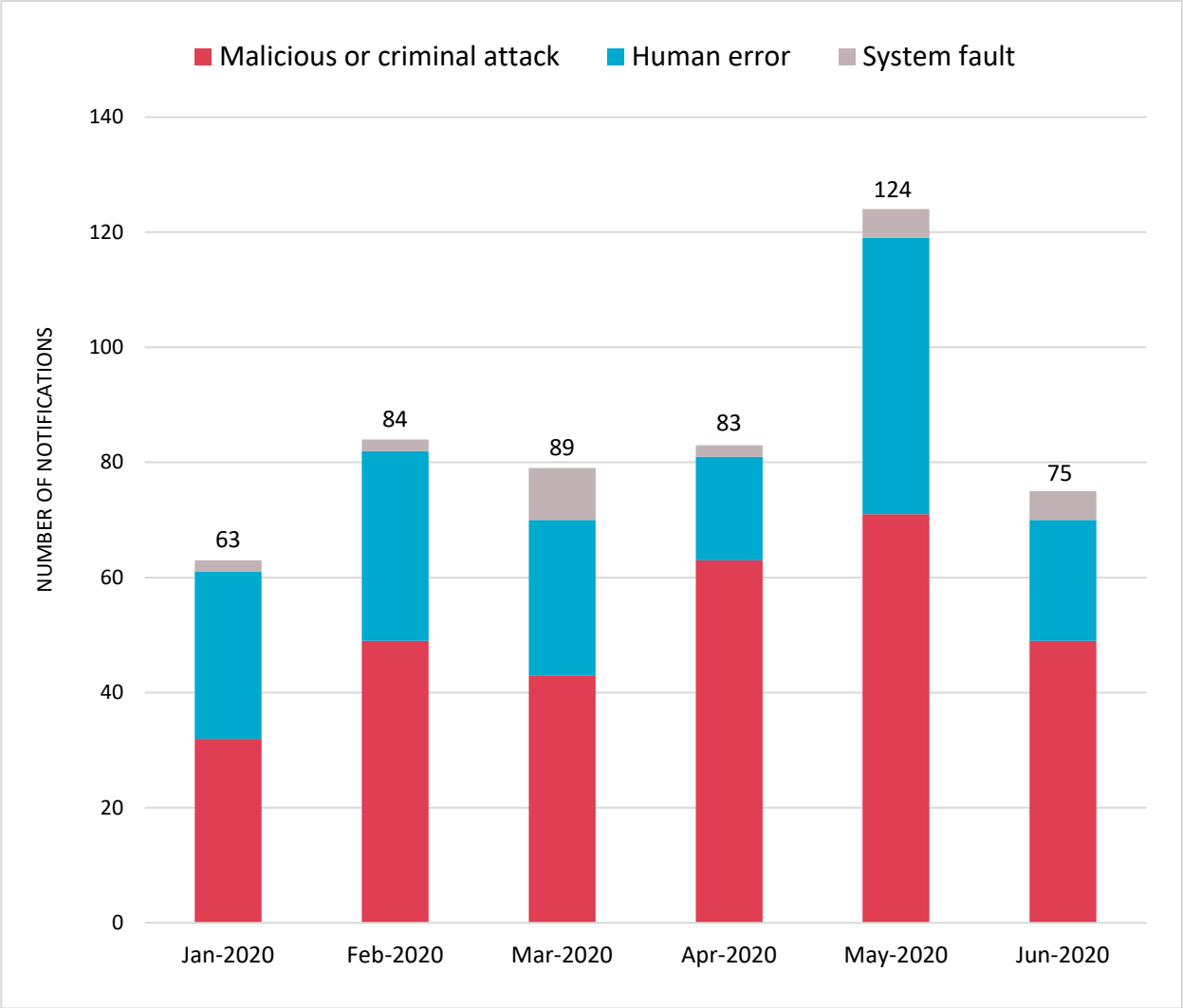
Chart 2 — Number of breaches reported under the NDB scheme — All sectors



Assessing a data breach

Between January and June 2020, the OAIC received a number of notifications where it was not clear whether the notifying entity had either undertaken an appropriate assessment of the data breach, or had determined the nature and extent of the 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. This should include whether the breach posed a risk of serious harm to affected individuals, the cause or source of the breach, the type of personal information that was accessed or disclosed, and the number of individuals who were at risk of serious harm as a result of the breach.

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. The OAIC's data breach response flowchart illustrates the steps that should be taken in assessing and responding to an eligible data breach.

Understanding the nature and extent of the breach

The capacity to conduct a timely and thorough assessment and investigation of a suspected data breach can be constrained when an entity does not comprehensively understand its own information environment.

Notifying entities who did not have audit or activity logging enabled on their network or email servers/accounts, or could not undertake retrospective traffic analysis of their internet gateway, had difficulty determining whether a malicious actor who had gained access to their network in a cyber attack had accessed or exported (exfiltrated) personal information.

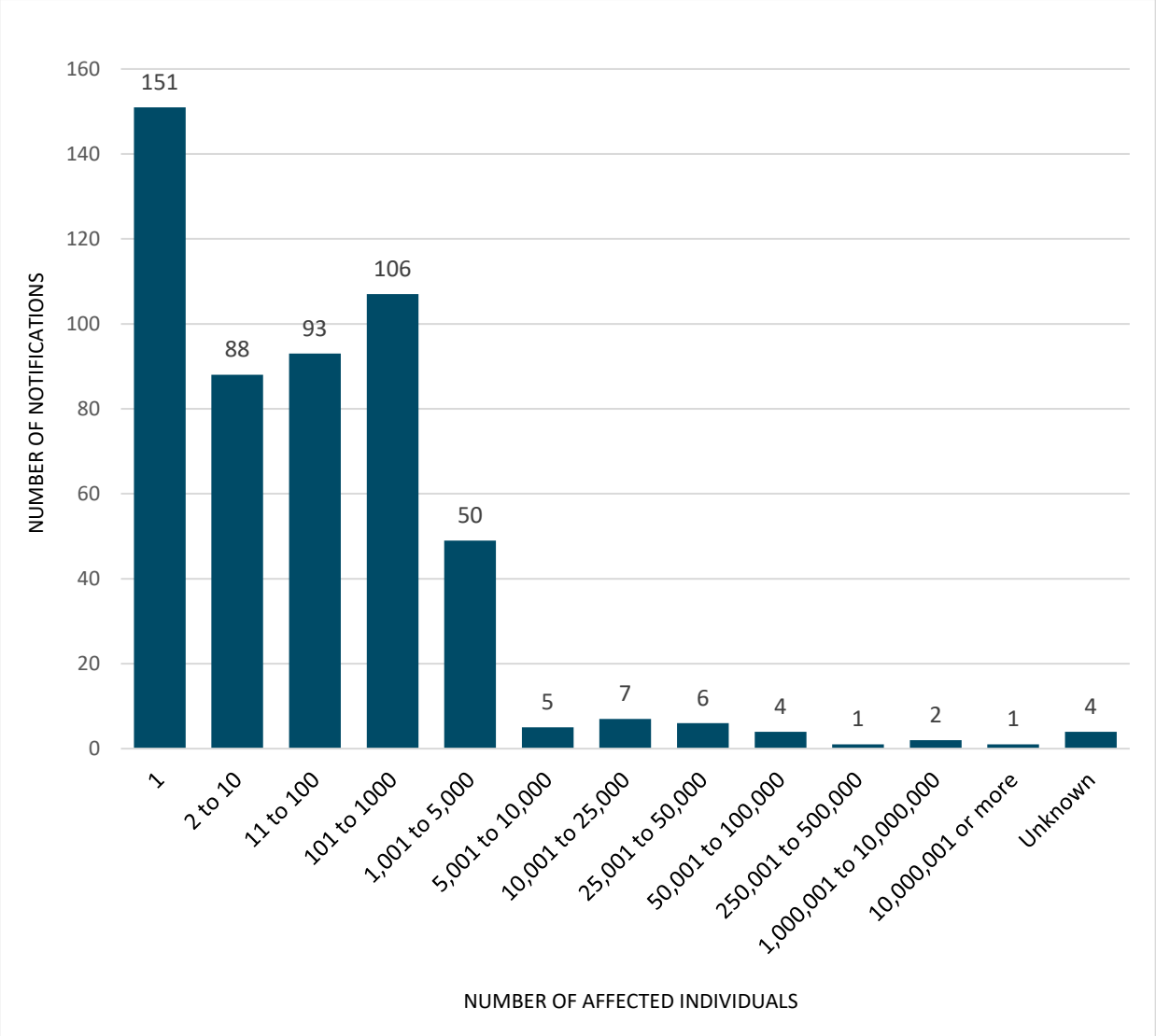
All entities covered by the Privacy Act should be aware of the personal information they retain within their information and communications technology (ICT) environment and where it is located. Effective ICT security requires protecting both hardware and software from misuse, interference, loss, unauthorised access, modification and disclosure.

If an entity does not have a clear understanding of the types of information it retains and where it stores it, not only will the entity find it difficult to meet its obligations under the NDB scheme if a data breach occurs, it may also be in breach of the requirements of Australian Privacy Principles 1 and 11 (APPs).

Number of individuals affected by breaches — All sectors

Most NDBs in the period involved the personal information of 100 individuals or fewer (64% of notified breaches). Breaches affecting between 1 and 10 individuals comprised 46% of notifications.

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



Note: Where bands are not shown (for example, 100,001 to 250,000), there were nil reports in the period. 'Unknown' includes notifications by entities with ongoing investigations 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

There have been multiple instances of incomplete notifications of data breaches where entities may not have fully met their obligations with regard to the content of the notification to individuals affected by a data breach.

For example, while entities notified affected individuals that their email addresses were involved in a data breach, on some occasions they did not advise that other personal information was also involved. This included personal information contained as attachments to emails received and sent from the compromised account, or in the cloud storage associated with the account.

Multiple notifications failed to include recommendations about the steps that individuals should take in response to the breach.

In these cases, the OAIC required the entity to re-issue the notification to include all the kinds of personal information that was involved, and provide the practical advice required to help individuals reduce the risk of harm.

Example of best notification practice

Entities reporting a data breach are required to provide practical guidance to affected individuals. As a best practice example, an organisation which experienced a data breach involving the financial, contact, identity details and Tax File Numbers (TFNs) of over 1000 people issued a detailed notification that provided:

- a comprehensive summary of the data breach and what the entity had done to contain and remediate the breach
- an itemised summary of all the types of personal information that had been exposed in the data breach
- a number of practical steps that those affected should take in response to the breach, including:
    - guidance on best practice in relation to the use of email and cyber security practices tailored to reflect the heightened risk of targeted spear phishing or fraudulent approaches to individuals affected by the breach
    - specific advice on steps individuals could take to reduce the risk of unauthorised access to bank accounts, credit cards and superannuation accounts
    - recommendations on options for placing credit bans on credit files
    - advice on how to contact Australian Government agencies about breaches of identity information such as Medicare number and TFN.

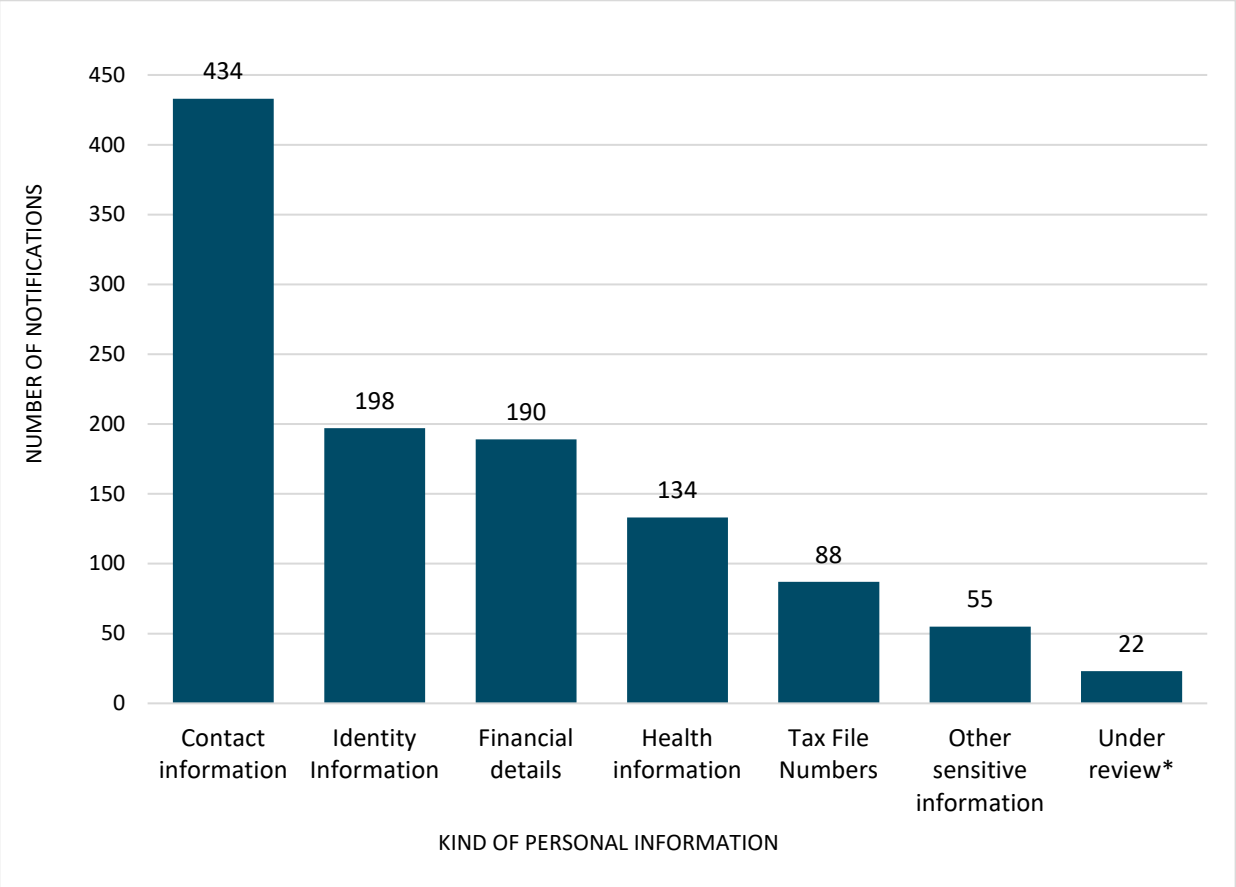
The OAIC's website includes practical guidance about steps individuals can take to reduce their risk of harm. When applicable, these steps should be included in notifications to affected individuals.

Kinds of personal information involved in breaches — All sectors

The majority of data breaches (84%) notified under the NDB scheme from January to June 2020 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. Over a third of data breaches notified during the period involved identity information.

Data breaches notified in this period also involved TFNs (17%), financial details, such as bank account or credit card numbers (37%) and health information (26%). 'Other sensitive information' (11%) 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.

* For breaches listed against this category, the notifying entity was still conducting its assessment of the breach at the time it notified the OAIC and had not finalised its review of what categories of personal information had been disclosed or accessed.

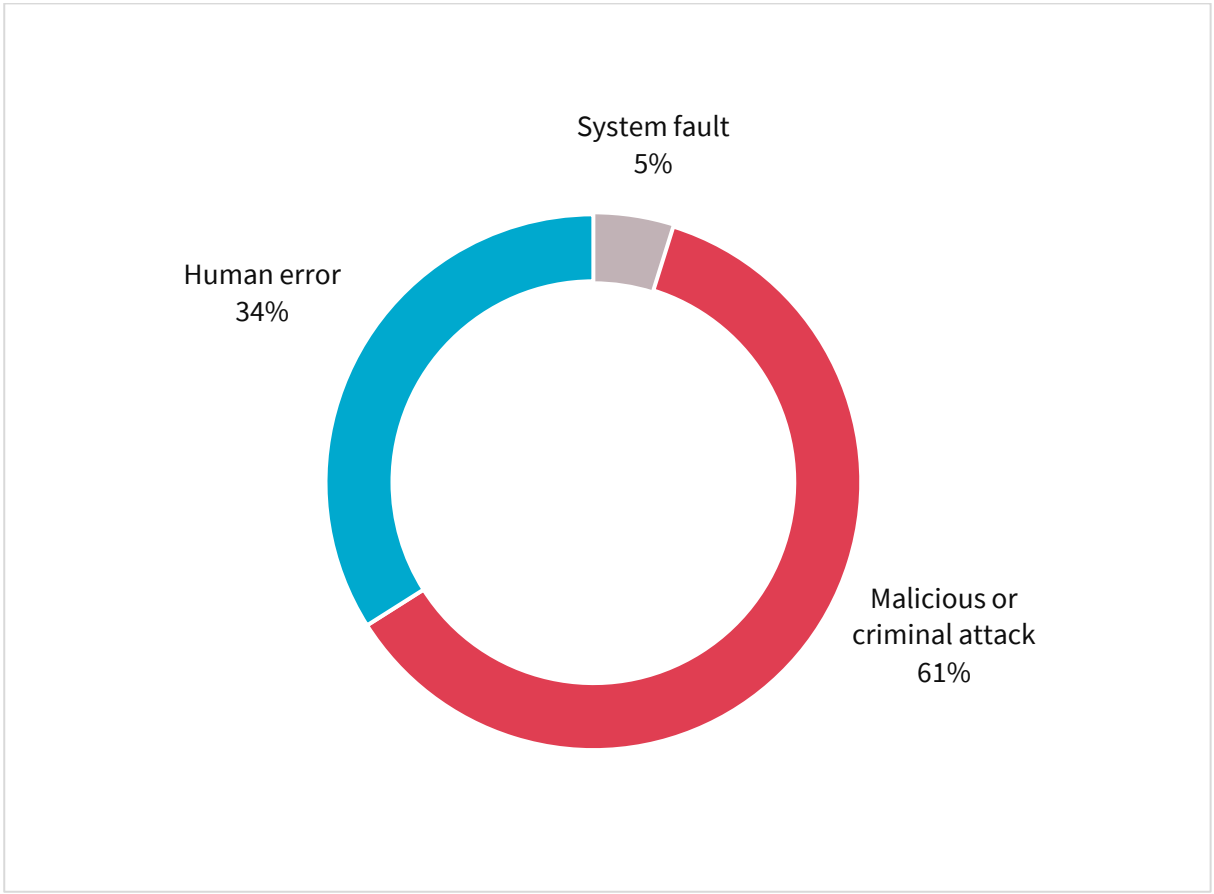
Source of breaches — All sectors

Malicious or criminal attacks were the largest source of data breaches notified to the OAIC between January and June 2020, accounting for 317 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 176 breaches, while system faults accounted for the remaining 25 breaches notified.

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 January to June 2020. The OAIC received 218 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 slight decrease in the number of data breaches attributed to malicious or criminal attacks during the reporting period compared to the previous six months.

The number of data breaches resulting from social engineering or impersonation has increased by 47% during the reporting period to 50 notifications. Actions taken by a rogue employee or insider threat accounted for 25 notifications. Theft of paperwork or storage devices resulted in 24 notifications.

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

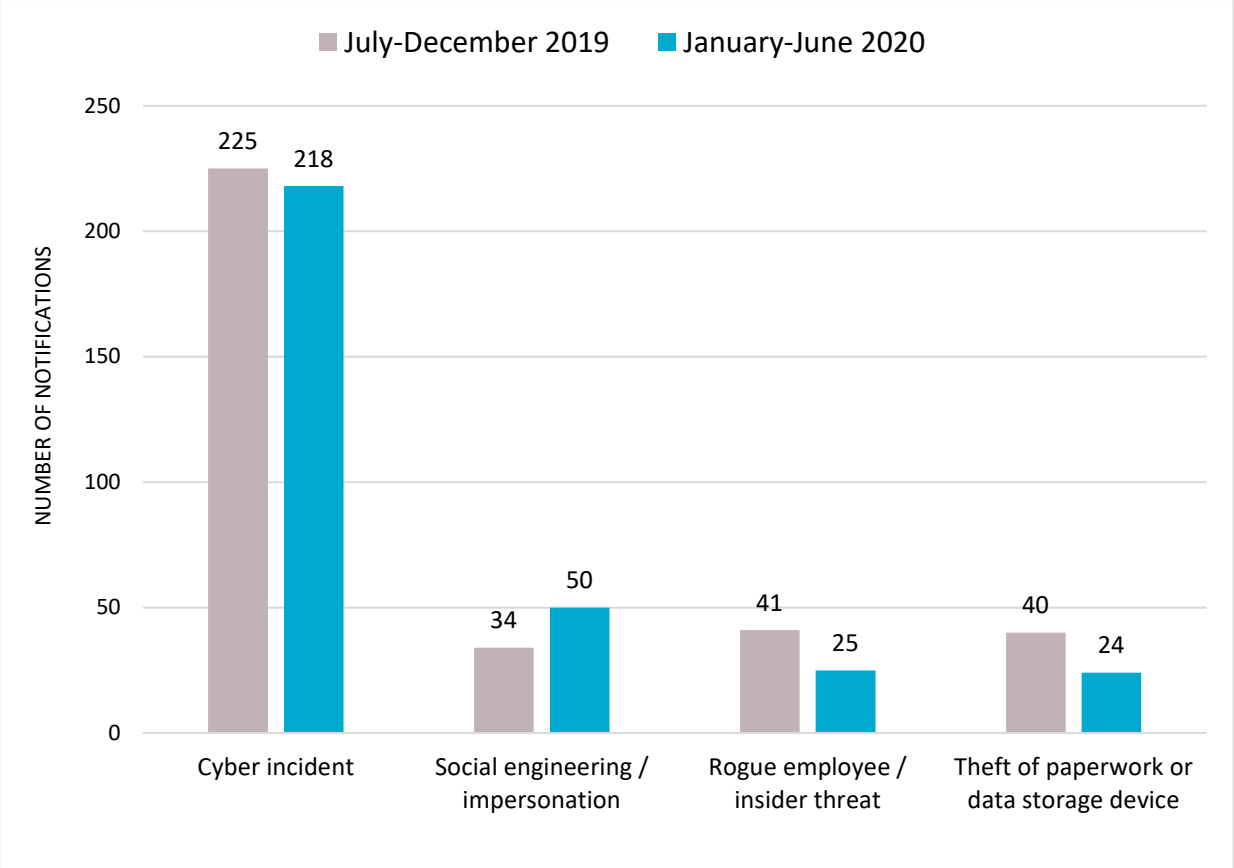
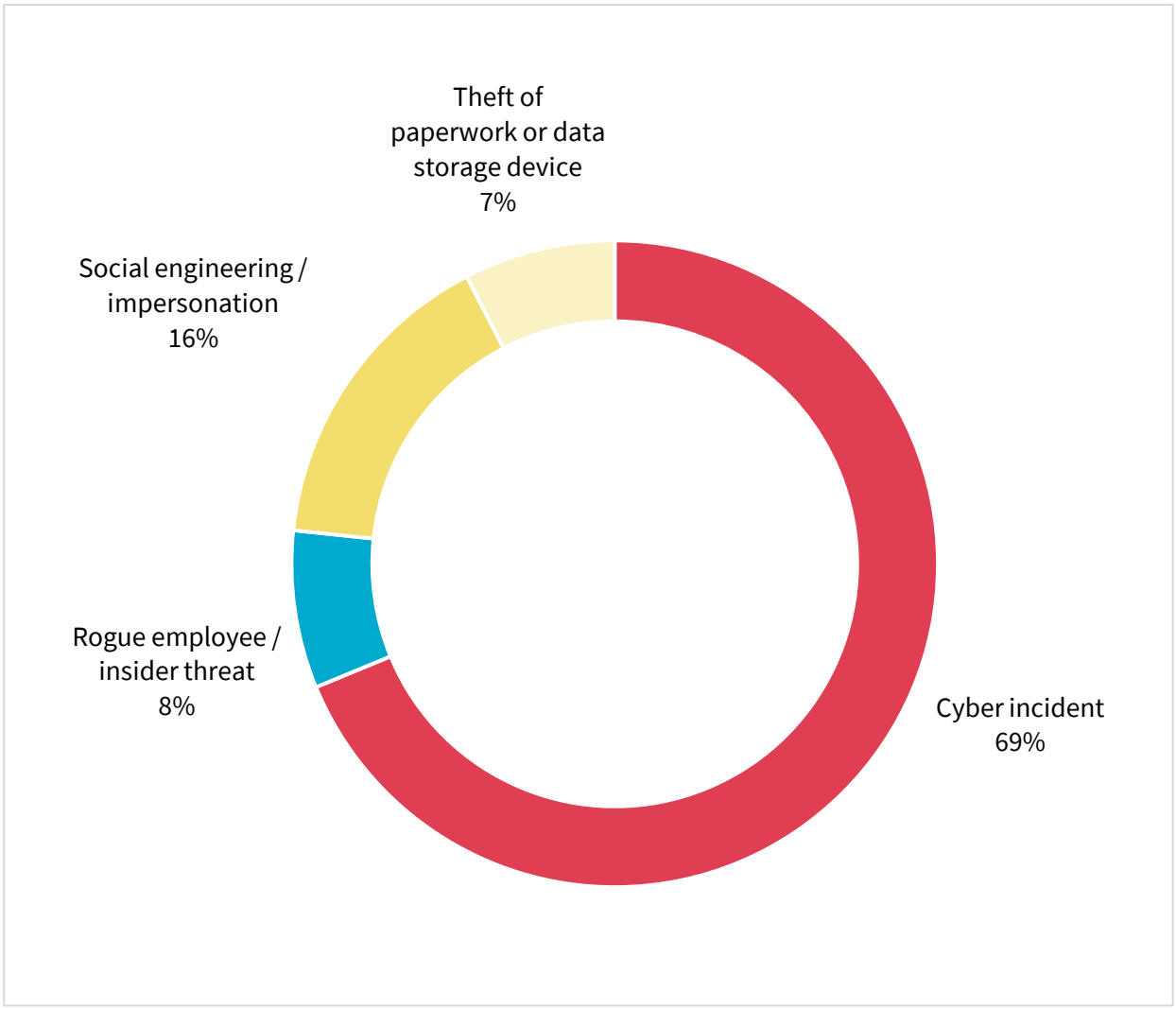


Chart 7 — Malicious or criminal attacks — All sectors

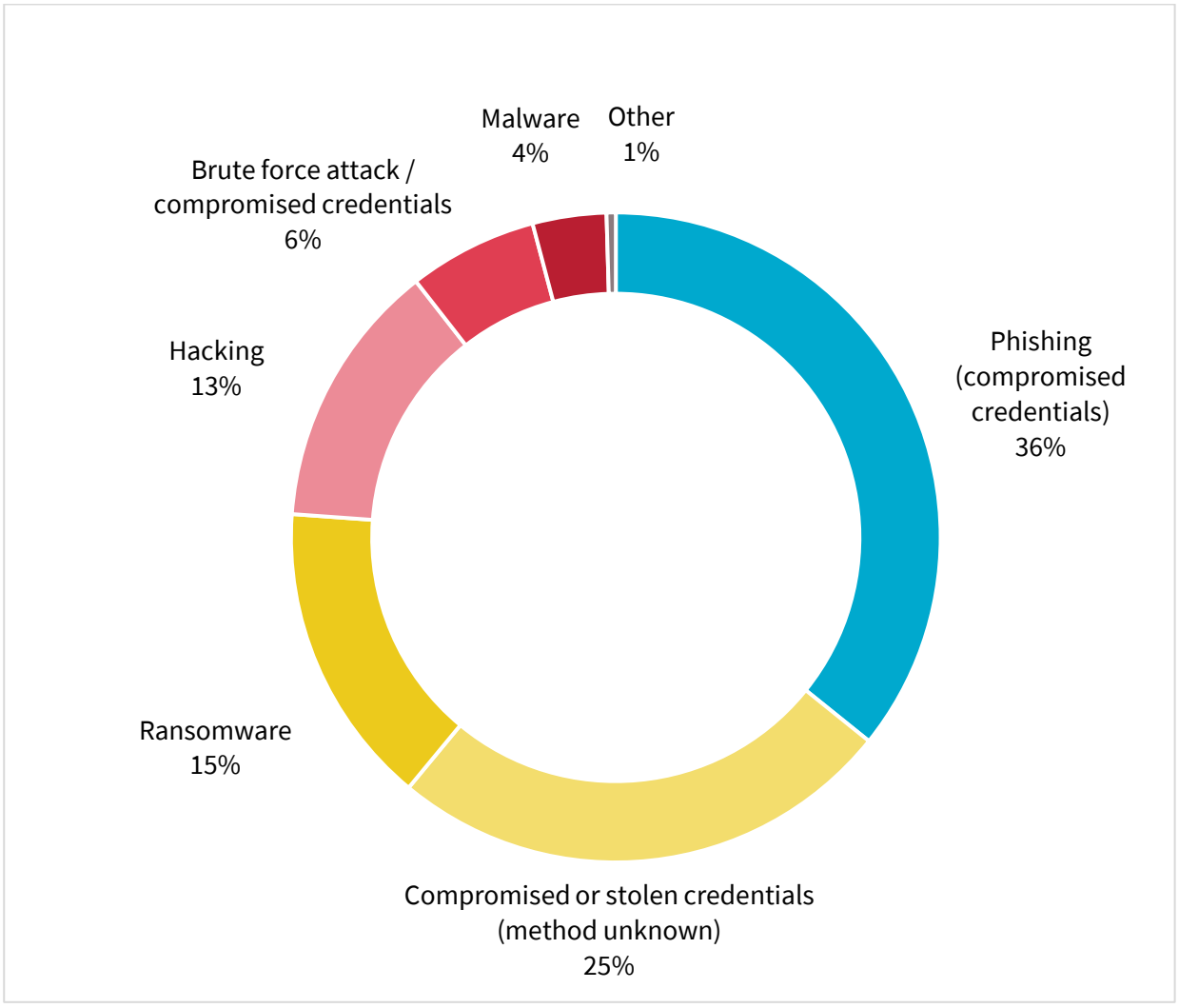


Cyber incident breaches — All sectors

The majority of cyber incidents during the reporting period were linked to malicious actors gaining access to accounts either through phishing attacks or by using compromised account details (compromised credentials, 133 notifications), ransomware attack (33 notifications) and hacking (29 notifications).

As with previous reporting periods, in a significant number of cyber incidents (55 notifications) the entity experiencing the breach was unable to identify how the malicious actor obtained the compromised credentials. The most common method of obtaining compromised credentials by malicious actors was through phishing (78 notifications).

Chart 8 — Cyber incident breakdown — All sectors



Human error breaches — All sectors

The second largest source of data breaches was human error (34% of all data breaches). Examples include sending personal information to the wrong recipient via email (39% of data breaches resulting from human error), unintended release or publication of personal information (16%) and sending personal information to the wrong recipient via post (12%).

Certain kinds of breaches can affect larger numbers of people. Failure to use the 'blind carbon copy' (BCC) function when sending group emails affected the largest numbers of people in this data breach category, with an average of 486 affected individuals per breach. Insecure disposal of personal information impacted an average of 250 people per breach.

Chart 9 — Human error breakdown — All sectors

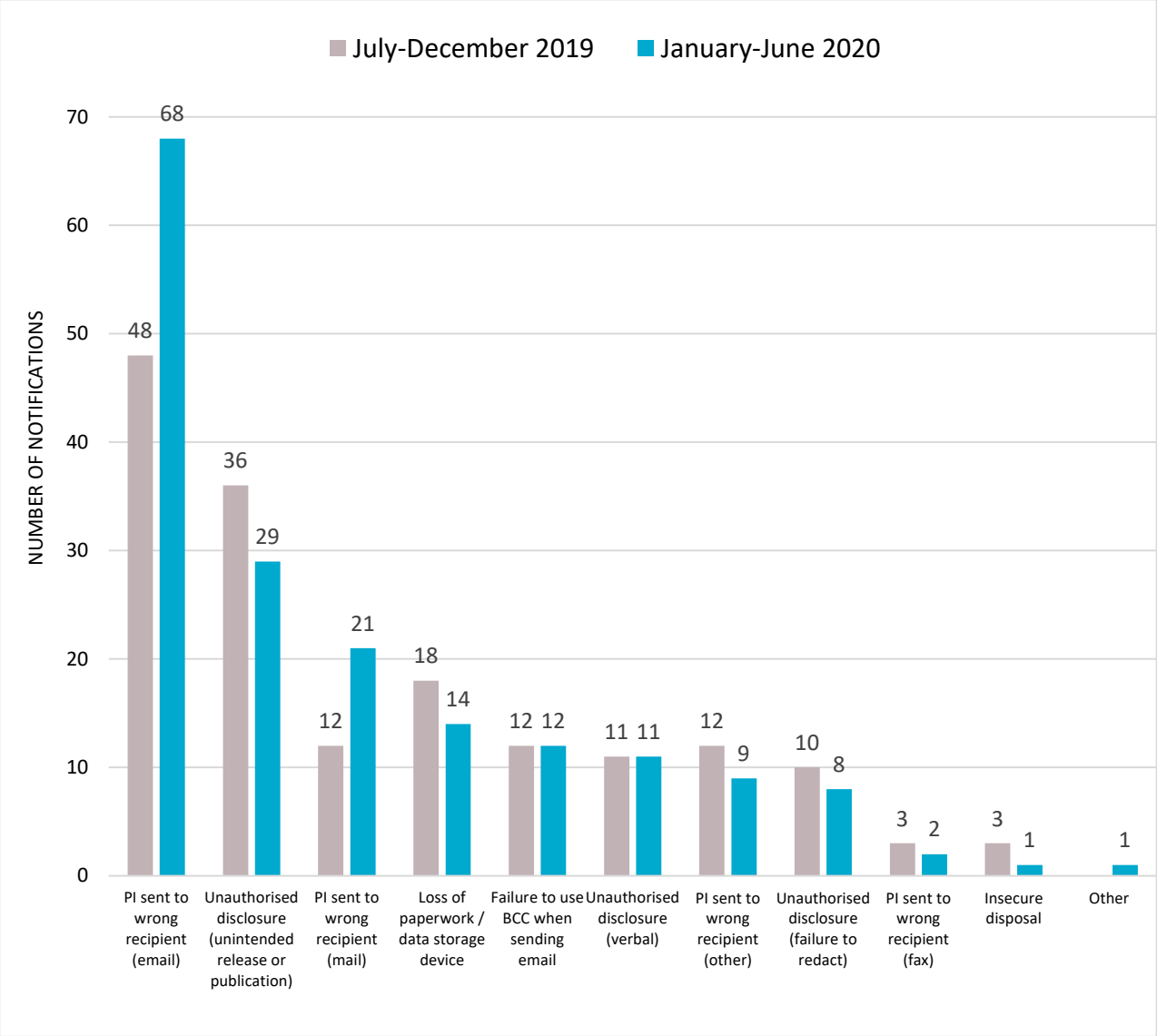


Table 3 — Human error breakdown by average number of affected individuals — All sectors

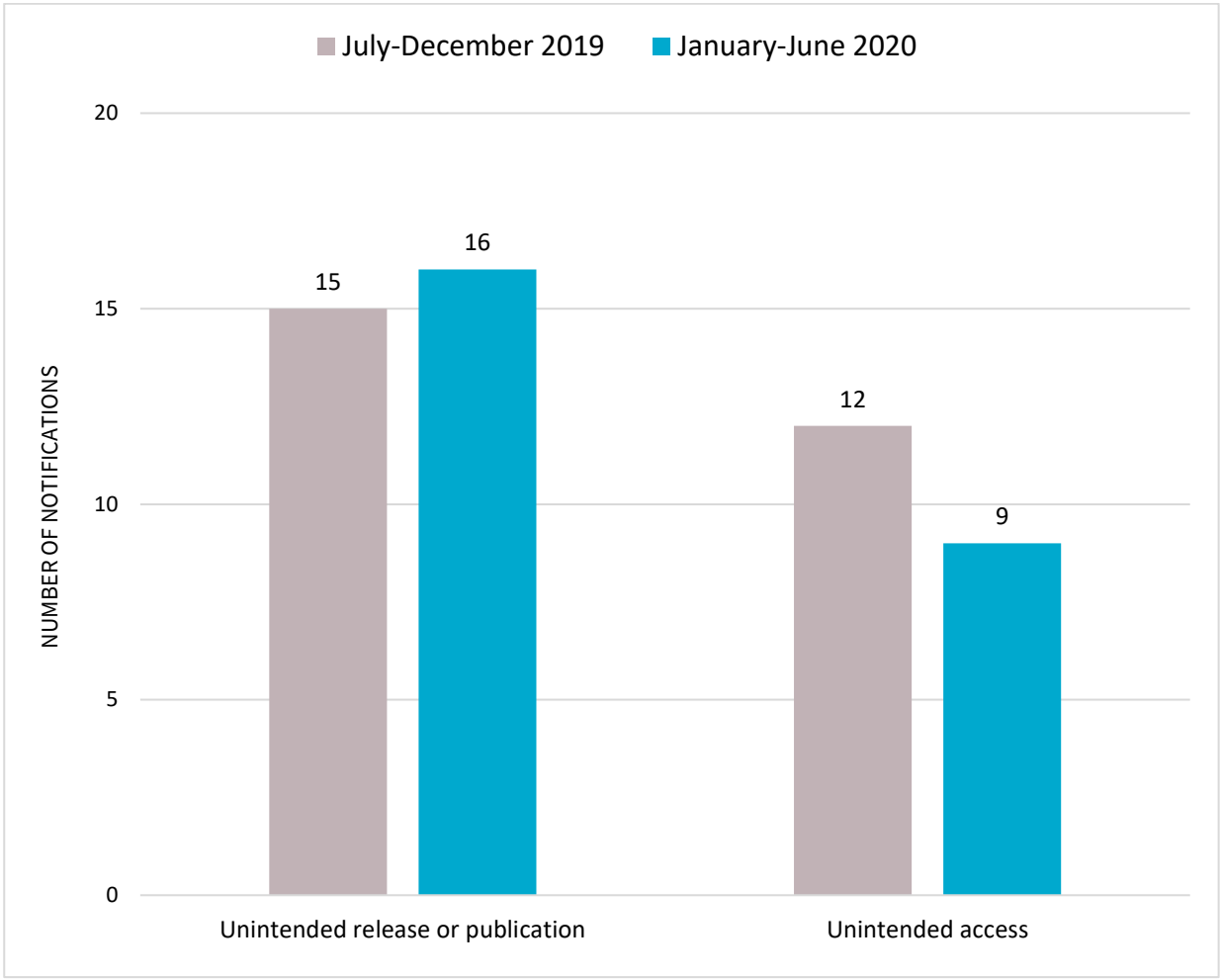
Kinds of personal information	No. of NDBs received Jan–Jun 2020	Average no. of affected individuals
PI sent to wrong recipient (email)	68	68
Unauthorised disclosure (unintended release or publication)	29	17
PI sent to wrong recipient (post)	21	53
Loss of paperwork/data storage device	14	131
Failure to use BCC when sending email	12	486
Unauthorised disclosure (verbal)	11	2
PI sent to wrong recipient (other)	9	1
Unauthorised disclosure (failure to redact)	8	1
PI sent to wrong recipient (fax)	2	1
Insecure disposal	1	250

System fault breaches — All sectors

System faults accounted for 5% of data breaches this reporting period. Unintended release or publication of personal information as a result of a system fault caused 16 data breaches, while unintended access to personal information as a result of a system fault caused nine data breaches.

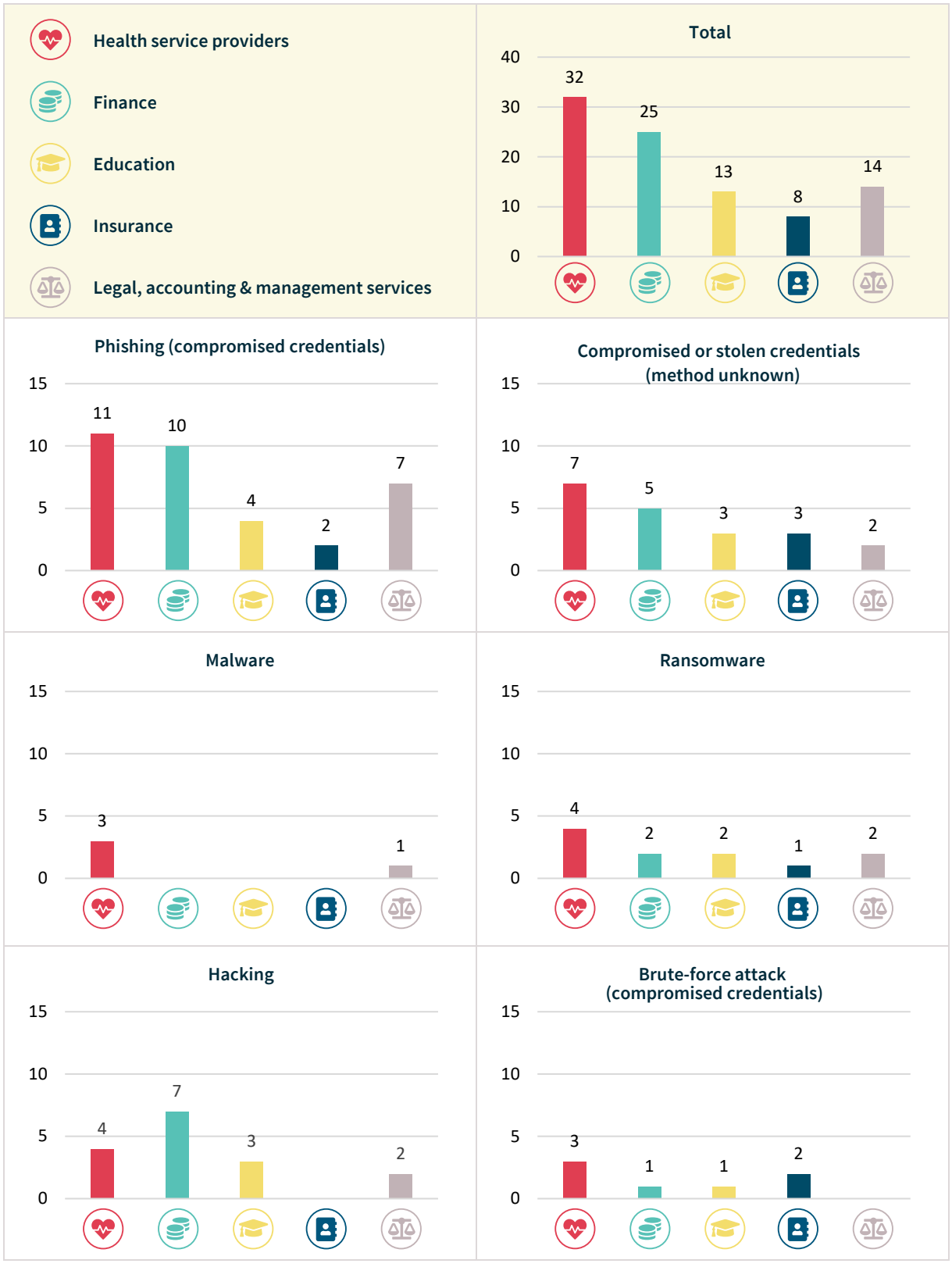
System fault breaches include data breaches that occur as a result of a business or technology process error.

Chart 10 — System fault breakdown — All sectors



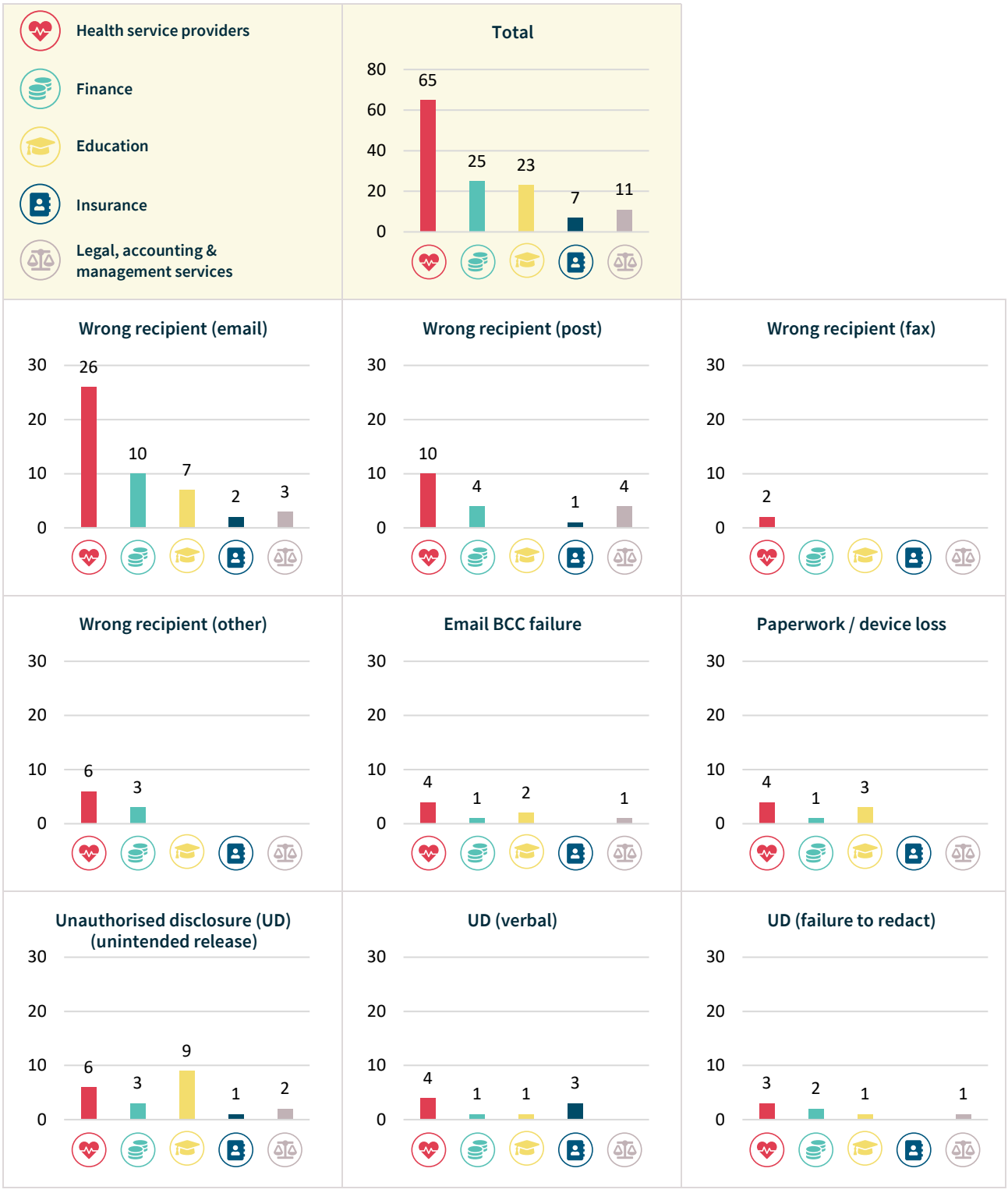
Cyber incident breaches — Top five industry sectors

Chart 13 — Cyber incident breakdown — Top five industry sectors



Human error breaches — Top five industry sectors

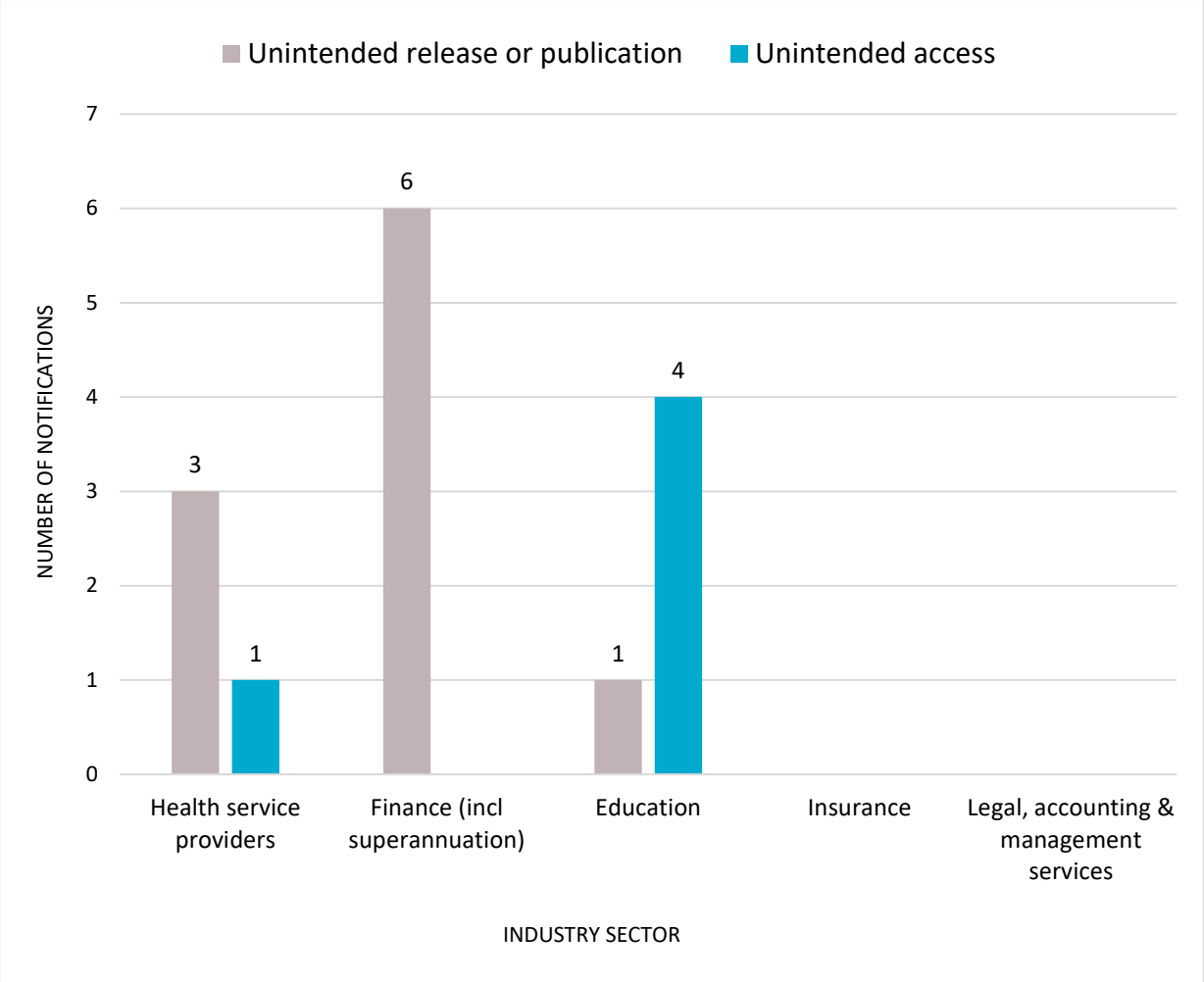
Chart 14 — Human error breakdown — Top five industry sectors



System fault breaches

This chart breaks down the 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.
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

Term	Definition
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 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.

[4] OAIC's Notifiable Data Breach Form