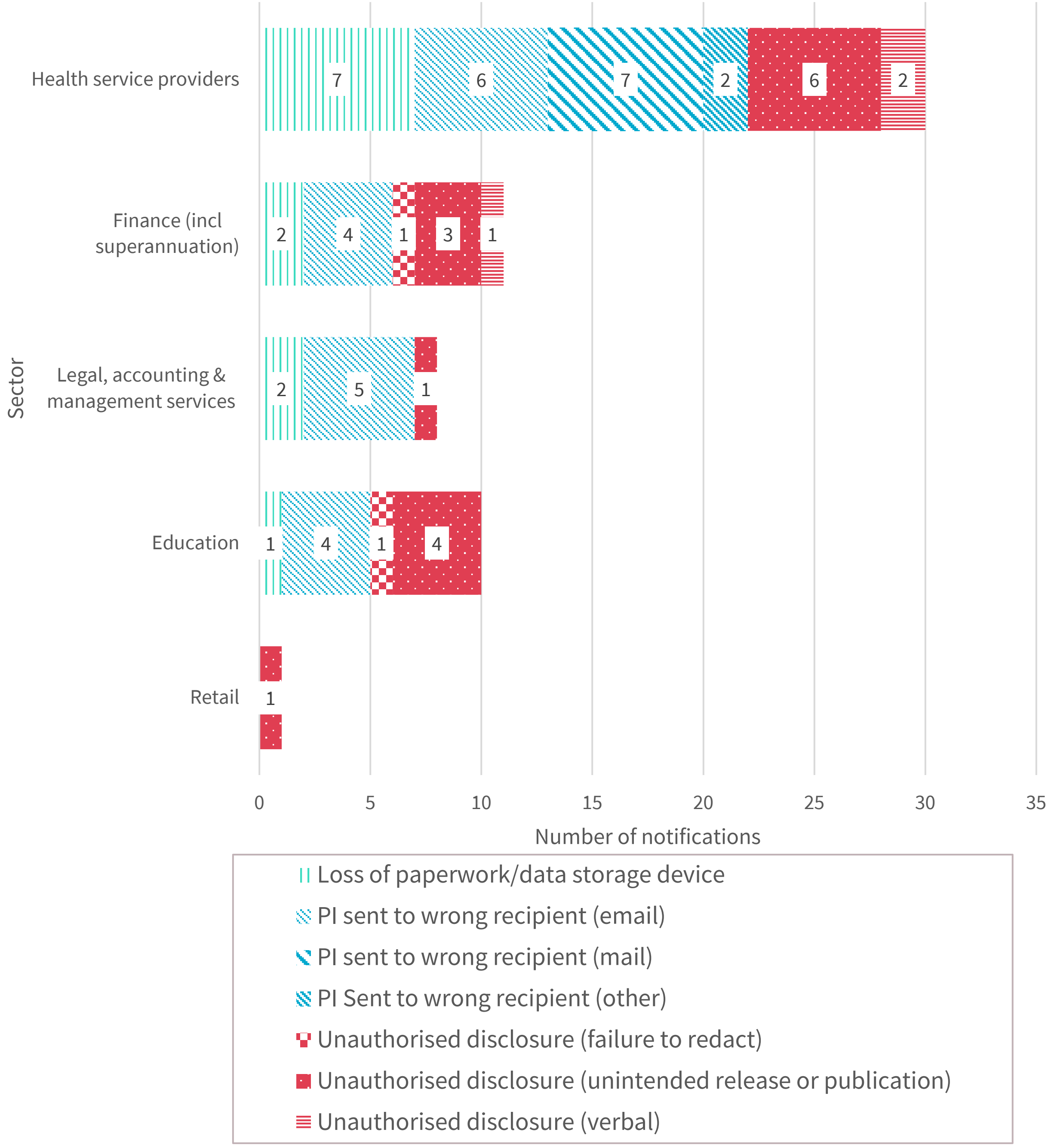
The legal, accounting and management services sector and the retail sector also reported the majority of data breaches resulted from malicious or criminal attacks.

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

Human error data breaches — Top five sectors

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

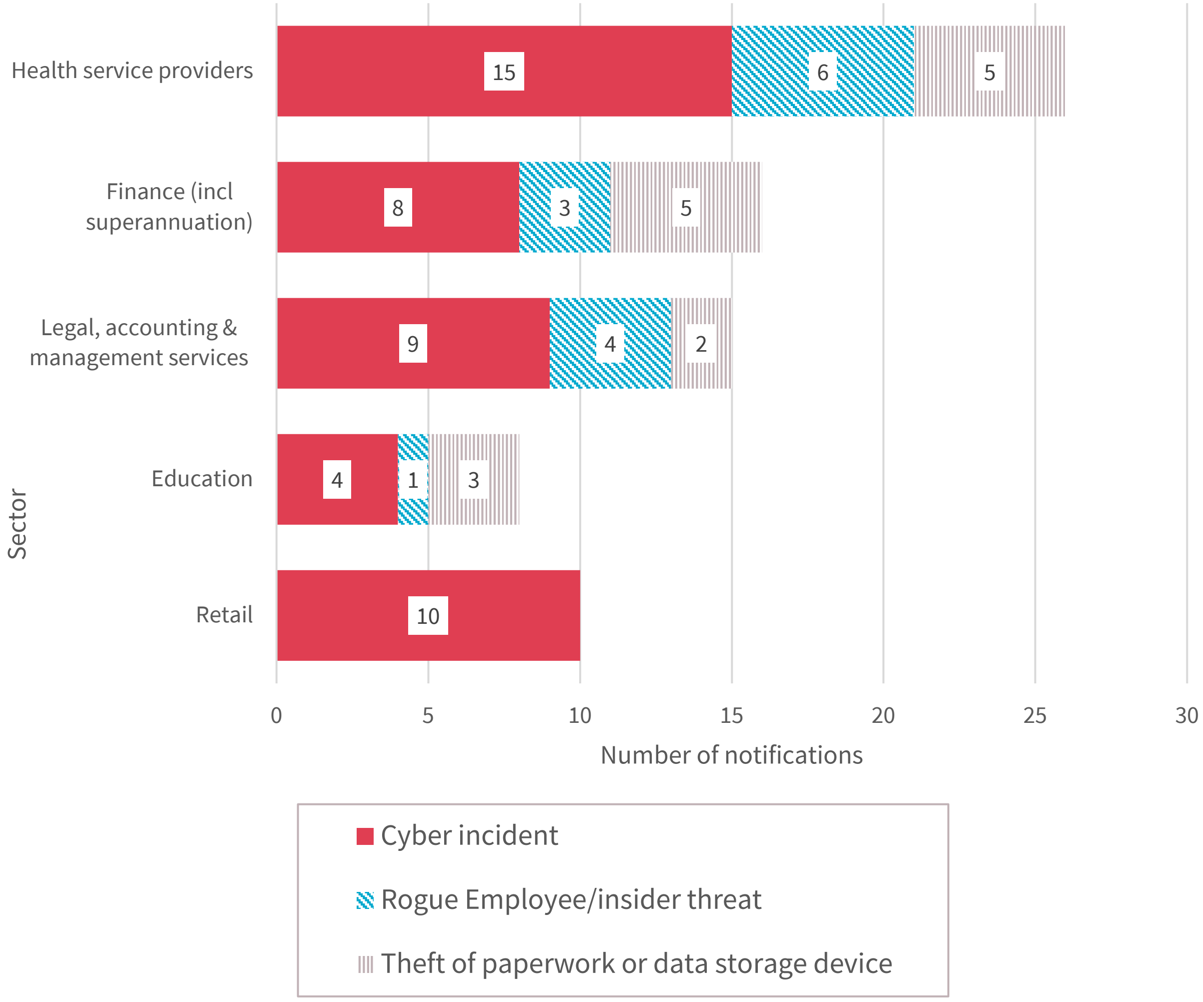
Chart 2.2 — Human error breakdown — Top five sectors



Malicious or criminal attack breaches — Top five sectors

This chart shows the types of data breaches identified as 'malicious or criminal attack' by the top five sectors during the quarter.

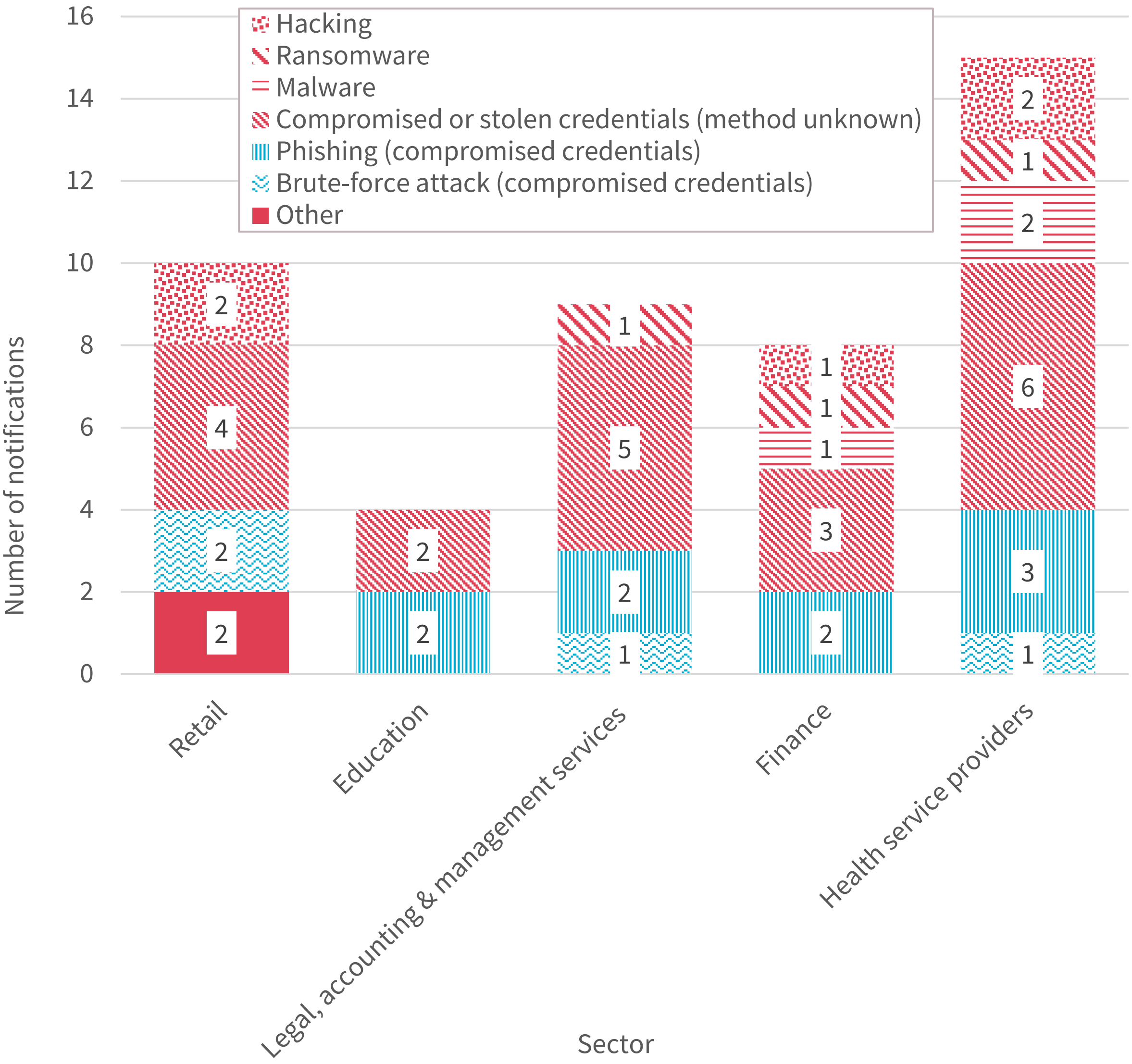
Chart 2.3 — Malicious or criminal attacks breakdown — Top five sectors



Cyber incident data breaches — Top five sectors

This chart shows the types of breaches identified as 'malicious or criminal attack — cyber incident' by the top five sectors during the quarter.

Chart 2.4 — Cyber incident breakdown — Top five sectors

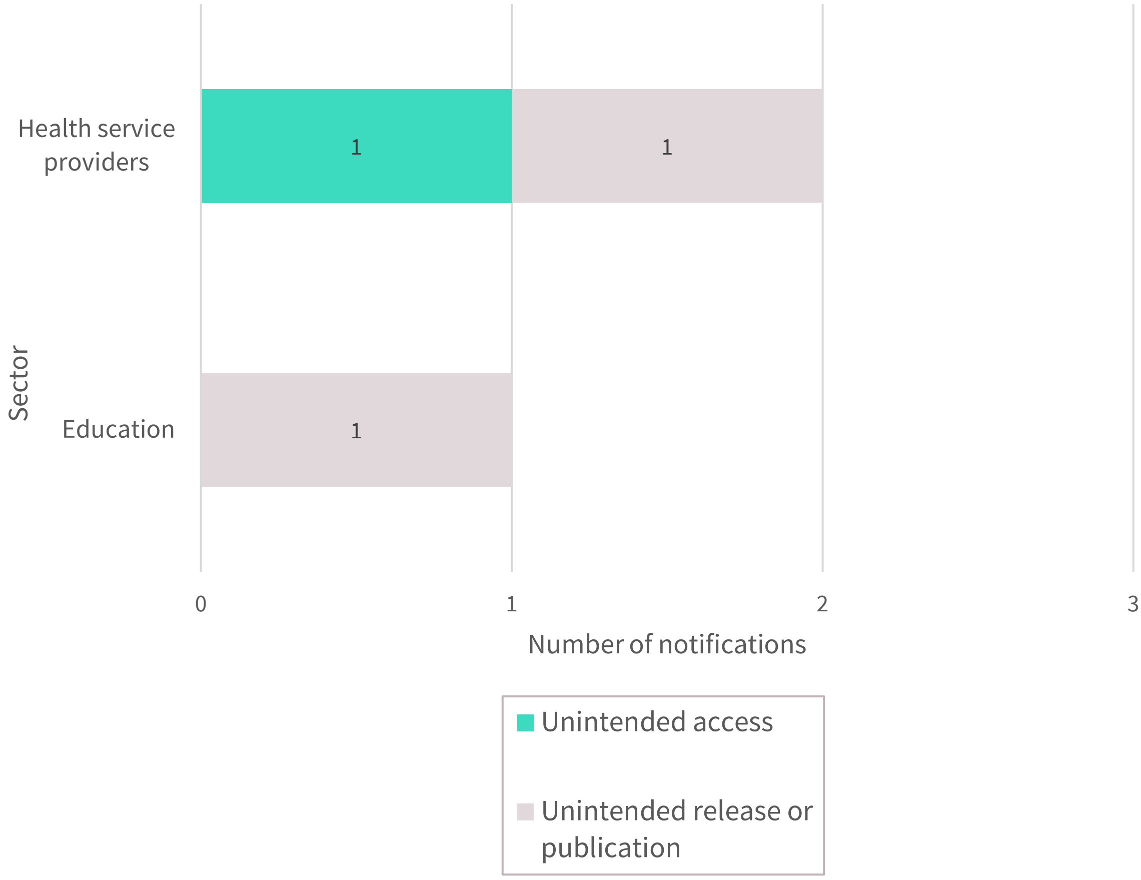


In line with the overall trend, the majority of cyber incidents reported by the top five sectors were linked to the compromise of credentials through phishing, brute-force attacks or by unknown methods (33 notifications overall).

System fault data breaches — Top five sectors

This chart breaks down the types of data breaches identified as 'system fault' by the top five sectors during the quarter.

Chart 2.5 — System fault breakdown — Top five sectors



The finance sector, the legal, accounting and management services sector and the retail 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

27
notifications

41%
human error

59%
malicious or criminal attacks

0%
system faults

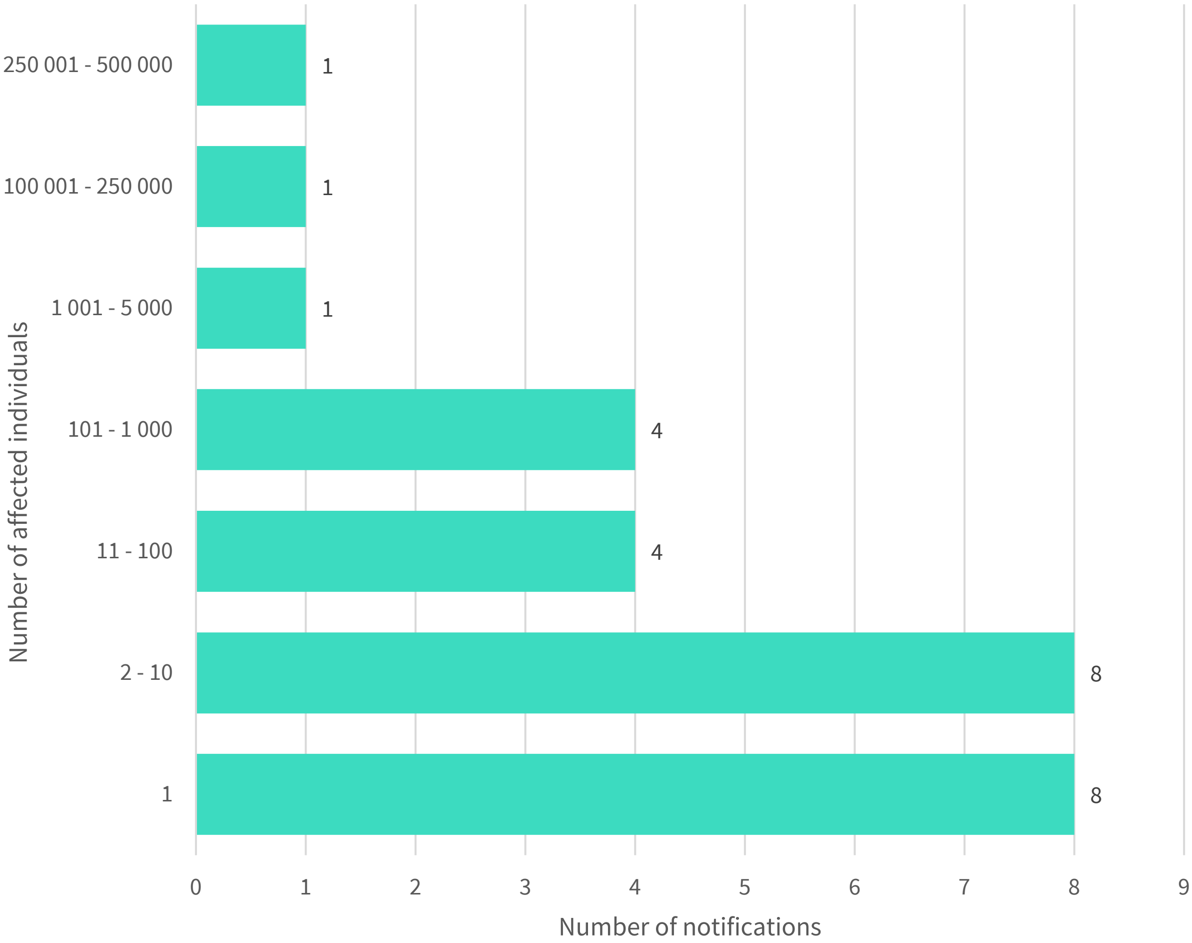
Number of data breaches reported under the NDB Scheme — Finance sector

Table 3.A — Number of data breaches reported under the NDB scheme by the finance sector by quarter

Quarter	Total number of notifications
April to June 2018	36
July to September 2018	35
October to December 2018	40
January to March 2019	27

Number of individuals affected by data breaches — Finance sector

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

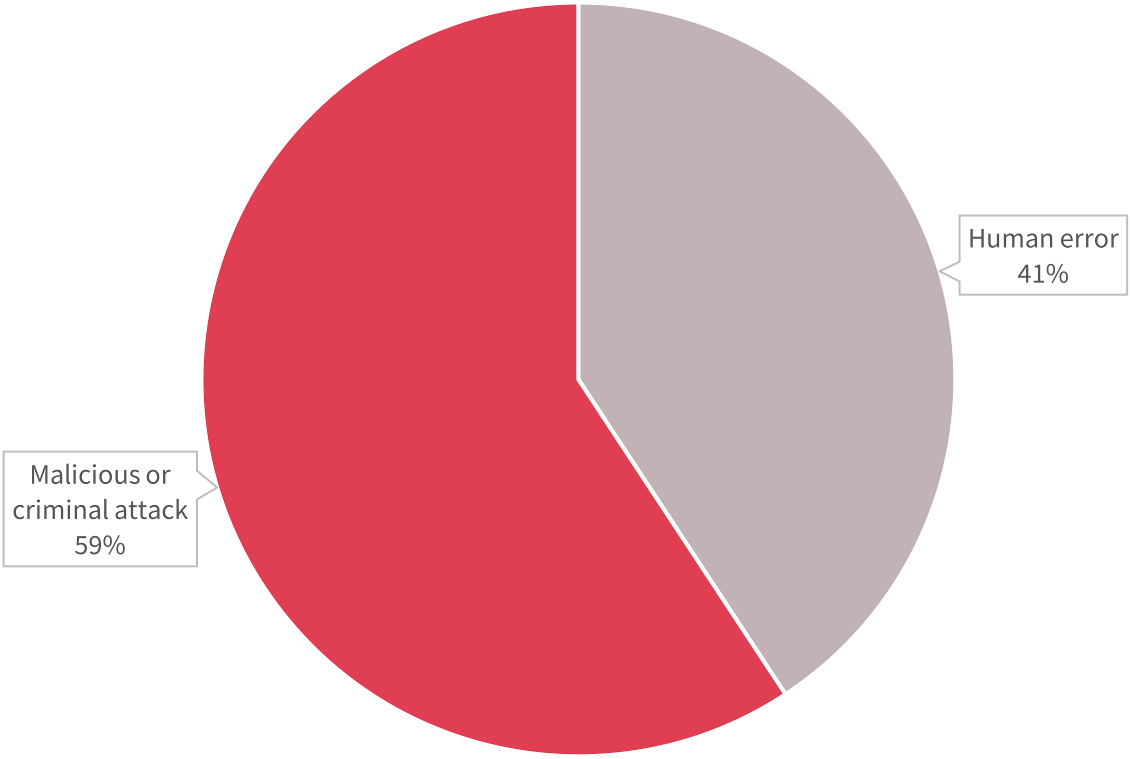


Note: Where bands are not shown there were nil reports in the period.

Most finance sector notifications in the period involved the personal information of 100 individuals or fewer (74 per cent of data breaches). Data breaches affecting between one and 10 individuals comprised 59 per cent of the notifications.

Source of data breaches — Finance sector

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



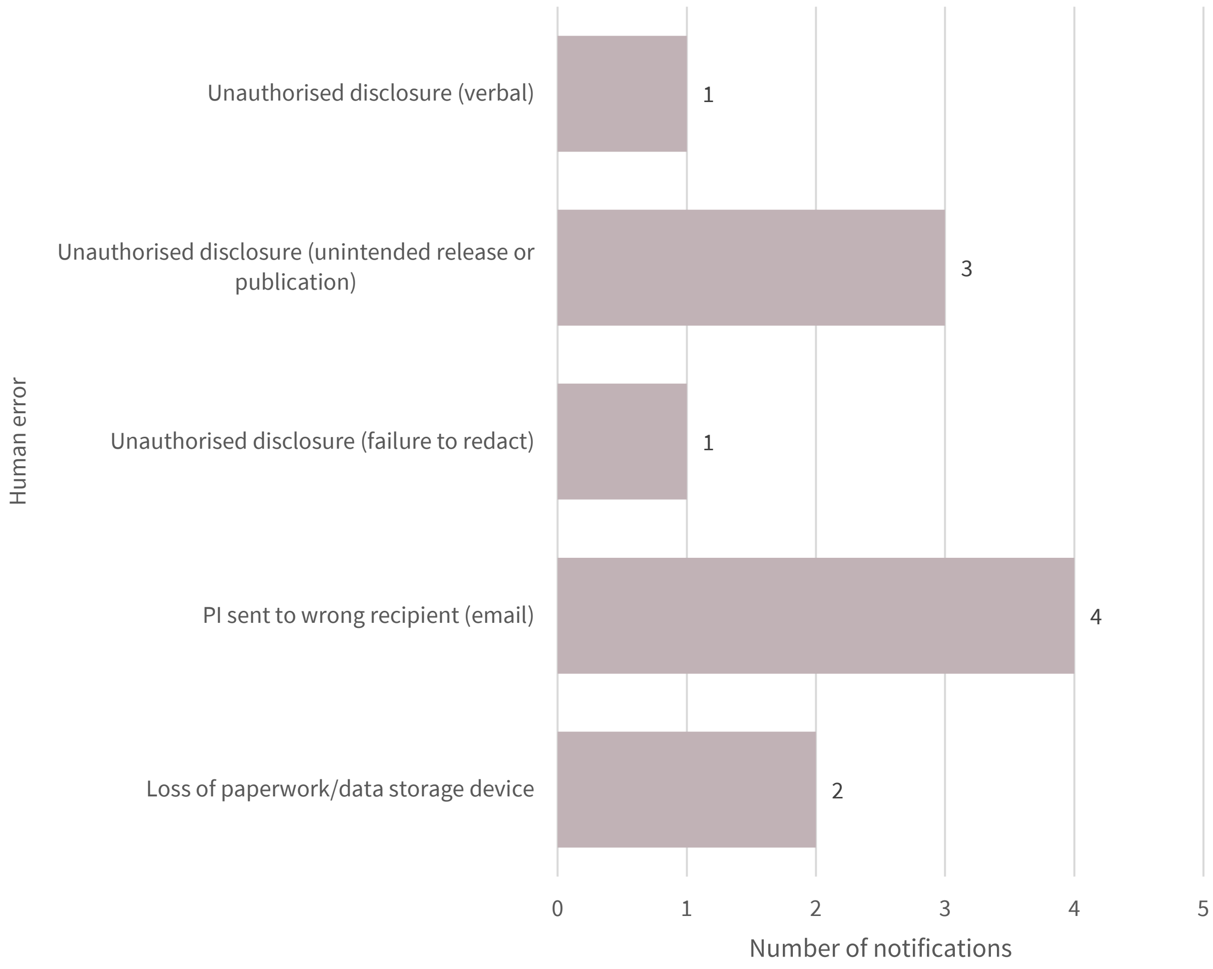
Malicious or criminal attacks were the cause of most notifications from the finance sector this quarter (16 notifications). This includes cyber incidents, such as using a phishing email to obtain credentials or the hacking of systems or networks. These attacks may also include a rogue employee improperly accessing or disclosing personal information.

Human error was the source of 11 notifications from the finance sector, such as personal information sent to the wrong recipient, loss of paperwork or data storage device, or the unauthorised release or publication of personal information.

Human error data breaches — Finance sector

This chart shows the types of data breaches identified as 'human error' by the finance sector during the quarter.

Chart 3.3 — Human error breakdown — Finance sector

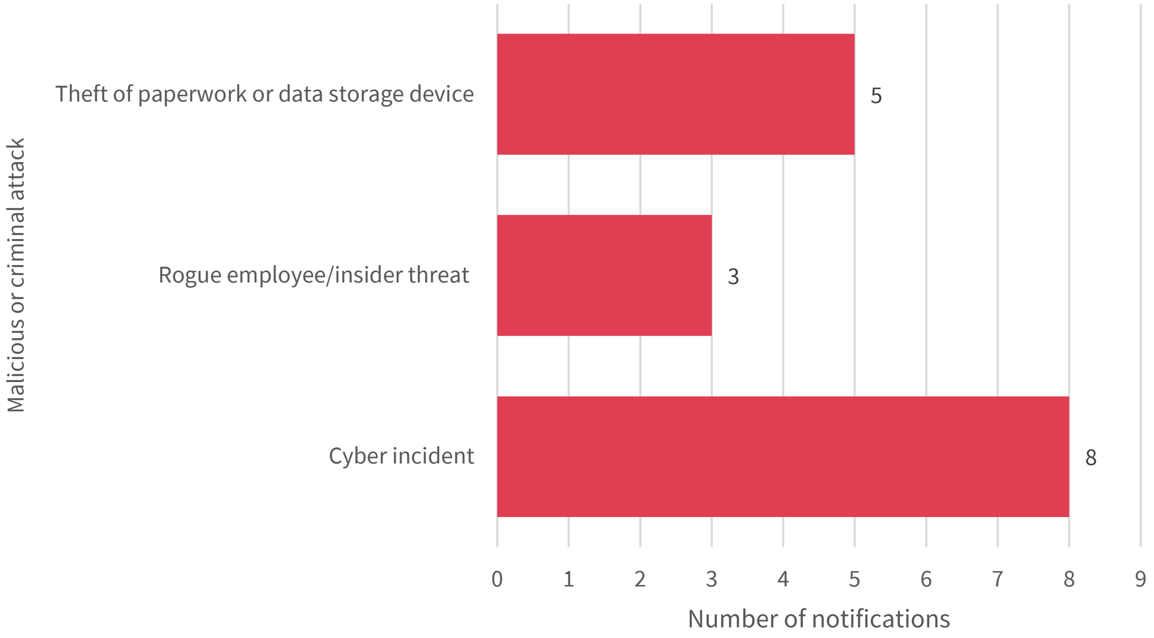


Human error was the second largest source of data breaches from the finance sector. Examples include sending correspondence containing personal information to the wrong recipient by email (36 per cent of human error notifications) and disclosing personal information through an unintended release or publication (27 per cent).

Malicious or criminal attack data breaches — Finance sector

This chart shows the types of data breaches identified as 'malicious or criminal attack' by the finance sector during the quarter.

Chart 3.4 — Malicious or criminal attacks breakdown — Finance sector

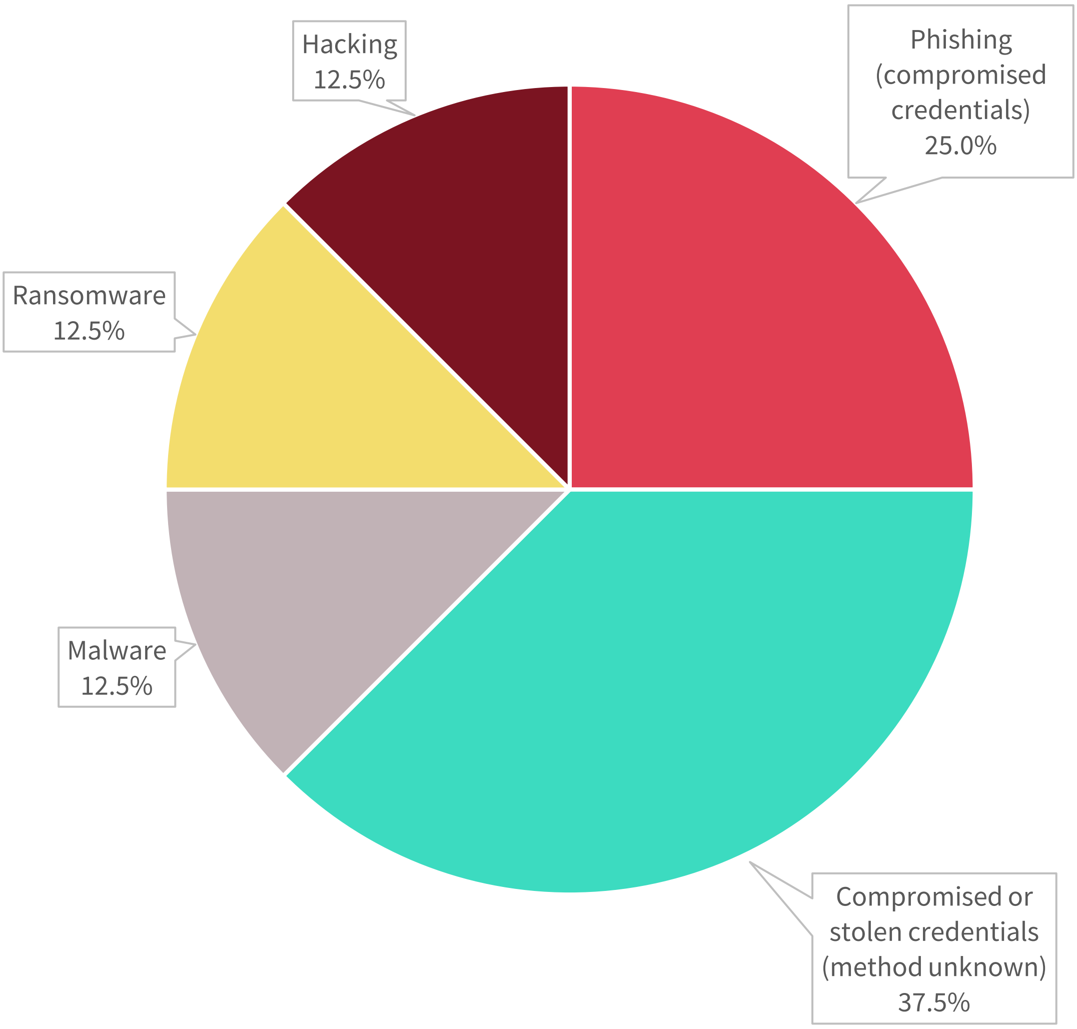


Malicious and criminal attacks were the leading cause of data breaches notified by the finance sector (59 per cent). Of these, cyber incidents were the most common type of attack (50 per cent), followed by theft of paperwork or data storage device (31 per cent), and rogue employees or insider threats (19 per cent).

Cyber incident data breaches — Finance sector

This chart shows the types of data breaches identified as 'malicious or criminal attack — cyber incident' by the finance sector during 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 (two notifications) or unknown methods (three notifications). Hacked websites or systems, malware and ransomware were each responsible for one notification.

System fault data breaches — Finance sector

System fault was not identified as the source of any data breaches notified by the finance sector during the quarter.

Health sector report

This section captures notifications made under the NDB scheme by entities in the health sector.

Summary — Health sector

58
notifications

52%
human error

45%
malicious or criminal attacks

3%
system faults

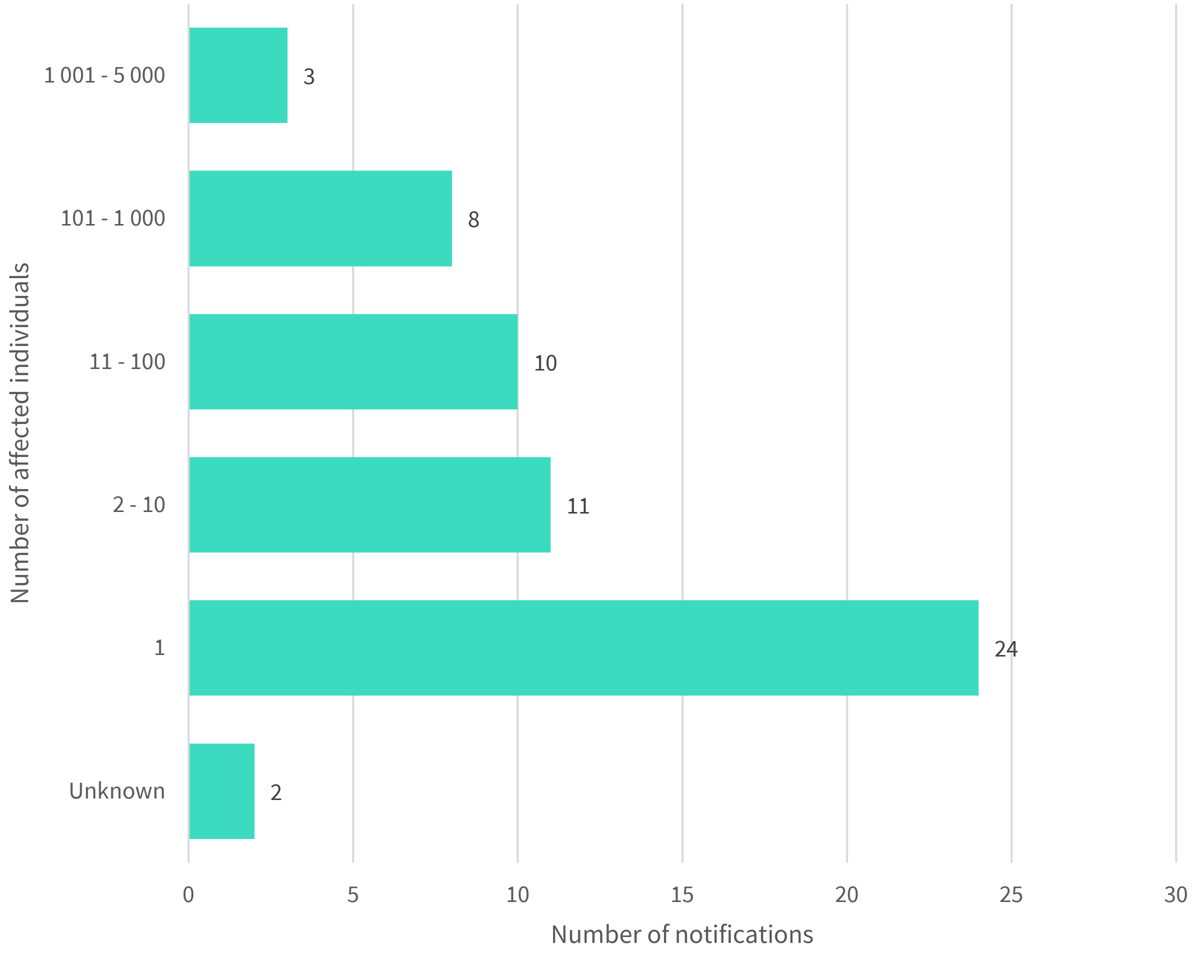
Number of data breaches reported under the NDB scheme — Health sector

Table 4.A — Number of data breaches reported under the NDB scheme by the health sector by quarter

Quarter	Total number of notifications
April to June 2018	49
July to September 2018	45
October to December 2018	54
January to March 2019	58

Number of individuals affected by data breaches — Health sector

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

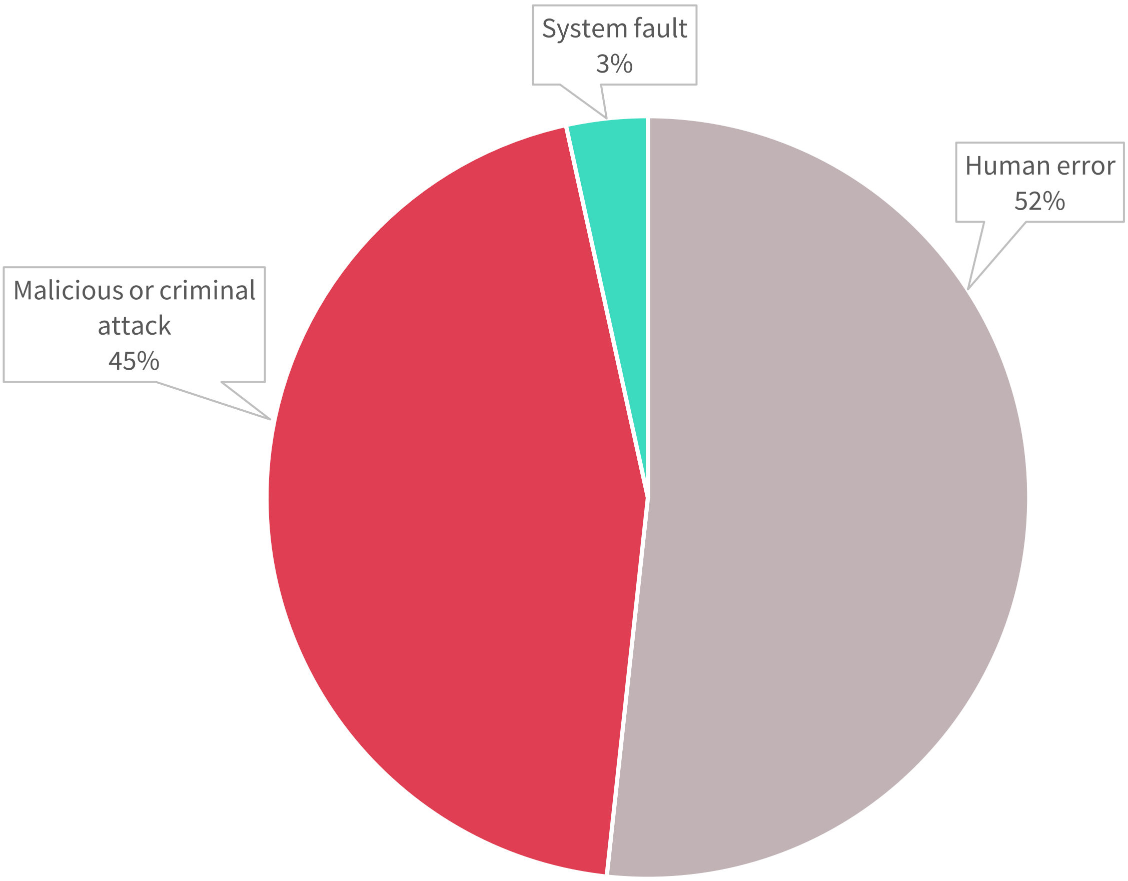


Note: Where bands are not shown there were nil reports in the period.

Most health sector notifications in the period involved the personal information of 100 individuals or fewer (78 per cent of breaches). Data breaches affecting between one and 10 individuals comprised 60 per cent of the notifications.

Source of the data breaches — Health sector

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



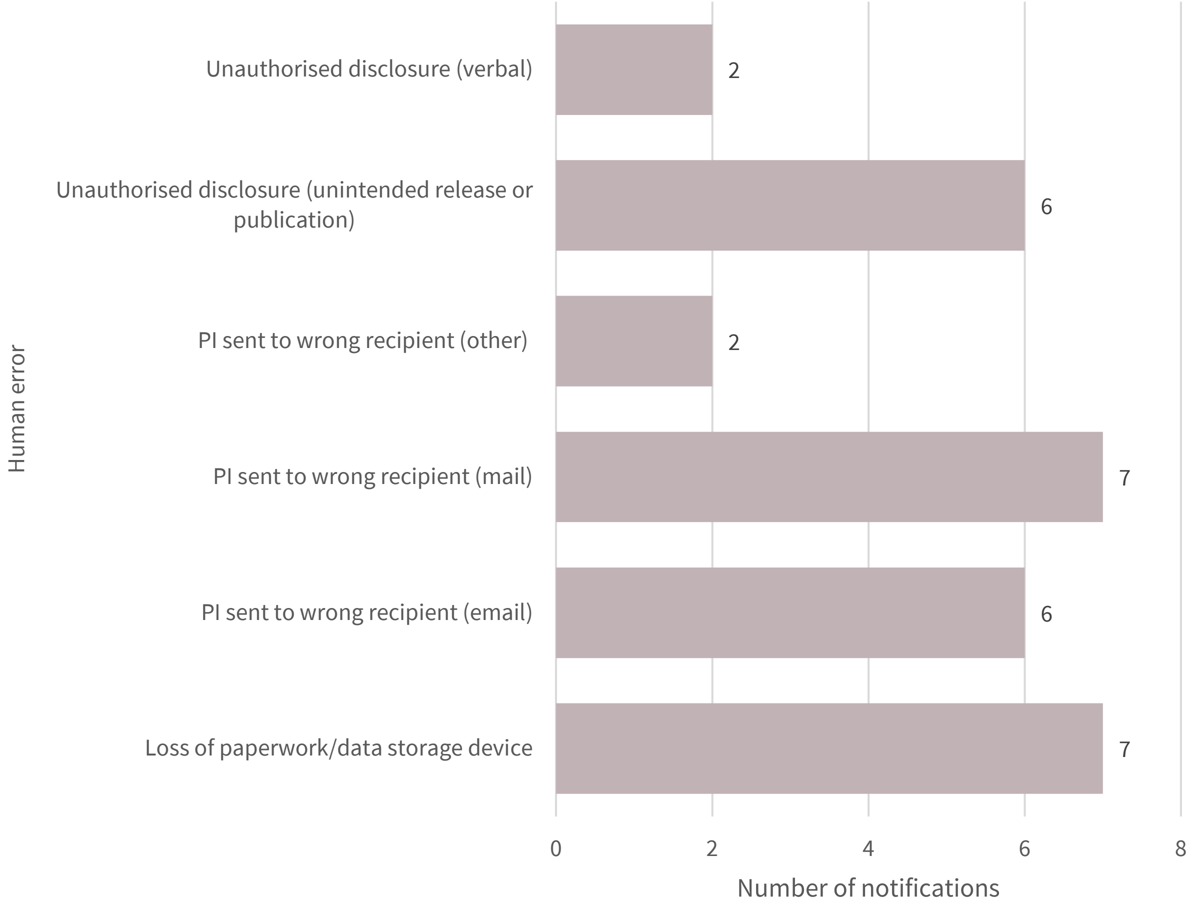
Human error was the leading source of notifications in the health sector (30 notifications). This includes communications sent to the wrong recipient, unintended release or publication of personal information, or loss of paperwork or a data storage device.

Malicious or criminal attacks were the source of 26 health sector data breaches, with system fault accounting for two data breaches.

Human error data breaches — Health sector

This chart shows the types of data breaches identified as 'human error' by the health sector during the quarter.

Chart 4.3 — Human error breakdown — Health sector

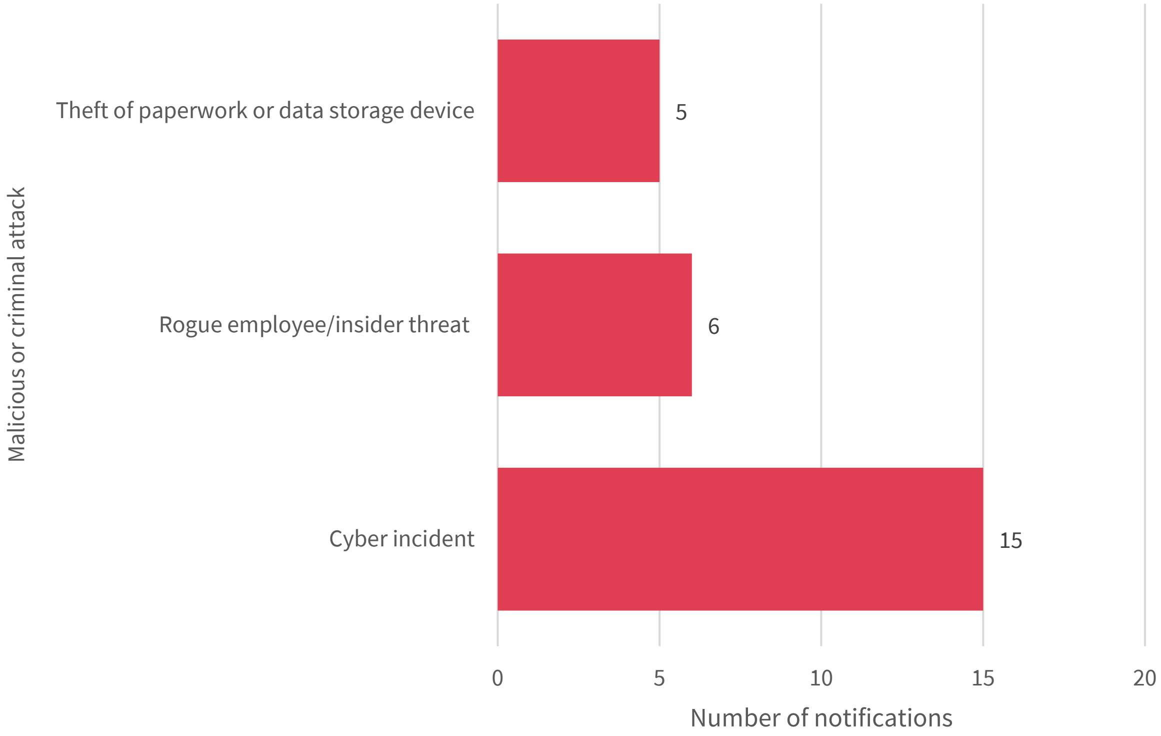


The largest source of data breaches in the health sector was human error (52 per cent), with examples including sending personal information to the wrong recipient by email (20 per cent of human error data breaches) or mail (23 per cent), unintended release or publication of personal information (20 per cent) or loss of paperwork or data storage device (23 per cent).

Malicious or criminal attack data breaches — Health sector

This chart shows the types of data breaches identified as ‘malicious or criminal attack’ by the health sector during the quarter.

Chart 4.4 — Malicious or criminal attacks breakdown — Health sector

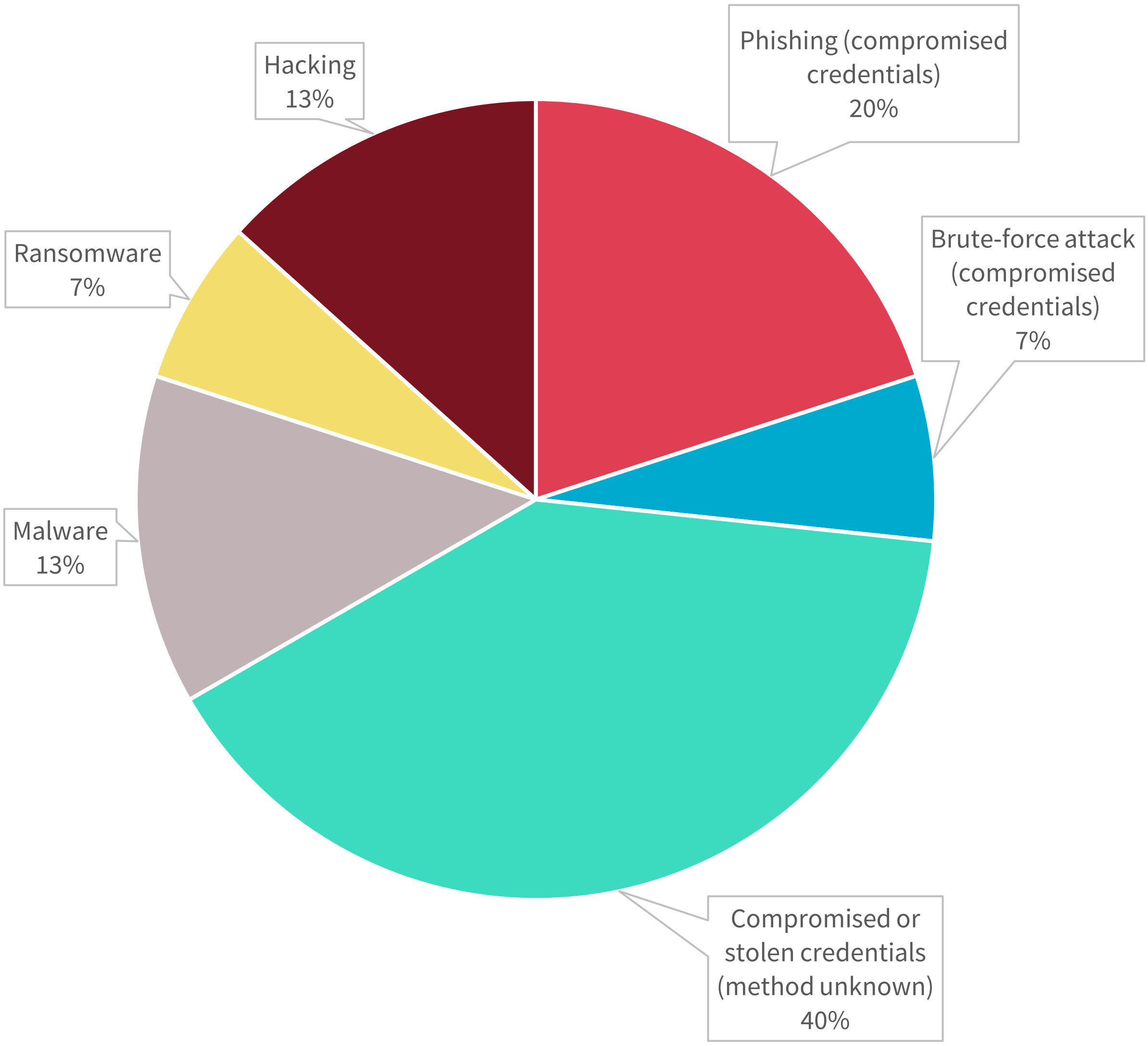


Malicious and criminal attacks were the second largest source of data breaches from the health sector this quarter. Cyber incidents were the most common type of attack, accounting for 58 per cent, while the actions of a rogue employee or insider threat was the second most common type of attack (23 per cent).

Cyber incident data breaches — Health sector

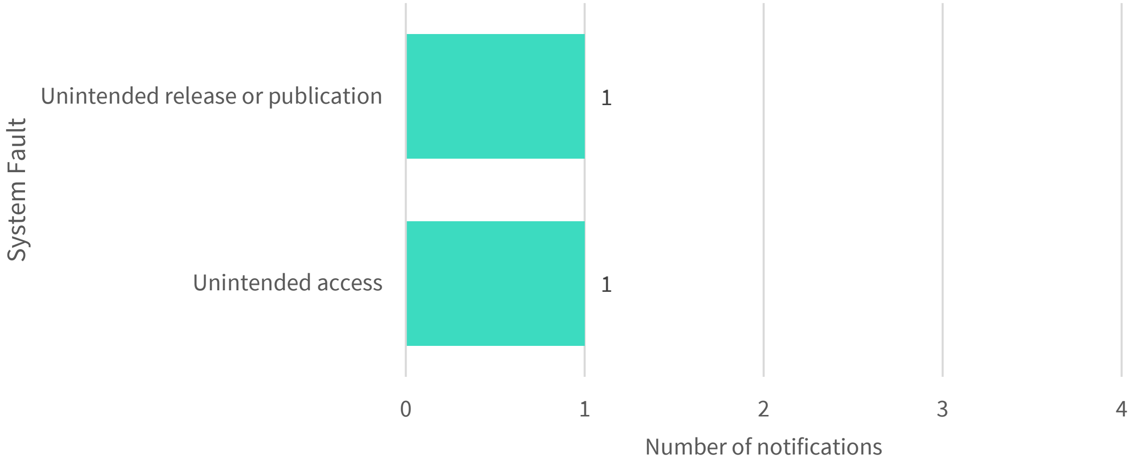
This chart shows the types of data breaches identified as 'malicious or criminal attack — cyber incident' by the health sector during the quarter.

Chart 4.5 — Cyber incident breakdown — Health sector



The health sector reported that six data breaches caused by cyber incidents were the result of compromised credentials through unknown methods. Phishing accounted for three notifications, followed by malware and hacking attacks (two notifications each). Brute-force and ransomware attacks were the source of one notification each.

System fault data breaches — Health sector



System faults account for two notifications from the health sector this quarter.

Glossary

Breach categories

Term	Definition
Human error	An unintended action by an individual directly resulting in a data breach, for example an 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 email 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 remove effectively 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