Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Quarterly Statistics Report

1 July – 30 September 2018

oaic.gov.au

OAIC

Final report issued: 30/10/18

Contents

Key statistics

245
notifications

37%
human error

57%
malicious or criminal attacks

6%
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 July 2018 and 30 September 2018 (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 industry sectors

Number of data breaches reported — All sectors

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

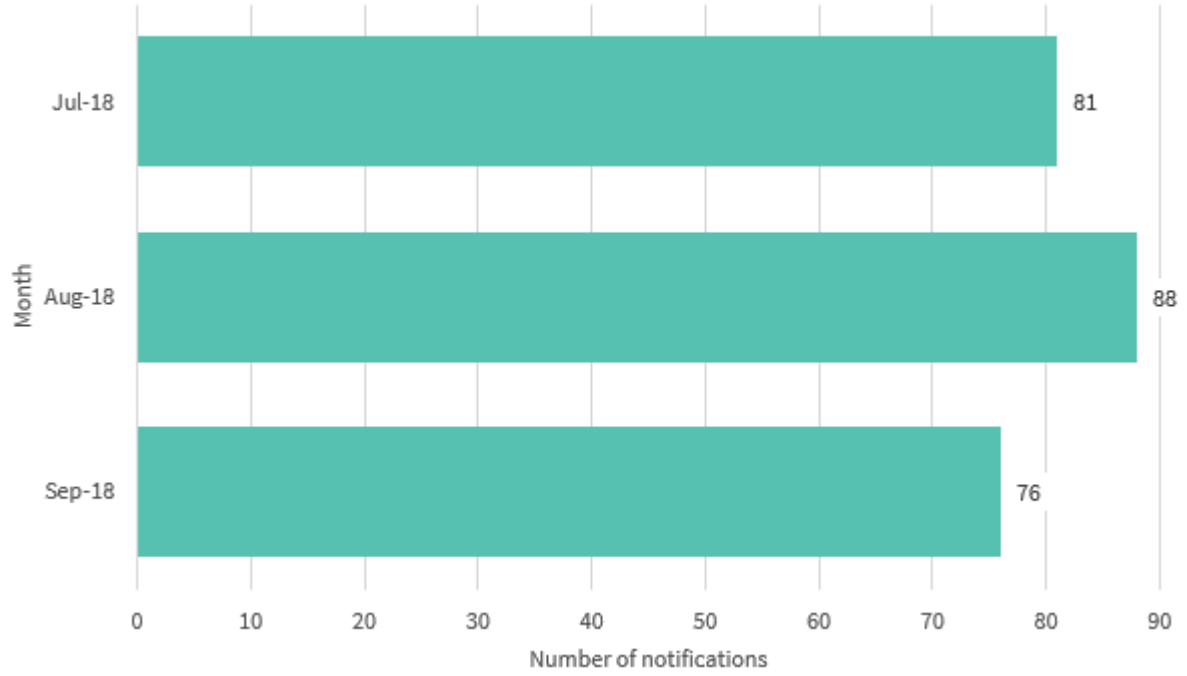
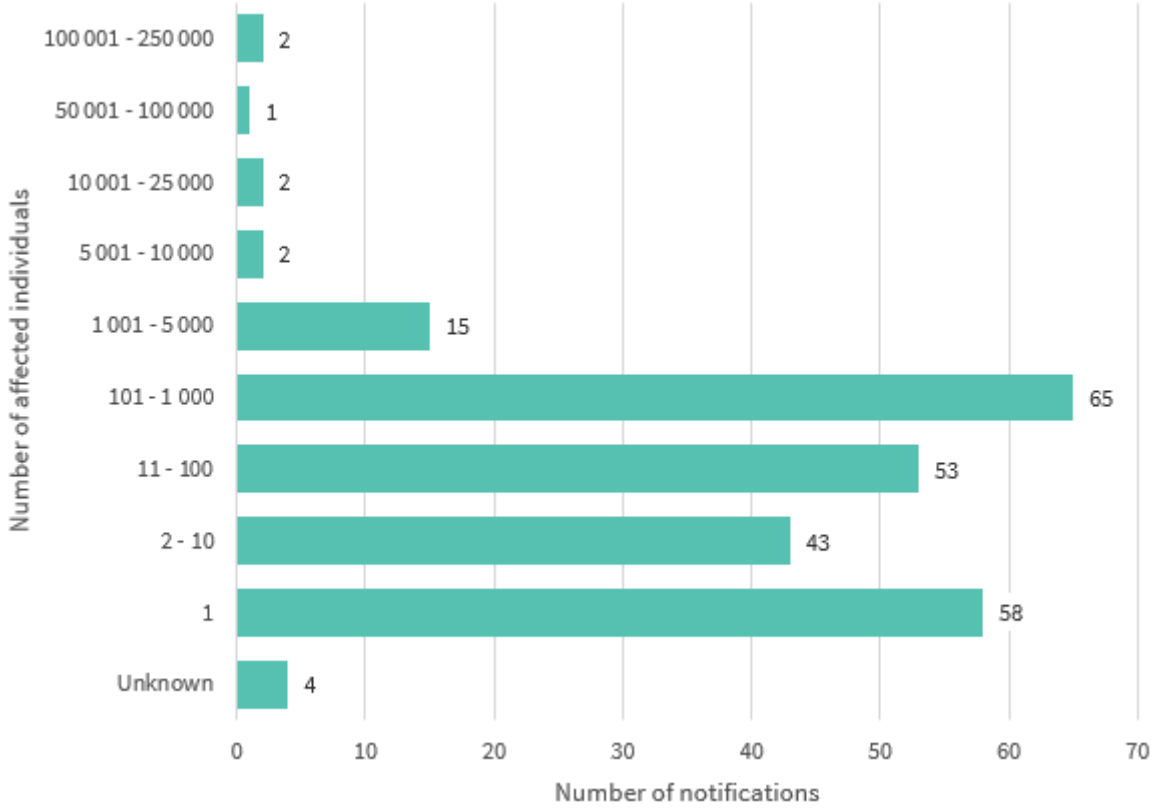


Table 1.A — Number of breaches reported under the Notifiable Data Breaches scheme by quarter — All sectors

Quarter	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

Number of individuals affected by breaches — All sectors

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



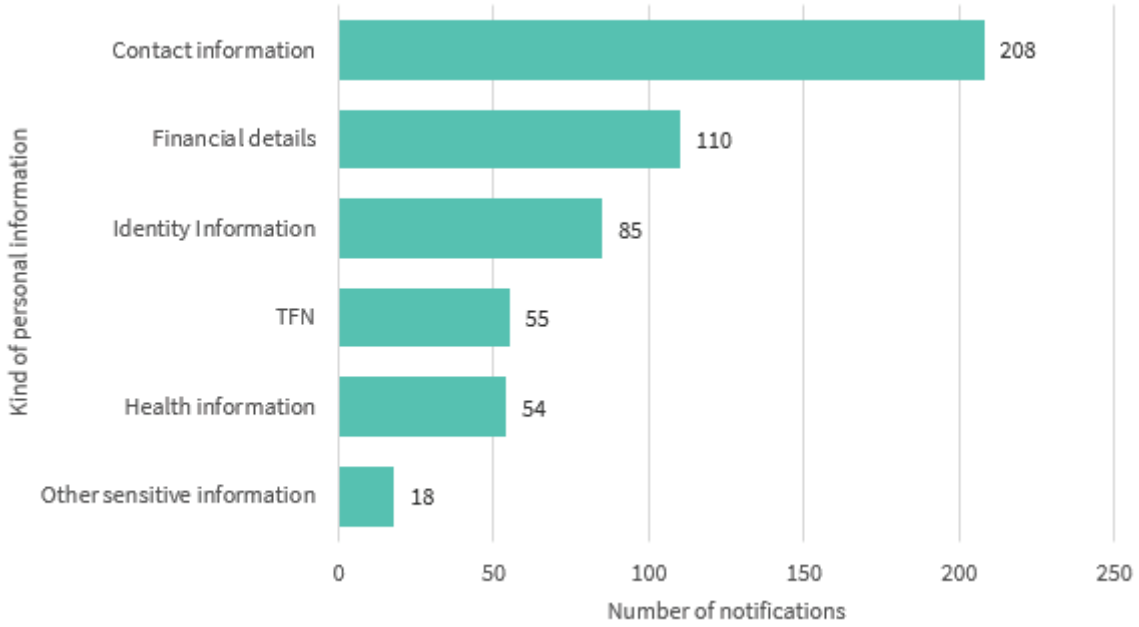
Note: Where bands are not shown (for example, 25 001 to 50 000), there were nil reports in the period. 'Unknown' includes notifications by entities whose investigations were ongoing at the time of this report.

Most data breaches in the period involved the personal information of 100 individuals or fewer (63 per cent of data breaches).

Data 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 total NDBs received
Contact information	85%
Financial details	45%
Identity information	35%
TFN	22%
Health information	22%
Other sensitive information	7%

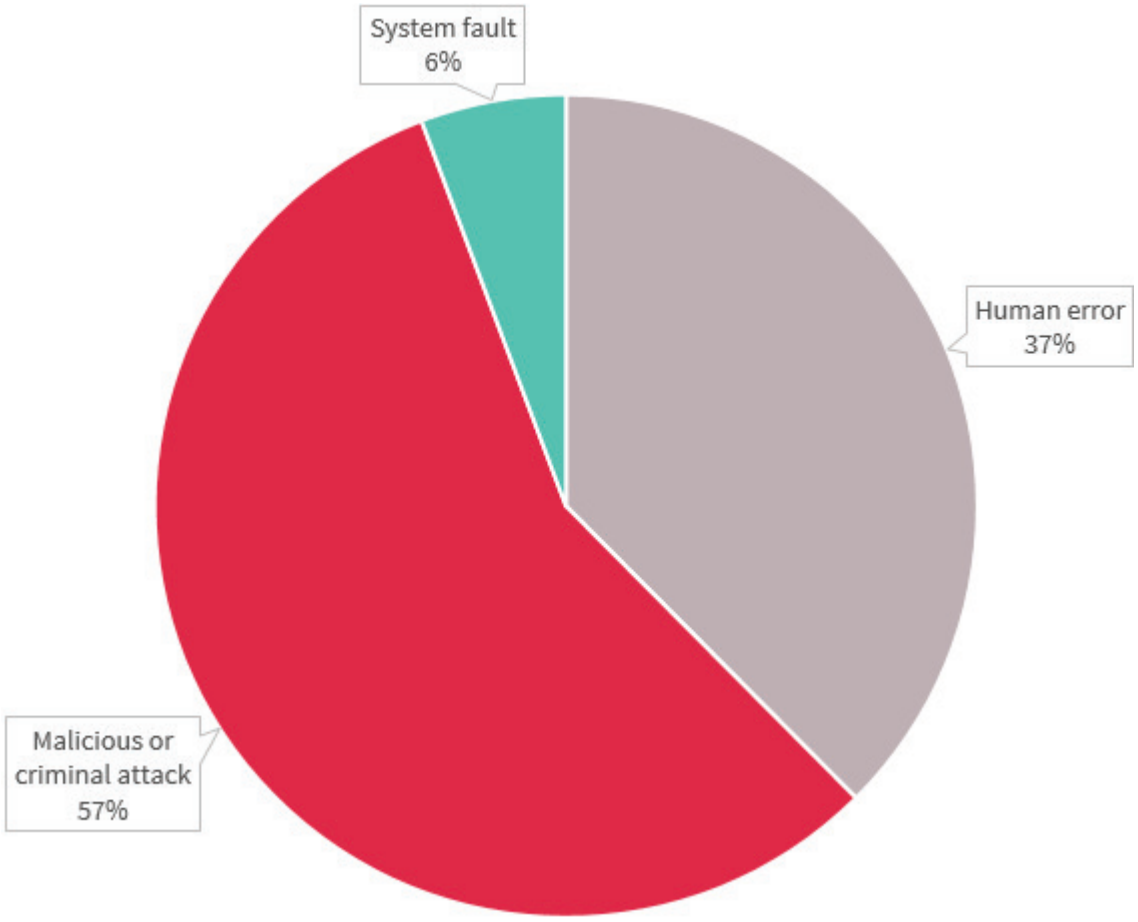
The majority of data breaches involved 'contact information', such as an individual's home address, phone number or email address. This is distinct from 'identity information', which refers to information that is used to confirm an individual's identity, such as passport number, driver's licence number or other government identifiers.

Entities also notified data breaches that involved financial details, such as bank account or credit card numbers, individuals' tax file numbers (TFNs), as well as health information. 'Other sensitive information' refers to categories of sensitive information as set out in section 6(1) of the Privacy Act, other than health information as defined in section 6FA.

Source of the breaches — All sectors

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

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



Malicious or criminal attacks accounted for 57 per cent of data breaches reported this quarter (139 notifications).

Malicious or criminal attacks differ from human error data breaches in that they are deliberately crafted to exploit known vulnerabilities for financial or other gain. Attacks included cyber incidents such as phishing, malware, ransomware, brute-force attack and hacking by other means, as well as social engineering or impersonation and actions taken by a rogue employee or insider threat. Theft of paperwork or storage devices was also reported as a source of malicious or criminal attacks. Many cyber incidents this quarter appear to have exploited vulnerabilities involving a human factor (such as clicking on a phishing email or disclosing passwords).

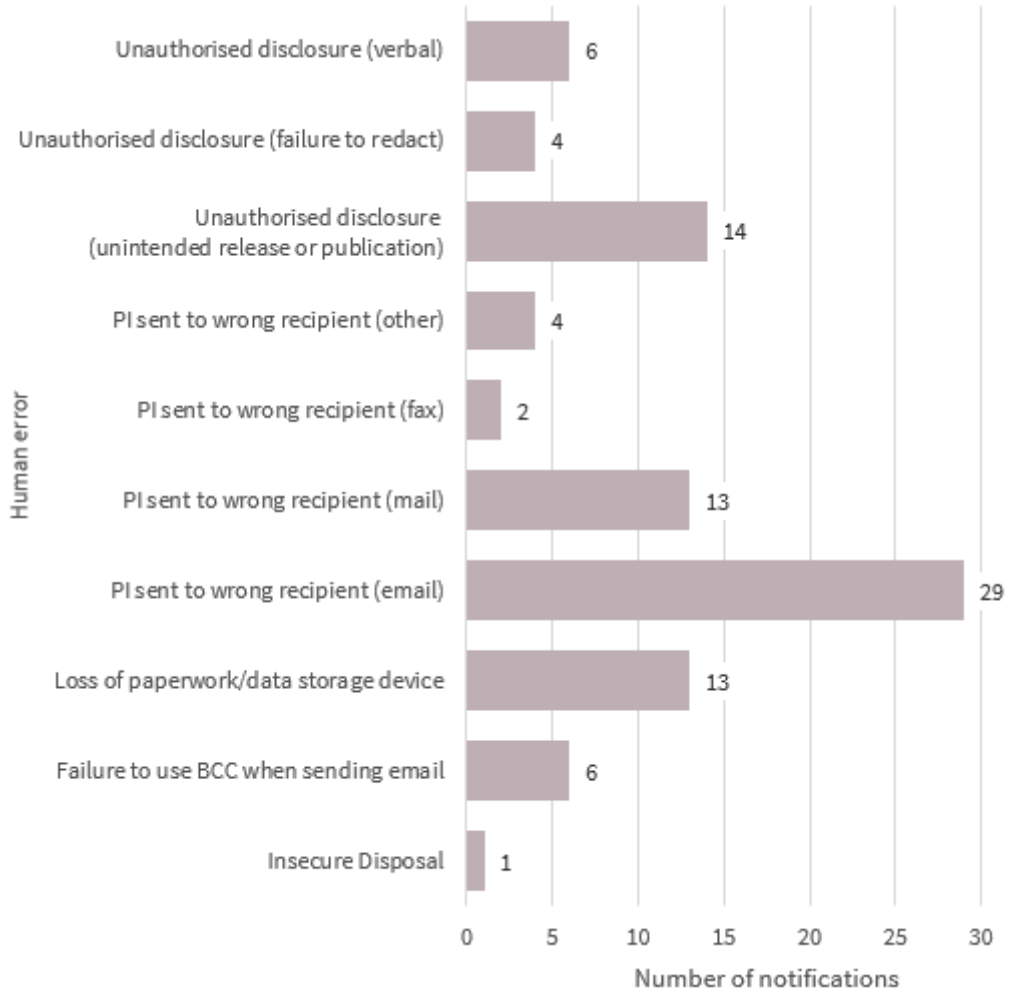
Human error remained a significant source of data breaches, accounting for 37 per cent of all incidents reported (92 notifications).

System faults accounted for 6 per cent of data breaches (14 notifications).

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. Sending personal information to the wrong recipient via email accounted for 12 per cent of all data breaches during the quarter. This was followed by the unintended release or publication of personal information (6 per cent), loss of paperwork/data storage device (5 per cent), and sending personal information to the wrong recipient via mail (5 per cent). This quarter also included incidents where personal information was provided to the wrong recipient via channels other than email, fax or mail, for example, delivery by hand or uploading to web portal.

However, certain kinds of data breaches can affect larger numbers of people. For example, in this quarter data breaches involving unauthorised disclosure as a result of a failure to redact personal information impacted the largest numbers of individuals (an average of 633 affected individuals per breach). Failures to use the 'blind carbon copy' (BCC) function when sending group emails impacted an average of 494 individuals per data breach. In contrast, human errors involving sending personal information to the wrong recipient generally impacted smaller groups of individuals.

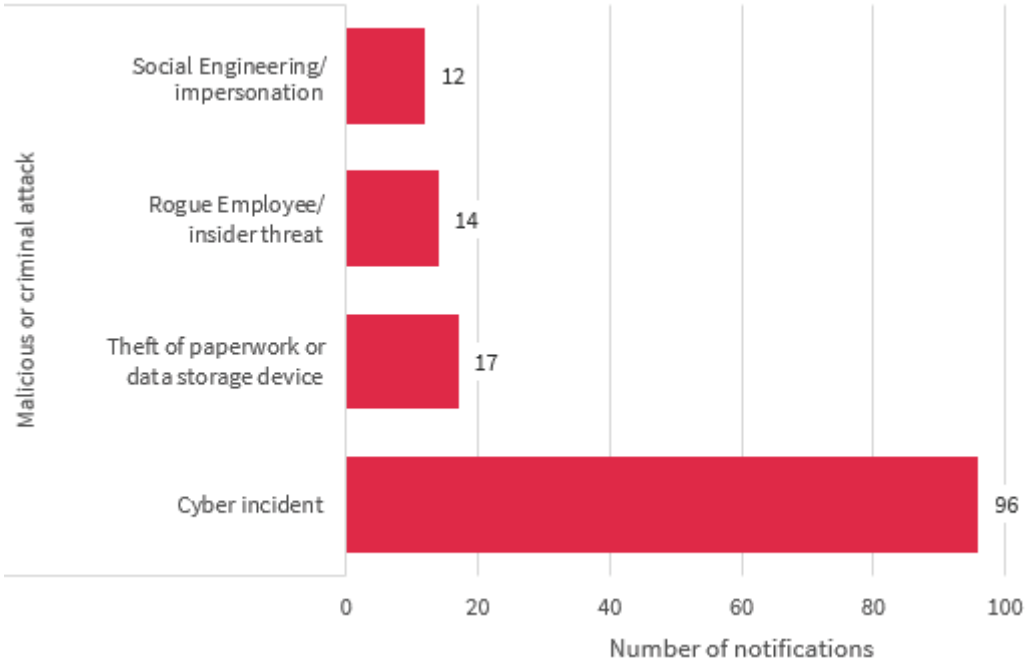
Table 1.C — Human error breakdown by average number of affected individuals — All sectors

Kinds of personal information	No. of NDBs received	Average no. of affected individuals
Unauthorised disclosure (failure to redact)	4	633
Failure to use BCC when sending email	6	494
Unauthorised disclosure (unintended release or publication)	14	94
Insecure disposal	1	79
PI sent to wrong recipient (email)	29	70
PI sent to wrong recipient (mail)	13	35
Unauthorised disclosure (verbal)	6	11
Loss of paperwork/data storage device	13	8
PI sent to wrong recipient (fax)	2	5
PI sent to wrong recipient (other)	4	4

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 57 per cent of all notifications.

Of the 139 data breaches resulting from a malicious or criminal attack, 69 per cent involved cyber incidents. Many cyber incidents in this quarter involved the exploitation of vulnerabilities involving a human factor (such as clicking on an attachment to a phishing email), as well as incidents involving malware, ransomware, and hacking by other means.

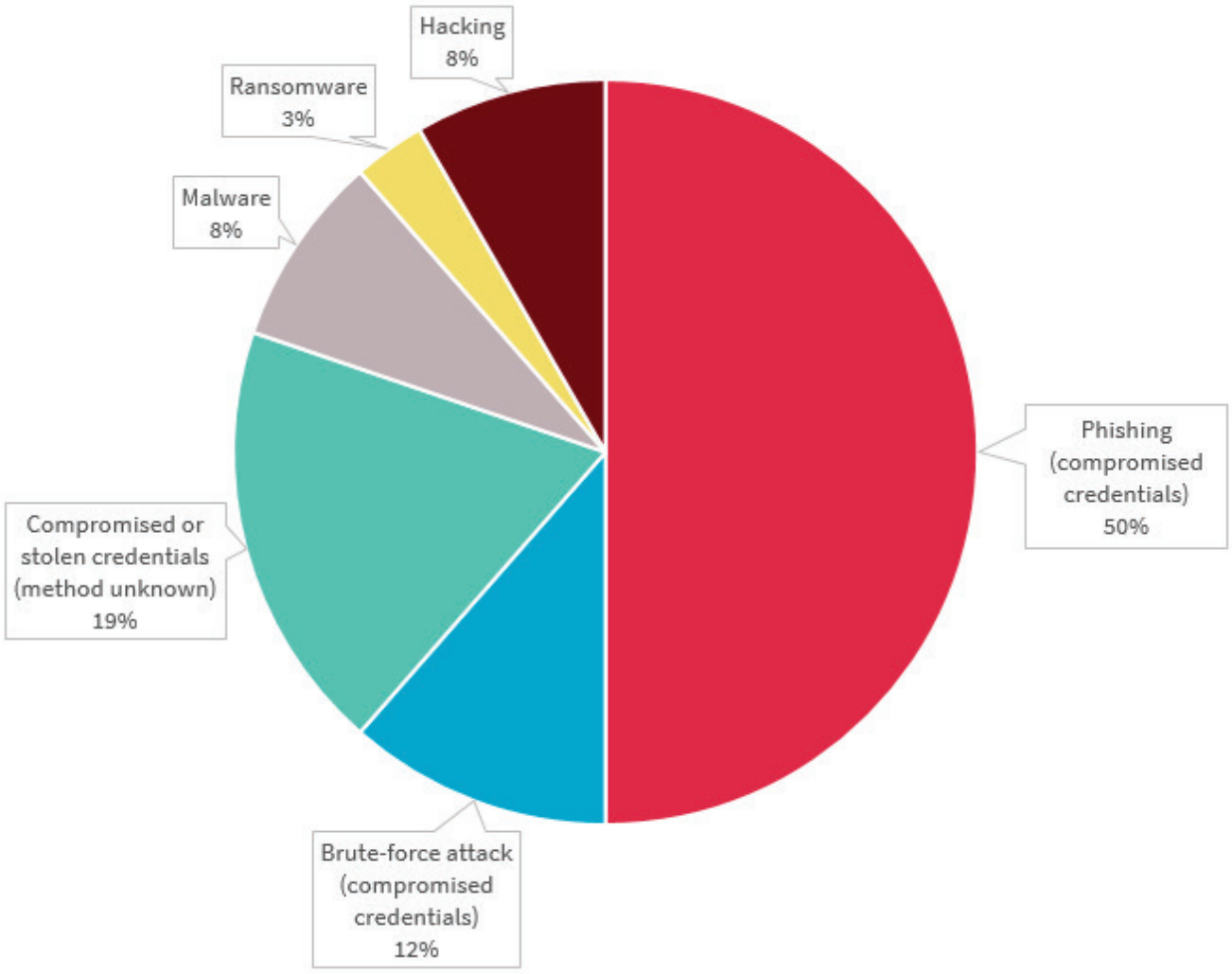
Theft of paperwork or storage devices was the second most reported source of malicious or criminal attacks (12 per cent).

Other sources included actions taken by a rogue employee or insider threat (10 per cent) and social engineering or impersonation (9 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

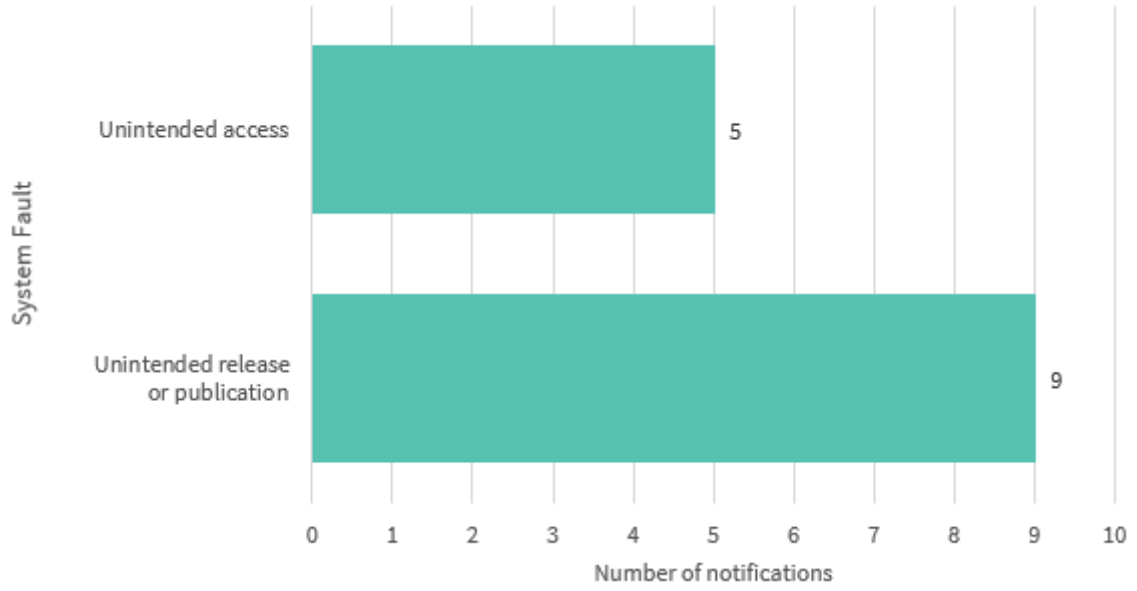


The majority of cyber incidents were linked to the compromise of credentials through phishing (48 notification), by unknown methods (18 notifications), or by brute-force attack (11 notifications).

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 6 per cent of data breaches this quarter.

Across all sectors, 9 data breaches related to the unintended release or publication of personal information as a result of a system fault. This includes 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.

Additionally, 5 data breaches related to unintended access to personal information as a result of a system fault, such as a coding error which allows an individual to access another individual's online account.

Comparison of top 5 industry sectors that reported breaches in the quarter

This section compares notifications made under the NDB scheme by the five industry sectors that made the most notifications in the quarter (top 5 industry sectors).

Top 5 industry sectors

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

Top 5 industry sectors	Data breaches received
Health service providers [1]	45
Finance (incl. superannuation) [2]	35
Legal, accounting & management services	34
Education [3]	16
Personal services [4]	13

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 July to September 2018, the top sector to report notifiable data breaches was the private health service provider sector (health sector) (18 per cent). The second largest source was the finance sector (14 per cent). This was followed by the legal, accounting and management services sector (14 per cent), the private education sector (education) (7 per cent), and the personal services 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).

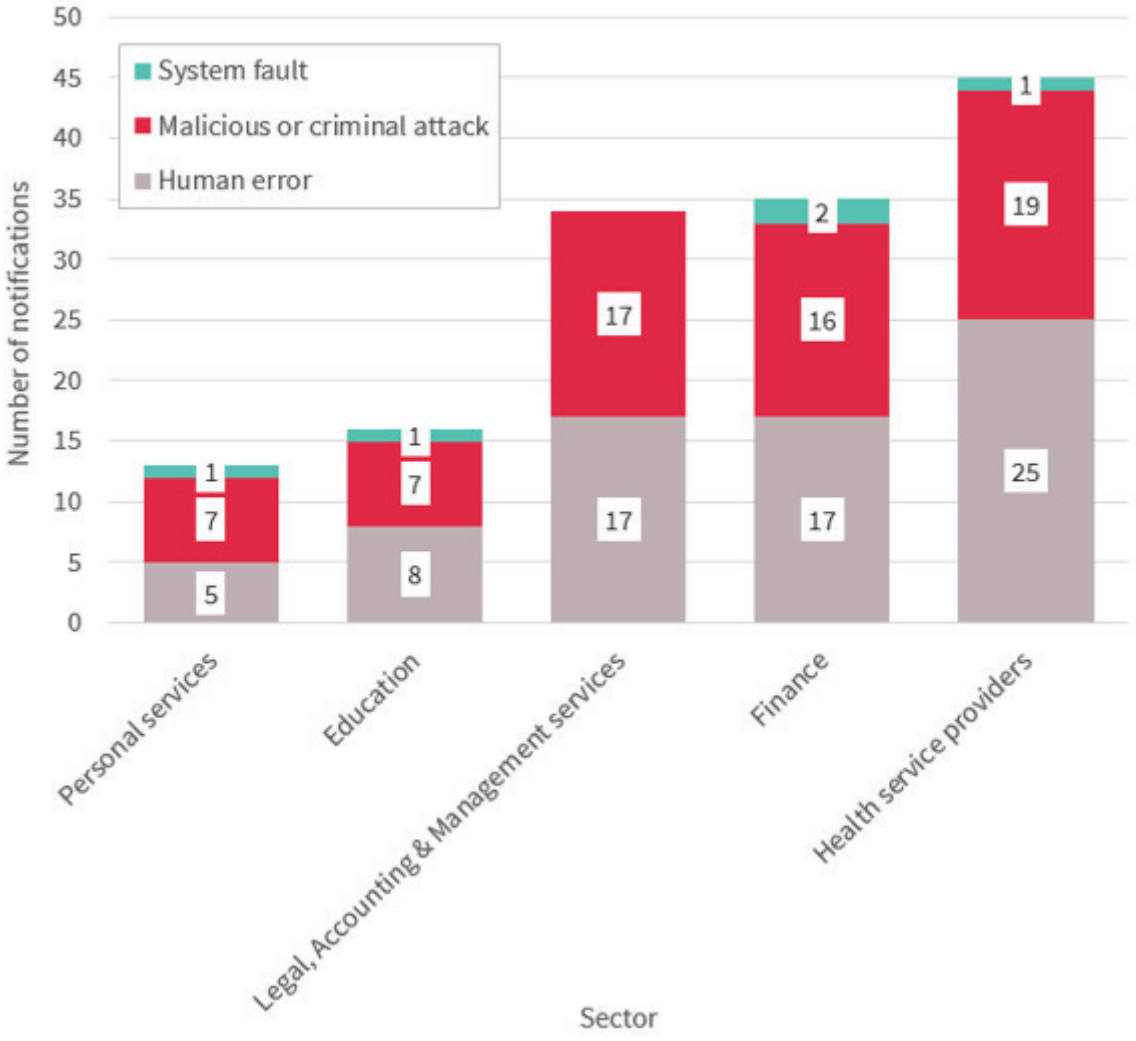
[3] This sector includes private education providers only, as APP entities, and the Australian National University. Public sector education providers are bound by State and Territory privacy laws, as applicable.

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

Source of breaches — Top 5 industry sectors

This chart breaks down the sources of data breaches as identified by notifying entities in the top 5 industry sectors in the quarter.

Chart 2.1 — Source of data breaches — Top 5 industry sectors



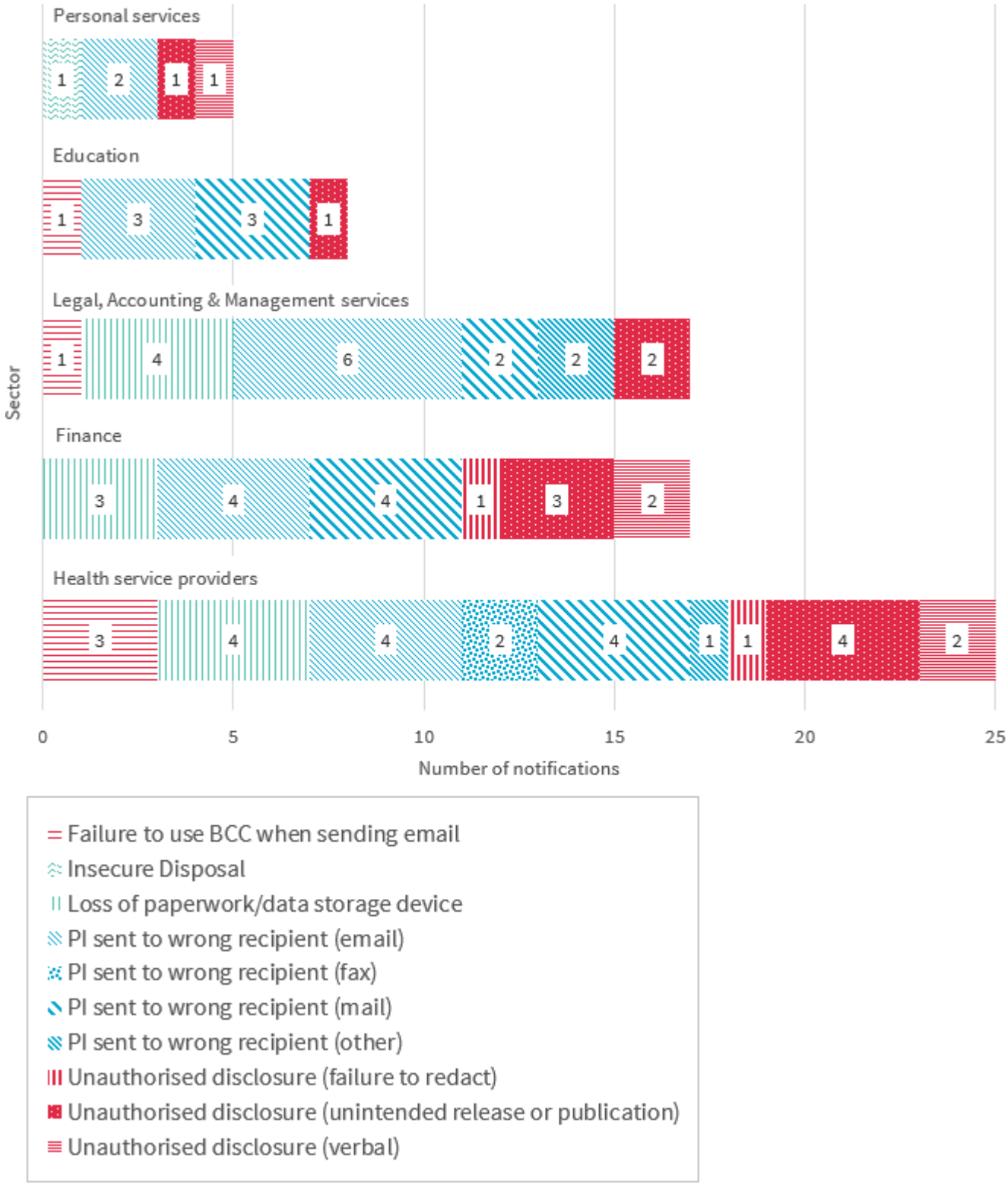
The highest reporting sector was health service providers (45 notifications). Of those notifications, 56 per cent of data breaches were the result of human error. Notifications from the finance sector, legal, accounting and management services and personal services were generally evenly split between human error and malicious or criminal attacks.

Four of the top five sectors notified at least one breach resulting from a system fault.

Human error breaches — Top 5 industry sectors

This table and chart breaks down the kinds of breaches identified as 'human error' by the top 5 industry sectors in the quarter.

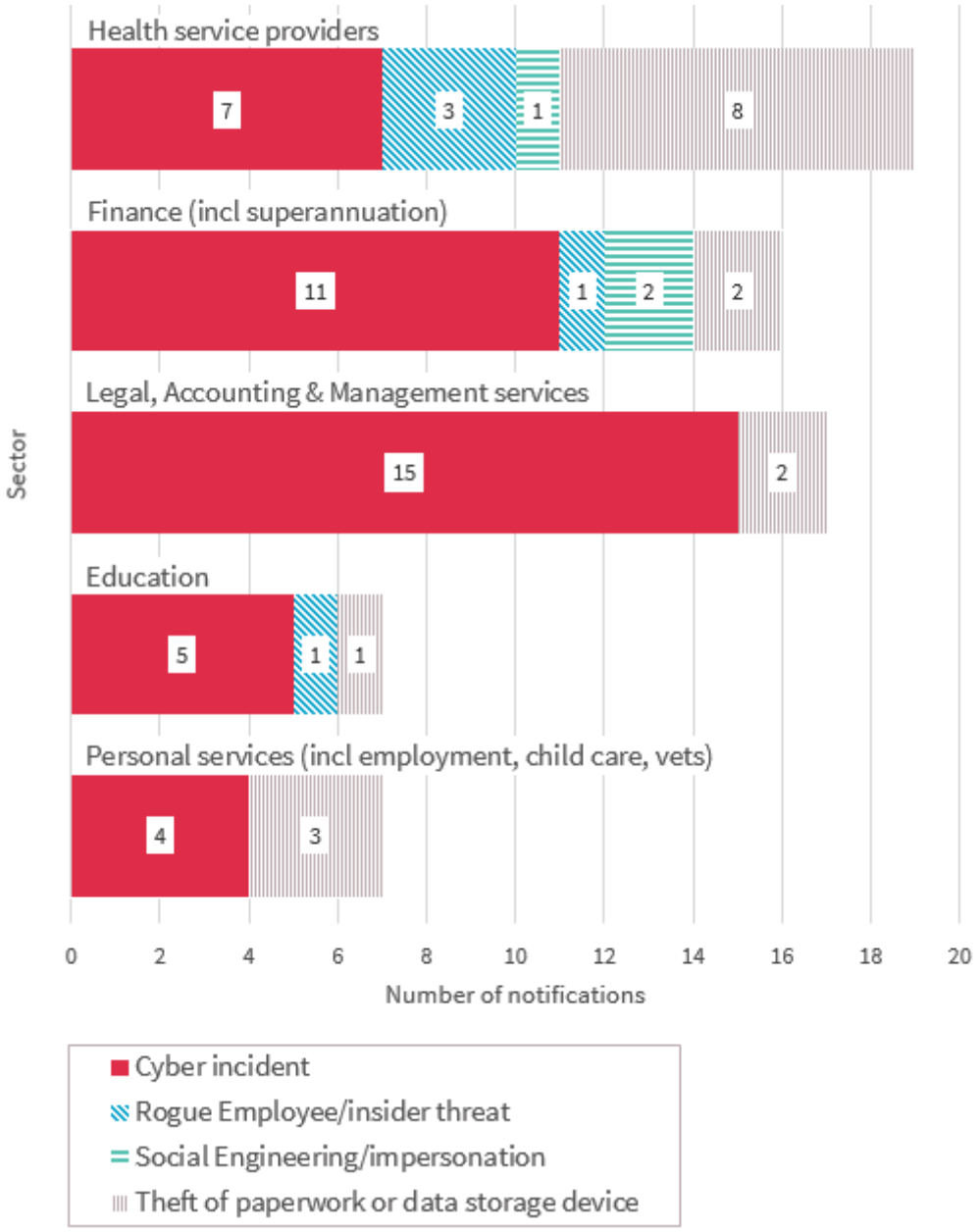
Chart 2.2 — Human error breakdown — Top 5 industry sectors



Malicious or criminal attack breaches — Top 5 industry sectors

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack' by the top 5 industry sectors in the quarter.

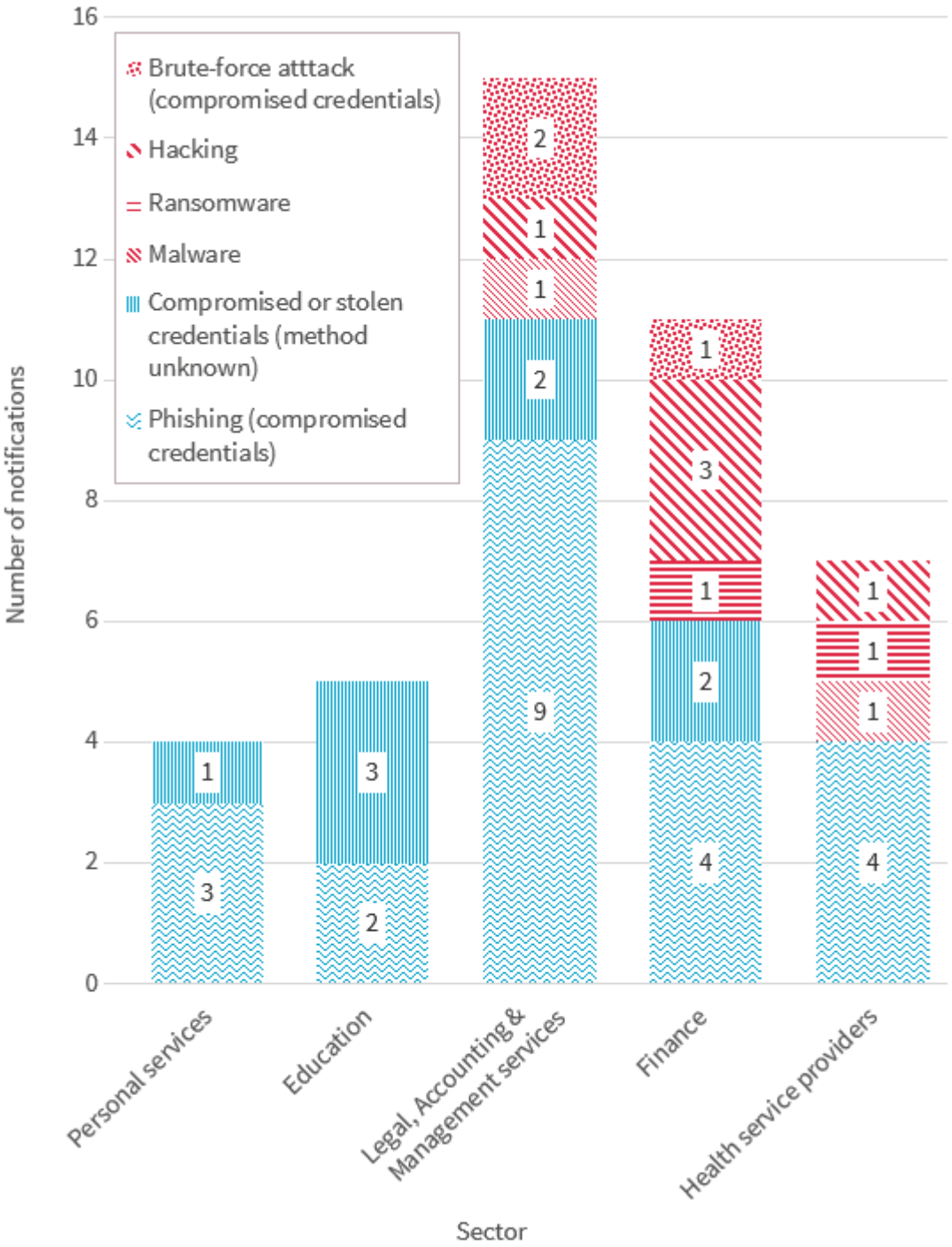
Chart 2.3 — Malicious or criminal attacks breakdown — Top 5 industry sectors



Cyber incident breaches — Top 5 industry sectors

This chart breaks down the kinds of breaches identified as 'malicious or criminal attack — cyber incident' by the top 5 industry sectors in the quarter.

Chart 2.4 — Cyber incident breakdown — Top 5 industry sectors

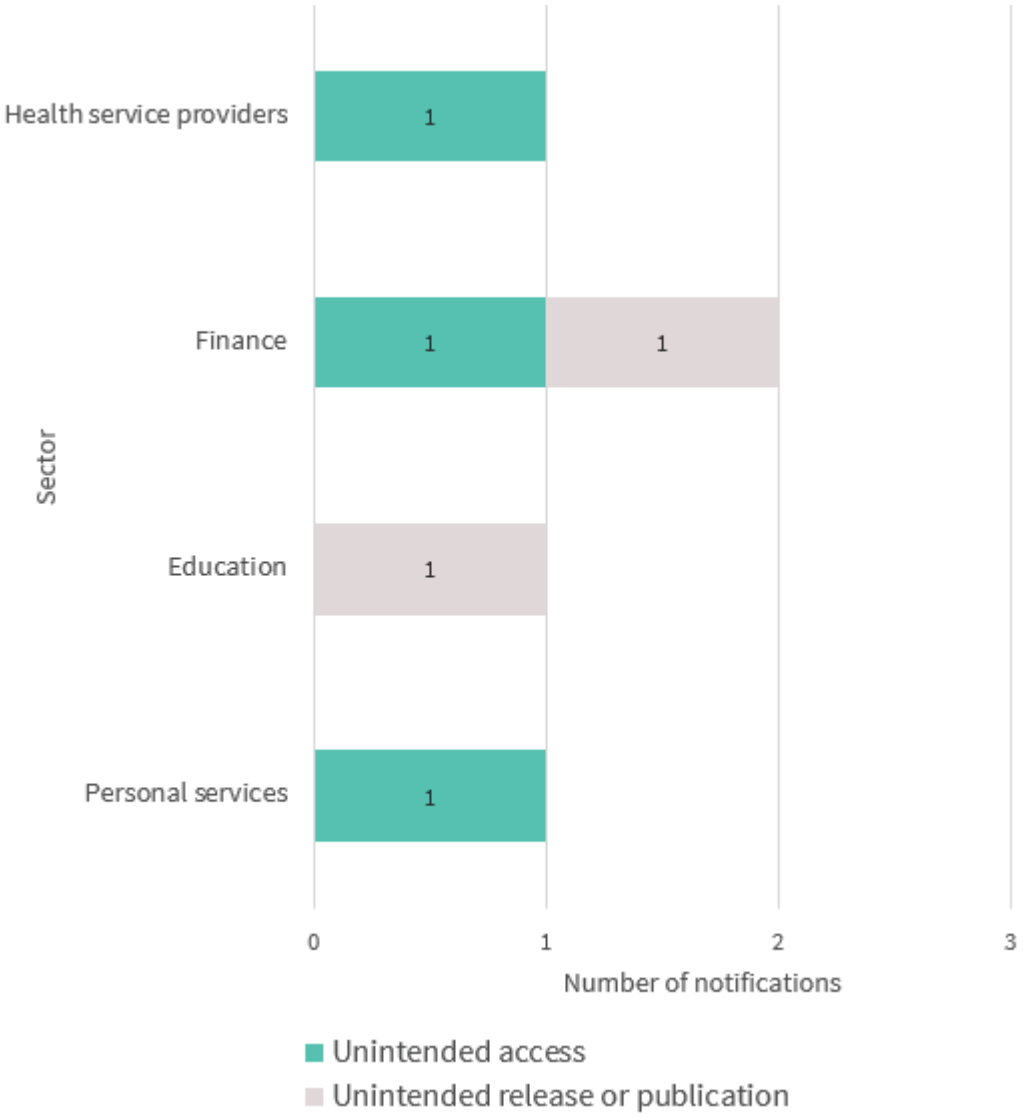


Similar to the overall trend, the majority of cyber incidents in the top five reporting sectors were linked to the compromise of credentials through phishing, brute-force attacks, or by unknown methods.

System fault breaches — Top 5 industry sectors

This chart breaks down the kinds of breaches identified as 'system fault' by the top 5 industry sectors in the quarter.

Chart 2.5 — System fault breakdown — Top 5 industry sectors

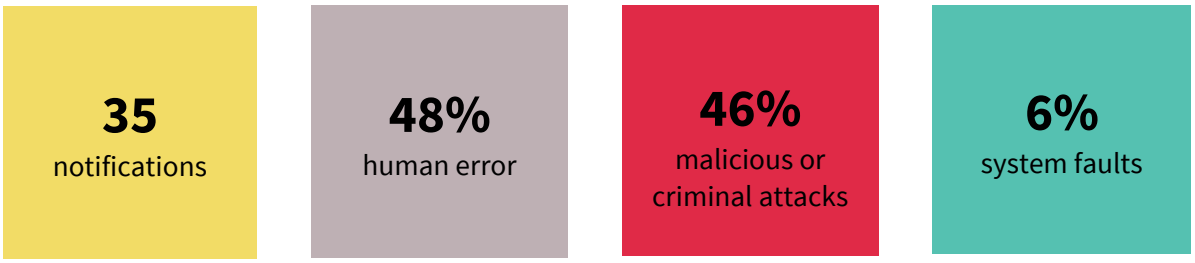


The legal, accounting and management services sector did not report any data breaches that were the result of a system fault.

Finance 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



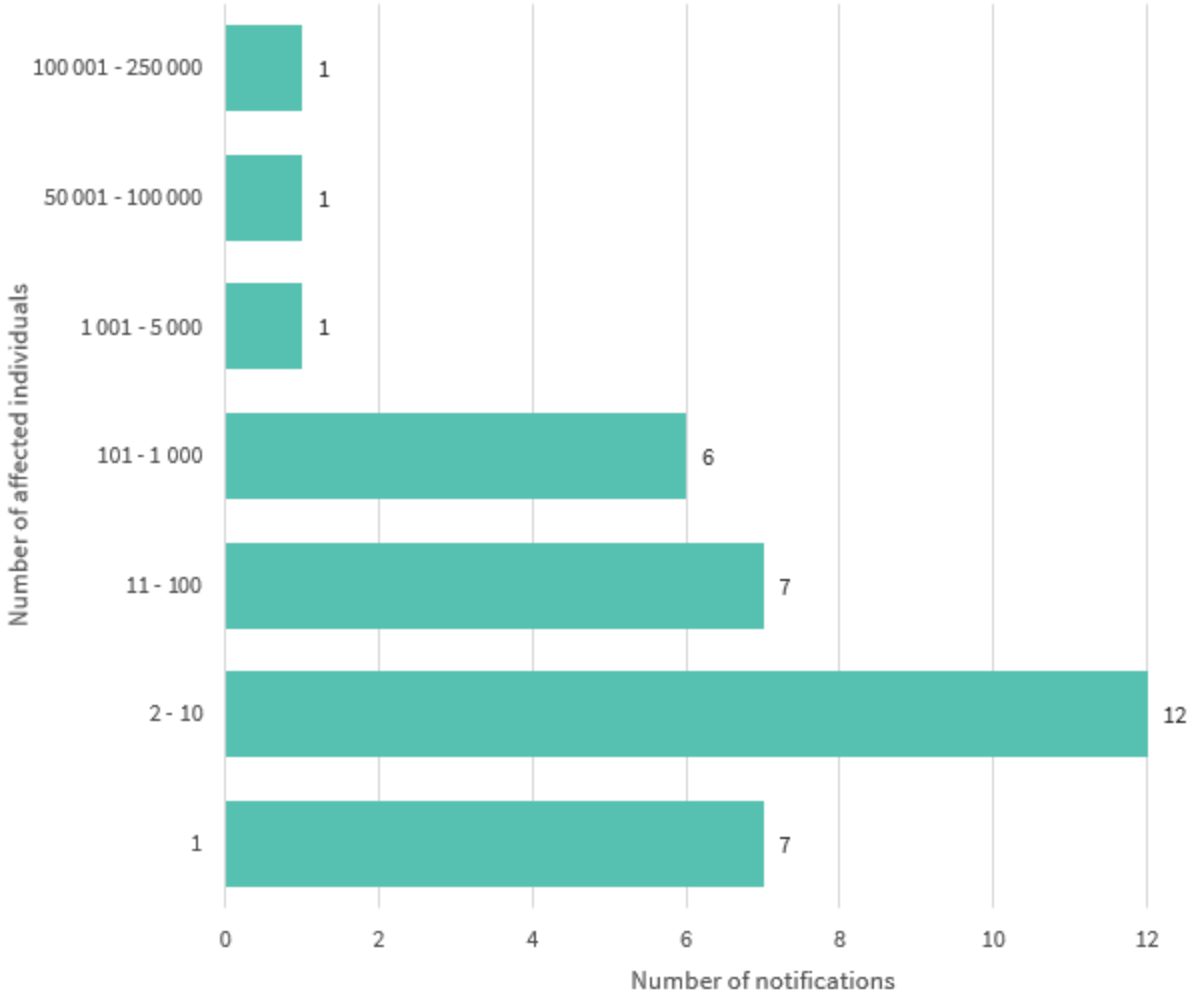
Number of breaches reported under the Notifiable Data Breaches Scheme — Finance sector

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

Number of individuals affected by breaches — Finance sector

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

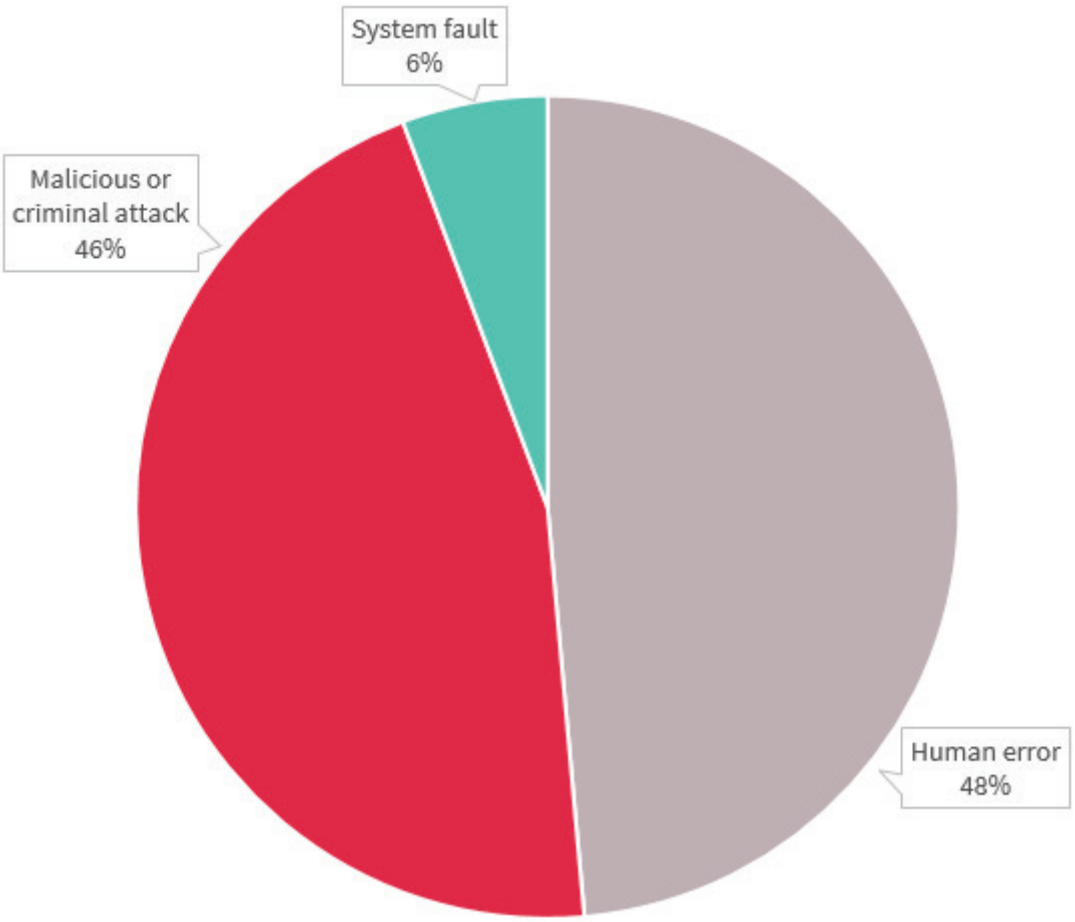


Note: Where bands are not shown, there were nil reports in the period.

Most notifications in the period from the finance sector involved the personal information of 100 individuals or fewer (74 per cent of breaches). Breaches impacting between 1 and 10 individuals comprised 54 per cent of the notifications. 26 per cent of notifications from the finance sector affected more than 100 individuals.

Source of the breaches — Finance sector

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



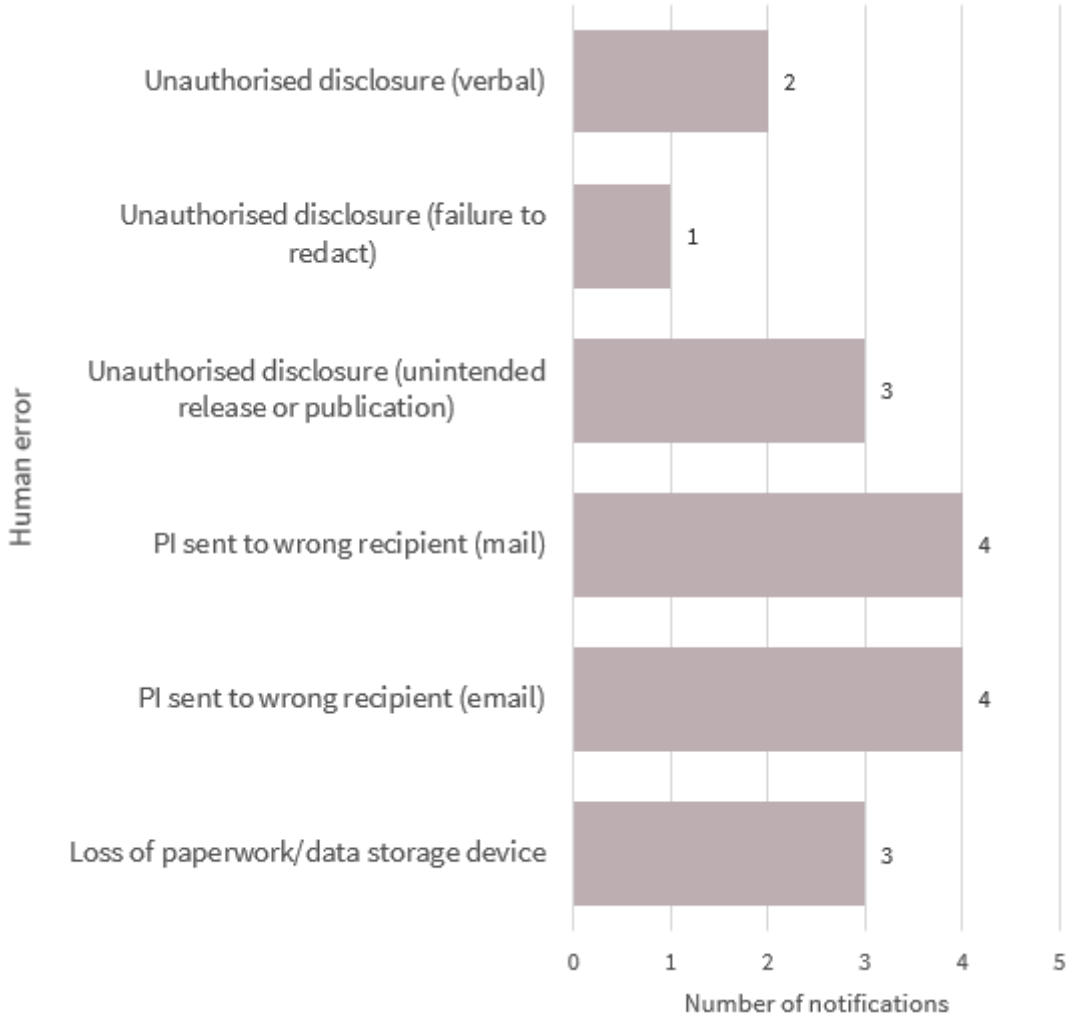
The majority of data breaches in the finance sector were the result of human error (17 notifications), followed by malicious or criminal attacks (16 notifications).

System fault accounted for 6 per cent of data breaches (2 notifications).

Human error breaches — Finance sector

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

Chart 3.3 — Human error breakdown — Finance sector

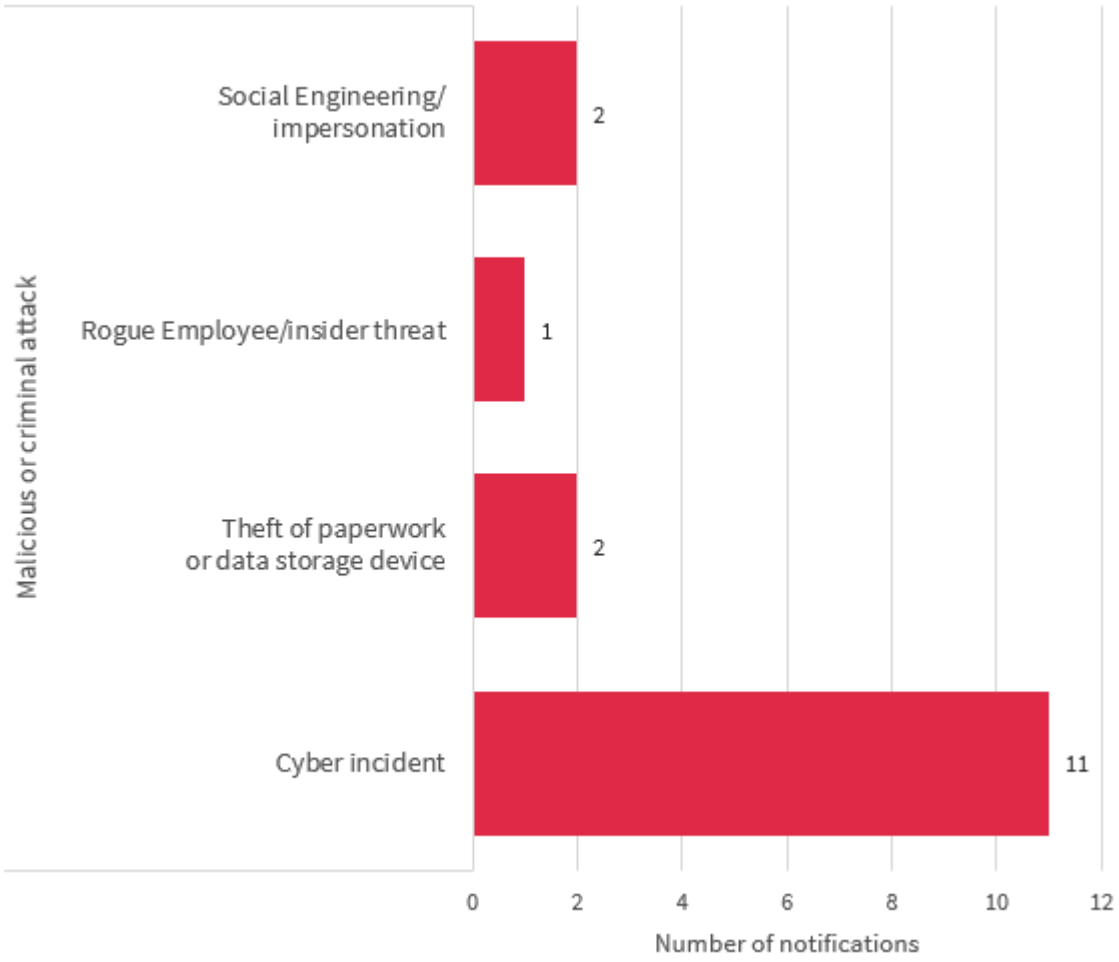


Almost half of data breaches by the finance sector were the result of human error (48 per cent). Human error data breaches by the finance sector included sending personal information to the wrong recipient by email or mail, as well as loss of paperwork or storage device.

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

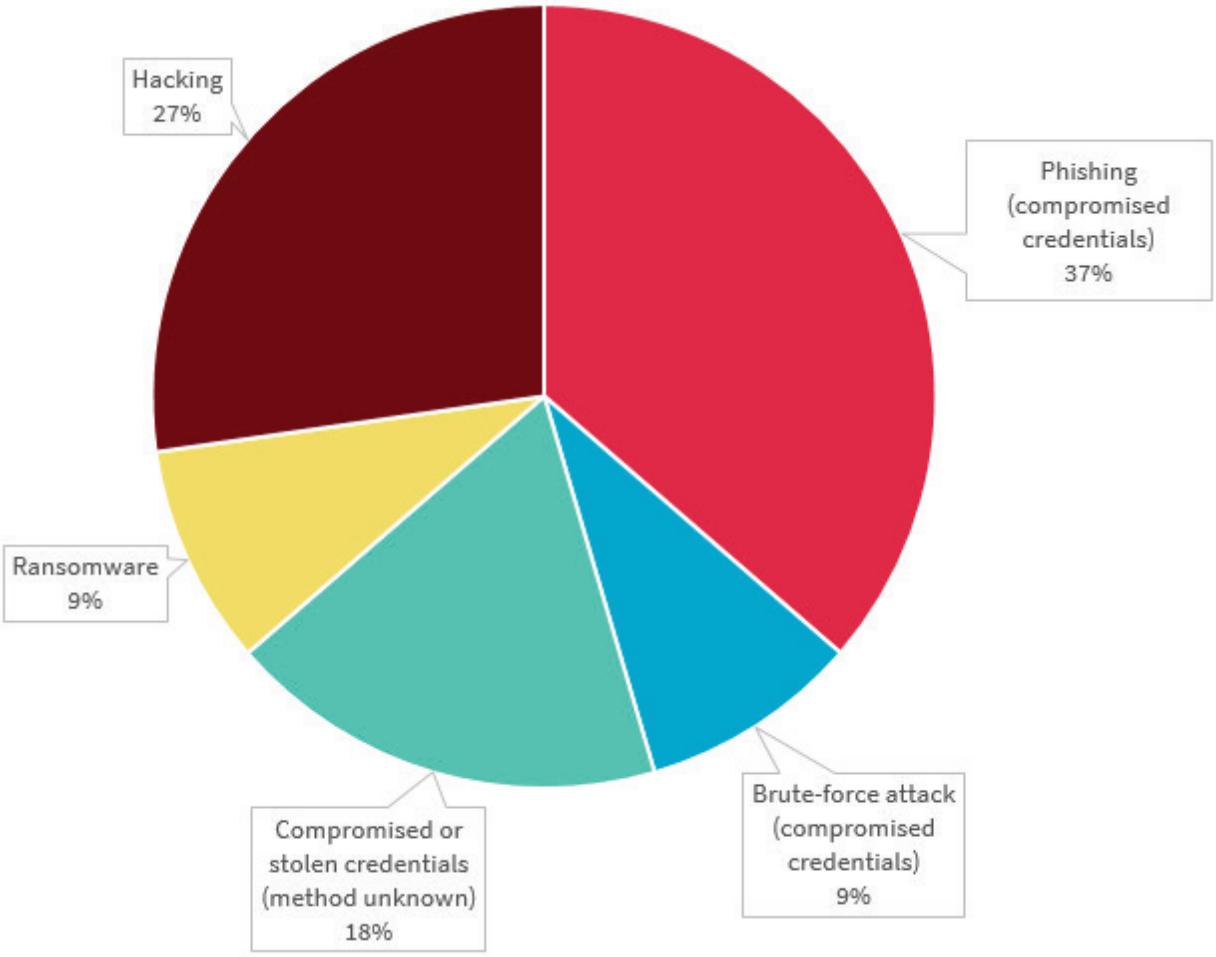


Malicious and criminal attacks accounted for 46 per cent of data breaches notified by the finance sector. Of these, cyber incidents were the most common type of malicious or criminal attack (69 per cent).

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



Of the cyber incidents notified by the finance sector, 7 data breaches were related to compromised or stolen credentials (such as phishing or brute-force attacks). Hacked websites or systems was the source for 3 notifications, and ransomware for 1 notification.

System fault breaches — Finance sector

Two notifications in the quarter identified the source of the data breach as a system fault leading to unauthorised access and disclosure of personal information.

Health sector report

This section captures notifications made under the NDB scheme by entities in the private health service provider (health) sector.[5]

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.

Summary — Health sector

45
notifications

56%
human error

42%
malicious or criminal attacks

2%
system faults

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

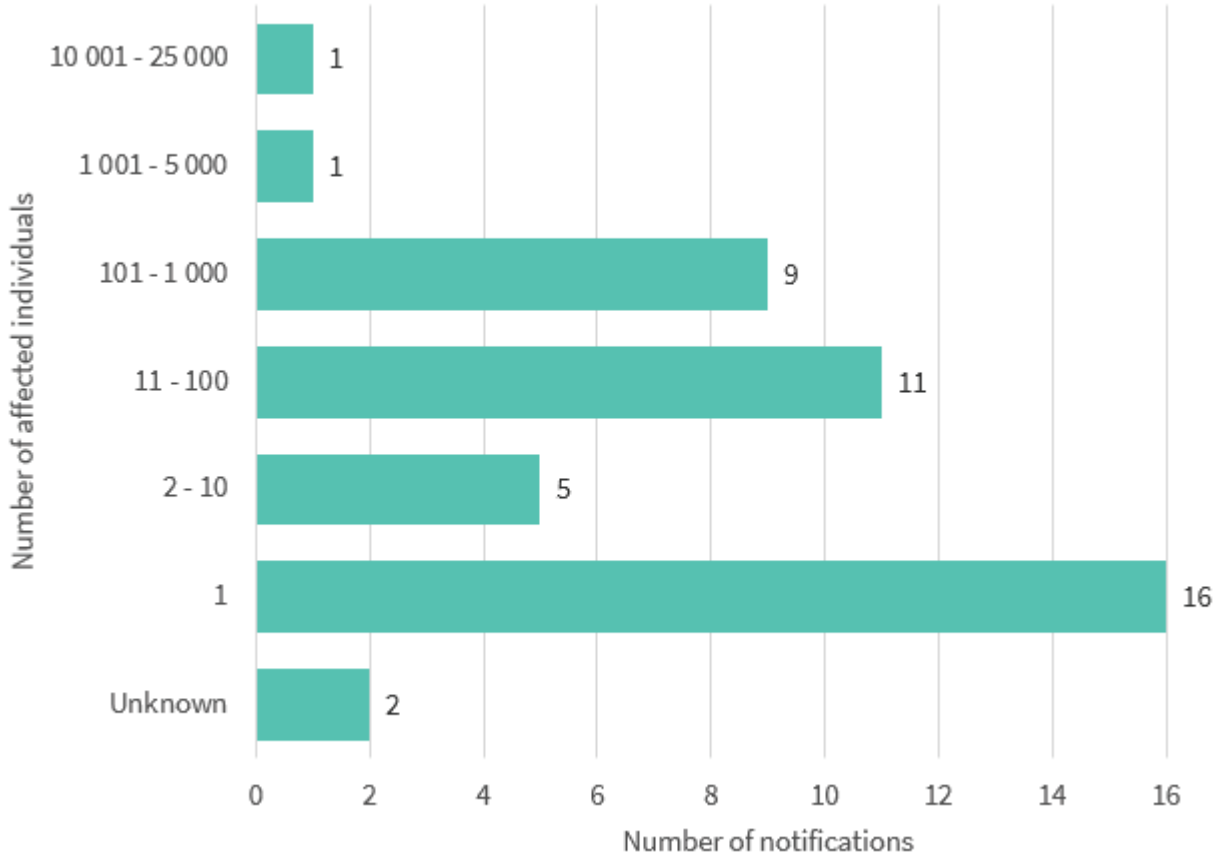
Table 4.A — Number of breaches reported under the Notifiable Data Breaches scheme by the health sector by quarter

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

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

Number of individuals affected by breaches — Health sector

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

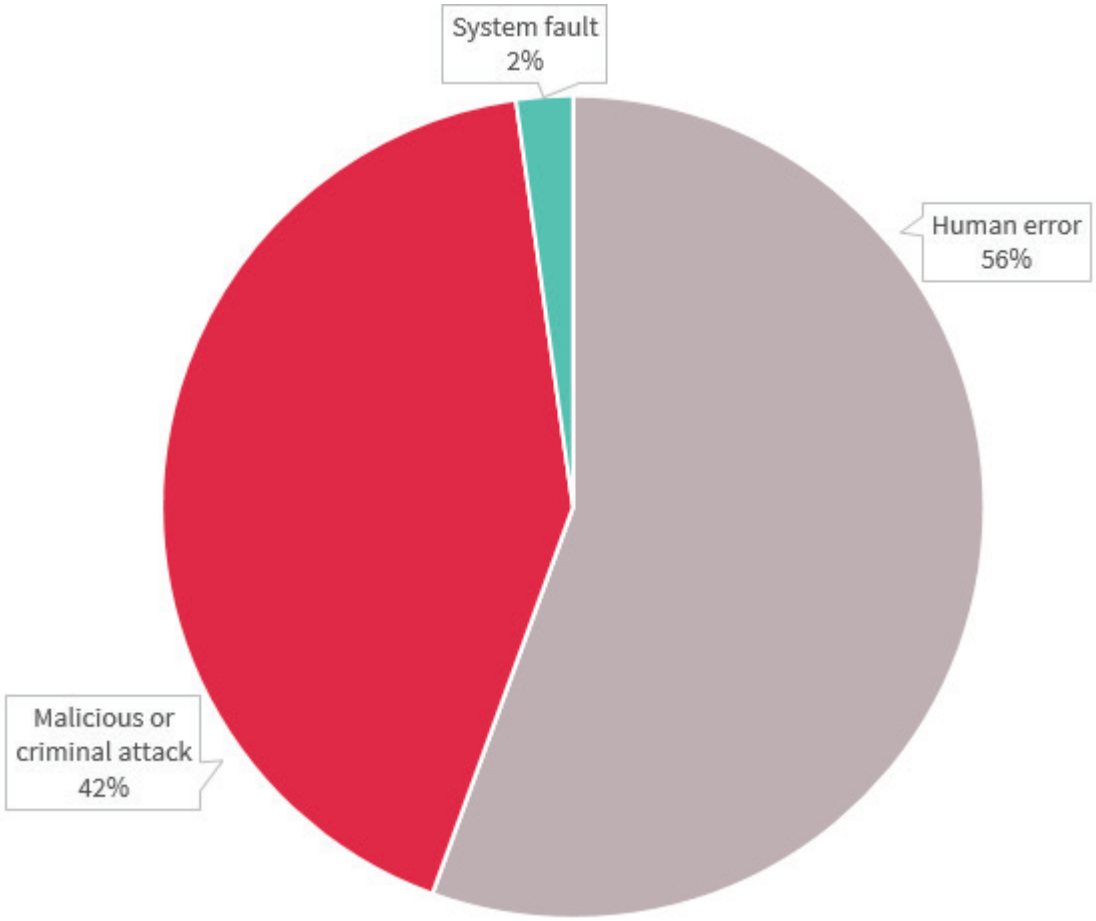


Note: Where bands are not shown, there were nil reports in the period.

The majority of data breaches from the health sector involved the personal information of 100 individuals or fewer (71 per cent of breaches). Data breaches impacting between 1 and 10 individuals comprised 47 per cent of the notifications, while 24 per cent of data breaches affected more than 100 individuals.

Source of the breaches — Health sector

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



Human error accounted for 56 per cent of data breaches in the health sector (25 notifications). This includes incidents in which a mistake made by a person caused the breach, such as communications sent to the wrong recipient or loss of paperwork or a storage device.

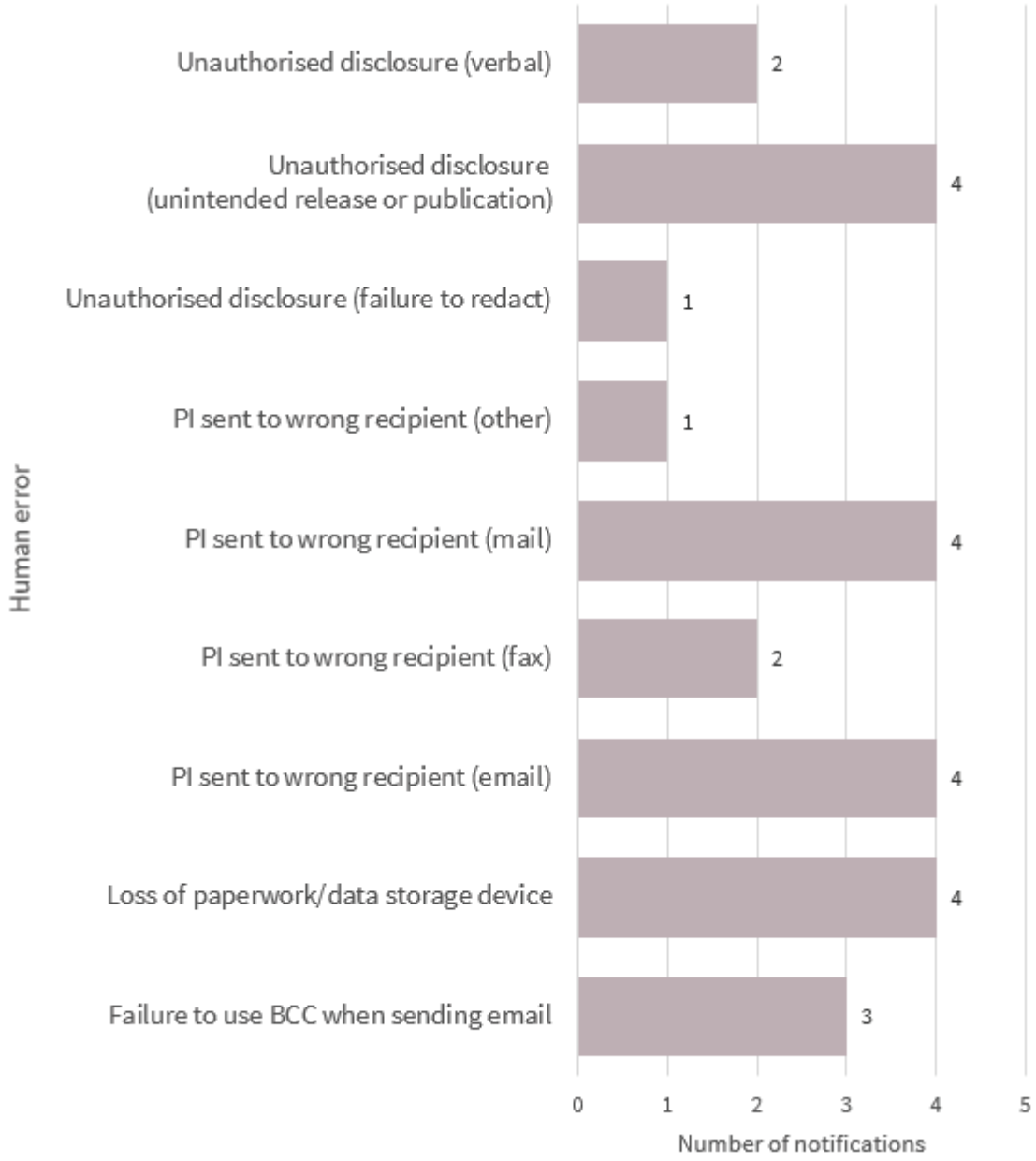
Malicious or criminal attacks accounted for 42 per cent of health sector data breaches (19 notifications).

Only one data breach reported by the health sector was the result of a system fault.

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

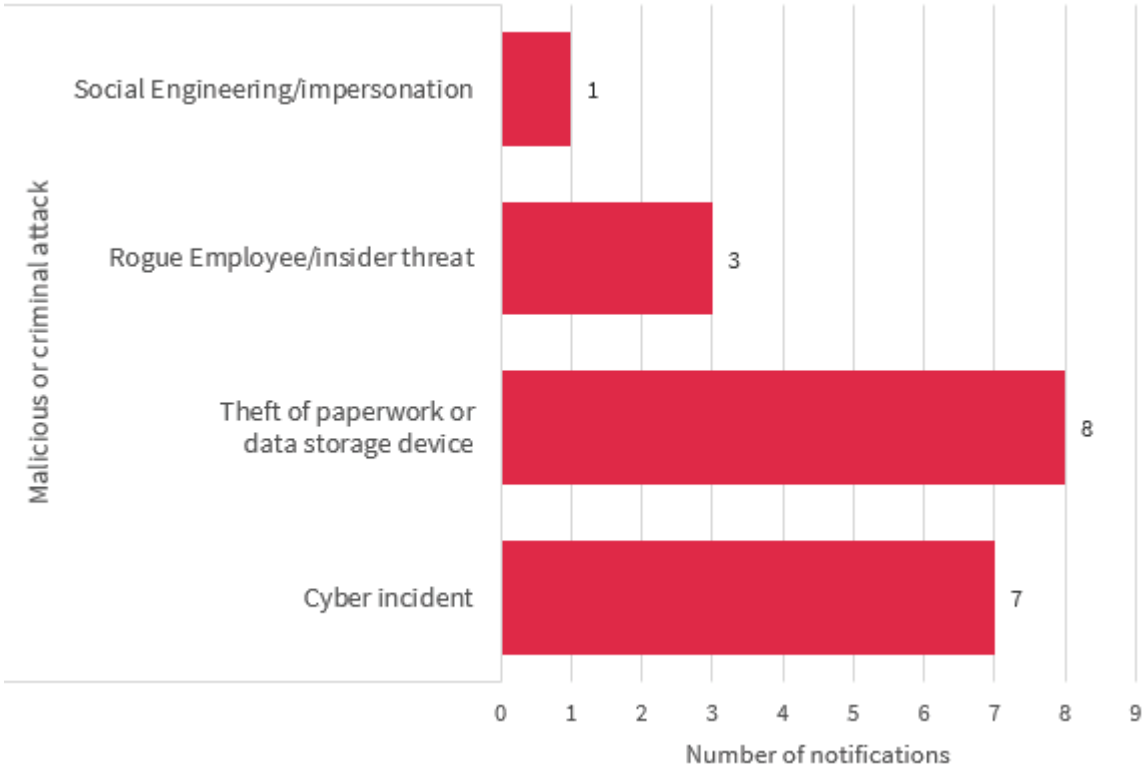


The source of the largest number of data breaches reported by the health sector was human error (56 per cent), with examples including sending personal information to the wrong recipient by email, mail, fax or by other means. Human error also includes the loss of paperwork or storage devices, and the unintended release or publication of personal information.

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

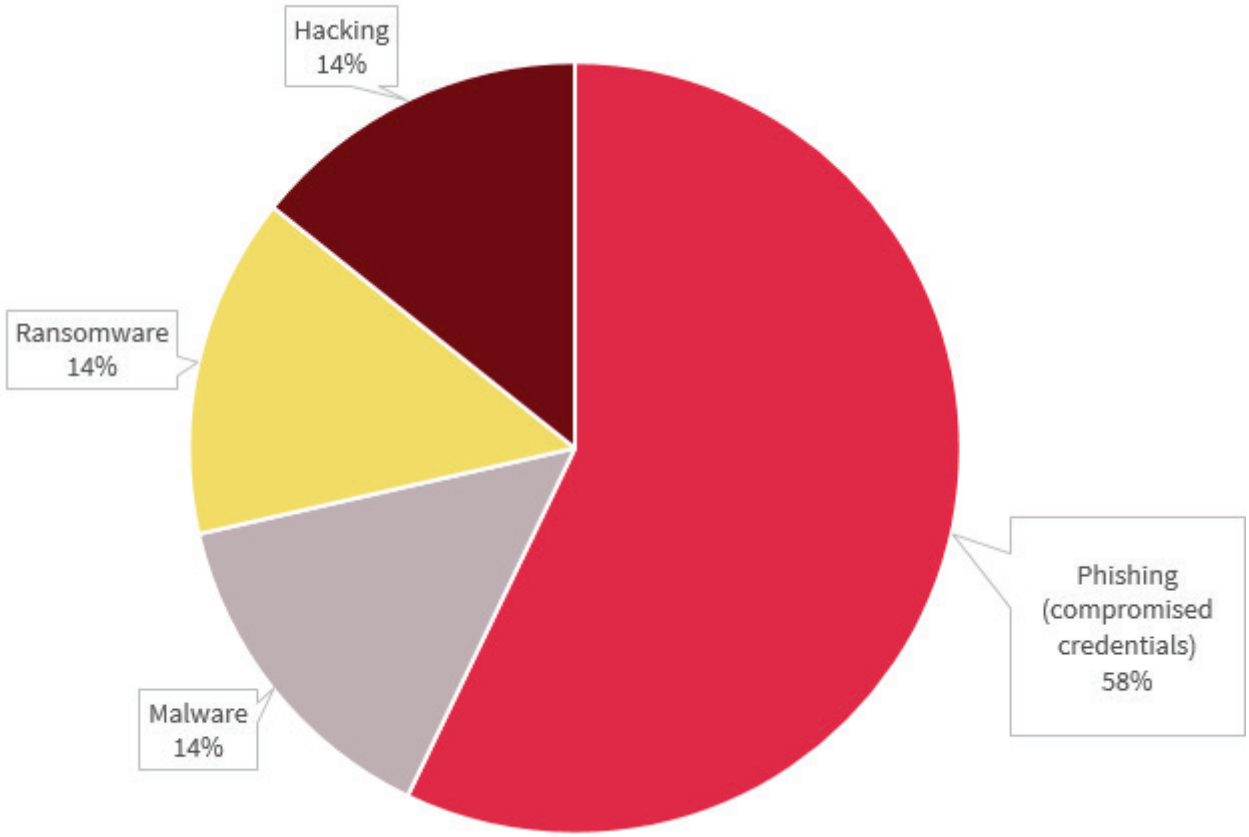


Malicious and criminal attacks were reported as the second largest source of data breaches from the health sector. Of these, theft of paperwork or storage devices was the most common type of attack (42 per cent), and cyber incidents were the second most common type of attack (37 per cent).

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 4 data breaches caused by cyber incidents were the result of compromised credentials through phishing attacks. Malware (1 notification), hacking by other means (1 notification) and ransomware attacks (1 notification) account for the remaining cyber incidents.

System fault breaches — Health sector

One notification from the health sector received during the quarter reported that a system fault resulted in unintended access to personal information.

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 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(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[6]

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.

[6] OAIC's Notifiable Data Breach Form