Australian Government

Office of the Australian Information Commissioner

Notifiable data breaches report

January to June 2024

16 September 2024

OAIC

Contents

Privacy Commissioner's foreword

Since the launch of the Notifiable Data Breaches (NDB) scheme in 2018, the Office of the Australian Information Commissioner (OAIC) has published statistical information about data breach notifications we have received. Our goal in doing so has been to help entities and the public understand privacy risks identified through the scheme, highlight areas that require attention and provide clarity around our regulatory approach.

Six years on, the NDB scheme is now mature, and we are moving into a new era in which our expectations of entities are higher, seen in our recent commencement of civil penalty proceedings against Medibank Private Limited and Australian Clinical Labs Limited. This enforcement action should send a strong message that keeping personal information secure and meeting the requirements of the NDB scheme must be priorities.

The OAIC is accelerating our shift to a more risk-based and enforcement and education-focused posture. Entities and the community can expect to see this reflected in a greater focus on directing our regulatory effort where it has the greatest impact, including areas where there is a high risk of harm to the community.

You will observe this report is a little different to previous ones. Our office is evolving our approach in sharing our insights and emerging trends with Australians and the regulated community. There is still statistical information; however, we have focused on providing more succinct guidance and trend observations to help entities comply with obligations.

From January to June this year, we received 527 data breach notifications. This is the highest number of notifications received since July to December 2020 and an increase of 9% compared to the previous 6 months.

Cyber security incidents continue to be a prevalent cause of data breaches, representing 38% of the total, as our increasing reliance on digital tools and online services exposes our details more frequently to malicious cyber actors. This serves as a reminder of how important it is that entities enact measures that guard against common threats, such as malicious actors using compromised credentials, ransomware and phishing, and update these measures as threats arise and change.

While 63% of data breaches affected 100 or fewer people, one incident reported affected over 10 million Australians. This is the second breach recorded to affect more than 10 million Australians and is the highest number of individuals affected by a breach since the NDB scheme came into effect.

Like the last reporting period, the Australian Government is in the top 5 sectors to notify data breaches. This highlights there is still work to do, both in the private and public sectors.

After 6 years of the NDB scheme, we expect entities to comply with their obligations. It is no longer acceptable for privacy to be an afterthought; entities need to be taking a privacy-centric approach in everything they do.

Carly Kind

Australian Privacy Commissioner

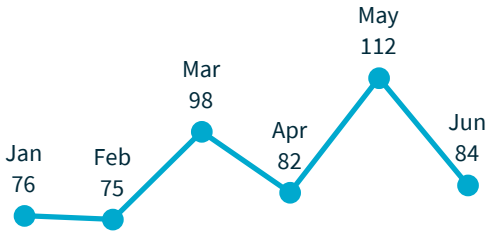
Statistics notes

- This report captures notifications received under the NDB scheme from 1 January to 30 June 2024.
- Statistics in this report are current as of 31 July 2024. Some data breach notifications are being assessed and adjustments may be made to related statistics. This may affect statistics for the period January to June 2024 published in future reports. Similarly, statistics from before January 2024 in this report may differ from those published in other reports.
- Statistical comparisons are to the period 1 July to 31 December 2023 unless otherwise indicated.
- Percentages in charts may not total 100% due to rounding.
- Where data breaches affect multiple entities, the OAIC may receive multiple notifications relating to the same incident. Notifications relating to the same incident are counted as a single notification (referred to as a 'primary notification') in this report to avoid information being duplicated, unless otherwise specified. The volume of secondary notifications may be indicative of the level of multi-party breach reporting. Secondary notifications may relate to a primary notification received in a prior reporting period.
- 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. Source of breach categories are defined in the glossary at the end of this report.
- Notifications made under the *My Health Records Act 2012* (Cth) are not included as they are subject to specific notification requirements set out in that legislation.

Snapshot

527
notifications

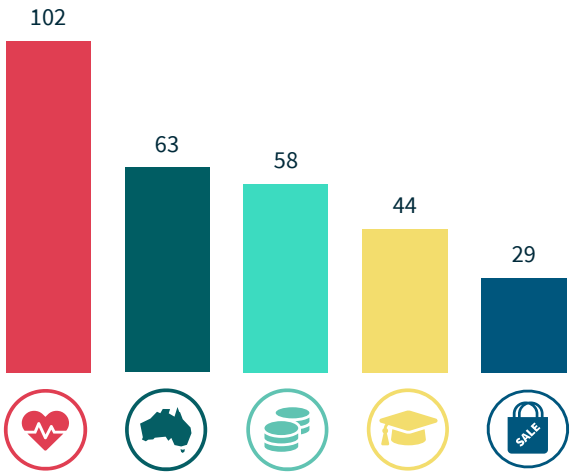
Up 9% compared to July – December 2023



Some data breaches affect more than one entity. The OAIC received an additional 17 secondary data breach notifications

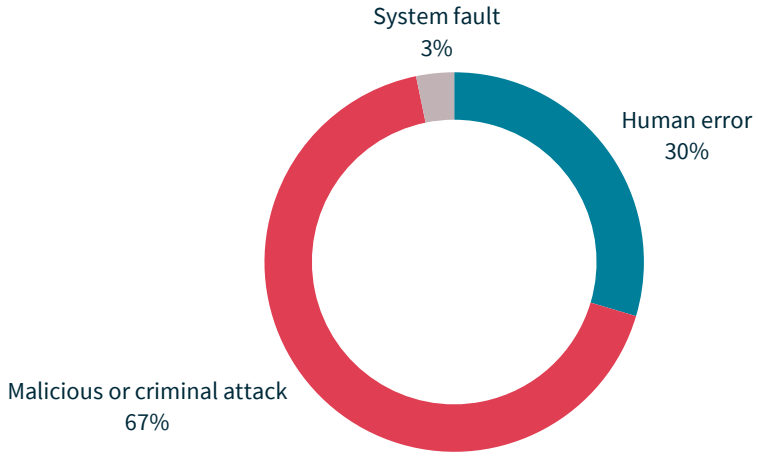
Top 5 sectors to notify data breaches

- Health service providers
- Australian Government
- Finance (incl. superannuation)
- Education
- Retail



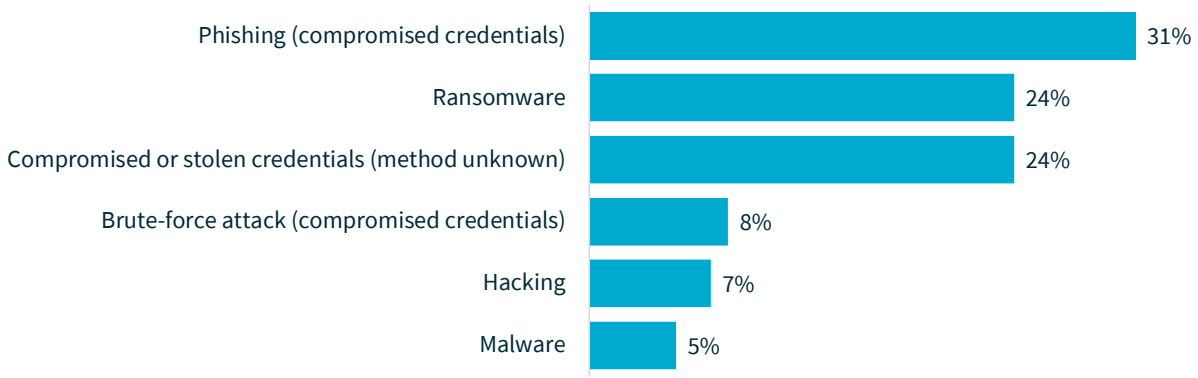
63%
of data breaches affected 100 people or fewer

Sources of data breaches



38% of all data breaches resulted from cyber security incidents (201 notifications; 57% of malicious or criminal attacks)

Cyber incident breakdown



Top causes of human error breaches

PI sent to wrong recipient (email) 38%

Unauthorised disclosure (unintended release or publication) 24%

Failure to use BCC when sending email 10%

A strategic approach to responding to data breaches

The Australian regulatory framework recognises the increasingly sophisticated nature of cyber risk and does not penalise entities for having been subject to a data breach.

However, entities are required under the *Privacy Act 1988* (Cth) to take reasonable steps to secure personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

The OAIC will not necessarily take regulatory action in response to every data breach. Rather, the OAIC strives to take a risk-based and harm-focused approach to regulation. The OAIC will be more likely to take regulatory action in response to issues:

- that create a risk of substantial harm to individuals and the community, especially to vulnerable people and groups
- that concern systemic harms or contraventions
- where action is likely to change sectoral or market practices or have an educative or deterrent effect
- that are subject to significant public interest or concern
- where action will help clarify aspects of policy or law, especially newer provisions of the Acts the OAIC administers.

The OAIC reviews information provided about data breaches to identify any systemic privacy risks. For example, the scope and severity of a data breach might be a symptom of an entity's failure to take reasonable steps to protect personal information it holds, before a data breach eventuates.

Where the root cause of a data breach indicates potential non-compliance with other requirements of the Privacy Act, the OAIC may take further regulatory action. Some of the regulatory tools open to the Information Commissioner include opening investigations, accepting enforceable undertakings and issuing determinations. The OAIC's *Privacy regulatory action policy* includes the factors considered in prioritising regulatory action and selecting the most appropriate power in the circumstances. Regulatory or enforcement activity is only undertaken in response to a small portion of data breaches.

In this reporting period, the Information Commissioner filed civil penalty proceedings in the Federal Court against Medibank Private Limited in relation to its October 2022 data breach. The OAIC also issued an intention and a direction to notify of an eligible data breach in relation to incidents that occurred in previous reporting periods and opened an investigation into the HWL Ebsworth Lawyers data breach.

Reasonable steps

Several of the Australian Privacy Principles (APPs), such as APPs 1, 8 and 11, and NDB scheme provisions require an entity to take 'reasonable steps' to comply with an obligation. In particular:

- APP 11.1 requires entities to take reasonable steps to protect personal information from misuse, interference and loss, as well as unauthorised access, modification or disclosure.
- APP 11.2 states an organisation must take reasonable steps to destroy or de-identify information it no longer needs for any purpose for which the information may be used or disclosed under the APPs.

As outlined in the OAIC's *Australian Privacy Principles guidelines* and *Guide to securing personal information*, what constitutes reasonable steps depends on circumstances such as:

- the nature of the entity, its size and resources
- the volume and sensitivity of personal information concerned
- possible adverse consequences for an individual in case of a breach.

Medibank civil penalty action

Medibank and its subsidiary ahm experienced a cyber attack in October 2022 in which one or more threat actors accessed the personal information of millions of current and former customers, which was subsequently released on the dark web.

The data breach led the OAIC to commence an investigation focused on how Medibank managed and secured personal information and whether the steps it took were reasonable in the circumstances to protect personal information from unauthorised access

In the civil penalty proceedings, the Information Commissioner alleges Medibank seriously interfered with the privacy of 9.7 million Australians by failing to take reasonable steps to protect their personal information from misuse and unauthorised access or disclosure in breach of the Privacy Act.

The Information Commissioner considers Medibank did not take reasonable steps to protect personal information it held given its size, resources, the nature and volume of the sensitive and personal information it handled, and the risk of serious harm for an individual in the case of a breach.

The Information Commissioner alleges it was reasonable for Medibank to adopt a number of measures to protect the information it held, and that there were deficiencies in the form and implementation of Medibank's cyber security and information security framework.

The case is before the Federal Court and is subject to the court's case management processes.

Spotlight on key themes and issues

Mitigating cyber threats
It is expected that entities will have appropriate and proactive measures in place to mitigate cyber threats and protect the personal information they hold.

Extended supply chain risks
Entities that outsource the handling of personal information can reduce the impact of a data breach in the supply chain by implementing a robust supplier risk management framework.

Addressing the human factor
Individuals remain a significant threat to the strength of an entity's privacy practices. Entities need to mitigate the potential for individuals to intentionally or inadvertently contribute to the occurrence of data breaches.

Misconfiguration of cloud-based data holdings
Entities need to be aware there is a shared responsibility for the security of data in the cloud.

Relevance of a threat actor's motivation in assessing a data breach
Entities should not rely on assumptions and should weigh in favour of notifying the OAIC and affected individuals when a breach occurs.

Data breaches in the Australian Government
Government agencies, especially those with service delivery functions, need to build community trust in their ability to protect the security of individuals' personal information.

Mitigating cyber threats

Cyber security incidents were the cause of 38% of all data breaches from January to June 2024.

Entities must take appropriate and proactive steps to protect against a range of cyber threats.

The OAIC encourages organisations to:

- implement multi-factor authentication for access to business systems, online services and data repositories, and for users when they perform a privileged action (using phishing-resistant multi-factor authentication will provide entities additional security that is not as susceptible to sophisticated cyber attacks)
- where multi-factor authentication is not available, enforce password management policies such as password complexity requirements or the use of strong passphrases, and ensure passwords are not being reused across systems
- layer security controls to avoid a single point of failure
- ensure users have appropriate levels of access to information assets depending on their role and responsibilities; monitor and regularly review accounts with more access permissions, removing access privileges where no longer required
- implement robust security monitoring processes and procedures to detect, respond to and report incidents, or unusual or suspicious activity, in a timely manner.

The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) recommends entities implement the Essential Eight, a set of baseline controls and security measures developed to help entities protect their internet-connected enterprise information technology systems and data holdings from cyber threats. ASD recommends Australian entities identify and plan for a target maturity level suitable for their operating environment.

In considering the appropriate security measures and steps to be taken to protect personal information from a cyber security incident, entities may also consider additional standards and frameworks such as:

- the ASD's *Information Security Manual*, a cyber security framework entities can apply to protect their systems and data from cyber threats
- the National Institute of Standards and Technology's Cyber Security Framework, which provides entities a guide on best practices to manage cybersecurity risks and improve their cybersecurity posture
- the International Organisation for Standardisation's ISO 27001 and ISO 27002, which establishes the requirements and procedures for creating an information security management system.

Frameworks provide a starting point for entities to establish appropriate processes, policies and administrative activities for practical information security management. Entities will need to consider a range of factors when choosing which framework and/or standards they will adopt, including specific industry and compliance requirements.

The ASD's ACSC incident management capabilities provide technical incident response advice and assistance to Australian entities that have been impacted, or may be impacted by a cyber security

incident. Entities should report any cybercrime, cyber security incident or vulnerability to the ASD's ACSC.

Ultimately, effective cyber security practices also require entities to practice 'privacy by design' across the information lifecycle, including the collection, retention, use, disclosure and destruction of personal information.

Extended supply chain risks

The risk of outsourcing personal information handling to third parties continues to be a prevalent issue. In this reporting period, there were large-scale data breaches that resulted from a compromise within a supply chain, such as the MediSecure and Outabox incidents.

Where a single data breach affects multiple entities, the OAIC may receive multiple notifications relating to the same incident, although only one entity is required to notify a data breach that affects multiple entities.

In this reporting period, the OAIC received 34 notifications relating to data breach incidents involving more than one entity. The OAIC proactively made inquiries with 35 entities impacted by multi-party data breach incidents to ensure compliance with NDB scheme obligations.

Multi-party data breaches observed in this reporting period highlight:

- the risks that exist beyond an entity's immediate third-party suppliers – in their extended supply chains
- delays in notifications to affected individuals.

Scenario 1

An entity engaged a third-party supplier to assist it with a database design and migration. Two years following the database migration, the entity became aware that data about its clients, including credit card information and government-issued identification numbers, was being sold on the dark web.

The root cause of the incident was unauthorised access to a legacy database via a developer subcontracted by the third-party supplier to assist with the database design. The entity was advised the developer had recently damaged their personal laptop while overseas and provided it to an overseas repairer for service. The audit logs indicated the legacy database was accessed using the developer's credentials when the laptop was being repaired.

The entity advised it had reviewed the third-party supplier's policies prior to engagement and confirmed the supplier's employees did not use their own devices. However, the entity was not aware the supplier had subcontracted the design work to the developer.

Scenario 2

An entity became aware its cloud service provider's systems were accessed without authorisation over a 4-day period. The cloud service provider engaged a forensic expert to investigate the incident and, due to the unstructured nature of the data, could not confirm what data had been accessed or exfiltrated (if any).

In this instance, the entity had a sound understanding of the personal information held in the cloud storage environment and assessed the sensitive personal information of about 80 individuals was potentially involved. The entity notified the affected individuals and the OAIC of the incident within 2 days of becoming aware of it.

After a 6-month forensic investigation, the cloud service provider provided the entity with a copy of the data impacted. The entity reviewed the data and notified a further 2 individuals assessed to be at risk of serious harm.

Managing third-party providers and supply chain risks

Entities can substantially minimise the impact of a data breach in the supply chain by implementing a strong supplier risk management framework together with more robust security measures. It is important that entities consider the risks of outsourcing personal information handling at the earliest stage of procurement.

As outlined in previous reports and the OAIC's *Guide to securing personal information*, steps that may be reasonable to take in relation to third-party providers, such as cloud storage, include:

- engaging suppliers that have demonstrated robust security controls and appropriate personal information handling measures
- uplifting the third-party vendor procurement process to consider:
  - what assurances vendors are required to provide prior to engagement
  - whether additional protections are required for high-risk data managed by third parties
- defining the scope of the personal information handling services to be provided
- having contractual clauses on retention or destruction of data
- ensuring contractual arrangements specify accountabilities in the event of data breaches that involve multiple parties, such as the responsible party for assessing harm, providing information and notifying the data breach (generally, the OAIC is of the view that the entity with the most direct relationship with individuals affected by the data breach should notify them)
- ensuring effective oversight of third-party providers, including regularly carrying out cyber security assessments and audits of existing vendors to evaluate the effectiveness of controls and practices, and confirm compliance with relevant security standards, contractual requirements and legal obligations.

The OAIC also recommends entities consider:

- including a contractual obligation for third-party providers to provide notice prior to engaging a subcontractor to handle any jointly held personal information
- having mechanisms in place that require a service provider or their subcontractor to notify an entity promptly of any data breach-related incidents.

Addressing the human factor

In this reporting period, human error breaches accounted for 30% of all data breaches. Additionally, 12% of all breaches were caused by phishing, where an employee inadvertently clicked on malicious links or downloaded a compromised attachment. Five per cent of all breaches were a result of a rogue employee or insider threat.

This is a timely reminder of how the human factor may pose a threat to the strength of an entity's personal information security, regardless of how secure an entity's systems are. Individuals may contribute to the risk of data breaches, intentionally or inadvertently.

Scenario 1

A health service provider became aware of a data breach in which a former employee accessed and disclosed personal information without authorisation.

The entity's investigation indicated that over 2 years, the employee accessed the personal information of over 20,000 individuals in its customer relationship management system. The employee disclosed the personal information to an external party for financial gain, via a work email and personal social media accounts, using their work-issued laptop.

As a result of the incident, the entity implemented additional monitoring capabilities to flag high volume record searches and access by staff, large copying and pasting of data, and uploading of files to social media websites and external web services.

Scenario 2

An entity's employee email account was compromised as a result of QR code phishing, also known as 'quishing'. The employee was deceived into scanning a QR code that appeared genuine, which generated a token that allowed the threat actor to by-pass multi-factor authentication.

To prevent reoccurrence of similar incidents, the entity increased cyber security awareness training from once to twice a year and sent out staff communication about QR code phishing. The entity also engaged an IT provider to review whether its email platform could block QR code phishing attempts in the future.

Mitigating the human factor

Mitigating the risk of the human factor as a root cause of data breaches involves not only reducing opportunity for errors with technical measures, but also educating staff. All staff should be aware of their privacy and security obligations.

Reasonable steps entities can take include:

- prioritising training staff on secure information handling practices
- holding regular training to keep staff up to date on the latest techniques used by threat actors and methods to detect phishing attempts
- minimising access to personal information to staff who require access to enable the entity to carry out its functions and activities
- proactive monitoring to identify possible unauthorised access by internal and external parties.

As outlined in the OAIC's *Guide to securing personal information*, entities also need to guard against internal threats, and assume human error will occur and design for it. The OAIC encourages entities to embed good privacy practices into all aspects of their functions and activities. This includes designing systems and processes that anticipate and minimise the risk of the human factor contributing to a data breach.

Misconfiguration of cloud-based data holdings

Cloud computing offers a range of potential benefits to an entity, including improvements to the entity's cyber security posture and mitigation of cyber threats, particularly where the entity does not have the resources or capability to develop its own cloud storage. However, accountability for protecting personal information in cloud computing does not solely rest on cloud service providers and is also contingent on the entity's responsibilities in managing and securing the cloud.

Entities need to be aware there is a shared responsibility for the security of its data in the cloud. While cloud service providers can take steps to ensure their servers and software are secure, data breaches can still occur when entities do not properly manage and maintain an appropriate security level in their cloud storage environments.

Data breaches in the reporting period indicate cloud security may be overlooked as entities digitally transform. The OAIC observed various data breaches where an entity misconfigured security settings due to human error, leaving the personal information it held vulnerable to unauthorised access or inadvertent public disclosure.

Scenario 1

An entity had engaged the services of a cloud service provider. The entity created a bucket for use by a third-party partner for the purpose of developing web and mobile phone applications. The default private setting was changed to public to facilitate this project's delivery.

When the web application went live, the entity's customers used it to upload documents containing their personal information. The documents, including scans of government-issued identification documents, were stored in the bucket.

However, before the application went live, the entity neglected to update the bucket's privacy configuration to private. The entity was unaware the bucket was publicly accessible until it was contacted by a cyber security researcher advising it of the exposed data.

Scenario 2

A health service provider used a cloud storage depository, set to private, to share information among its multiple clinic locations. The entity often uploaded referral documents containing health information to the depository.

The entity was notified by a cyber security researcher that the contents of the depository were publicly accessible. The entity investigated the incident and found an employee had inadvertently changed the security settings of the folder containing the referral documents to public while uploading a referral to the depository.

As a result of the incident, the entity minimised the access permissions to the depository and implemented policies and processes to upload referrals going forward.

Securing the cloud

Cloud security and management should be a priority for any entity using cloud-based storage. Do not assume that cloud security responsibility lays with the provider.

Reasonable steps to secure personal information stored on cloud environments and mitigate risks of misconfiguration may include:

- implementing strong access controls such as multi-factor authentication, IP access controls and encryption
- having policies, processes and procedures in place to govern and attribute responsibilities for the creation, proper configuration and management of cloud data storage
- scheduling regular security assessments to audit and review cloud configurations
- extending risk analysis and security monitoring to cover cloud storage environments.

Additional resources

The ASD's ACSC has guidance on cloud security, including a Blueprint for Secure Cloud, an online tool to support the design, configuration and deployment of collaborative and secure cloud and hybrid workspaces.

Major cloud service providers also provide guidance on shared responsibility between the providers and entities in cloud security:

- Microsoft: Shared responsibility in the cloud
- Amazon Web Services: Shared Responsibility Model
- Google: Shared responsibilities and shared fate on Google Cloud.

Relevance of a threat actor's motivation in assessing a data breach

During this reporting period, the OAIC observed an increase in instances where an entity relied on its perception of a threat actor's motivation in assessing a suspected eligible data breach. In some cases involving ransomware attacks, the entity assessed it was unlikely the data breach would cause serious harm to the affected individuals based on the threat actor's assurance they would destroy and not publish data upon ransom payment.

The OAIC reminds entities to take a cautious approach and consider the non-exhaustive list of 'relevant matters' that may assist entities to assess the likelihood of serious harm. Given the objective of the NDB scheme to empower individuals impacted by data breaches through notification, entities should avoid relying on assumptions where facts cannot be established and should weigh in favour of notifying the OAIC and affected individuals.

Scenario 1

An employee of an entity used its client database to access personal information, including contact details and addresses of the employee's spouse and relatives who all were carers of a client of the entity. The rogue employee had access to the client database to perform their duties but was not required to access that client's profile.

The entity reported the incident to the OAIC. However, it claimed it had assessed it unlikely the data breach would result in serious harm for the affected individuals, so it did not notify those individuals. This was on the basis that:

- the entity was not aware of any harm to the individuals during the period of unauthorised access, as it had received no complaints about the matter
- the rogue employee accessed, but did not interfere with the affected individuals' client profiles during the period of unauthorised access
- the rogue employee claimed their motivation for the unauthorised access was not malicious.

The OAIC was of the view the entity should notify the affected individuals of an eligible data breach. This was because a reasonable person would consider the rogue employee's pre-existing relationships with the affected individuals increased the likelihood of serious harm. Whether the entity received information about the rogue employee's motivation or any complaints from the affected individuals was irrelevant to the consideration of harm, especially where the affected individuals were not aware of the incident.

The OAIC notified the entity of the intention to issue a direction to notify an eligible data breach under s 26WR(3) of the Privacy Act and invited the entity to make a submission about the proposed direction. In response, the entity notified the affected individuals of the breach.

Scenario 2

An entity experienced a ransomware attack, resulting in a high volume of personal information it held being accessed and exfiltrated. The entity decided to pay the ransom requested by the threat actor to contain the breach. The threat actor assured the entity that due to the ransom payment; they would not publish and had destroyed the copies of the exfiltrated data they held.

While the entity had notified affected individuals of the data breach, it advised the OAIC it did not believe an eligible data breach had occurred. This was because it paid the ransom requested by the threat actor as a remedial action and received assurance the data would not be published and would be destroyed.

The OAIC provided guidance on reasonable assessments to the entity.

Reasonable assessments

In undertaking a reasonable assessment of a suspected eligible data breach, entities should exercise caution in relying upon a threat actor's assurances.

The OAIC considers paying a ransom to a cyber criminal would not be sufficient to prevent serious harm to affected individuals. This is consistent with ASD's ACSC advice to never pay a ransom and the Australian Government's advice that paying a ransom does not guarantee that data will be recovered, nor does it prevent data from being sold or leaked online.

It is unlikely a reasonable person would accept that a cybercriminal is trustworthy or likely to honour any such agreement with respect to personal information. Where a cybercriminal has targeted data held by an entity, dealt with the data in an unauthorised manner and demanded a ransom under threat of further unauthorised dealings, this casts considerable doubt on the credibility of any assurances.

Data breaches in the Australian Government

While individuals can generally choose the private sector organisations with which they share their personal information, they often do not have a choice in providing their personal information to government agencies to access their services. It is essential that government agencies, especially those with service delivery functions, model best practice and build community trust in their ability to protect the security of personal information they hold.

In this reporting period, the Australian Government continued to be in the top 5 sectors by notifications and, for the first time, reported the second most data breaches of all industry sectors, its highest position. Australian Government agencies reported 63 data breaches, 12% of all notifications.

Of all sectors, the Australian Government reported the most data breaches involving social engineering or impersonation (42% of all breaches of this kind). These breaches experienced by agencies typically involved a threat actor impersonating a customer and gaining access to their customer account by using legitimate identity credentials that bypassed the agency's identity verification procedures.

Of the top 5 sectors, the Australian Government continued to have the largest proportion (87%) of notifications where the agency identified the incident over 30 days after it occurred. The Australian Government also continued to have the largest proportion (78%) of notifications made to the OAIC more than 30 days after the agency become aware of the incident. Some of these delays occurred where an agency's business area became aware of an incident and failed to promptly escalate it to the area responsible for coordinating the agency's response to data breaches. This delay in escalation contributed to delays by the agency in commencing an assessment and notifying the OAIC of the data breach.

Agencies should check they have an effective and up-to-date data breach response plan for identifying, assessing, containing and notifying data breaches. They should also ensure all business areas are aware of and comply with the plan.

Authenticating users

Entities should have processes in place to identify users and have access control measures in place to ensure only authorised persons access their systems.

Multi-factor authentication should be implemented as part of these processes. As advised by ASD's ACSC, multi-factor authentication requires individuals to use a combination of at least 2 of the following factors to access their accounts:

- something you know (for example, a PIN, password or passphrase)
- something you have (for example, a smartcard, physical token, authenticator app, SMS or email)
- something you are (for example, a fingerprint, facial recognition or iris scan).

The OAIC's *Guide to securing personal information* also contains information on identity management and authentication.

Statistics

Notifications received – All sectors

Table 1: Notifications received in 2023–24

Reporting period	Number of notifications
July to December 2023	485
January to June 2024	**527**
Total	**1,012**

Chart 1 – Notifications received by month from July 2022 to June 2024

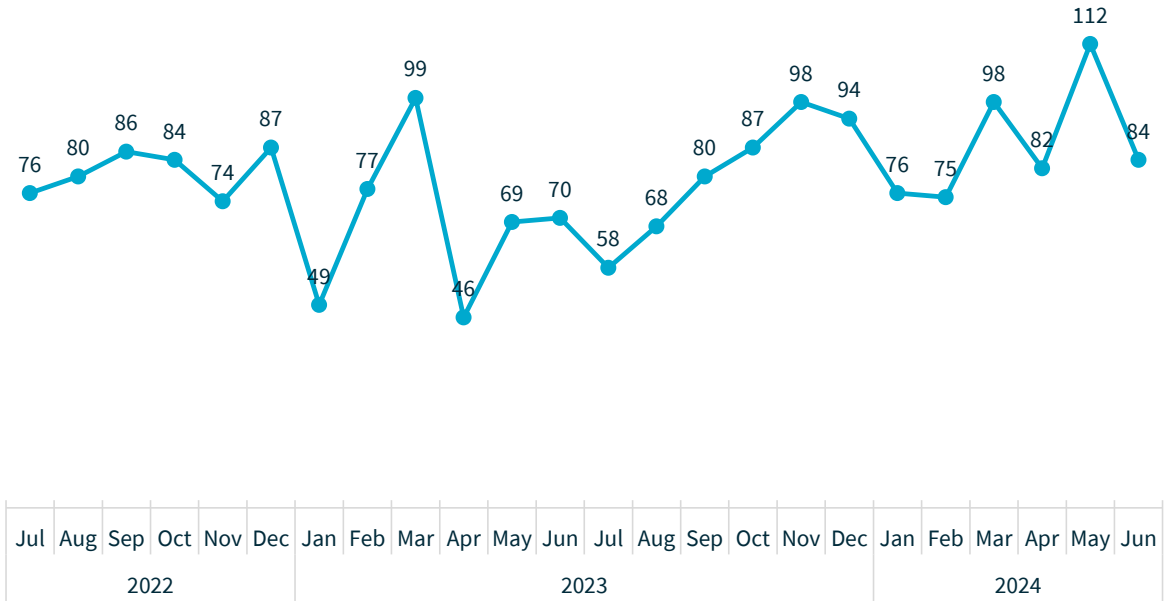
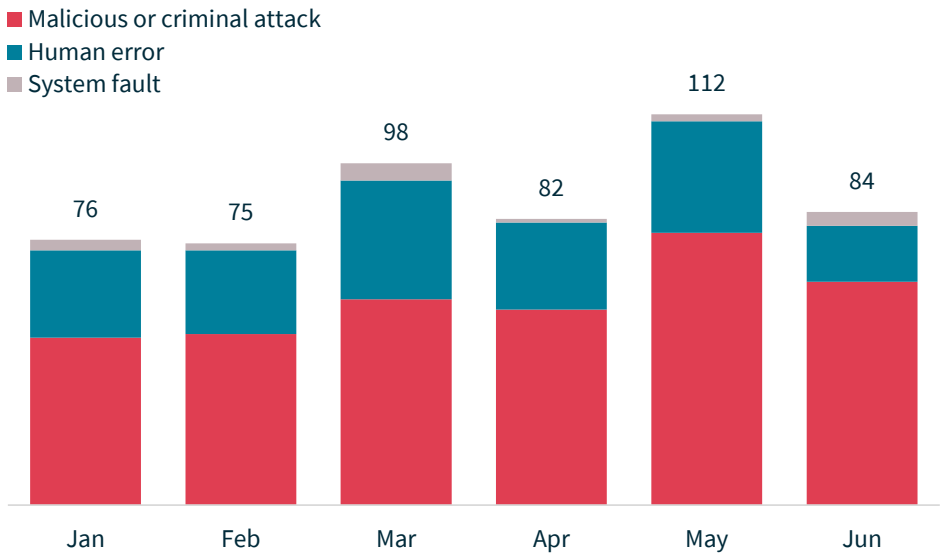
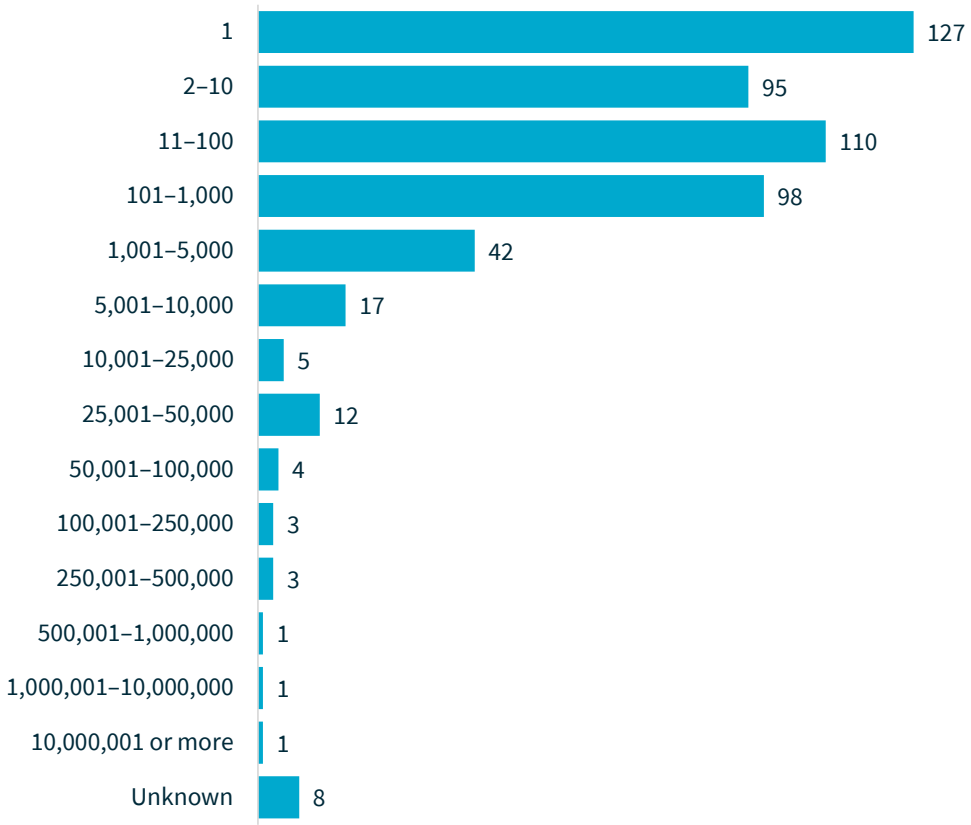


Chart 2 – Notifications received by month showing the sources of breaches



Number of individuals affected by breaches

Chart 3 – Number of individuals worldwide affected by breaches



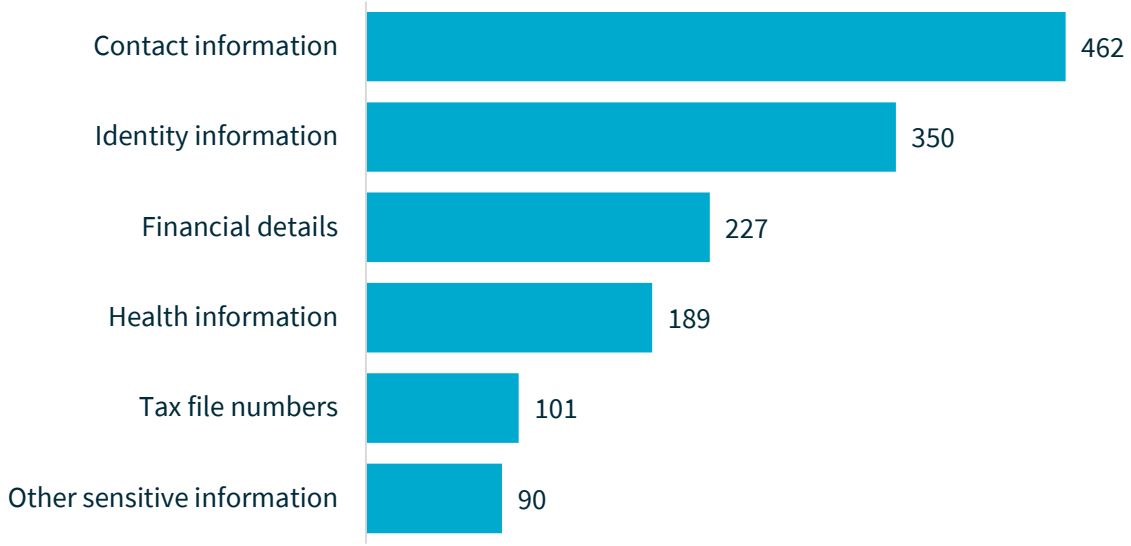
These figures reflect the number of individuals worldwide whose personal information was compromised in data breaches notified to the OAIC, as estimated by notifying entities.

Table 2: Large-scale data breaches affecting Australians

Number of Australians affected by large-scale breaches	Jul–Dec 2023	Jan–Jun 2024
100,001–250,000	5	3
250,001–500,000	1	3
500,001–1,000,000	1	1
1,000,001–10,000,000	2	0
10,000,001 or more	0	1
Total number of breaches affecting over 100,000 Australians	**9**	**8**

Kinds of personal information involved in breaches

Chart 4 – Kinds of personal information involved in breaches



Data breaches may involve more than one kind of personal information.

Time taken to identify breaches

The figures in this section relate to the time between an incident occurring and the entity becoming aware of it. They do not relate to the time taken by the entity to assess whether an incident qualified as an eligible data breach.

For notifications in the 'unknown' category, the entity was unable to identify the date the breach occurred.

Chart 5 – Time taken to identify breaches

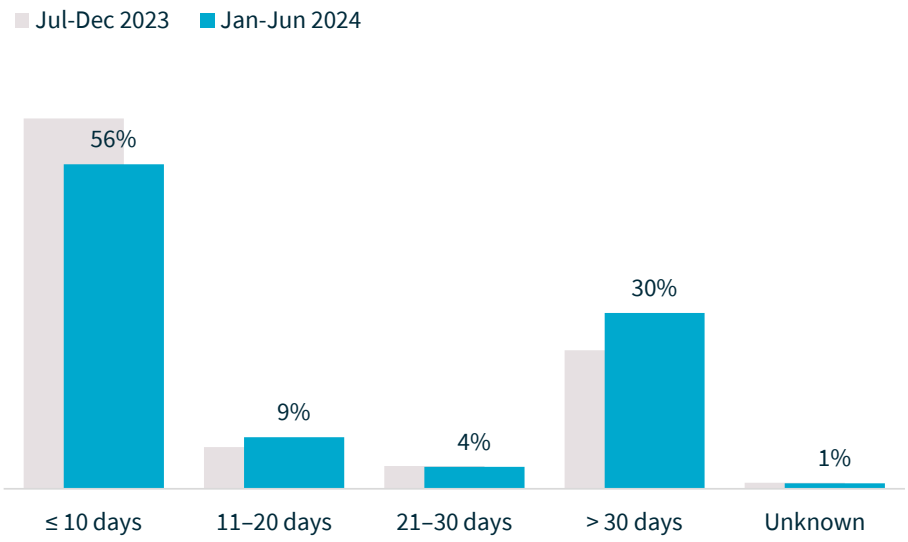
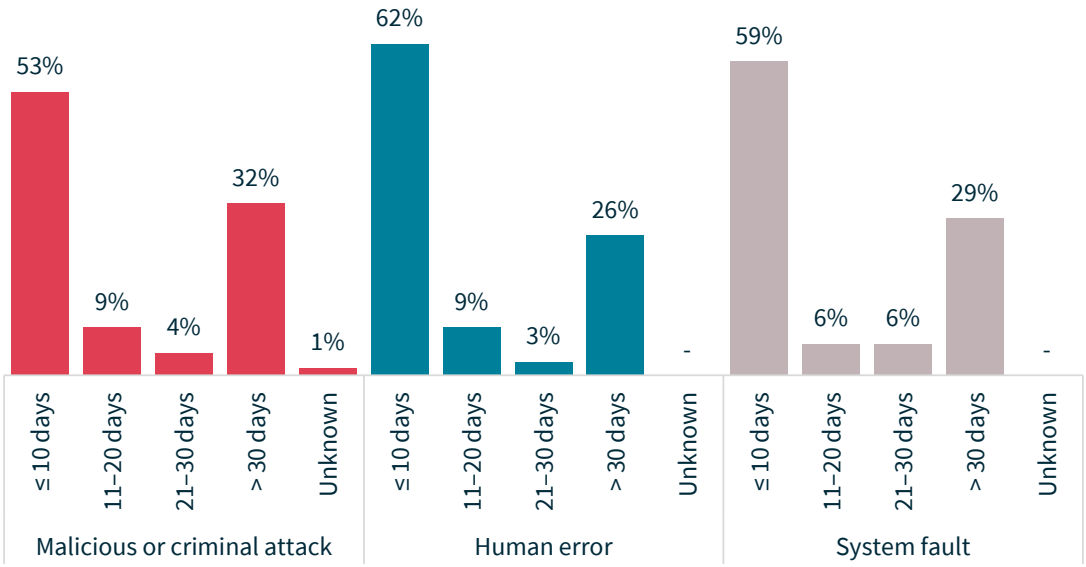


Chart 6 - Time taken to identify breaches by source of breach



Time taken to notify the OAIC of breaches

The figures in this section relate to the time between when an entity became aware of an incident and when they notified the OAIC. They do not relate to the time between when the entity determined the incident to be an eligible data breach and when they notified the OAIC.

Chart 7 – Time taken to notify the OAIC of breaches

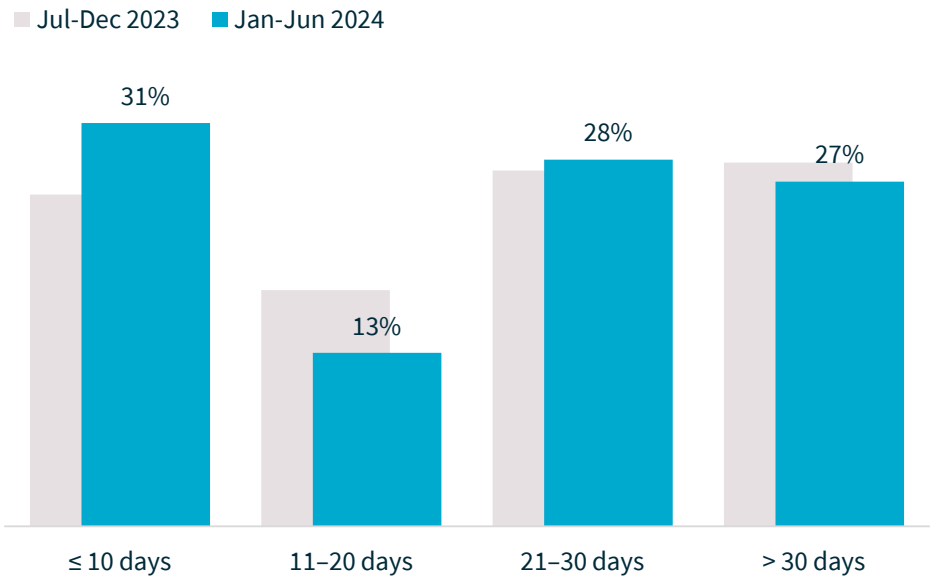
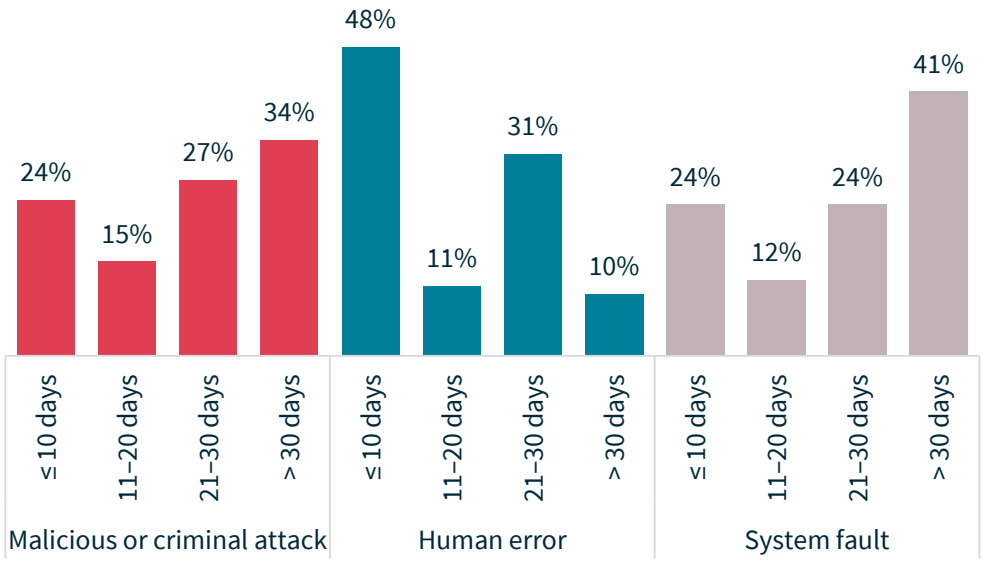
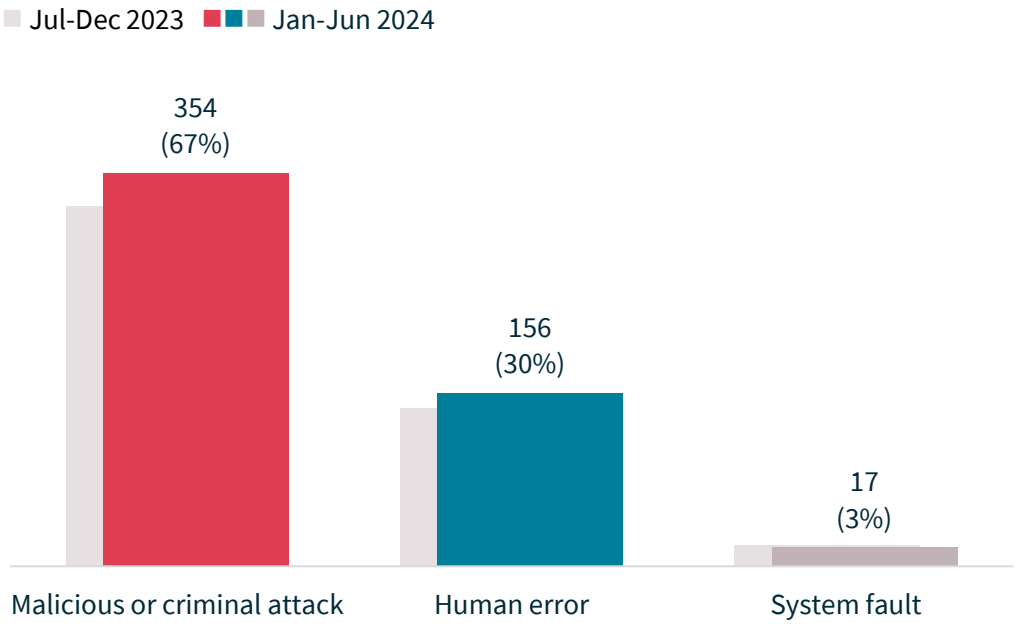


Chart 8 – Time taken to notify the OAIC of breaches by source of breach



Source of breaches

Chart 9 - Source of data breaches



Malicious or criminal attacks

Chart 10 – Causes of breaches resulting from malicious or criminal attacks

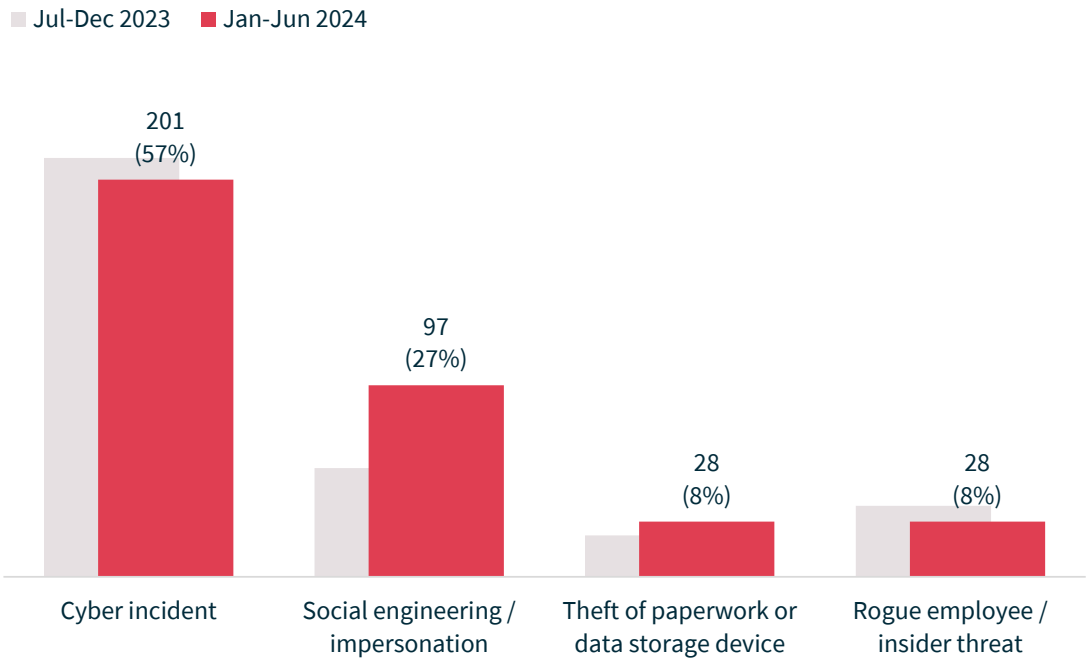


Table 3: Malicious or criminal attack breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Cyber incident	201	107,123	341
Rogue employee / insider threat	28	4,709	13
Theft of paperwork or data storage device	28	617	23
Social engineering / impersonation	97	129	19
Total	**354**	**60,584**	**68**

Cyber incidents

Chart 11 - Cyber incident breakdown

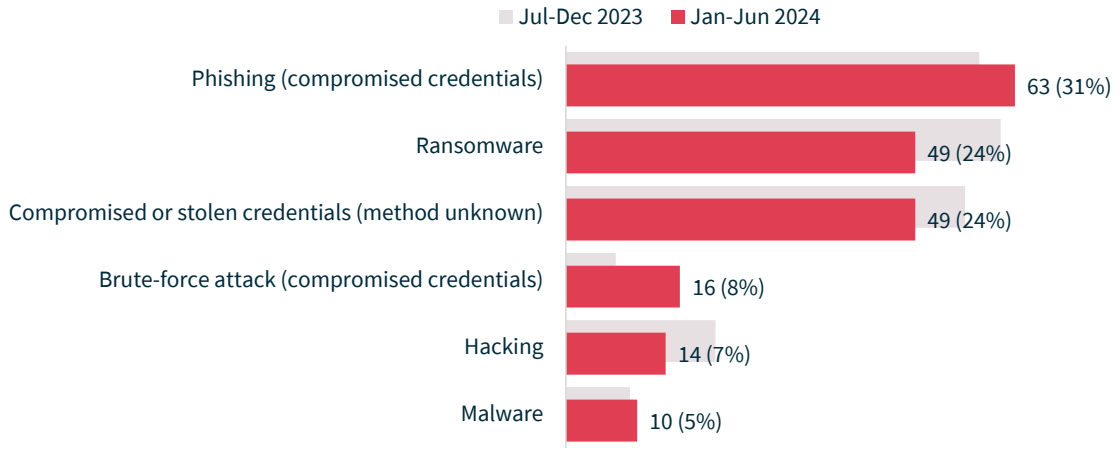


Table 4: Cyber incident breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Hacking	14	468,713	2,000
Ransomware	49	295,555	632
Brute-force attack (compromised credentials)	16	21,557	654
Compromised or stolen credentials (method unknown)	49	9,376	62
Malware	10	5,067	707
Phishing (compromised credentials)	63	709	147
Total	**201**	**107,123**	**341**

Human error

Chart 12 – Human error breakdown

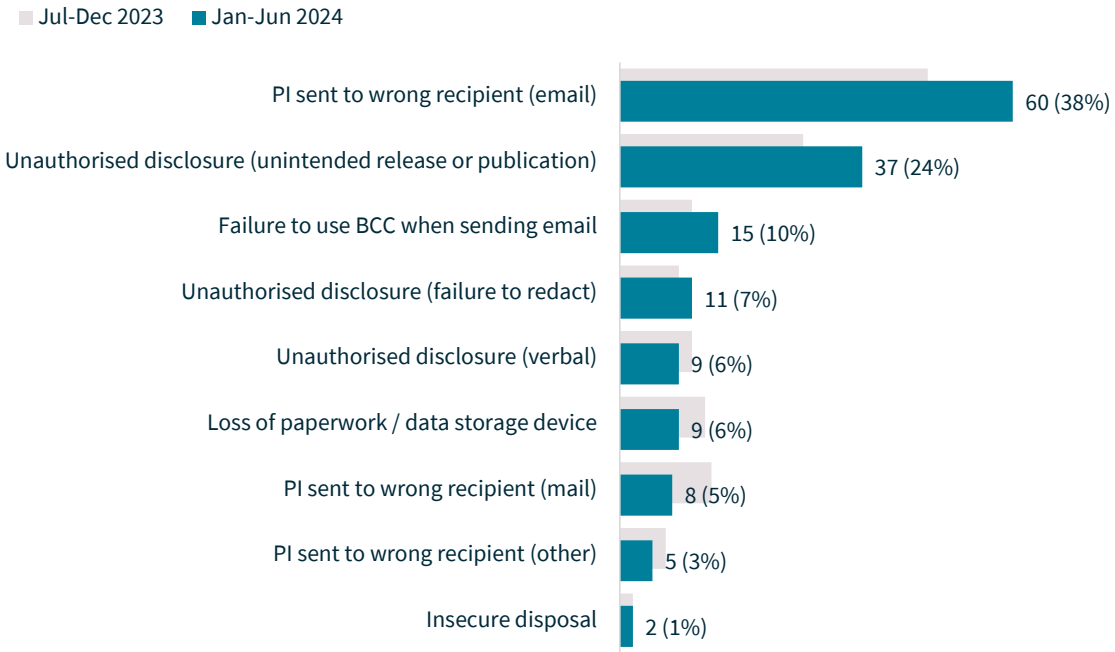
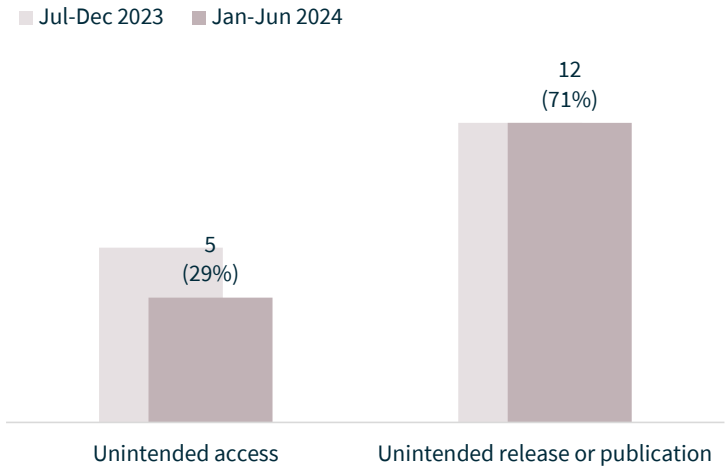


Table 5: Human error breakdown by average and median numbers of affected individuals worldwide

Source of breach	Number of notifications	Average number of affected individuals	Median number of affected individuals
Unauthorised disclosure (unintended release or publication)	37	4,158	4
PI sent to wrong recipient (email)	60	1,026	1
Failure to use BCC when sending email	15	174	50
PI sent to wrong recipient (other)	5	116	45
Insecure disposal	2	15	15
Loss of paperwork / data storage device	9	12	6
PI sent to wrong recipient (mail)	8	5	1
Unauthorised disclosure (failure to redact)	11	1	1
Unauthorised disclosure (verbal)	9	1	1
Total	**156**	**1,405**	**2**

System faults

Chart 13 – System fault notifications



Comparison of top 5 sectors

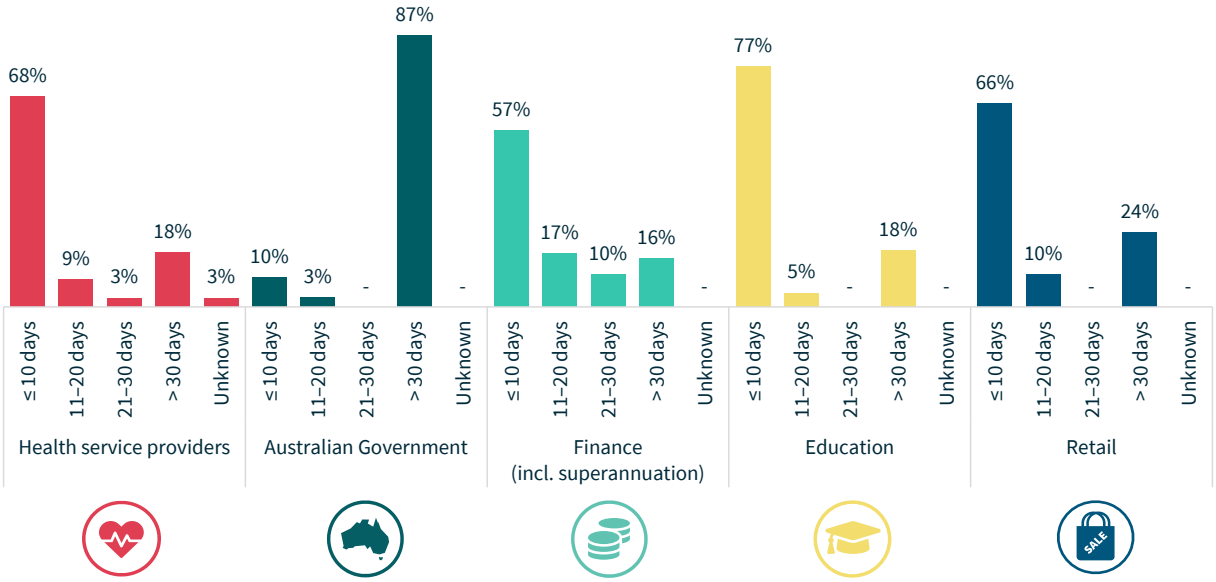
Table 7: Top 5 sectors by notifications

Sector	Number of notifications	Percentage of all notifications received
Health service providers	102	19%
Australian Government	63	12%
Finance (incl. superannuation)	58	11%
Education	44	8%
Retail	29	6%
Total	**296**	**56%**

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.

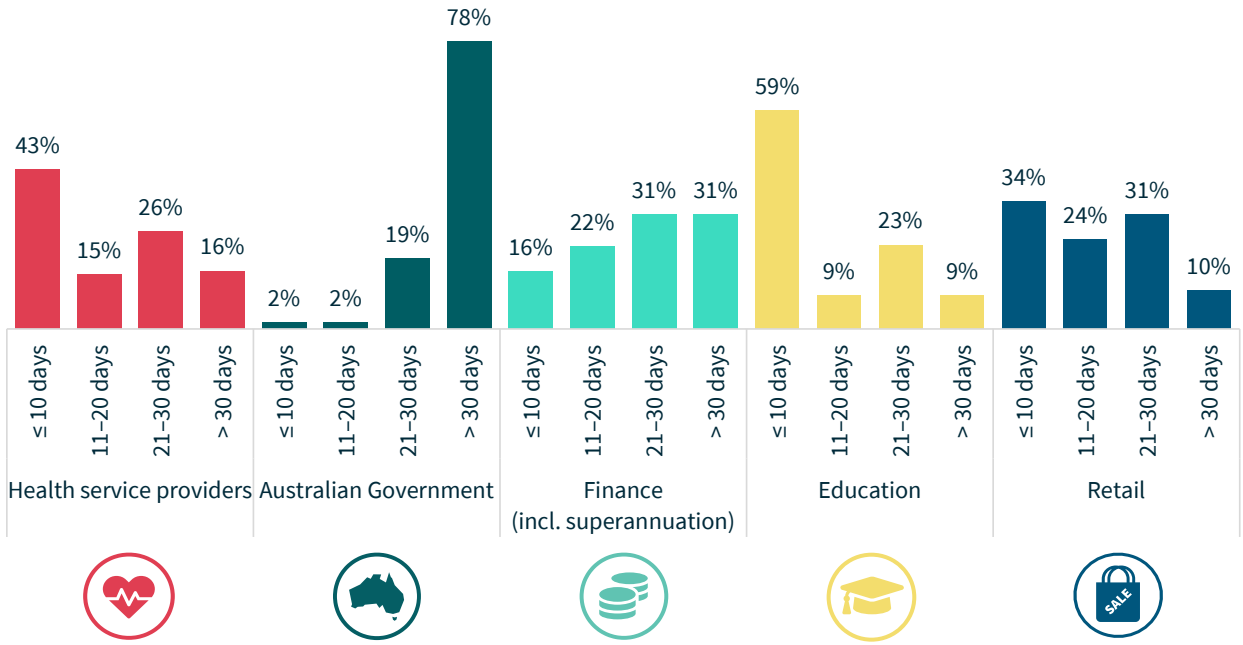
The finance sector includes banks, wealth managers, financial advisors, superannuation funds, and consumer credit providers (regardless of annual turnover).

Chart 14 – Time taken to identify breaches – Top 5 sectors



For notifications in the 'unknown' category, the entity was unable to identify the date the breach occurred.

Chart 15 – Time taken to notify breaches – Top 5 sectors



For notifications in the 'unknown' category, the entity was unable to advise the OAIC the date it became aware of the incident.

Chart 16 – Source of data breach notifications – Top 5 sectors

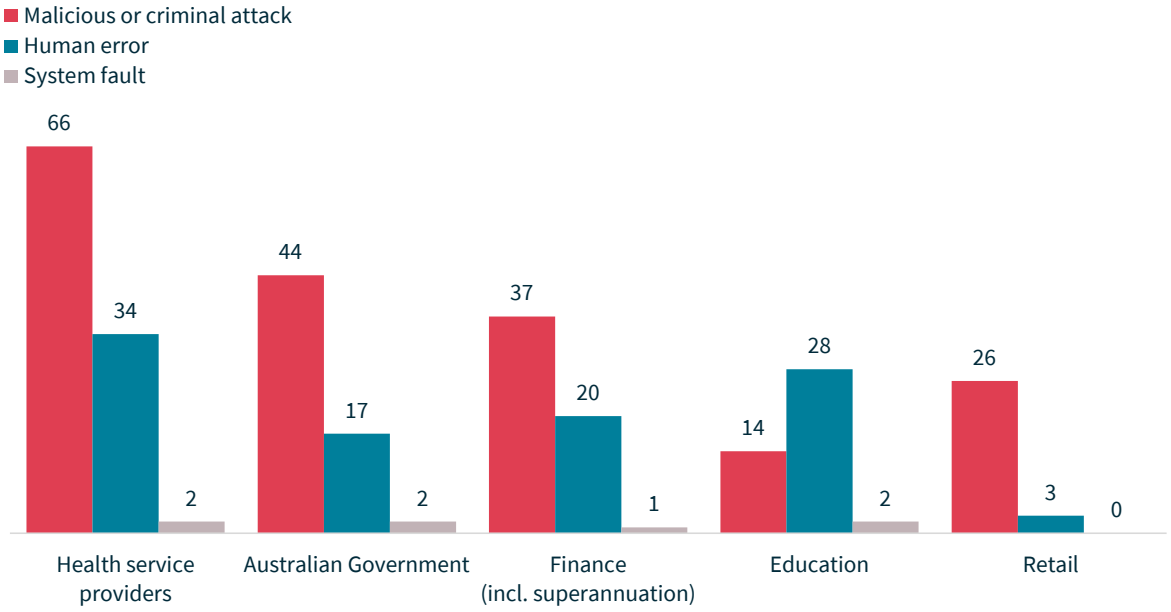


Chart 17 – Malicious or criminal attacks breakdown – Top 5 sectors

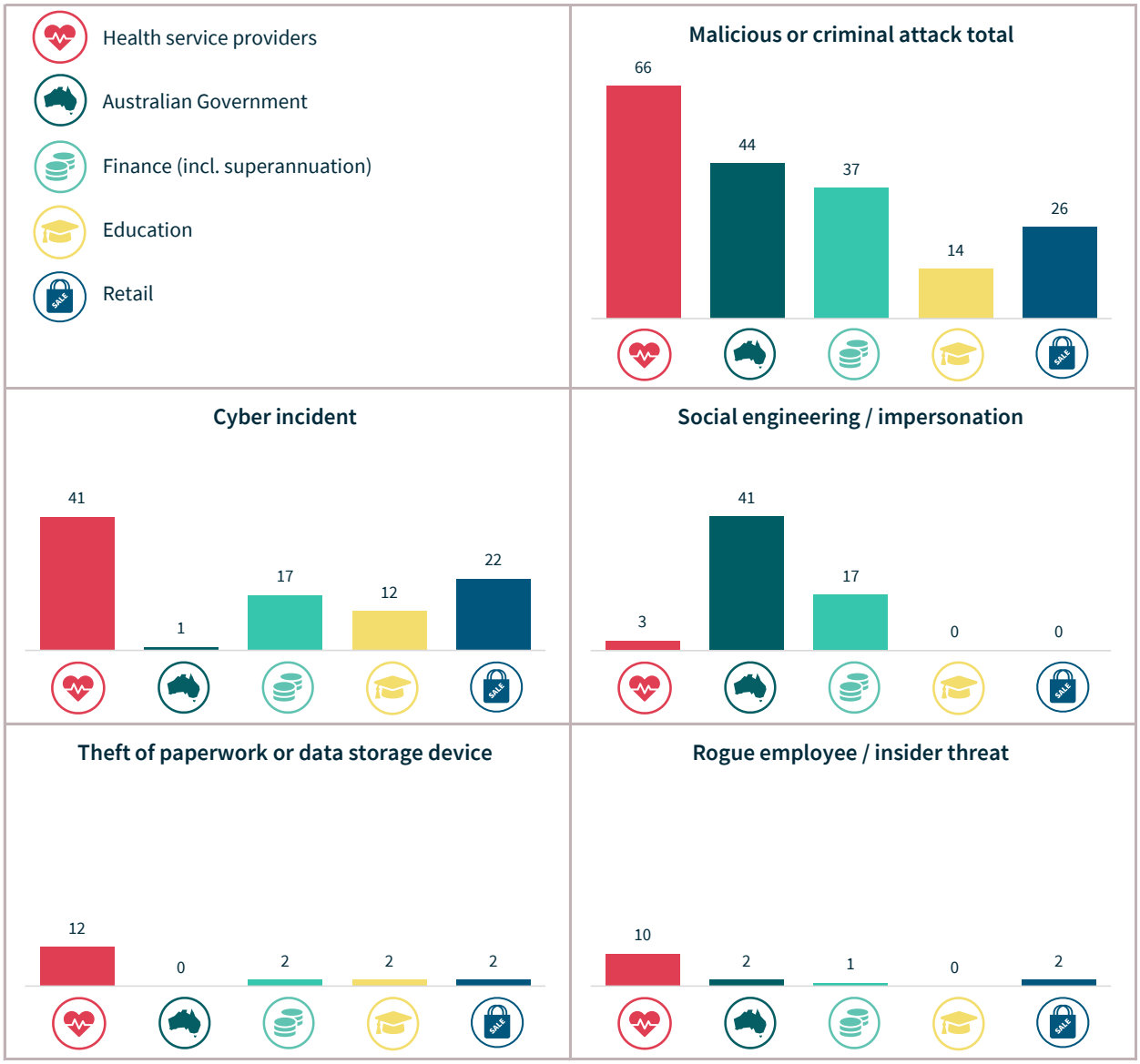


Chart 18 – Cyber incident breakdown – Top 5 sectors

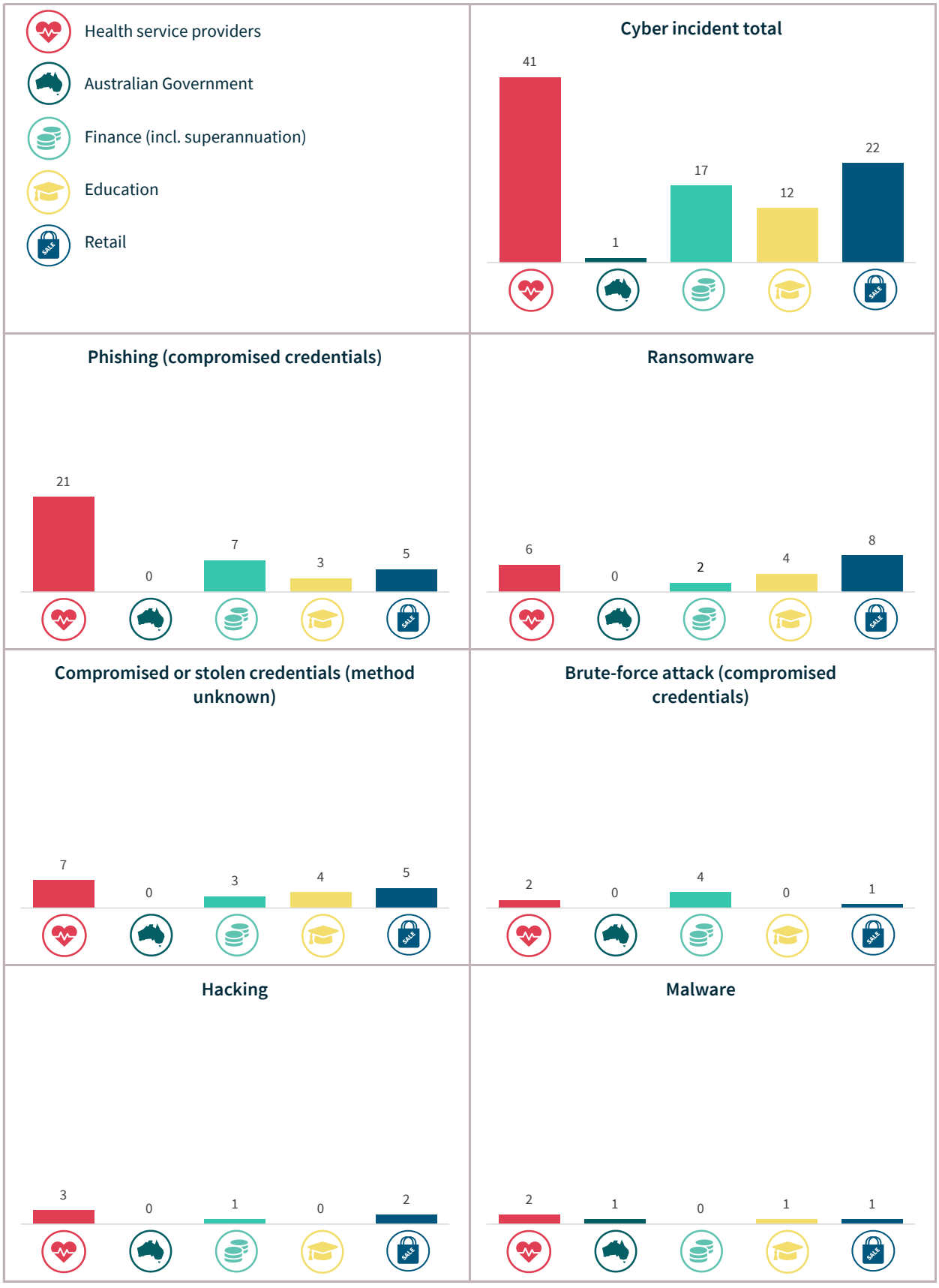
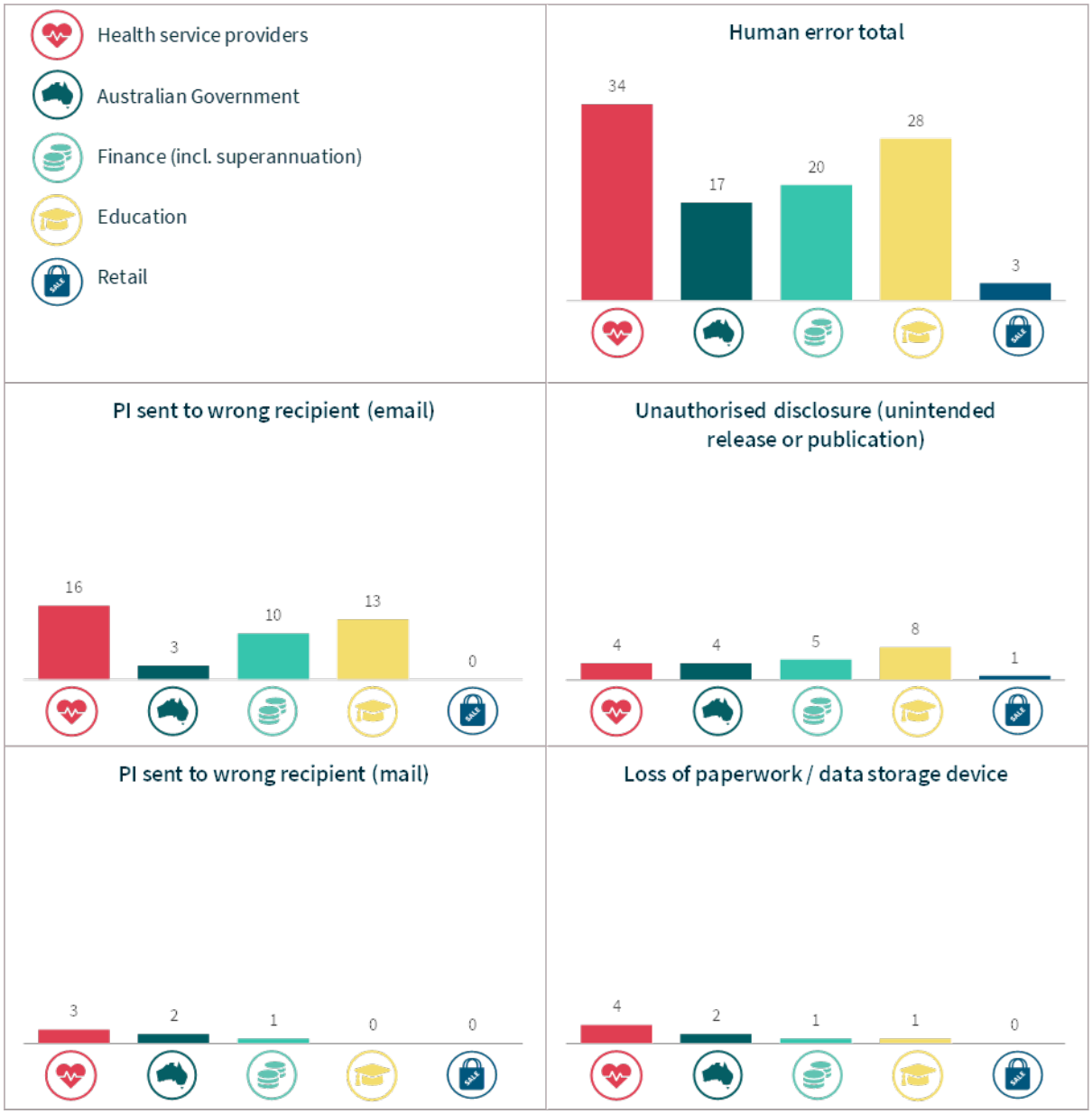
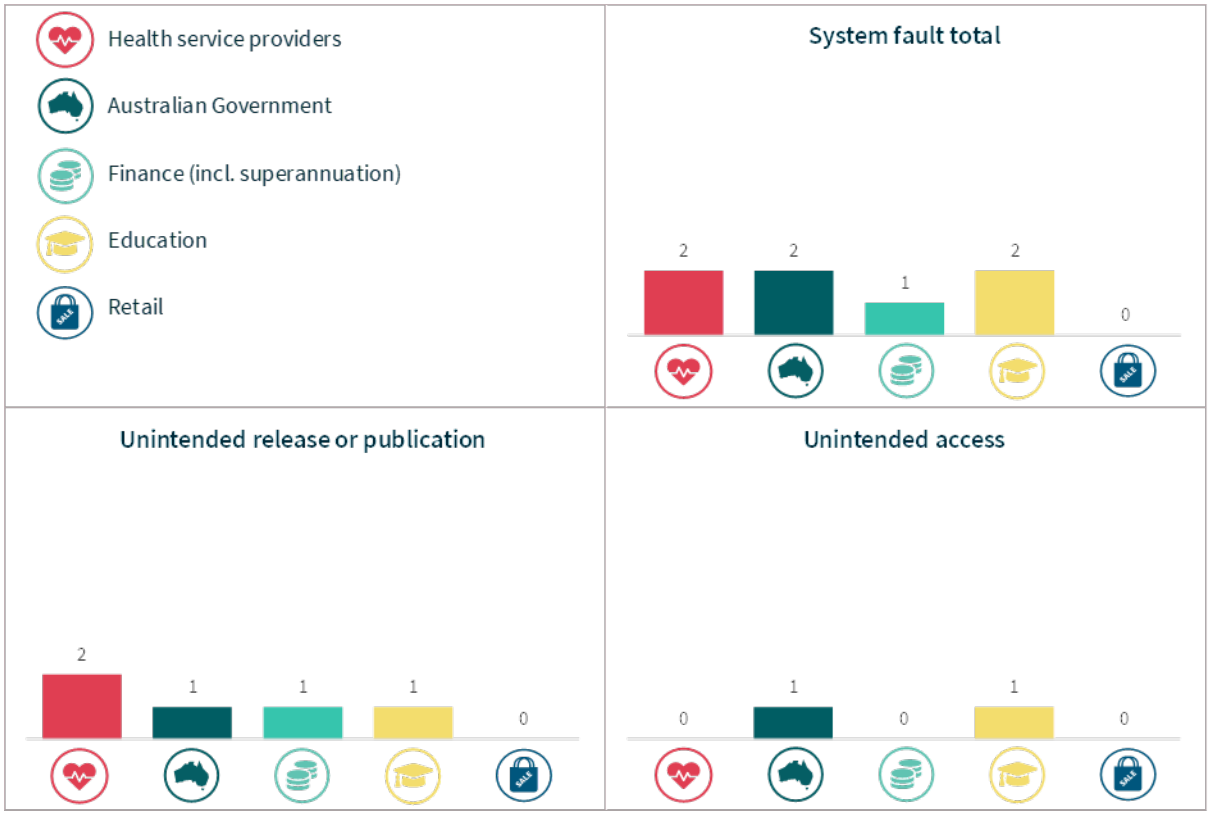


Chart 19 – Human error breakdown – Top 5 sectors




Unauthorised disclosure (verbal)
3
0
1
0
2
Failure to use BCC when sending email
3
1
1
3
0
Unauthorised disclosure (failure to redact)
0
5
1
0
0
PI sent to wrong recipient (other)
0
0
0
2
0
Insecure disposal
1
0
0
1
0
PI sent to wrong recipient (fax)
0
0
0
0
0

Chart 20 – System fault breakdown – Top 5 sectors



Glossary

Term	Definition
Contact information	Information that is used to contact an individual, for example, a home address, phone number or email address
Eligible data breach	An eligible data breach occurs when: • Personal information has been lost, or accessed or disclosed without authorisation • It is likely to result in serious harm to one or more individual • The organisation or Australian Government agency has not been able to prevent the likely risk of serious harm with remedial action
Financial details	Information relating to an individual's finances, for example, bank account or credit card numbers
Health information	As defined in s 6 of the Privacy Act
Identity information	Information that is used to confirm an individual's identity, such as a passport number, driver licence number or other government identifier
Other sensitive information	Sensitive information, other than health information, as defined in s 6 of the Privacy Act, for example, sexual orientation, political or religious views
Personal information (PI)	Information or an opinion about an identified individual or an individual who is reasonably identifiable
Sensitive information	Sensitive information is personal information that includes information or an opinion about an individual's: • racial or ethnic origin • political opinions or associations

Term	Definition
	• religious or philosophical beliefs • trade union membership or associations • sexual orientation or practices • criminal record • health or genetic information • some aspects of biometric information
Tax file number	An individual's personal reference number in the tax and superannuation systems, issued by the Australian Taxation Office
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
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 addresses 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
PI sent to wrong recipient (email)	Personal information sent to the wrong recipient via email, for example, as a result of a misaddressed email or having a wrong 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 an incorrectly entered fax number or having a wrong fax number on file

Term	Definition
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 having a 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
Unauthorised disclosure (failure to redact)	Failure to effectively remove or de-identify personal information from a record before disclosing it
Unauthorised disclosure (unintended release or publication)	Unauthorised disclosure of personal information in a written format, including paper documents or online
Unauthorised disclosure (verbal)	Disclosing personal information verbally without authorisation, for example, calling it out in a waiting room
Malicious or criminal attack	A malicious or criminal attack deliberately crafted to exploit known vulnerabilities for financial or other gain
Brute-force attack (compromised credentials)	A typically unsophisticated and exhaustive process to determine a cryptographic key or password that proceeds by systematically trying all alternatives until it discovers the correct one
Compromised or stolen credentials (method unknown)	Credentials are compromised or stolen by methods unknown
Cyber incident	A cyber incident targets computer information systems, infrastructures, computer networks or personal computer devices
Hacking (other means)	Unauthorised access to a system or network (other than by way of phishing, brute-force attack or malware), often to exploit a system's data or manipulate its normal behaviour
Malware	Short for 'malicious software'. A software used to gain unauthorised access to computers, steal information and disrupt or disable

Term	Definition
	networks. Types of malware include trojans, viruses and worms
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment
Rogue employee/ insider threat	An attack by an employee or insider acting against the interests of their employer or other entity
Phishing (compromised credentials)	Untargeted, mass messages sent to many people asking for information, encouraging them to open a malicious attachment, or visit a fake website that will ask the user to provide information or download malicious content
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
Theft of paperwork or data storage device	Theft of paperwork or data storage device
System fault	A business or technology process error not caused by direct human error