Australian Government

Office of the Australian Information Commissioner

Notifiable Data Breaches Report

July–December 2019

28 February 2020

OAIC

Contents

About this report

The Office of the Australian Information Commissioner (OAIC) publishes periodic statistical information about notifications received under the Notifiable Data Breaches (**NDB**) scheme to assist entities and the public to understand the operation of the scheme. This report captures notifications made under the NDB scheme for the period from 1 July 2019 to 31 December 2019.

Where data breaches affect multiple entities, the OAIC may receive multiple notifications relating to the same data breach. Notifications relating to the same data breach 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 for statistical purposes. Source of breach categories are defined in the glossary at the end of this report.

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

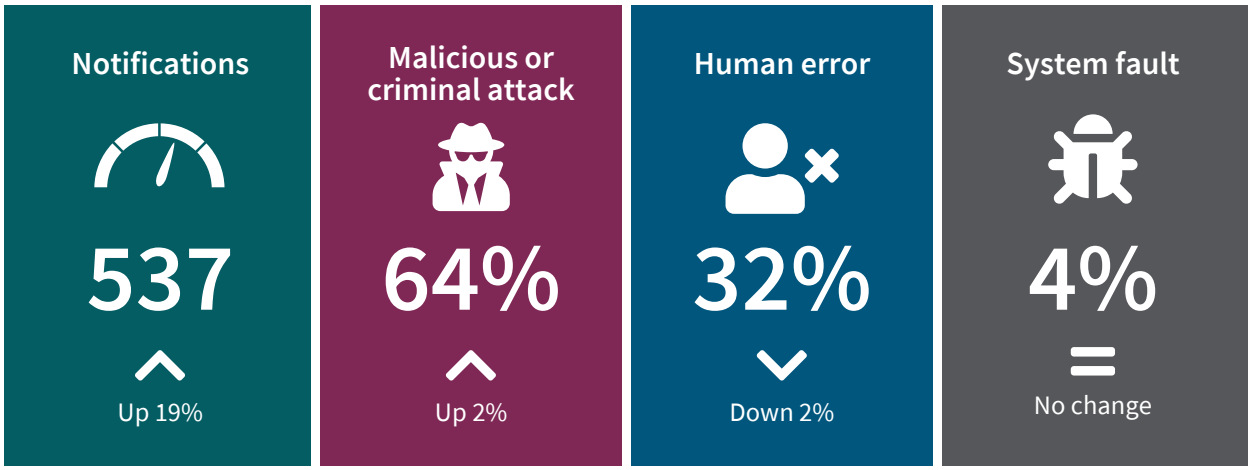
Executive summary

The Notifiable Data Breaches (NDB) scheme was established in February 2018 to improve consumer protection and drive better security standards for protecting personal information. It applies to agencies and organisations who are covered by the *Privacy Act 1988* and are required to take reasonable steps to secure personal information.

This is the first statistical report on the NDB scheme to cover a six-month period. It shows a 19 per cent increase in the number of data breaches reported to the Office of the Australian Information Commissioner (OAIC) between July and December 2019, compared to the first half of the year.

Initially, the OAIC published statistical reports every quarter to help identify any trends and improve awareness and understanding of data breach risks and prevention. The OAIC also published a Notifiable Data Breaches Scheme 12-month Insights Report in May 2019 which examined these trends and highlighted best practice approaches to preventing and responding to data breaches.

Now that the scheme is well established as an effective reporting mechanism, this six-monthly report will continue to track the leading causes and sources of data breaches. It will also highlight emerging issues and areas for ongoing attention by entities entrusted with protecting personal information.



Comparisons are to January to July 2019

Key findings for the July to December 2019 reporting period:

- 537 breaches were notified under the scheme, up from 460 in the previous six months
- Malicious or criminal attacks (including cyber incidents) remain the leading cause of data breaches, accounting for 64 per cent of all notifications
- Data breaches resulting from human error account for 32 percent of all breaches, down from 34 per cent in the last reporting period
- The health sector is again the highest reporting sector, notifying 22 per cent of all breaches
- Human error caused 43 per cent of data breaches in the health sector, compared to an average of 32 per cent across all notifications
- Finance is the second highest reporting sector, notifying 14 per cent of all breaches

- Most data breaches affected less than 100 individuals, in line with previous reporting periods
- Contact information remains the most common type of personal information involved in a data breach.

What is an eligible data breach?

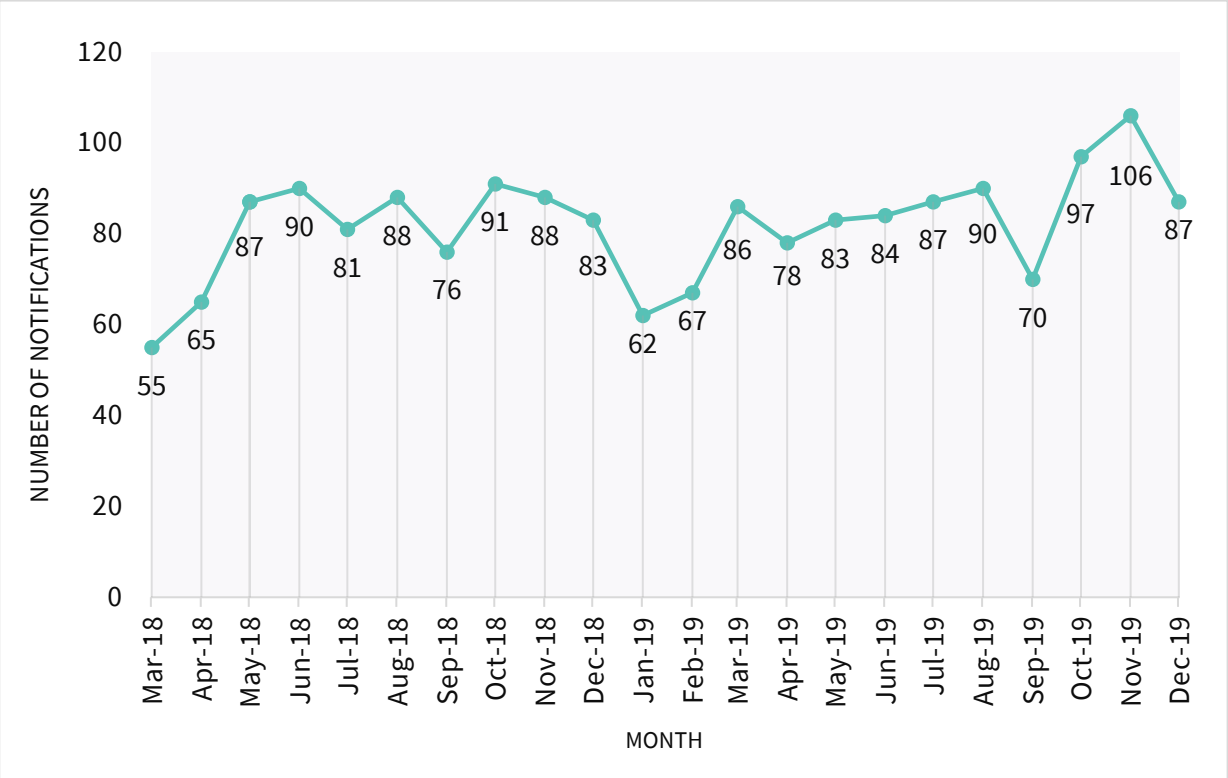
Under the NDB scheme, a data breach is an 'eligible data breach' where:

- there is unauthorised access to or unauthorised disclosure of personal information (or the information is lost in circumstances where unauthorised access to, or unauthorised disclosure of, the information is likely to occur)
- a reasonable person would conclude it is likely to result in serious harm to any of the individuals whose personal information was involved in the data breach, and
- the entity has not been able to prevent the likelihood of serious harm through remedial action.

If an entity suspects that an eligible data breach has occurred, they must undertake an assessment into the relevant circumstances.

If an entity is aware that there are reasonable grounds to believe that there has been an eligible data breach, they must notify affected individuals and the OAIC as soon as practicable.

Chart 1 — Data breach notifications under the NDB scheme



Notifications received July–December 2019

The number of NDBs reported to the OAIC between 1 July and 31 December 2019 increased by 19 per cent compared to the previous six months. The highest number of reported data breaches occurred in November 2019, with 106 notifications — the most reported in any calendar month since the scheme began in February 2018.

Table 1 — Number of breaches reported under the NDB scheme

	Total number of notifications
Total received July to December 2019	537
Total received January to June 2019	460
Total received (2019)	**997**

Top industry sectors to notify breaches

Health service providers[1] (the health sector) reported 117 data breaches during the reporting period. This sector has consistently reported the most data breaches compared to other industry sectors since the start of the NDB scheme.

Table 2 — Top industry sectors by notifications

Top five industry sectors	NDBs received Jul–Dec 2019
Health service providers	117
Finance (incl. superannuation)[2]	77
Education[3]	49
Legal, accounting & management services	40
Personal services[4]	23

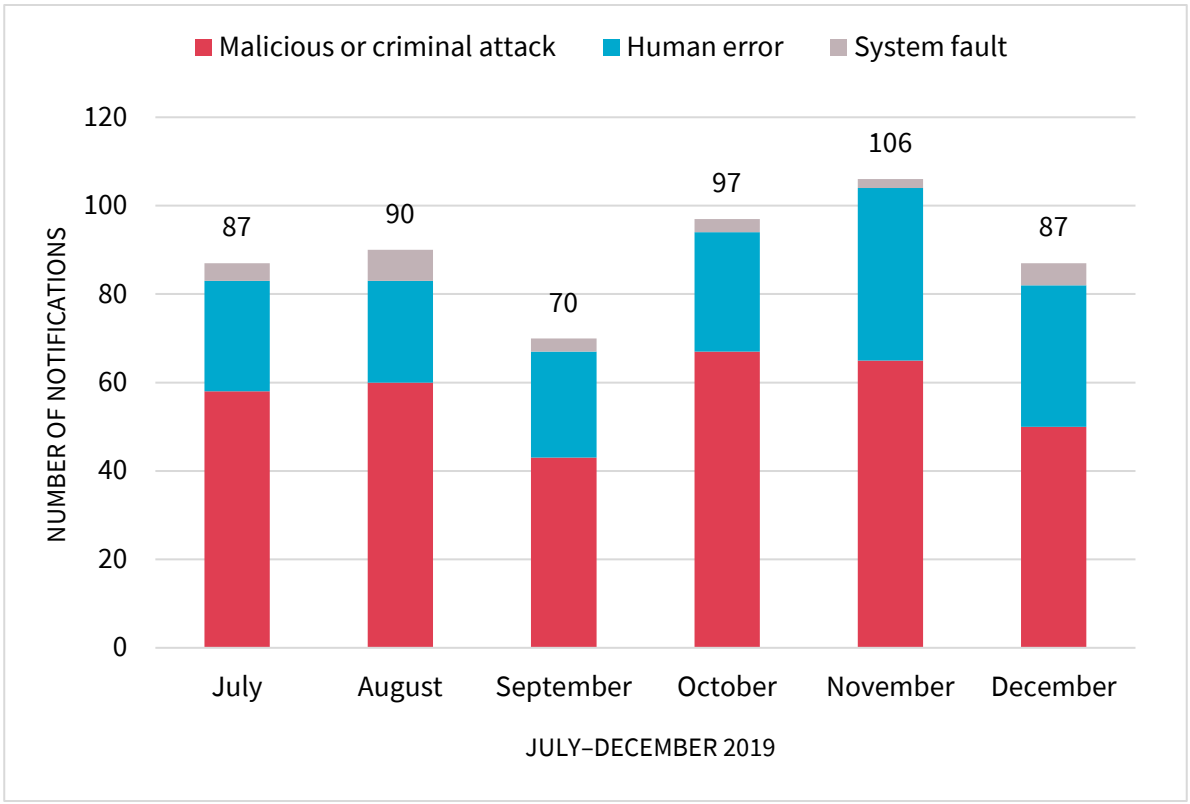
[1] A health service provider generally includes any private sector entity that provides a health service within the meaning of s 6FB of the Privacy Act, regardless of annual turnover. State or Territory public hospitals and health services are generally not covered — they are bound by State and Territory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

[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. Public sector education providers are bound by State and Territory privacy laws, as applicable.

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

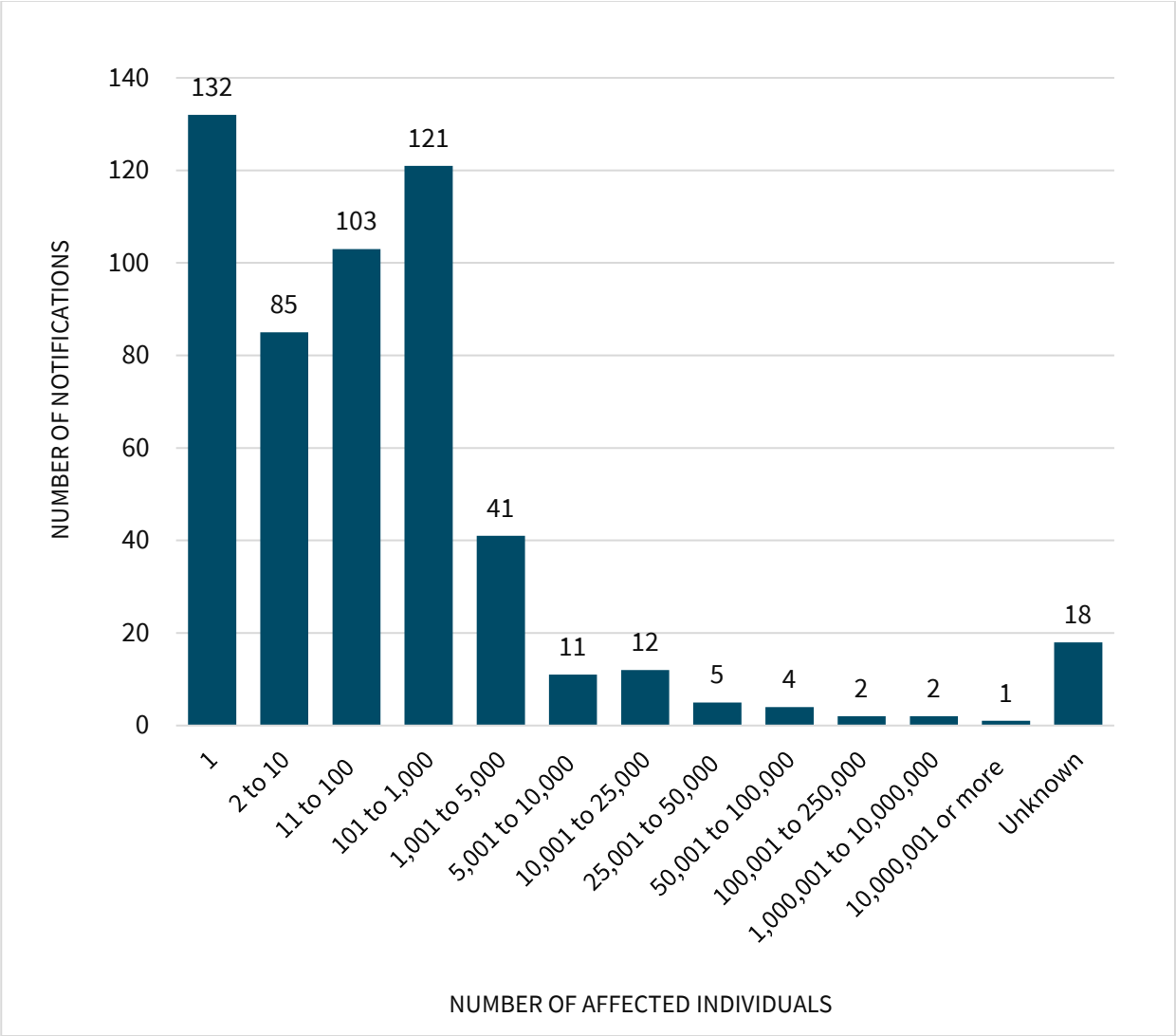
Chart 2 — Number of breaches reported under the NDB scheme — All sectors



Number of individuals affected by breaches — All sectors

Most NDBs in the period involved the personal information of 100 individuals or fewer (60 per cent of notified breaches). Breaches impacting between 1 and 10 individuals comprised 40 per cent of notifications.

Chart 3 — Number of individuals affected by breaches — All sectors



Note: Where bands are not shown (for example, 250,001 to 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.

For the bands 1,000,001 to 10,000,000 and 10,000,001 or more, these figures reflect the number of individuals worldwide whose personal information was compromised in these data breaches, not only individuals in Australia, as estimated by the notifying entities.

Notifying individuals affected by a breach

A key requirement of the NDB scheme is that entities experiencing an eligible data breach must provide affected individuals with a description of the data breach and the kind of information involved, along with recommendations about the steps that individuals should take in response to the breach.

The specific recommendations will depend on the entity's functions and activities, the circumstances of the breach, and the kind of information that was involved. Recommendations should include practical steps that are easy for the individuals to take.

For example, where breaches involve sensitive personal information such as banking details or identity documents such as passports, driver licences or Medicare cards, appropriate recommendations may include requesting a new identity document or asking that an alert be placed on an account.

Across the reporting period, most entities reporting a data breach provided practical guidance to affected individuals, as required by the Privacy Act.

However, there have been instances where an initial notification did not meet the requirements of the NDB scheme because it did not include the details of the types of personal information that were compromised or provide practical steps that people could take in response.

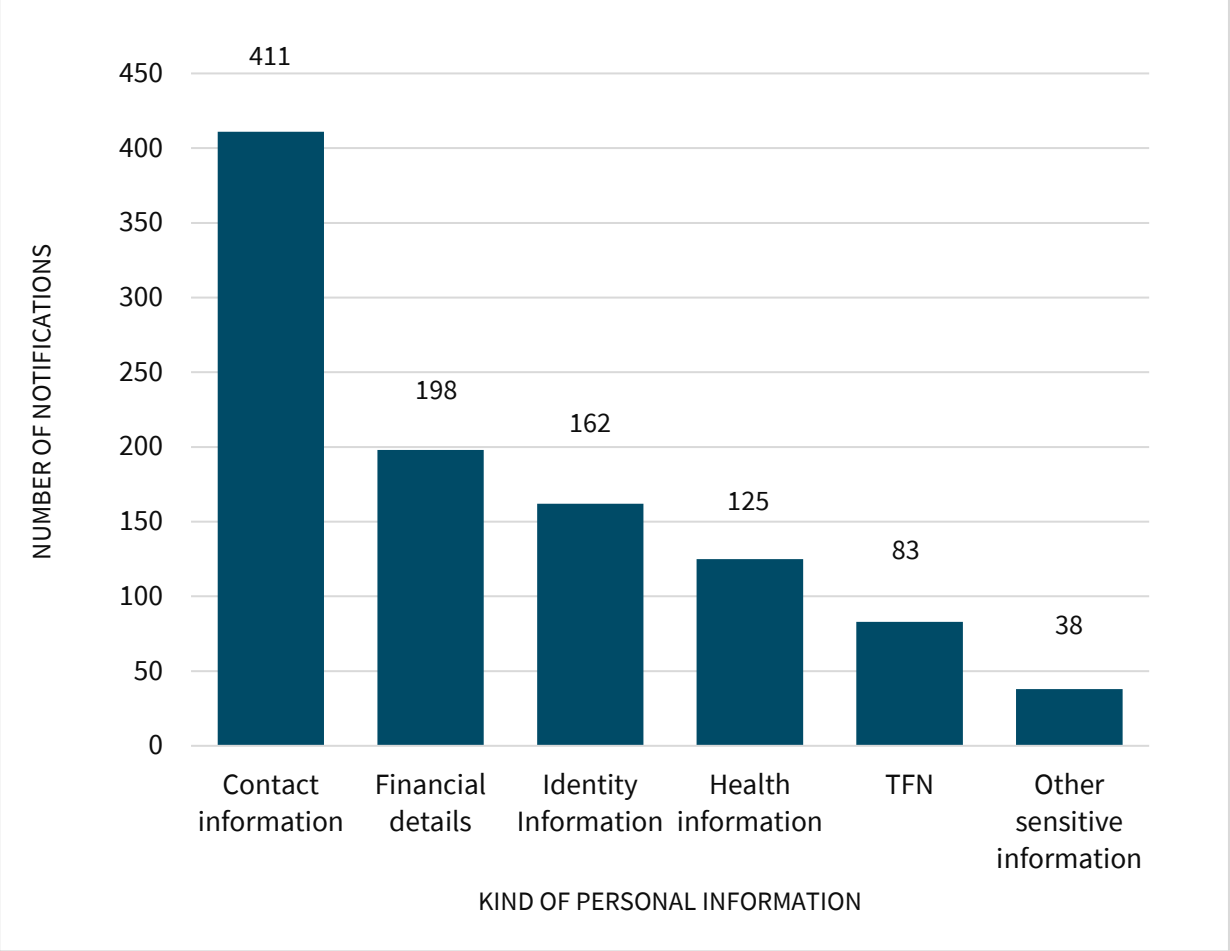
In these cases, the OAIC asked the entity to re-issue the notification to include the practical advice required to help individuals reduce the risk of harm.

Kinds of personal information involved in breaches — All sectors

The majority of data breaches (77 per cent) notified under the scheme between July and December 2019 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 licence number or other government identifiers. Almost a third of data breaches notified between July and December 2019 involved identity information.

Data breaches notified during the reporting period also involved individuals' tax file numbers (TFNs) (15 per cent); financial details, such as bank account or credit card numbers (37 per cent); and health information (23 per cent). 'Other sensitive information' (7 per cent) refers to categories of sensitive information as set out in section 6 of the Privacy Act, other than health information as defined in section 6FA.

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



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

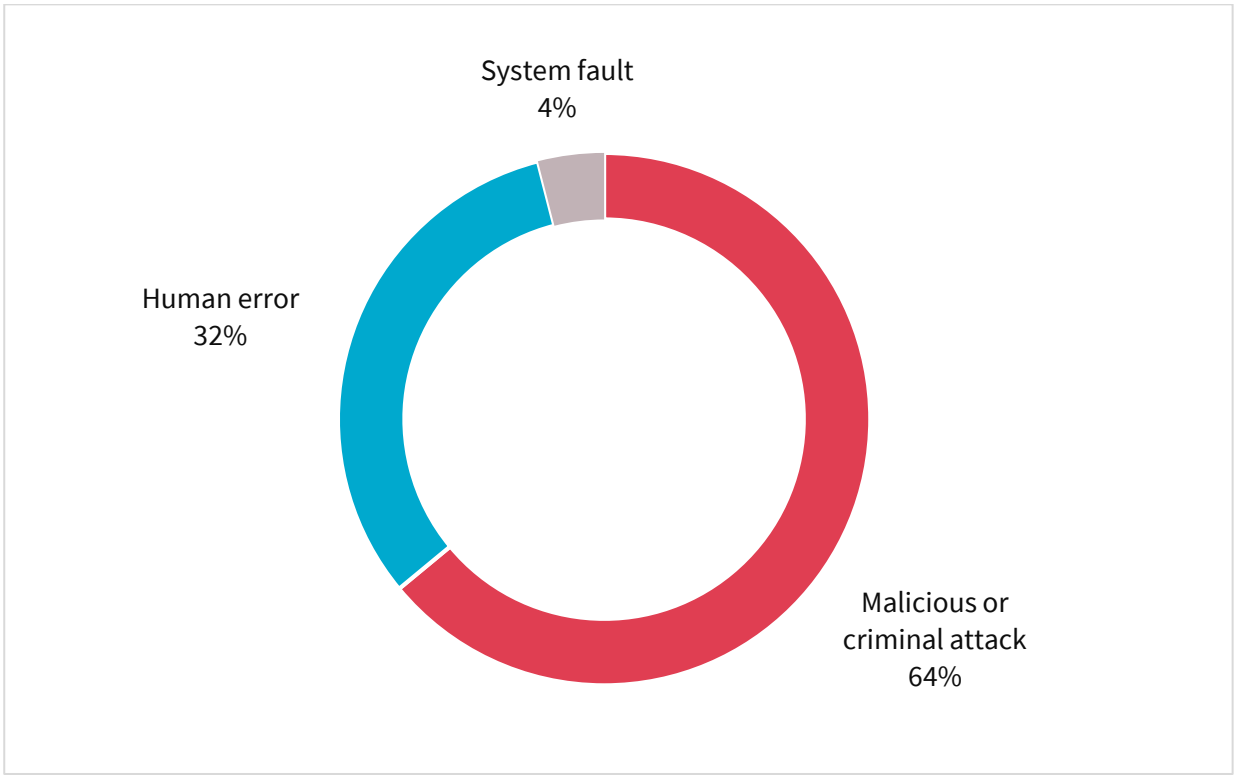
Source of breaches — All sectors

Malicious or criminal attacks were the largest source of data breaches notified to the OAIC between July and December 2019, accounting for 343 breaches. Malicious or criminal attacks are defined as attacks that are deliberately crafted to exploit known vulnerabilities for financial or other gain.

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

Human error remained a major source of breaches, accounting for 170 breaches, while system faults accounted for the remaining 24 breaches notified between July and December 2019.

Chart 5 — Source of data breaches — All sectors



Malicious or criminal attack breaches — All sectors

Cyber incidents were the largest source of malicious and criminal attacks from July to December 2019. The OAIC received 230 notifications under this category, with phishing, malware, ransomware, brute-force attack and compromised or stolen credentials the main source of the data breaches.

Many cyber incidents in this reporting period appear to have exploited vulnerabilities involving a human factor (such as clicking on a phishing email or disclosing passwords).

There was a substantial increase in the number of data breaches attributed to malicious or criminal attacks during the reporting period compared to the previous six months, including a rise in breaches attributed to cyber incidents from 192 to 230.

Theft of paperwork or storage devices was also a significant source of malicious or criminal attacks (40 notifications). Other sources included social engineering or impersonation (33 notifications) and actions taken by a rogue employee or insider threat (40 notifications).

Chart 6 — Breaches resulting from malicious or criminal attacks — All sectors

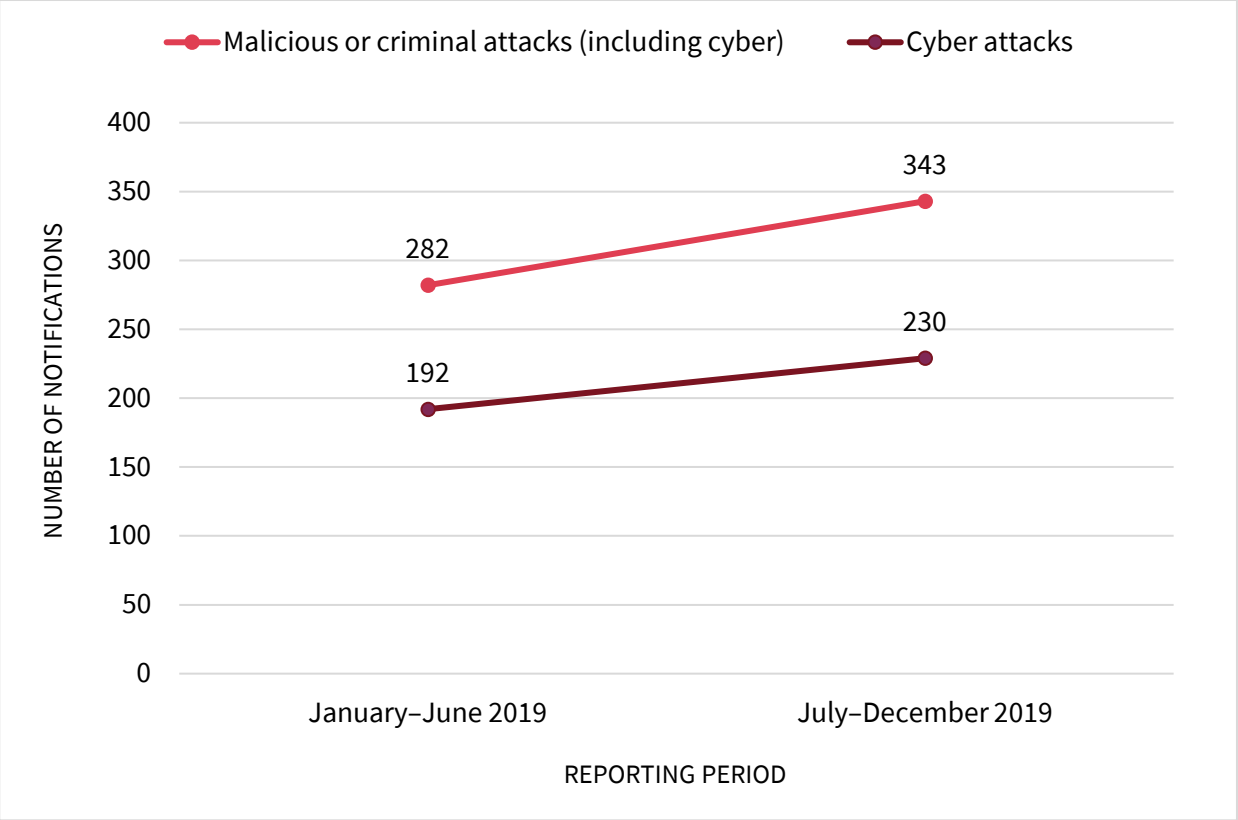
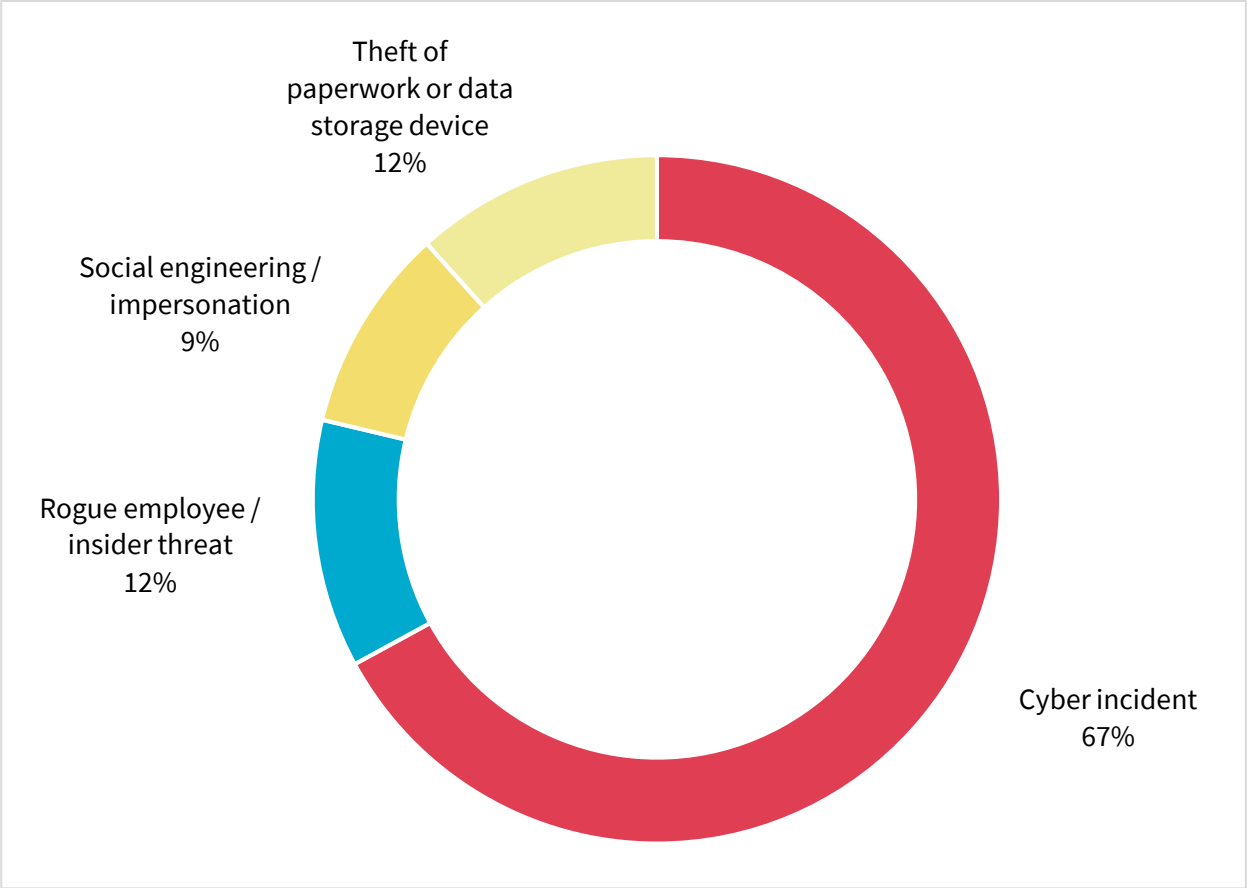


Chart 7 — Malicious or criminal attacks — All sectors



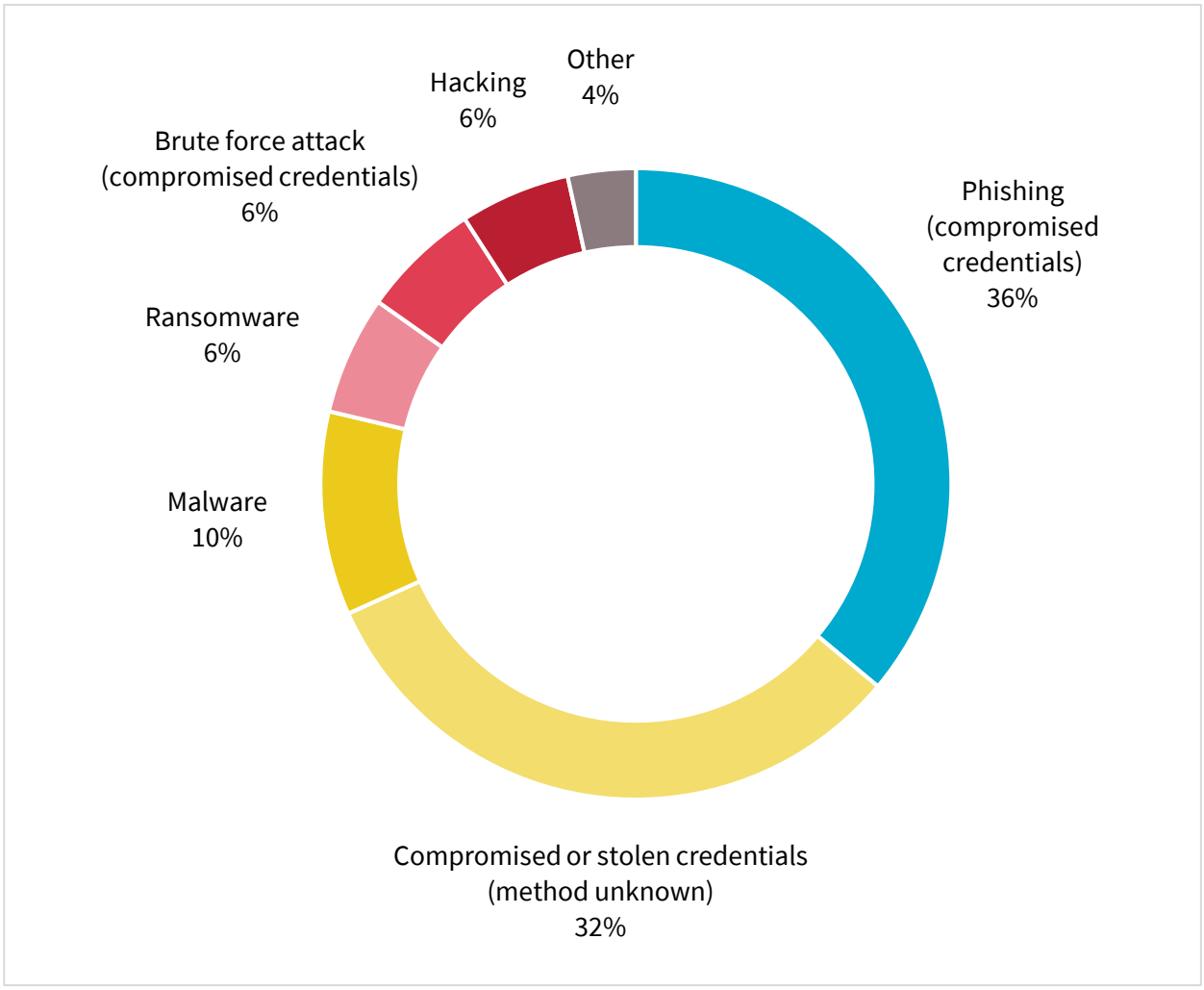
Cyber incident breaches — All sectors

The majority of cyber incidents during the reporting period were linked to the compromise of credentials through phishing (83 notifications), malware (24 notifications) and brute-force attack (14 notifications). In many of these incidents the malicious actor gained access to personal information stored in email accounts.

However, in a significant number of cyber incidents (74 notifications) the entity experiencing the breach was unable to identify how the malicious actor obtained the compromised credentials.

Nevertheless, many breaches resulting from cyber incidents still included a human element, given the malicious actor often required their target to do something, such as respond to a password request that claimed to be from a legitimate source or service provider.

Chart 8 — Cyber incident breakdown —All sectors



Use of email inboxes for primary storage of information

The compromise of account credentials via phishing emails remains one of the most common causes of data breaches across the reporting period, accounting for 15 per cent of all breaches. A further 14 per cent of all data breaches were attributed to compromised or stolen credentials, which often provided a malicious actor with direct access to personal information stored in the compromised email account.

In a number of these instances the malicious actor gained access to thousands — and in some cases tens of thousands — of stored emails. These frequently contained a significant amount of personal information from a large number of individuals, including sensitive information such as financial and bank account details, tax file numbers and health information.

The malicious actors were then able to exploit this access in two ways:

- using the compromised email account to conduct further phishing campaigns or targeted business email compromise attacks against other individuals or businesses, including individuals whose contact details were stored within the email account
- exploiting the personal information contained within the account for targeted spear phishing attacks against specific individuals or to carry out identity fraud.

In this context, the use of email applications and services for the primary storage of significant quantities of personal information makes it easier for malicious actors to gain access to sensitive personal information that can be exploited for criminal gain.

In these instances, further access to an entity's network or servers is not needed because sensitive personal information is directly accessible from the email account. This can also make it difficult for a forensic investigation of the breach to determine the full extent of the information that was compromised where the email account lacks audit and access logging.

Human error breaches — All sectors

The second largest source of data breaches was human error (32 per cent of all data breaches), with examples including sending personal information to the wrong recipient via email (29 per cent of data breaches resulting from human error), unintended release or publication of personal information (24 per cent) and the loss of paperwork or data storage device (11 per cent).

However, certain kinds of breaches can affect larger numbers of people. For example, in this reporting period personal information being sent by email to incorrect recipients impacted the largest numbers of people in this data breach category, with an average of 340 affected individuals per breach. Failure to use the 'blind carbon copy' (BCC) function when sending group emails impacted an average of 303 people per breach.

Chart 9 — Human error breakdown — All sectors

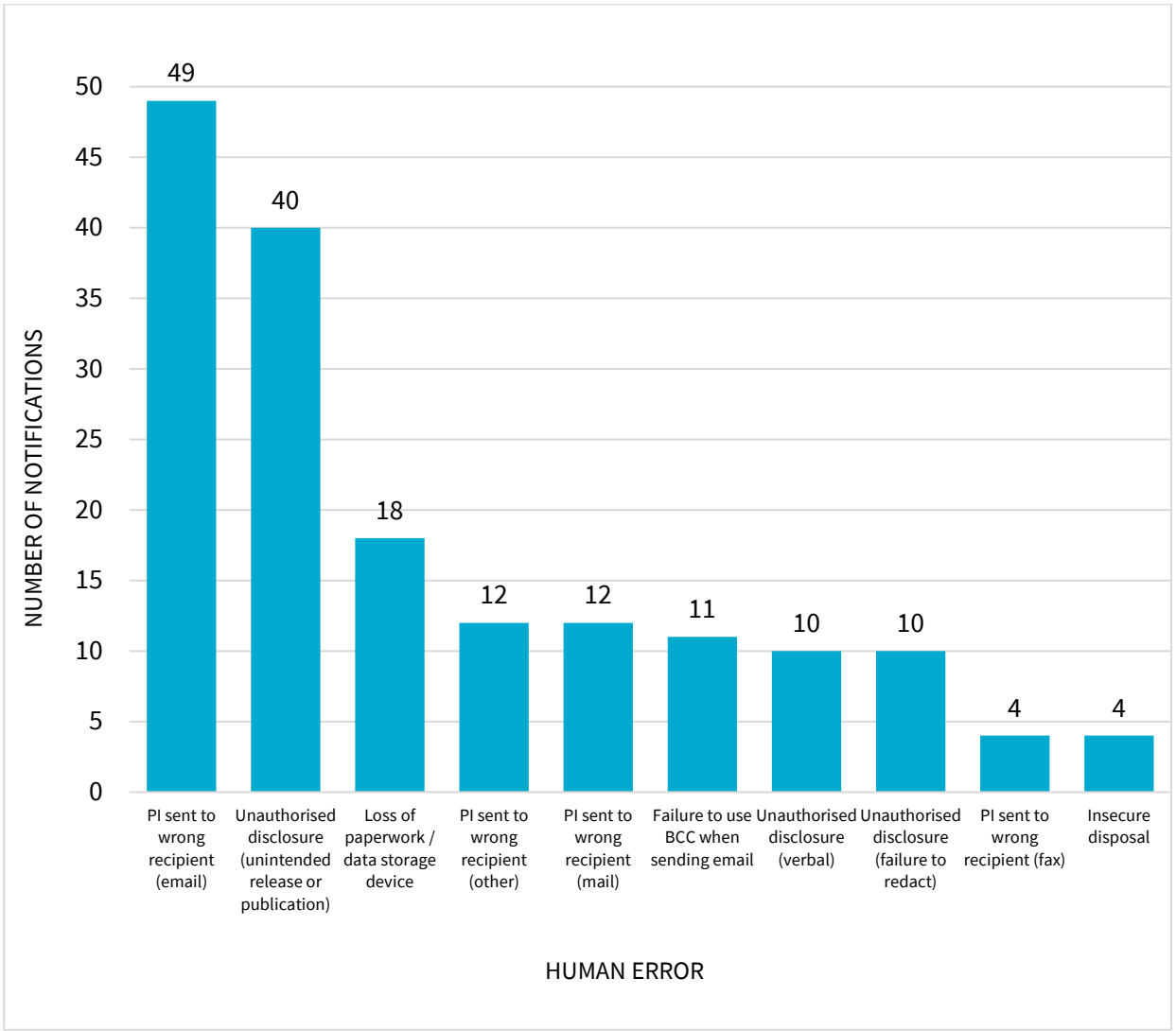


Table 3 — Human error breakdown by average number of affected individuals — All sectors

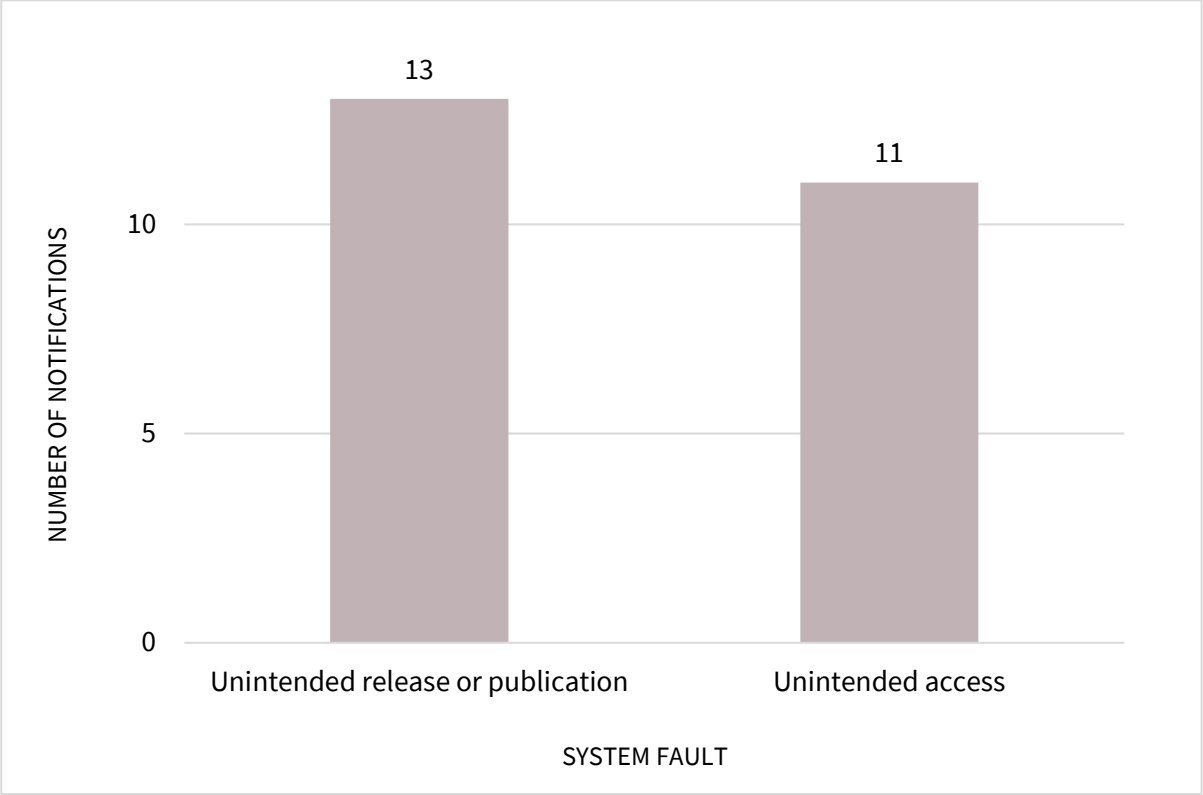
Kinds of personal information	No. of NDBs received Jul—Dec 2019	Average no. of affected individuals
Loss of paperwork/data storage device	18	57
Failure to use BCC when sending email	11	303
Unauthorised disclosure (failure to redact)	10	8
Unauthorised disclosure (unintended release or publication)	40	831
Unauthorised disclosure (verbal)	10	1
Insecure disposal	4	1,574
PI sent to wrong recipient (email)	49	340
PI sent to wrong recipient (mail)	12	1
PI sent to wrong recipient (other)	12	14
PI sent to wrong recipient (fax)	4	5

System fault breaches — All sectors

System faults accounted for four per cent of data breaches this reporting period. Unintended access to personal information as a result of a system fault caused 11 data breaches, while unintended release or publication of personal information as a result of a system fault caused 13 data breaches.

System fault breaches included data breaches that occurred as a result of a business or technology process error. During the reporting period, system fault data breaches were predominantly due to either coding errors in web-facing applications which resulted in the unintended release or publication of personal information, or a failure to securely configure web-facing applications which potentially exposed personal information on the internet.

Chart 10 — System fault breakdown — All sectors



Comparison of top five industry sectors

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

From July to December 2019, health service providers reported 117 data breaches, or 22 per cent of all data breaches in the period. 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.

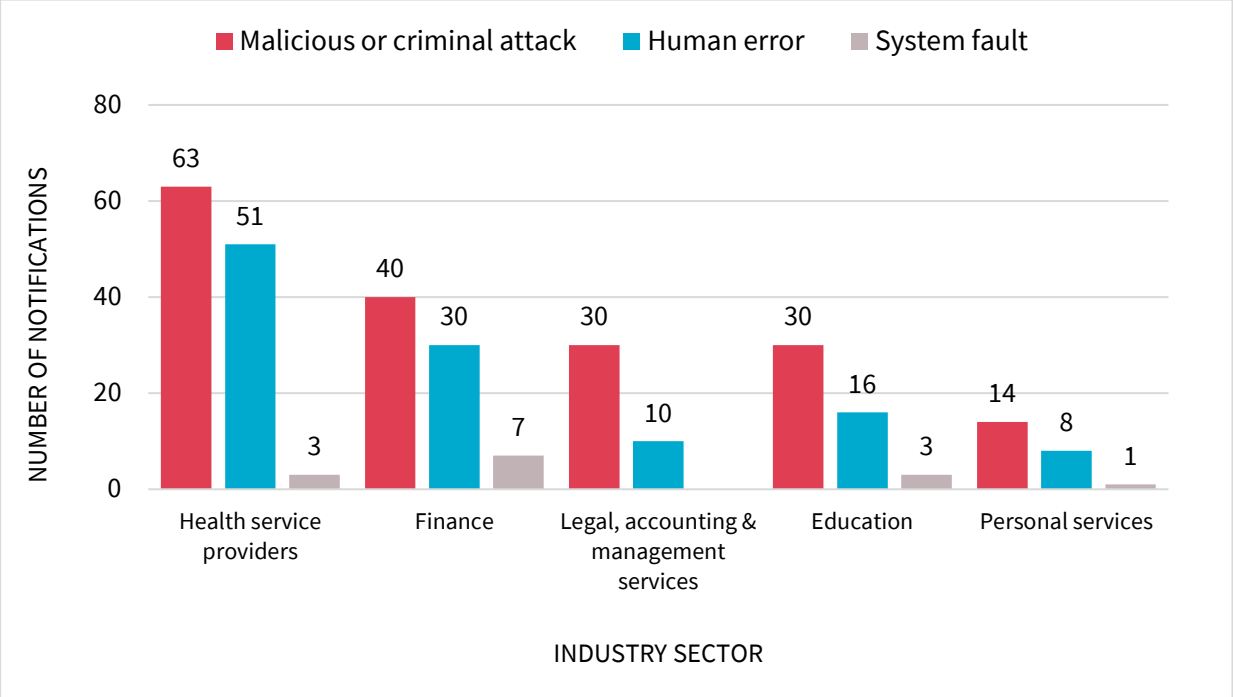
The second largest source of NDBs was the finance sector (14 per cent), followed by education (9 per cent), legal, accounting and management services (7 per cent), and personal services (4 per cent). Personal services include employment, training and recruitment agencies, childcare centres, vets and community services.

Source of breaches — Top five industry sectors

Malicious or criminal attacks caused 54 per cent of data breaches reported by the health sector (63 notifications), while 43 per cent resulted from human error (51 notifications).

Notifications from the finance sector indicated that 52 per cent of data breaches resulted from malicious or criminal attacks (40 notifications), and 40 per cent from human error (30 notifications). The proportion of data breaches resulting from human error in both the health and finance sectors was higher than the average across all notifications (32%). Four of the top five sectors notified at least one breach resulting from a system fault.

Chart 11 — Source of data breaches — Top five industry sectors



Transmission of personal information

From July to December 2019, almost a third of all data breaches reported related to breaches caused by human error (170 notifications). This included 49 incidents where personal information was emailed to the wrong recipient, and 18 involving the loss of paperwork or data storage devices such as phones, laptops and USB drives.

Email is an important method of communication between individuals and businesses. However, given that nearly 10 per cent of all data breaches reported to the OAIC from July to December 2019 resulted from personal information being emailed to the wrong person, the use of email for the transmission of personal information carries risks.

This is particularly the case when email is used for the transmission of sensitive personal information such as bank account or credit card details, identifying documents (passport or driver licence details), tax file numbers, health and medical information, or other information which could lead to a risk of serious harm if disclosed to the wrong individual.

All entities who handle, store, or transmit sensitive personal information should consider how to protect personal information during every stage of its life cycle, including by considering whether it is necessary to transmit personal information in order to carry out their functions or activities.

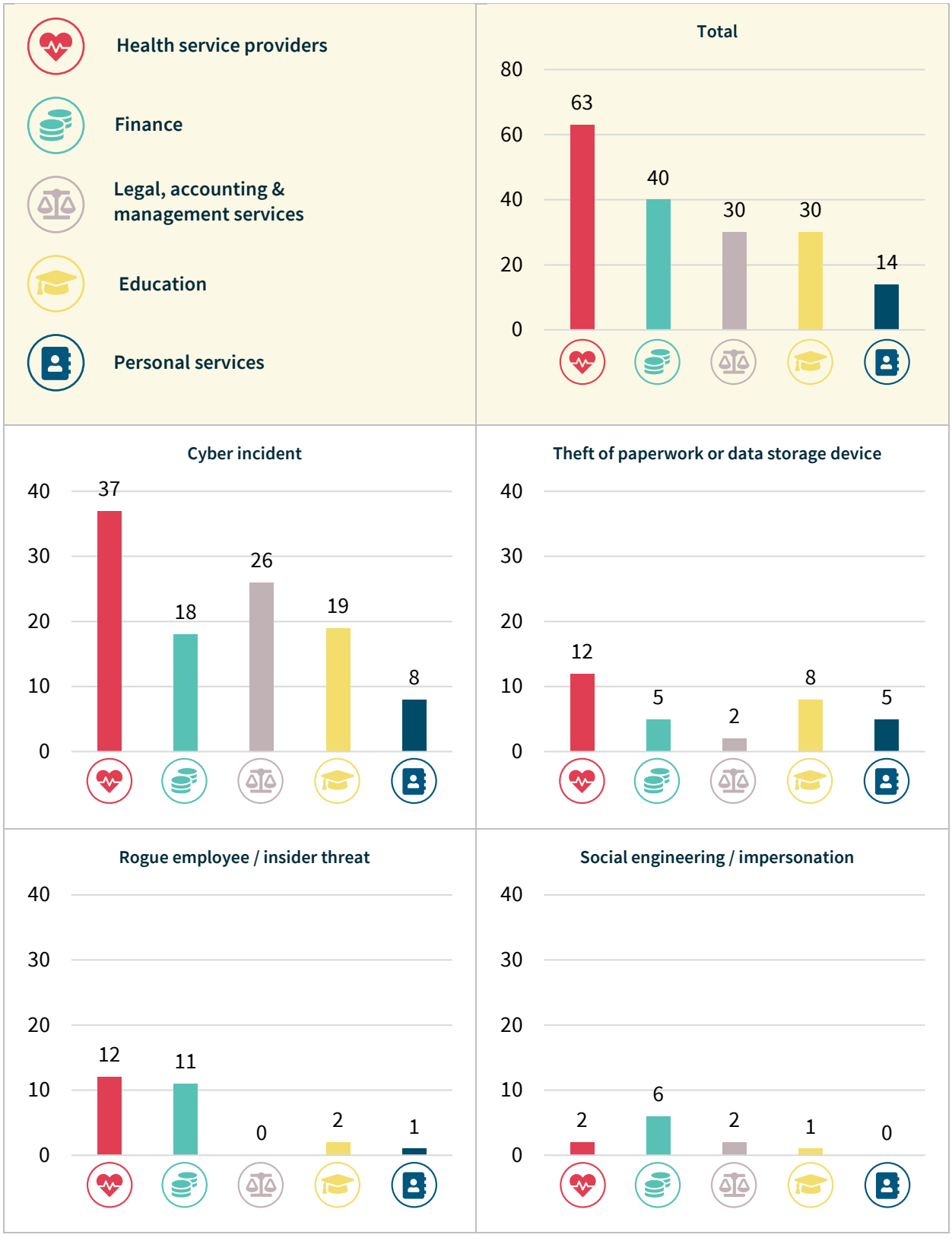
Entities are also responsible for planning how to handle personal information by embedding privacy protections into the design of information handling practices. This may include:

- automated 'warnings' requiring the author of an email to confirm the address of the recipient before a message is sent
- deleting emails containing personal or sensitive information from both the inbox and sent box and storing relevant documents in a secure document management system
- password protecting or encrypting documents containing sensitive information which are sent via email.

Some entities use postal or courier services to send sensitive information to individuals, including material stored on portable media such as USB drives. Given the risk of loss in transit or incorrect delivery, entities using postal or courier services should also consider additional security protections, such as encrypted or password-protected portable media storage.

Malicious or criminal attack breaches — Top five industry sectors

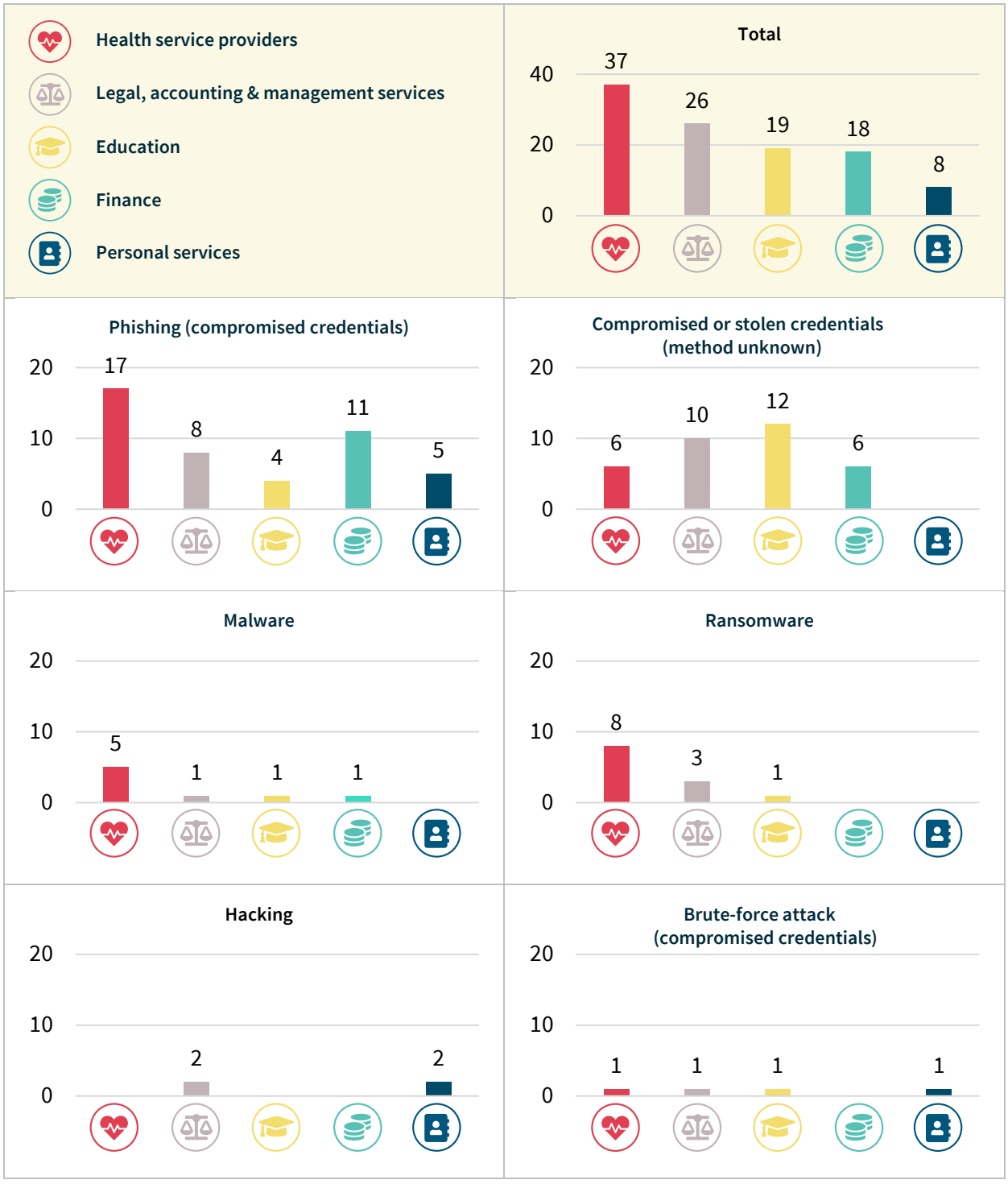
Chart 12 — Malicious or criminal attacks breakdown — Top five industry sectors



Cyber incident breaches — Top five industry sectors

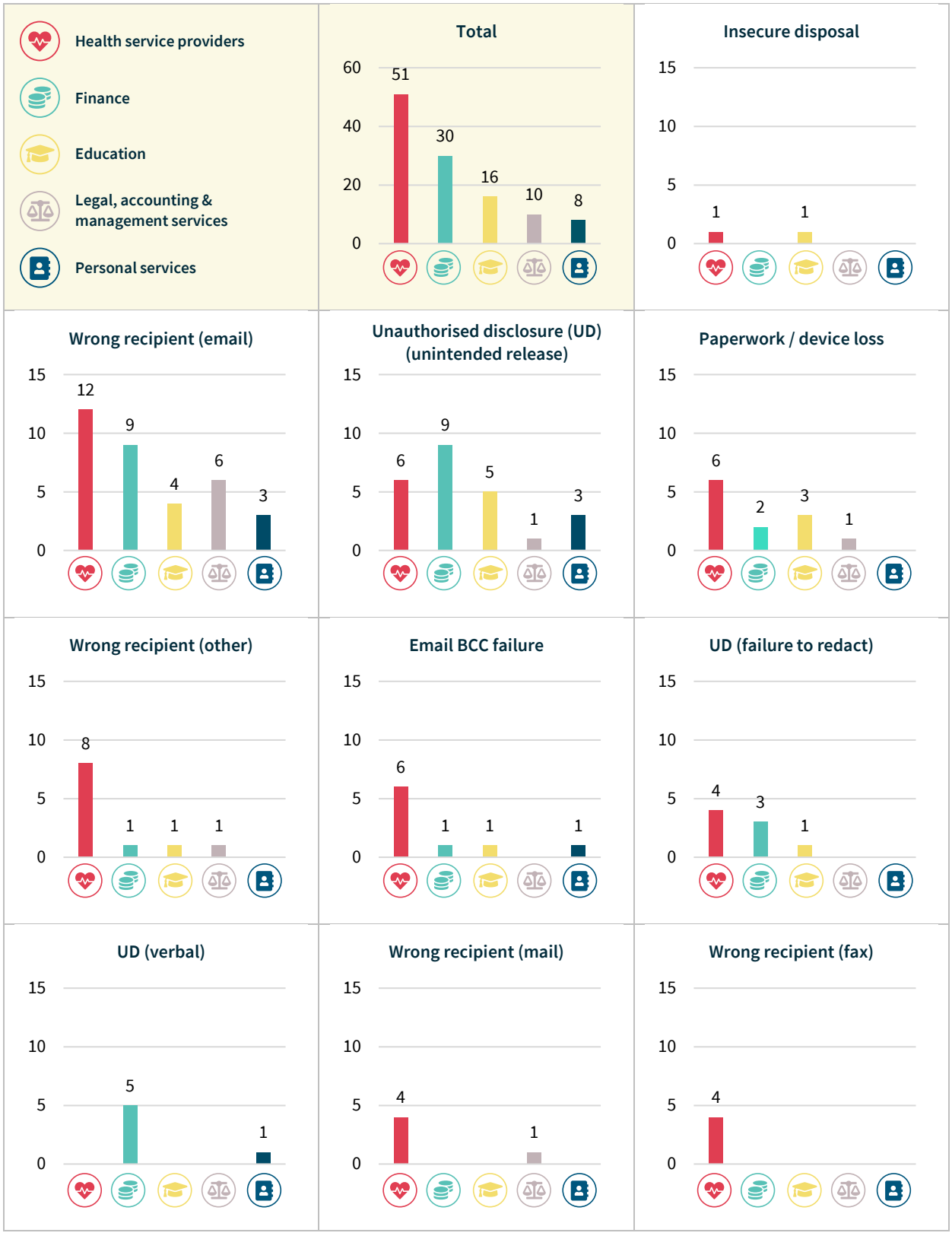
Similar to the overall trend, a majority of cyber incidents reported by the top five industry sectors between July and December 2019 were linked to phishing or compromised credentials. This trend was strongest in the finance sector where these attacks accounted for 94 per cent of all data breaches attributed to cyber incidents.

Chart 13 — Cyber incident breakdown — Top five industry sectors



Human error breaches — Top five industry sectors

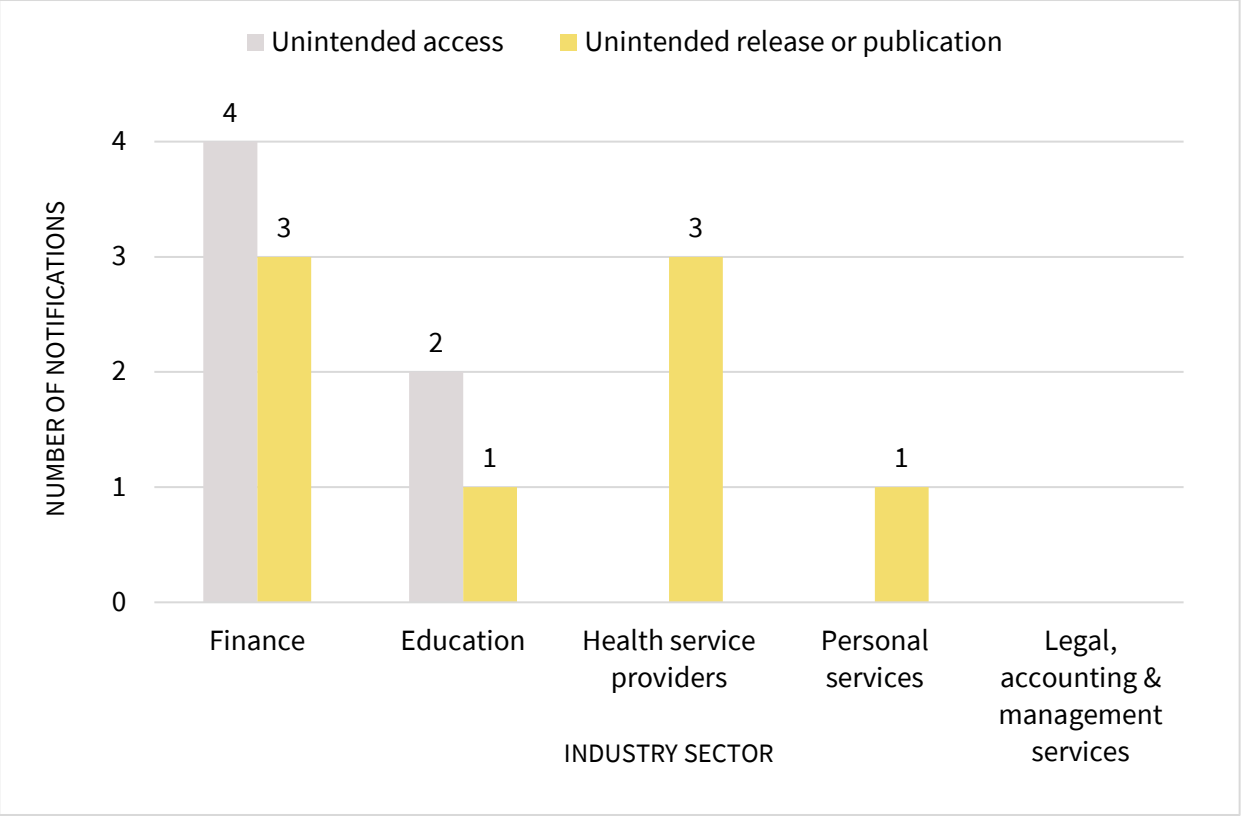
Chart 14 — Human error breakdown — Top five industry sectors



System fault breaches

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

Chart 15 — System fault breakdown — Top five industry sectors



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 a 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' 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.

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[5]

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 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.

[5] OAIC's Notifiable Data Breach Form