information and privacy commission
new south wales

Mandatory Notification of Data Breach Scheme Trends Report

November 2023 to June 2024

October 2024

Contents

About this report

Part 6A of the *Privacy and Personal Information Protection Act 1998* (PPIP Act) established the Mandatory Notification of Data Breaches Scheme (MNDB Scheme), which requires public sector agencies to notify the Privacy Commissioner and affected individuals in the event of an eligible data breach involving personal or health information that is likely to result in serious harm. The MNDB Scheme commenced on 28 November 2023.

The Information and Privacy Commission (IPC) publishes quarterly statistical information on the number of eligible data breach notifications received under the MNDB Scheme. This report is intended to provide agencies and the public with information on trends concerning the causes and impacts of eligible data breaches.

As the operation of the MNDB Scheme continues to mature, the Privacy Commissioner will review the dataset and may introduce further reporting categories where the data indicates relevant insights which may impact agency practices in managing data breaches.

Data Notes

Statistics in this report are current as of 30 June 2024. Some notifications received during the reporting period were under assessment as of the date of publication and adjustments may be made to related statistics following finalisation. This may affect statistics for the period of November 2023 to June 2024 published in future reports.

Percentages in some charts may not total 100% due to rounding.

The reported cause of a data breach is based on information provided by the reporting agency. In some instances, more than one cause has been identified by the agency. As a result, percentages for relevant charts total more than 100%. Cause of breach categories are defined in the glossary at the end of this report.

No statistical comparisons are made to breaches reported under the former voluntary data breach notification scheme due to the differing eligibility thresholds operating under the two schemes.

Case studies provided in the report are based on notifications received during the reporting period. These have been deidentified and, in some cases, details have been altered or summarised to ensure that affected individuals are not identifiable. They are included to supplement the trends from the reporting period and provide insights into learnings.

Privacy Commissioner's Foreword

As a community we have seen the serious harms that data breaches have had on individuals whose personal information was disclosed – financial loss, identity theft, emotional distress, embarrassment and reputational damage.

Whether caused by accidental human error or malicious actors seeking financial advantage, data breaches are a real and significant risk for NSW public sector agencies. A data breach has real consequences for both the agency and affected individuals. If not managed swiftly and effectively, data breaches undermine trust and confidence in an agency, its capacity to safeguard valuable personal information and in the services and functions undertaken by government agencies.

The number of people in Australia who have been impacted by a data breach has grown considerably due to a series of large-scale data breaches at the national level. In 2023, the Office of the Australian Information Commissioner (OAIC) reported that in the previous 12 months, 47% of adult Australians had been notified by an organisation that their personal information had been involved in a data breach.[1]

The IPC's own NSW Community Attitudes Survey 2024 has also shown a significant increase in the number of people in NSW who have been affected by a data breach:

- Almost one third (31%) of respondents indicated being affected by a data breach, a 14% increase from 2022.
- Only half of respondents (51%) were provided advice by agencies on what to do next.
- Almost one quarter of respondents (22%) affected by a data breach indicated that they were not offered advice or assistance, an increase of 14% from the previous reporting period.
- Overwhelmingly, 89% of respondents agreed that they should be provided assistance when their data is breached.

The MNDB Scheme was established to ensure that NSW public sector agencies respond swiftly to data breaches when they occur and provide transparent information to those individuals affected by a breach. The Scheme imposes obligations on agencies to mitigate the harm that may arise from a data breach, make notifications to the affected individuals and the Privacy Commissioner when an eligible data breach occurs, take steps to prevent further breaches occurring and provide advice to individuals on the steps they should take following a data breach.

The MNDB Scheme requires agencies to adopt privacy practices that go to the heart of accountability and transparency. The timely provision of notifications ensure that individuals are informed of risks to their personal information and equipped with the knowledge to protect their privacy, their identity and their financial security.

How an agency prepares for and responds to a data breach will determine whether it retains the trust and confidence of the public. Open and transparent notifications are core to this process.

Additionally, the MNDB Scheme provides agencies with the opportunity to:

- better understand the privacy risks that can arise from their operations,
- identify and address the human and cyber elements that contribute to data breaches occurring, and
- minimise the risk that individuals and community will experience harm from data breaches.

[1] Office of the Australian Information Commissioner (2023) Australian Community Attitudes to Privacy Survey 2023, Office of the Australian Information Commissioner, Australian Government, p60.

This first report provides preliminary insights into the operation of the MNDB Scheme drawing from statistical data on the notifications received and our engagement with agencies. While the early trends described should be interpreted in context of the number of notifications received, we have observed some clear themes which are detailed in the following section.

Going forward, the IPC will continue to provide guidance and support to agencies as they operationalise their data breach response function and grow their maturity in complying with the requirements of the MNDB Scheme. As further data is collected, the IPC will provide additional insights and observations concerning agency practices in responding to data breaches.

Sonia Minutillo

Acting Privacy Commissioner

What have we seen?

This report looks back on the first seven months of the operation of the MNDB Scheme. It provides an opportunity to reflect on the purposes of the scheme, highlight good practices adopted by agencies in responding to data breaches and identify lessons learned and opportunity for better practice. Although it remains early in the operation of the Scheme, the data available to date does provide early indications of agency capability and maturity in responding to data breaches when they occur.

The following key themes have emerged from notifications received during the reporting period:

Notifications are gradually increasing

The overall number of notifications received in the first seven months of the MNDB Scheme was moderate, although the results show early indications of an increase in notifications towards the end of the reporting period. It is expected that as agency maturity grows under the MNDB Scheme and they further embed changes to policy and procedures required to ensure compliance with the Scheme, the number of notifications is expected to be responsive to these developments.

All agencies should take the opportunity to review the effectiveness of their policies and procedures for assessing data breaches. In particular, agencies are encouraged to consider their assessment processes to ensure that threshold assessments are appropriately weighted and calibrated.

The data outlined in the current report will provide a baseline for comparison in future reporting periods.

Cyber security uplift should be a focus for all sectors

The results contained within this report reinforce the need for agencies across all sectors to invest in measures to address the risks associated with cyber incidents. Data in this current report suggest that this is an area requiring a particular focus in the University and Local Government sectors having regard to the proportion of the total cyber incidents notified by these sectors during the reporting period.

The report's findings echo concerns raised by the Auditor-General for NSW in relation to the cyber security maturity and the funding of cyber security uplift programs in the University and Local Government sectors.[2]

While human error was the dominant cause of data breaches across all sectors, cyber incidents were involved in 25 per cent of all notifications. The types of cyber incidents seen during the reporting period varied with no single attack vector standing out as dominant.

The IPC strongly encourages leaders across the sectors to engage with the risks arising from cyber security. Investment to uplift ICT security and staff capability are key to improving the safety and security of personal information held by agencies. While the NSW Cyber Security Policy is not mandatory for the Local Government or University sectors, its adoption is recommended to build a foundation of strong cyber security practice.

Data Breach Readiness

Readiness is key to responding to a data beach in a timely, effective and efficient manner that succeeds in limiting the harm to affected individuals.

---

[2] Auditor-General for NSW (12 June 2024), Universities 2023 Financial Audit, Audit Office of NSW, NSW Government, p47.

Auditor-General for NSW (26 March 2024), Cyber Security in Local Government, Audit Office of NSW, NSW Government.

An essential element of data breach readiness is a comprehensive data breach policy, as well as an up-to-date privacy management plan. These documents form a key part of an agency's privacy governance arrangements. A data breach policy should outline an agency's overall strategy for managing data breaches from start to finish. At a minimum it should establish the roles and responsibilities of agency staff in relation to managing a breach, and the steps the agency will follow when a breach occurs. This should include a broad consideration of the functions the agency undertakes and where this intersects with other agencies or service providers.

The adage that "*failing to plan is planning to fail*" is an essential truth in data breach response. Good preparation will best position an agency to respond swiftly to a data breach. A comprehensive data breach policy will provide staff with a clear plan to follow that will enable the agency to:

- manage a data breach in a timely manner
- swiftly notify affected individuals
- mitigate the effort and expense an agency will need to remediate the incident, and
- meet its compliance obligations under the MNDB Scheme.

Agencies should regularly review their data breach policy and privacy management plan to ensure they remain current and responsive to changes in the agency's functions or structure, and the changing ways agencies deliver services. They should also be reviewed post incident and be responsive to any lessons learned.

Similarly, agencies should also undertake regular data breach simulations to test their data breach readiness and highlight any deficiencies in data breach response plans. These simulations could be standalone exercises and incorporated as part of the agencies regularly scheduled testing of its cyber security framework or business continuity plan. Being data breach ready means being proactive, not reactive. It means preparing your teams, your policies and your protocols.

Delegations

Swift action is key to a successful a data breach response. To facilitate a timely response, agencies should ensure that appropriate delegations are in place so that the right people have the authority to act and make decisions quickly.

Agencies should ensure that delegations are made to officers at the appropriate level of seniority and with the necessary expertise to respond to a data breach in compliance with the PPIP Act. At a minimum, these officers will need to understand and apply the legislation and statutory guidelines.

In preparing delegations, the agency should consider the risk associated with the specific decisions being made under the delegation. Decisions which may result in higher risk, or decisions in which consideration of an exemption under Part 6A are being considered may be more appropriately delegated to more senior staff.

Effective notifications

Notifications to individuals are most effective when they provide clear advice on what has happened, and the steps individuals should take in response. Effective notifications should provide all the information required under section 59O of the PPIP Act, be written in plain English and provide clear instructions for recommended steps the individual can take or the services that may be contacted for assistance. Poor communications which confuse, are overly complex to understand or alarm the recipient can compound the impact of the data breach.

The timing of notifications to affected individuals should be carefully considered to ensure that affected individuals can implement recommended actions, seek access to relevant support services or seek advice or further information from the agency in a timely manner.

In some circumstances notifications to affected individuals may be undertaken by a public notification. Any public notifications issued by an agency should be accompanied by an effective mechanism for raising awareness through meaningful channels. That means not using channels that are infrequently accessed or are likely to be overlooked by the public. In addition to publication on the agency's public notification register, agencies should implement appropriate methods to publicise any public notifications they issue consistent with their obligations under the MNDB Scheme.

Provision of assistance

Where a data breach impacts high numbers of individuals or involves particularly sensitive personal information, agencies should consider establishing a dedicated webpage or support line to provide affected individuals with a centralised contact point to seek further information about the breach, ask questions about the recommended actions made in the notification or seek support to reduce harm arising from the breach.

Agencies should take a comprehensive approach to the provision of meaningful assistance following a data breach recognising that the assistance required may differ in individual circumstances. Agencies should not adopt a one size fits all approach to provision of assistance.

Contracted service providers

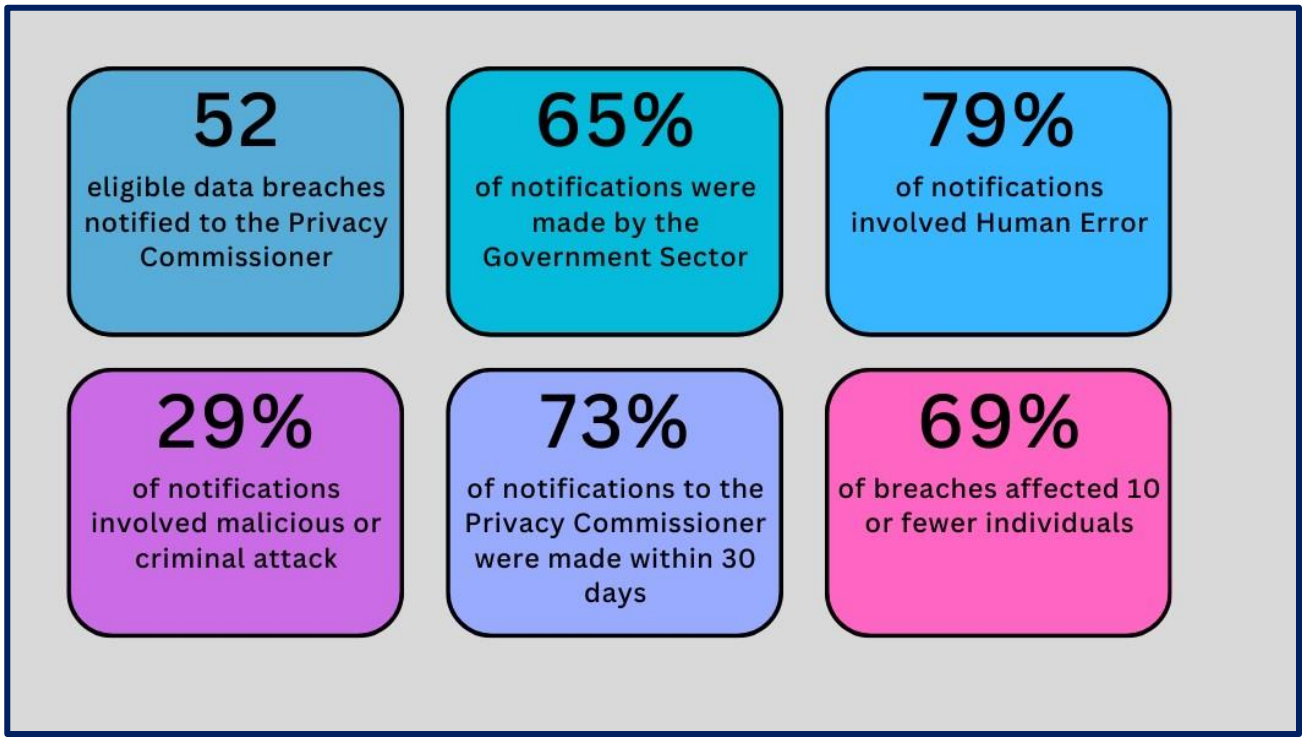
A small number of breaches notified by agencies in the reporting period involved private sector entities performing services under contract to an agency.

To facilitate prompt assessment of breaches involving contracted service providers, agencies must ensure that their data breach policies, data breach response plans and service contracts adequately address all arrangements necessary in the event of a data breach, including those involving a service provider. This should include providing access to all the information necessary for the agency to assess harm, determining which entity will undertake notification and any other matters relevant to responding to, and managing, a data breach.

Breaches involving service providers can be complicated and more difficult for an agency to manage, particularly where the breach occurs within a sub-contracted entity that may be several steps removed from the agency itself. These "chain of contracts" scenarios are common where agencies are providing complex services which involve numerous service providers. The Privacy Commissioner has issued guidance to help agencies understand their obligations in these circumstances.

Summary of key findings

Key findings for the 28 November 2023 and 30 June 2024 reporting period:



Sector Snapshot

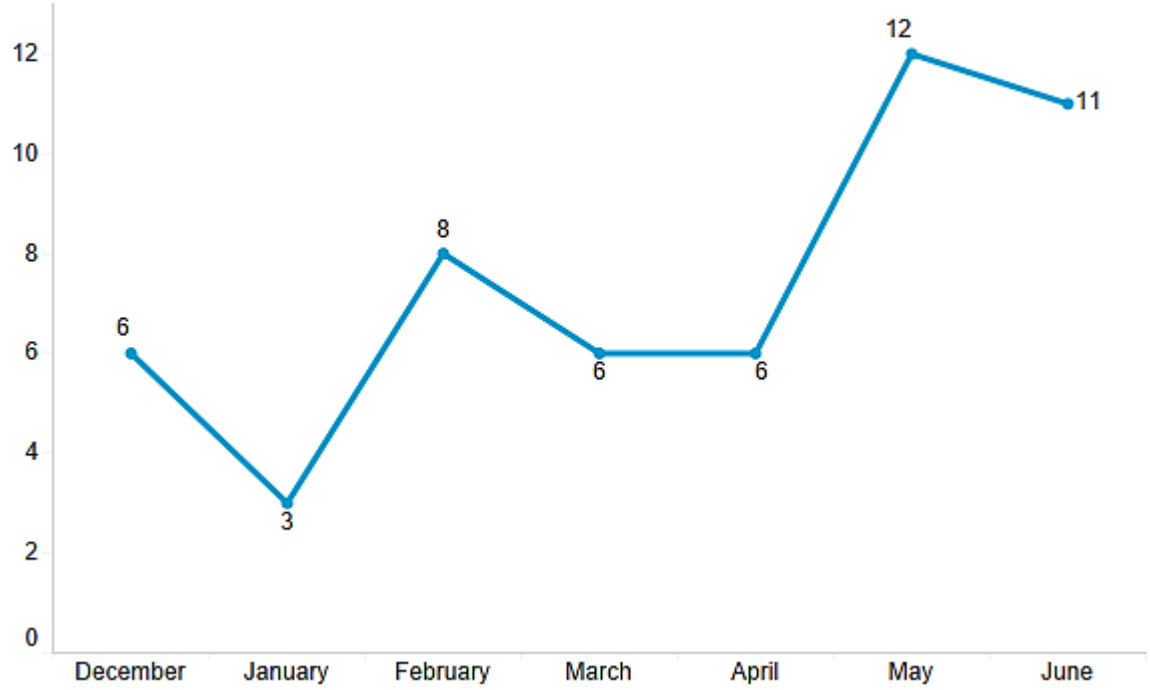
	Government	Local Government	University
Number of notifications	34	9	9
% of data breaches caused by human error	79%	78%	78%
% of data breaches caused by a criminal or malicious attack	26%	22%	44%
Number of affected individuals	1,173	7,054	62,951
% of data breaches discovered within 10 days of occurrence	71%	78%	44%
% of data breaches where assessment was completed within 30 days of discovery	67%	89%	100%

1. Number of notifications

Number of notifications received between 28 November 2023 and 30 June 2024

The Privacy Commissioner received 52 notifications of an eligible data breach during this reporting period (Figure1).

Figure 1: Number of notifications received per month



Notifications were received at a stable rate with a monthly average of six notifications received across the first five months of the reporting period. An increase in notifications was observed in May and June 2024, with 12 and 11 notifications received, respectively.

Notifications by breach types

Most notifications received during the reporting period related to an unauthorised disclosure of personal information (71%), followed by unauthorised access (21%) and loss of personal information (8%) (Figure 2).

Figure 2: Number of notifications by type of data breach

Type of Breach	Count
Unauthorised disclosure	37
Unauthorised access	11
Loss of personal information	4

This finding is consistent with the results for the causes of eligible data breaches detailed in section 2 of this report which show that unintended release or publication of personal information and misdirected emails were the primary causes of data breaches during the reporting period.

Types of Data Breaches

There are three types of data breach which can occur under the MNDB Scheme:

Type	Definition
Unauthorised access	Personal information held by an agency is accessed by someone who is not permitted to do so.
Unauthorised disclosure	An agency (intentionally or accidentally) discloses personal information in a way that is not permitted by the PPIP Act or HRIP Act.
Loss of personal information	Personal information is removed from the possession or control of the agency. Loss may occur because of a deliberate or accidental act or omission of the agency, or due to the deliberate action of a third party. Loss of personal information will only result in an eligible data breach where such loss is likely to result in unauthorised access or disclosure of this information.

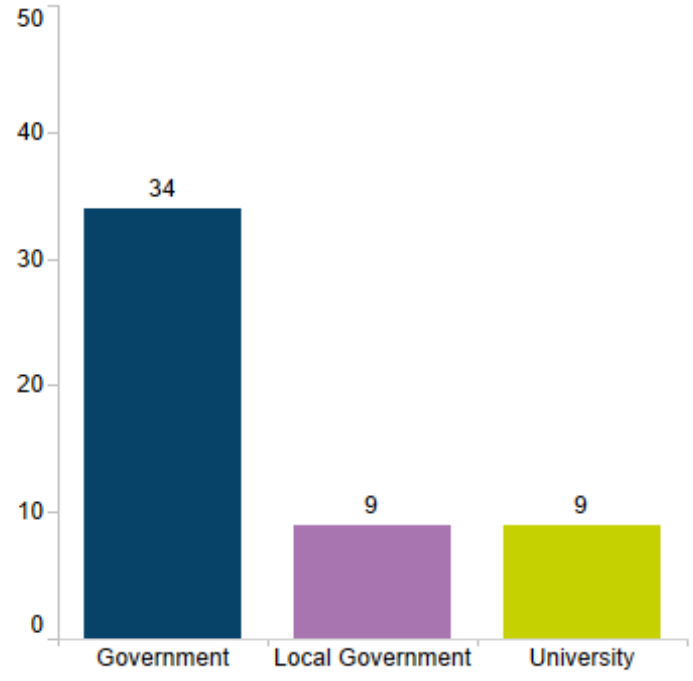
A glossary of common terms is included at page 29 of the report.

Notifications by sector

The majority of all notifications (65%) were received from the Government sector, followed by the Local Government (17%) and University (17%) sectors (Figure 3).

No notifications were received from the State-Owned Corporations or Ministers sectors during the reporting period.

Figure 3: Number of notifications by sector



Good Practice Tips - Responding to breaches and reducing harm to affected individuals.

In addition to the obligation to notify eligible data breaches, agencies are also required to:

- make all reasonable attempts during the data breach assessment to mitigate the harm done by a suspected data breach,
- assist affected individuals by providing advice on recommended actions they can take to reduce harm they may experience because of a data breach; and
- advise the Privacy Commissioner and affected individuals of any actions taken or planned to ensure personal information is secure or to control or mitigate harm.

Notifications received to date illustrate actions taken by agencies to respond to data breaches. These actions reflect commonly provided advice on information governance and cyber security practices. These included:

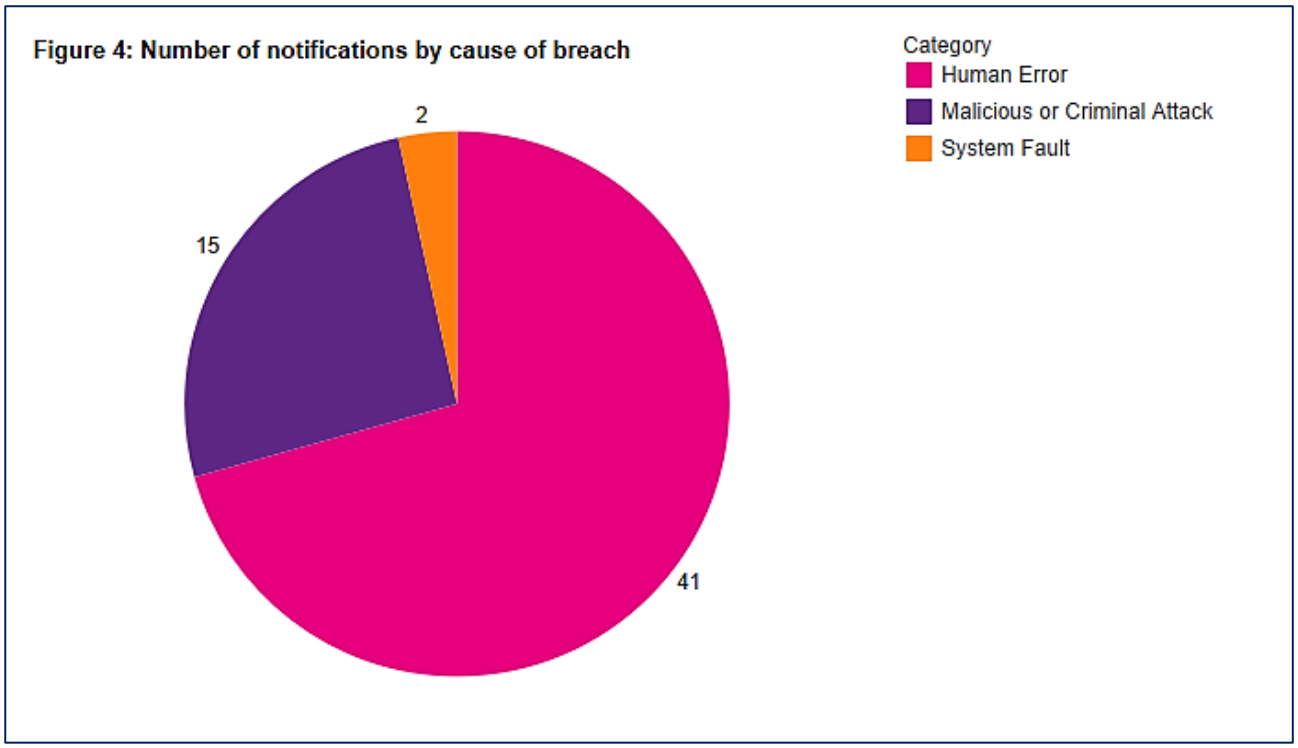
- acting quickly to ensure documents were returned or permanently deleted before being accessed by the unintended recipient and obtaining confirmation of deletion via statutory declaration.
- turning off access to vulnerable systems until they can be secured.
- implementing business rules concerning use of email distribution lists to ensure only current and authorised staff are included within distribution groups.
- enabling the use two-factor authentication as an additional security mechanism
- reviewing access privileges for all ‘admin’ accounts used at different levels of system administration to ensure they are configured in line with the principle of ‘least privilege’ access.
- adopting a secure file sharing system to replace sharing information via posting hard copies, external storage devices (for example USBs) or attachments sent by email.
- undertaking additional education and training for staff who handle personal information.
- implementing a system to review documents before sharing via a link to a secure document transfer platform
- establishing a dedicated data breach support function including a dedicated mailbox or phone line to provide support and assistance to affected individuals.
- engaging specialised services to provide support and assistance to affected individuals.
- applying a tailored notification strategy to provide specialised supports appropriate to the individual and their needs
- reimbursing affected individuals for the costs of replacing compromised identity documents or credentials
- paying for dark-web monitoring services that will scan for the disclosed information on the dark web, helping to notify impacted individuals that their information is in circulation.

2. Causes of data breaches

The primary cause of data breaches during the reporting period was human error (79%), followed by malicious or criminal attack (29%) and system fault (4%) (Figure 4).

Percentages reported in this section of the report equal more than 100% as an individual data breach may have more than one cause recorded where multiple factors contributed to the breach.

Figure 4: Number of notifications by cause of breach



More information on common terms used in this report, including the definitions for the causes of data breaches can be found in the glossary at page 29.

Causes by sector

Consistent with the results detailed at Figure 4, human error was the main cause of data breaches in each of the three sectors, followed by criminal or malicious attack (Figure 5).

In the Government sector:

- 79% of notifications involved human error
- 26% of notifications involved a criminal or malicious attack.

In the Local Government sector:

- 78% of notifications involved human error
- 22% of notifications involved a criminal or malicious attack,
- 11% of notifications involved a systems fault.

In the University sector:

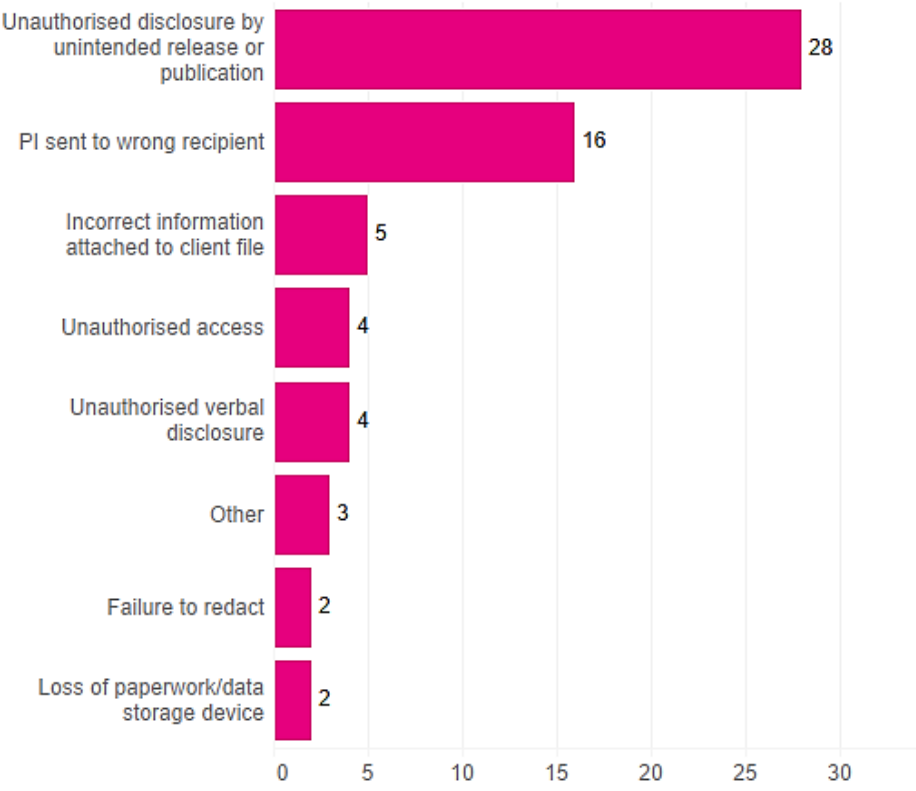
- 78% of notifications involved human error
- 44% of notifications involved a criminal or malicious attack,
- 11% of notifications involved a systems fault.

Figure 5: Number of notifications by cause of breach per sector

Human Error

Human error was the most common cause of data breaches during the reporting period, with 79% of notifications (41 notifications) involving a human error cause (Figure 6).

Figure 6: Number of notifications by cause of breach - Human Error



The top three causes of human error data breaches were:

- unauthorised disclosure by unintended release or publication of personal information (68% or 28 notifications)
- personal information sent to the wrong recipient (39% or five notifications), and
- incorrect information attached to a client file (12% or three notifications).

These results are consistent with data published by the OAIC which found that 68% of data breaches notified by Australian Government agencies were caused by human error.[3] Of the 26 human error breaches notified by Australian Government agencies:

- 50% involved personal information being sent to the wrong person
- 42% were the result of unauthorised disclosure of personal information, and
- 8% involved the loss of paperwork or data storage devices.

Similarly, the most recent data published by the UK Information Commissioner's Office (ICO), shows that 73% of data breach incidents notified in Quarter 1 2024 (January – March 2024) were categorised as non-cyber.[4] Within this category, data emailed to the wrong recipient was the most common incident type at 18% of notifications.

The frequency of notifications caused by human error during the reporting period highlights the importance of embedding robust privacy practices into the design of systems and processes of work, including ensuring staff have access to documented policies, procedures, and business rules. Implementing relevant technological solutions within an agency's systems can also assist staff to safely manage personal information and minimise the risks associated with human error.

An agency's staff can be its most valuable asset for ensuring that personal information is safely and securely handled. This relies on the agency creating a pro-privacy culture where all staff have an appreciation of their role and an understanding of the personal information holdings of the agency and in turn then protecting the personal information the agency holds. Agencies should apply access controls to personal information relevant to the functions and activities of staff and provide receive regular training on end-to-end information management, document security and privacy awareness to ensure that staff have the knowledge and capabilities required to effectively meet the agencies obligations to manage personal information appropriately and safely in compliance with the PPIP Act.

[3] Office of the Australian Information Commissioner (February 2023), Notifiable Data Breaches Report July to December 2023, Office of the Australian Information Commissioner, Australian Government, p34.

[4] UK Information Commissioner's Office, Data Security Incident Trends Dashboard, Data security incident trends | ICO.

Non-cyber breaches are defined as "a type of breach that does not have a clear online or technological element which involves a third party with malicious intent. For example, incidents involving paper filing systems or information accidentally emailed to the wrong recipient."

Case Study - Email and human error breaches

Notifications received during the reporting period have highlighted the frequency of human error data breaches resulting from email communications. Communication via email is ubiquitous across government and the private sector. It provides a low cost, convenient method for seeking or providing information, arranging meetings and transferring files. However, the speed and convenience of email can also contribute to accidental data breaches.

The most common type of data breaches arising from the use of email during the reporting period have included:

- emails being sent to the wrong recipient, and
- emails being sent with an incorrect attachment which contained the personal information of another person.

Example 1:

An agency referred a client to an external service provider via email. The service provider's email address was entered incorrectly, using the format firstname.lastname@business.com.au

The correct email address differed by one digit: firstname.lastname1@business.com.au. This resulted in the personal and health information of the client being sent to the wrong recipient.

In response, the agency:

- contacted the intended recipient and confirmed the correct email address
- contacted the unintended recipient to contain and secure the personal information, and
- conducted a post incident review and identified educative and process/ practice safeguards for implementation.

Example 2:

An agency sent out a notice to a client via email using two email addresses listed on the client's file. The notice contained the client's personal information, including their home address. One of the email addresses belonged to the client's former partner who was not authorised to receive notices on the client's behalf. The unauthorised disclosure of the client's address put them at risk of possible physical harm as well as the financial cost of additional security measures at the dwelling.

In response to the breach the agency:

- removed the unintended recipient as a contact person for the affected individual
- requested that the recipient delete the email and confirm deletion, and
- implemented a process to confirm current contact details with the client via phone when more than one email address is stored on file.

Example 3:

An agency sent an email to an incorrect recipient with an unencrypted spreadsheet attached. The spreadsheet contained personal information of the agency's clients, including name, contact details, invoice numbers and outstanding amounts due on invoices.

In response the agency:

- recalled the email and contacted the unintended recipient to request deletion of the email, and
- implemented revised business rules for email use including use of secure platform sharing links and password protection when sending attachments.

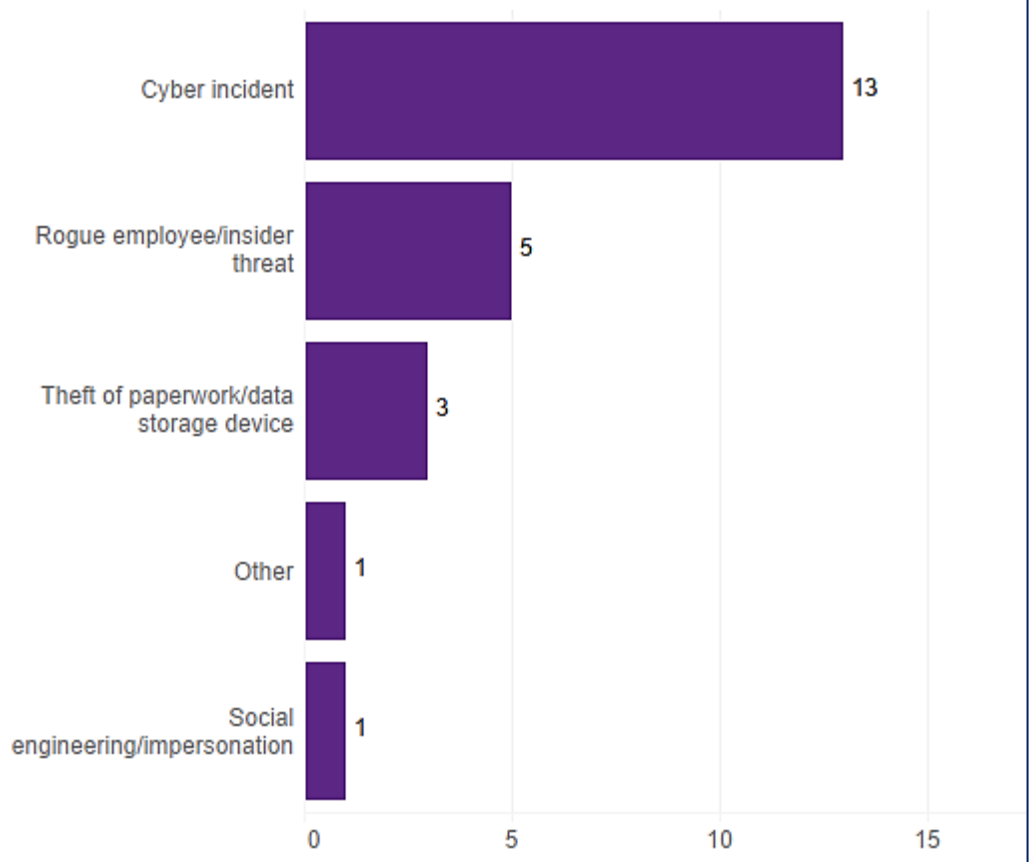
Malicious or Criminal Attack

The majority of breaches caused by a malicious or criminal attack during the reporting period involved a cyber incident (87% or 13 notifications) (Figure 7).

The top three cause of malicious or criminal attacks breaches were:

- cyber incident (87% or 13 notifications),
- rouge employee or insider threat (33% or five notifications), and
- theft of paperwork/data storage device (20% or three notifications).

Figure 7: Number of notifications by cause of breach - Malicious or Criminal Attack



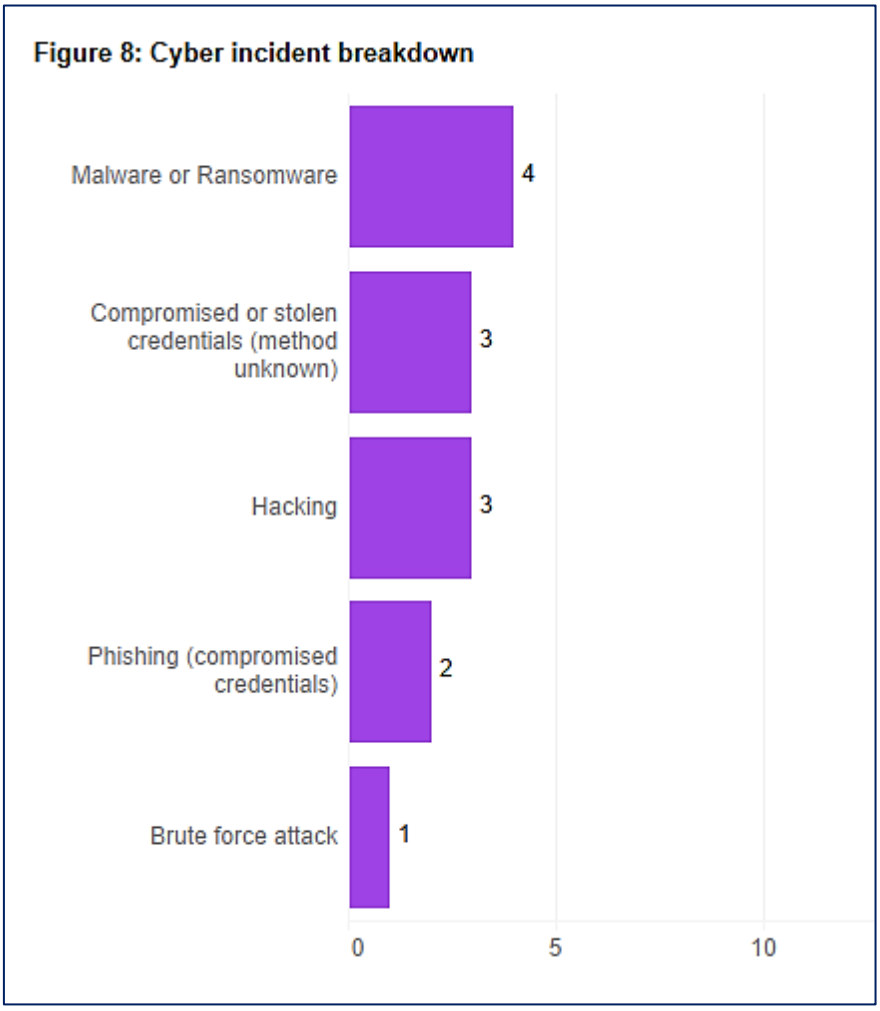
Cyber incidents

In the reporting period, 25% of the total notifications received involved a cyber incident.

As shown in Figure 8, the top three causes of a cyber incident were:

- use of malware/ransomware (31% or four notifications)
- compromised or stolen credentials (23% or three notifications), and
- hacking (23% or three notifications).

Figure 8: Cyber incident breakdown



Systems Fault

Only two notifications received during the reporting period were caused by a systems fault. At this early stage, the overall number of notifications caused by system fault are not sufficient to draw any insights concerning this category of data breach.

3. Type of personal information involved

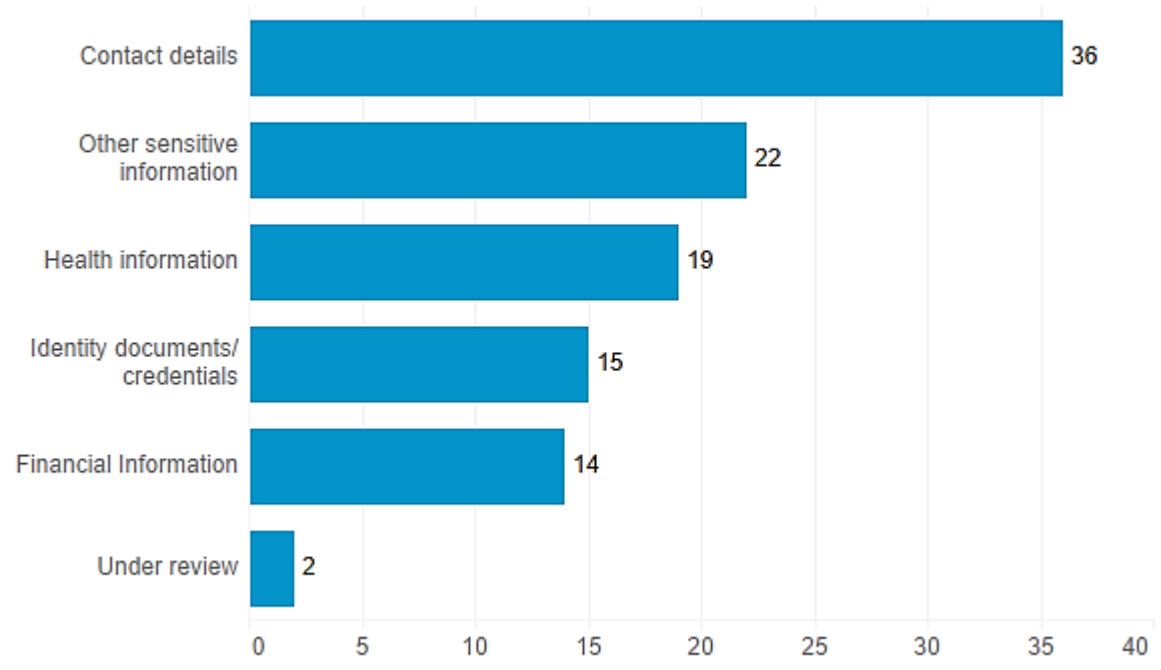
Contact information was the most common type of personal information involved in data breaches during the reporting period (Figure 9). This category includes information such as an individual's name, residential address, phone number or email address.

Some notifications involved more than one type of personal information.

The majority of data breaches notified (69%) involved contact information, followed by:

- other sensitive information (42%)
- health information (37%), and
- identity information or credentials (29%).

Figure 9: Number of notifications by type of personal information



The category "Under review" is used where an agency is yet to determine the type of information impacted by the breach at the point in time when the notification is made to the Privacy Commissioner. Data concerning notifications in this category may be revised following updates to the Privacy Commissioner as the agency completes its investigation.

4. Impacts of the breach

Number of individuals affected by an eligible data breach

Eligible data breaches notified to the Privacy Commissioner during this period affected 71,178 individuals.

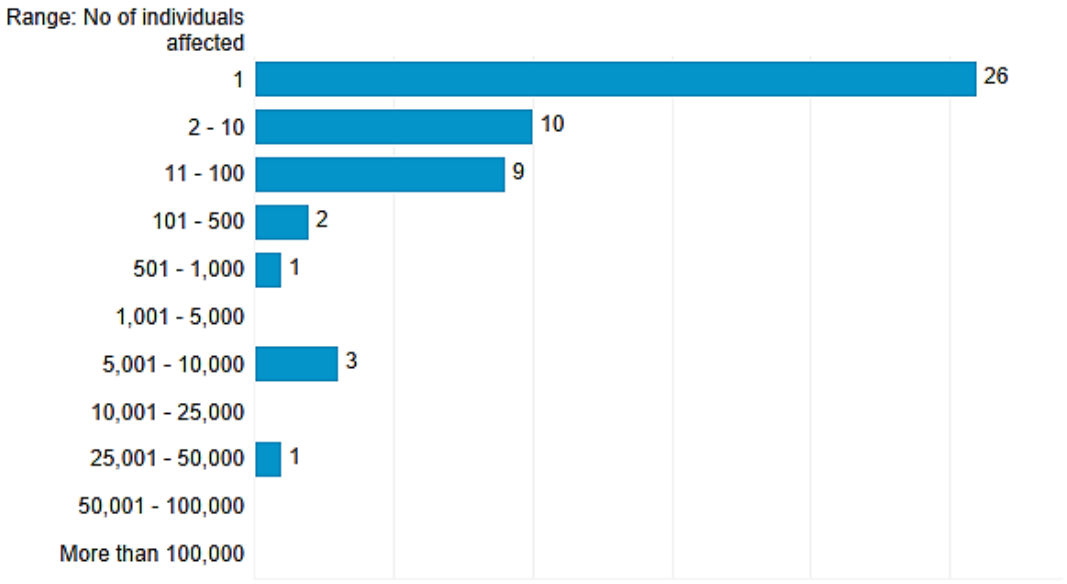
The majority of notifications (69%) affected 10 or fewer individuals, while 50% of notifications affected a single individual (Figure 10).

A small number of notifications were larger in scale, with three notifications affecting between 5,001 – 10,000 individuals and one notification affecting between 25,001 and 50,000 individuals.

This result is consistent with data from other jurisdictions:

- The OAIC reported that 44% of data breaches notified between July and December 2023 affected 10 or fewer individuals.[5]
- The UK ICO reported that 50% of data breach incidents between January and March 2024 involved 10 or fewer individuals.[6]

Figure 10: Notifications by number of individuals affected



Number of individuals affected by an eligible data breach by sector

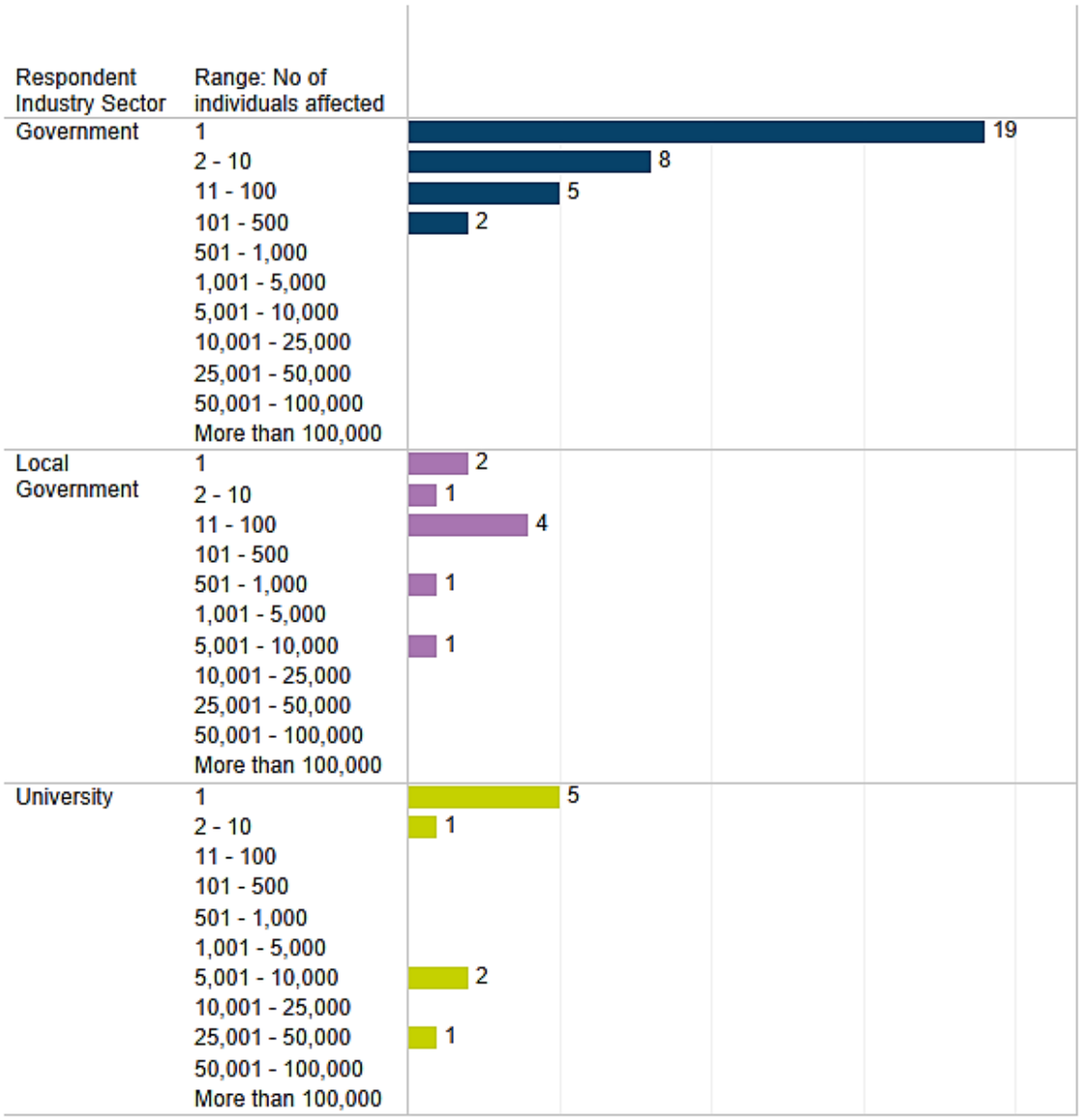
Figure 11 sets out the number of individuals affected by data breaches during this period across the different sectors.

Some caution should be exercised in interpreting the results given the early stage of operation of the Scheme. Caution should be exercised in drawing conclusions concerning the impact of data breaches solely based on the number of individuals affected. The scale of a data breach does not correlate directly to the level of potential harm to affected individuals. A range of complex factors are relevant in measuring the full impacts of a data breach.

[5] OAIC, Notifiable Data Breaches Report, p10.

[6] UK ICO, Data Security Incidents Trends Dashboard.

Figure 11: Number of individuals affected by sector



Government sector

The majority of notifications made by the Government sector affected 10 or fewer individuals (79% or 27 notifications).

This result is consistent with the trends observed in relation to the causes of data breaches within this sector. Human error causes, such as misdirected emails and sending incorrect attachments, which usually affect smaller numbers of individuals were the predominant cause recorded in the Government sector.

Local Government sector

Notifications in the Local Government sector generally impacted 100 or fewer individuals (77% or seven notifications). Of the nine notifications made by this sector:

- 33% (three notifications) affected 10 or fewer individuals,
- 44% (four notifications) affected between 11-100 individuals.

Like the Government sector, these notifications were largely caused by human error.

University sector

While the majority of notifications in the University sector affected 10 or fewer individuals (67%), this sector also recorded the majority of the larger scale data breaches received during the reporting period.

Of the nine notifications received from the University sector:

- 22% (two notifications) affected between 5,001 and 10,000 individuals, and
- 11% (one notification) affected between 25,001 and 50,000 individuals.

Cyber incidents in the University sector were the cause of the larger scale breaches notified.

Case study - Notifications to affected individuals.

An agency detected unauthorised access to data held within its cloud storage system, with potential to impact up to 48,000 individuals. The agency had not yet completed its investigation of the incident at the time it made a notification to the Privacy Commissioner and had not yet confirmed (a) the number of individuals affected or (b) the number of individuals at risk of serious harm.

The agency proactively issued early communications to all potentially affected individuals informing them that the agency was investigating the incident and would notify any individuals identified to be at risk. Following completion of its investigation, and the assessment of risk of harm, the agency determined that the breach affected approximately 5,400 individuals and notifications were issued to those individuals.

This case study highlights the need for agencies to carefully consider the communication strategies adopted when responding to a data breach.

Agencies must notify affected individuals as soon as reasonably practicable after determining that a breach is an eligible data breach. In considering the timing of a notification, agencies should carefully balance timely notification with ensuring that affected individuals are provided with reliable and accurate information about the breach.

Most importantly, notifications should provide recipients with meaningful information about what has occurred, an accurate sense of what risks may arise for them and what practical measures they can take to protect themselves.

5. Timeframes

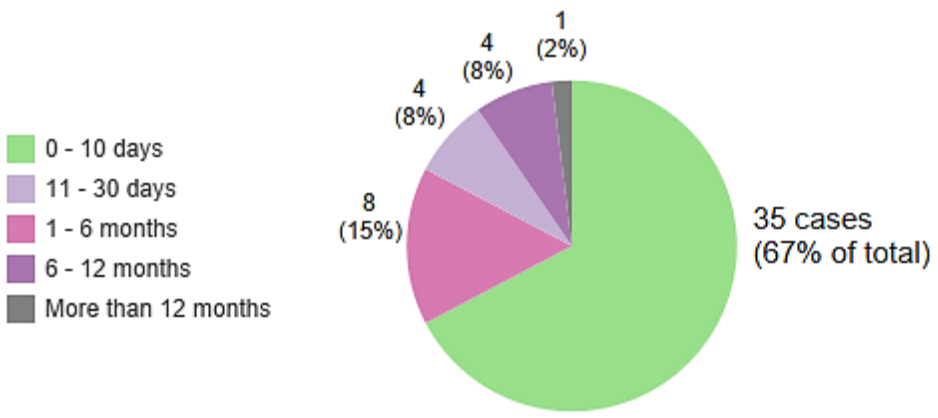
Time taken to identify data breaches

To respond to a data breach, an agency must first know that it has occurred. Acting quickly when a breach is discovered is essential to reducing the impact for both the affected individuals and the agency. Having a defined process for making, assessing and triaging data breach reports will help agencies quickly activate their data breach response plan when a breach is identified or suspected.

The time taken to identify or become aware of a breach will vary based on the individual context and circumstances in which the breach occurred. Discovery of the breach is the precursor action that triggers the requirements to undertake a data breach assessment.

During the reporting period, 67% of data breaches were identified within 10 days of occurring. A quarter of breaches (25%) were identified more than 30 days after occurring (Figure 12).

Figure 12: Number of days between breach occuring and breach discovered



These results compare favourably with data published by the OAIC which found that in notifications by Australian Government agencies the data breach was identified:

- within 10 days of occurring in 37% of notifications,
- between 11 and 30 days after occurring in 11% of notification, and
- more than 30 days after occurring in 50% of notifications.[7]

Time taken to identify data breaches by sector

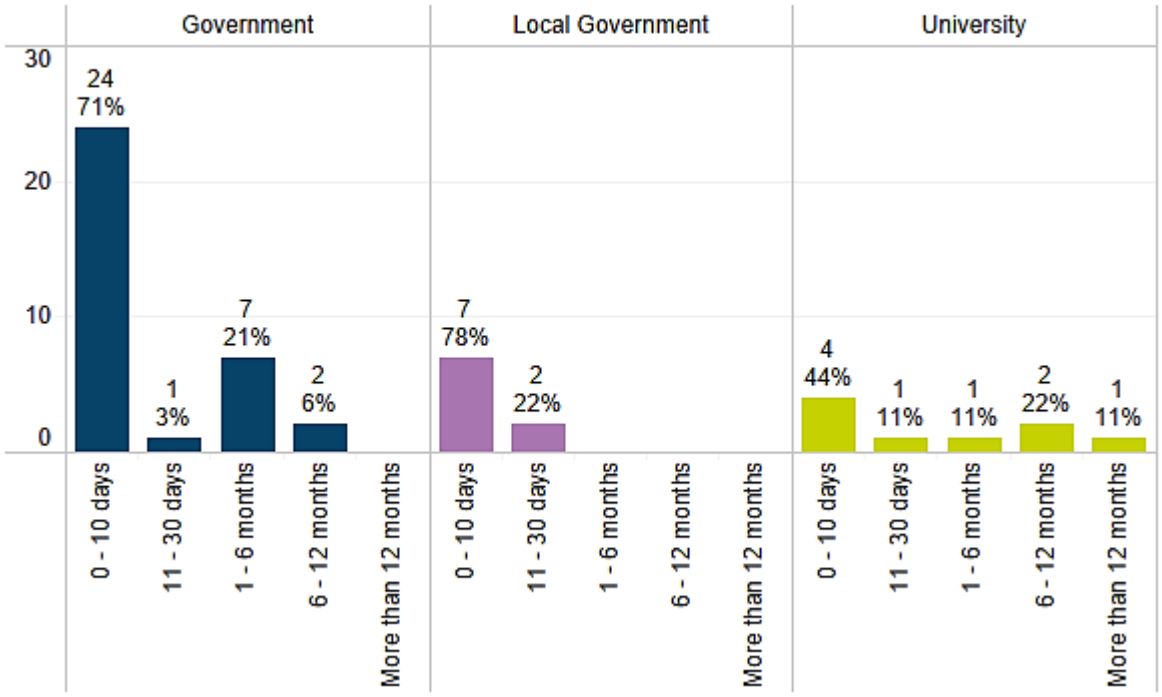
Figure 13 shows the number of days between the occurrence of an eligible data breach and an agency's discovery of the breach by sector.

The majority of data breaches in the Local Government (78%) and Government (71%) sectors were identified within 10 days of occurring. In comparison, 44% of breaches in the University sector were identified within 10 days.

[7] Office of the Australian Information Commissioner, *Notifiable Data Breaches Report July to December 2023*, 22 February 2024, p31

Of the nine notifications in the University sector, 33% (three notifications) were discovered 6 months or more after the breach occurred.

Figure 13: Number of days between breach occuring and breach discovered by sector



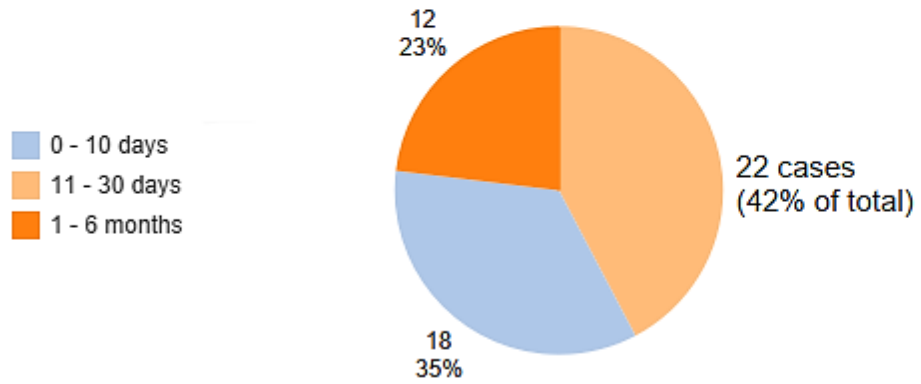
Time taken to notify the Privacy Commissioner

When an agency becomes aware of a possible data breach, it must, undertake an assessment within 30 calendar days to determine whether it is an eligible data breach. The agency must immediately notify the Privacy Commissioner once it has determined that an eligible data breach had occurred. Measuring the time between discovery of a data breach and the making of a notification to the Privacy Commissioner, provides insight into the amount of time taken by agencies to undertake data breach assessments.

Overall, 77% of agencies notified the Privacy Commissioner within 30 days of becoming aware of a data breach (Figure 14). This result suggests that agencies are taking the required steps to meet the obligation under section 59E of the PPIP Act to conduct a data breach assessment within 30 calendar days.

Of the total notifications received, 35% were made within 10 days of becoming aware of a suspected data breach. This is likely to be reflective of the fact that the majority of data breaches notified to date have been caused by human error (such as misdirected emails) rather than more sophisticated, targeted cyber incidents which generally require a longer period to assess.

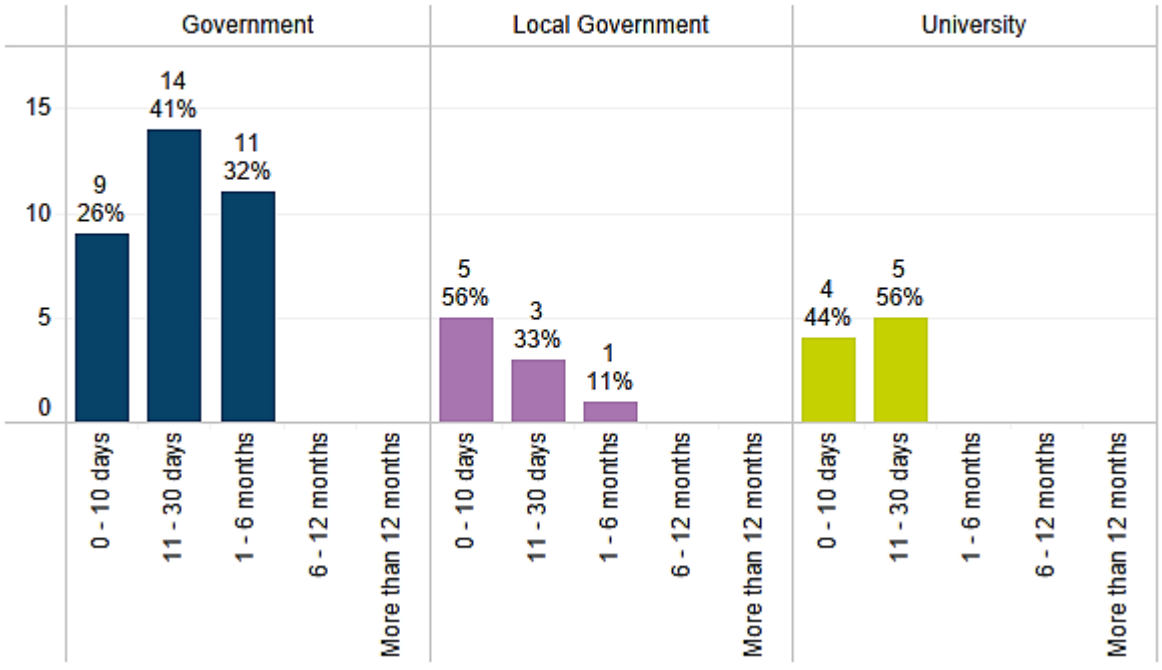
Figure 14: Notifications grouped by days between breach discovered and Privacy Commissioner notified



Time taken to notify the Privacy Commissioner by sector

Figure 15 shows the number of days between an agency's discovery of a breach and the notification to the Privacy Commissioner by sector.

Figure 15: Notifications grouped by days between breach discovered and Privacy Commissioner notified by sector



In the Government sector, 67% of notifications to the Privacy Commissioner were made within 30 days of becoming aware of a data breach. The remaining 32% of notifications were made between 1 – 6 months after becoming aware of the data breach.

Agencies are reminded of the requirement under section 59E to undertake a data breach assessment within 30 calendar days of becoming aware that there may have been a data breach. This is a timely reminder of the Scheme's requirement to carry out an expeditious assessment under section 59E and to immediately notify the Privacy Commissioner once the Agency has decided an eligible data breach has occurred.

Where a data breach assessment cannot reasonably be completed within 30 days, the agency head may approve an extension of the assessment period. Agencies must provide a written notice to the Privacy Commissioner where an extension is approved. It is the Privacy Commissioner's expectation that this notice should contain sufficient information to demonstrate the agency's need to extend the assessment period.

In the Local Government sector, 89% notifications to the Privacy Commissioner were made within 30 days of becoming aware of a data breach.

In the University sector, 100% of notifications to the Privacy Commissioner were made within 30 days of becoming aware of a data breach.

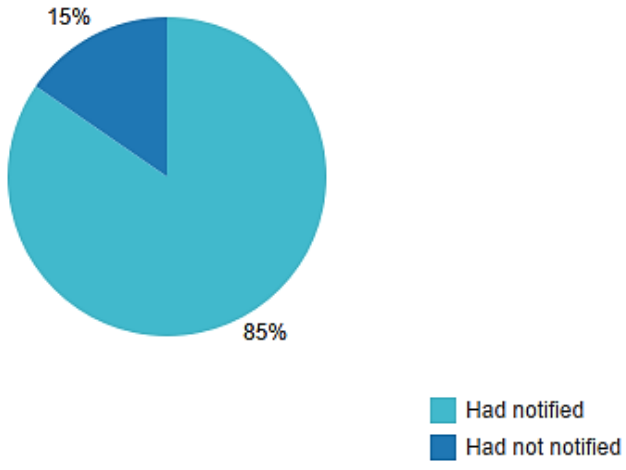
Timing of notifications made to affected individuals

Figure 16 shows that 85% of agencies had notified affected individuals of the eligible data breach before making a notification to the Privacy Commissioner.

This suggests that most affected individuals were notified of the data breach within 30 days or less from the date the agency become aware of the breach. Given that timely notification is a key factor in protecting individuals from the harm that can result from a data breach, this early trend is pleasing to note.

However, like the results detailed at Figure 14 for notifications to the Privacy Commissioner, this result may be primarily reflective of the fact that human error was the dominant cause of the eligible data breaches notified during the reporting period.

Figure 16: Percentage of agencies that had notified affected individuals



Abbreviations

The following table lists the commonly used abbreviations within this report.

Acronyms or abbreviation	Explanation
ICO	Information Commissioner's Office (UK)
IPC	Information and Privacy Commission NSW
MNDB Scheme	Mandatory Notifiable Data Breach Scheme
OAIC	Office of the Australian Information Commissioner
PPIP Act	*Privacy and Personal Information Protection Act 1998*

Glossary

The following table defines common terms used in this report.

Term	Definition
Cause of data breach	The act, event or omission that led to the data breach occurring. The different cause of breach categories are further defined below.
Contact information	Information that is used to contact an individual, for example a home address, phone number or email address.
Eligible data breach	As per section 59D of the PPIP Act, an eligible data breach occurs when: • personal information held by an agency is accessed or disclosed without authorisation or is lost in circumstances that are likely to result in unauthorised access or disclosure, **and** • a reasonable person would conclude that this would be likely to result in serious harm to an individual to whom the information relates.
Financial information	Information relating to an individual's finances, for example, their bank account details or credit card numbers.
Health information	As defined in section 6 of the HRIP Act - information about an individual's physical or mental health, disability, and information connected to the provision of a health service.
Identity information	Information that is used to confirm an individual's identity, for example their passport number, driver licence number of other government issued identifier.

Term	Definition
Personal information	As defined in section 4 of the PPIP Act - information or an opinion about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. For the purposes of the MNDB Scheme 'personal information' also includes 'health information' as defined under the HRIP Act (s59B of the PPIP Act).
Type of data breach	Refers to the factual event that constituted the data breach (s59D of the PPIP Act): • unauthorised access to personal information, • unauthorised disclosure of personal information, or • loss of personal information in circumstances where unauthorised access or unauthorised disclosure is likely to occur.
Human Error	An unintended action by an individual directly resulting in a data breach
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.
Failure to redact personal information	Failure to effectively remove or de-identify personal information from a record before it is disclosed.
Incorrect information attached to client file	Personal information is attached to an incorrect client file which is subsequently accessed.
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.
Personal information sent to wrong recipient	Personal information sent to the wrong recipient via email, fax, mail or other method.
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 access	Accessing personal information without authority or for a purpose not related to their duties or functions.
Unauthorised verbal disclosure	Disclosing personal information verbally without authorisation, for example, calling it out in a waiting room or providing via a conversation.
Unauthorised disclosure by unintended release or publication	Unauthorised disclosure of personal information in a written format, including via 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 or paperwork/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 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	Short for 'malicious software.' A software used to gain unauthorised access to computers, steal information and disrupt or disable networks. Types of malware include trojans, viruses and worms.
Ransomware	Malicious software that makes data or systems unusable until the victim makes a payment.
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.
Brute force attack	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.
Hacking	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.
Business email compromise	A form of cybercrime that uses email fraud to attack business, government and non-profit organisations to achieve a specific outcome that negatively impacts the target organisation.
System Fault	A business or technology process error not caused by direct human error.

Term	Definition
Mail merge failure	A system failure which results in personal information being misdirected to the incorrect individual.
Unintended release or publication	A system failure which results in the release or publication of personal information.