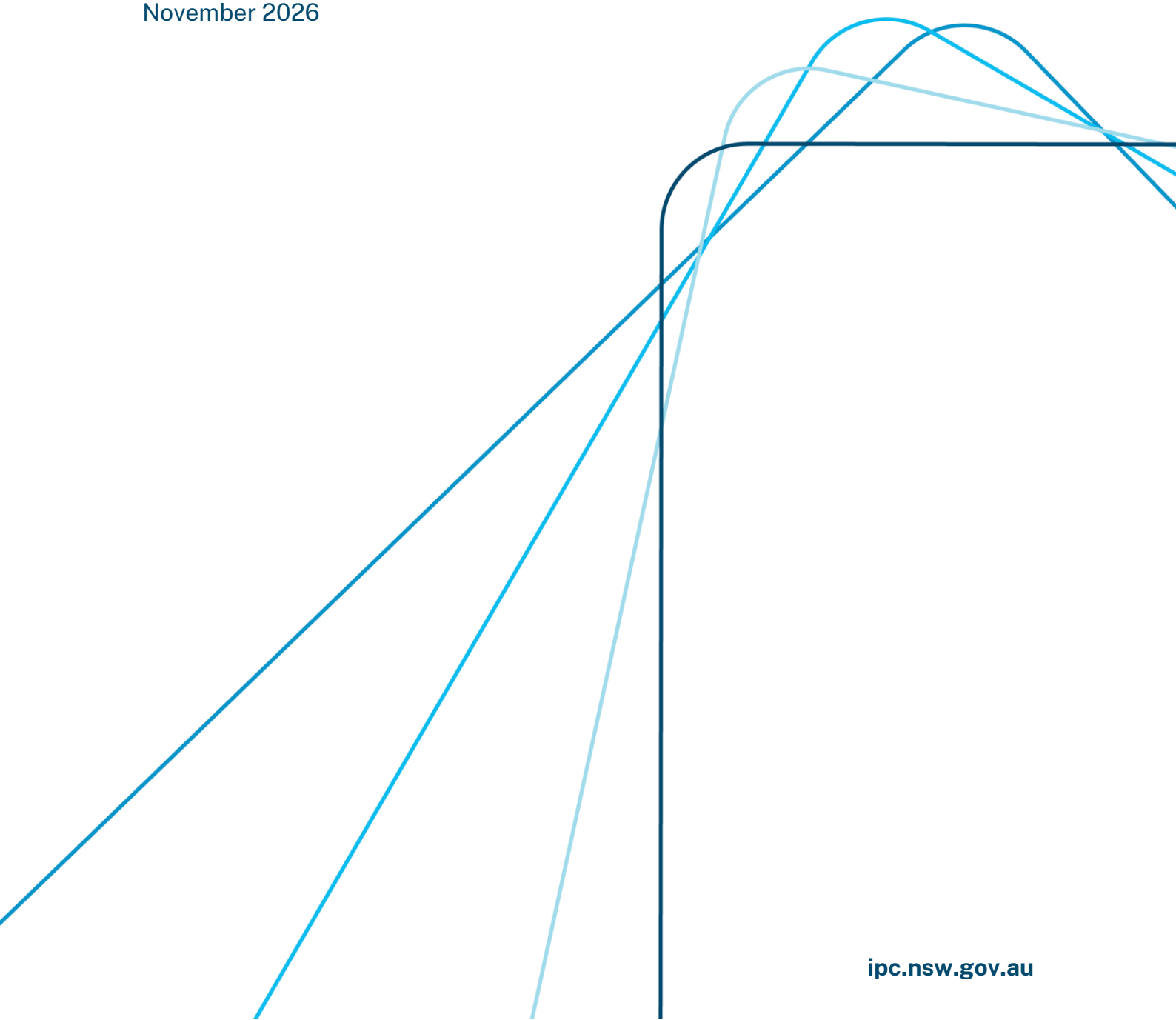
Information and Privacy Commission NSW

Mandatory Notification of Data Breach Scheme Trends Report

July 2024 – June 2025

November 2026



Contents

Privacy Commissioner's Foreword 4

1. *What have we seen?* 5
2. *Snapshot of key findings* 9
3. *Sector snapshot of key findings* 10
4. *Analysis of key findings* 11
5. *Abbreviations* 29
6. *Glossary* 29

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 data breaches, numbers by sector, by breach type and numbers of individuals affected 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

- This Report considers notifications received under the MNDB scheme from 1 July 2024 – 30 June 2025.
- Data reported is current as of May 2026.
- Statistics previously published in the 2024 Trends Report and quarterly statistical data releases may differ to the statistics shown in this Report. This is due to some eligible data breaches being under assessment at the time of reporting and adjustments made following publication.
- Statistical comparisons are to the period November 2023 – 30 June 2024 unless otherwise stated. This is referred to as the “prior period”.
- Percentages in 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 may total more than 100%. Cause of breach categories are defined in the glossary at the end of this Report.
- 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

In today's digital ecosystem, personal information is being collected, used and shared at an unprecedented scale. Data has become a strategic resource, increasingly underpinning decision making, enabling innovation and driving opportunities for improved outcomes. Its value depends on community confidence and trust that agencies are demonstrating they can safely manage that information and protect personal information from misuse and loss.

When a data breach occurs, what is lost is more than a loss of information. It is also a loss of trust and confidence. The consequences of a data breach can be far reaching with the potential to not only significantly harm individuals but disrupt systems and impact critical operations. As the value and influence of data grows exponentially, so too does an agency's responsibility to protect personal information.

Previously we have reported on the rising number of people in NSW impacted by a data breach. This number continues to have an upward trajectory. The recent Community Attitudes Survey 2026 shows:

- over **1 in 10 people** have been affected by a data breach involving the Government with nearly 1 in 3 people unsure if they have been impacted.
- a large majority reported they are very or quite concerned. Concern about all types of data breaches have remained high since measurement begun in 2020.
- around **3 in 4 people** have become aware of the breach through news coverage, social media or through friends and family rather than through direct communication from the agency.
- support following a breach is inconsistent, with over **1 in 3 people** reporting to have received no support. This is an increase of almost 33% from the previous reporting period.
- pleasingly, the majority (**3 in 5 people**) who have received support from the NSW Government were satisfied with the outcome.

These results suggest that despite the legal requirement to notify individuals of eligible data breaches, communication of data breaches is sometimes fragmented or ineffective. Although there may be practical challenges to directly notifying people in some instances, it is essential that agencies take all reasonable steps to ensure notifications are made in a timely and effective manner. Those agencies that adopt a customer centric approach coupled with meaningful support are best positioned to maintain trust overtime.

As the scheme moves into the third year of operation, agencies should be moving beyond technical compliance and actively building a pro privacy culture that integrates privacy across all operations and workplace practices.

Sonia Minutillo

Privacy Commissioner

Information and Privacy Commission NSW

November 2026

1. What have we seen?

This Report provides insights into the trends observed during the 2024/25 reporting period.

The previous reporting period captured data for a seven-month period from the commencement of the MNDB Scheme on 23 November 2024 to 30 June 2024. This current reporting period reflects the first full year of operation of the Scheme. Data collected over the past year provides an evidence base to identify key trends, generate deeper insights and informing potential regulatory action.

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

Steady increase in notifications

An average of 10 data breach notifications per month were received, compared with an average of 7 data breach notifications per month in the first seven months of the operation of the MNDB Scheme.

The growing number of data breaches notified in the reporting period may indicate that an increased number of agencies have implemented systems and procedures to identify and assess data breaches and support compliance with their notification obligations.

Figure 1 – Number of notifications reported under the scheme

	Total number of notifications
Total received in the reporting period (1 July 2024 – 30 June 2025)	116
Total received in the previous reporting period (28 November 2023 – 30 June 2024)	52

Human error

Most data breaches notified during the reporting period were not the result of external attackers or sophisticated cyber-attacks but involved staff carrying out their daily tasks and functions.

Human error remains the leading cause of data breaches in 2024/25, with 84% of all breaches notified in the reporting period involving human error. Similar to the prior year, most human error notifications involved the accidental disclosure of personal information to an unintended recipient, for example by way of a misdirected email.

While the number of persons impacted by each human error data breach is usually small, the impacts on those individuals can nevertheless be significant.

The breaches seen across 2024/25 clearly illustrate the need to implement measures across three key areas to reduce the number and impact of human error data breaches:

- **Robust policies and procedures** – clear policies and procedures that provide structure and guidance for staff to undertake their functions, understand their obligations and how to respond if things go wrong.
- **Staff training and awareness** - provide regular, practical training about privacy, information management and data breaches. Where possible, use real-world case studies to illustrate the impact of breaches for both the agency and affected individuals. Awareness is more effective when staff can see the real consequences of breaches.
- **Technical and administrative safeguards** – review and amend the technical controls that apply to reduce inadvertent data breaches, for example agencies could consider:

- Email settings: Disable or restrict autofill, mandate use of Blind Carbon Copy (bcc) for mass broadcast mail and implement pre-send warning systems to flag external recipients or bulk sends.
- File handling policies: Ensure staff check spreadsheets for hidden data before sharing.
- Review access controls: Regularly audit access permissions on shared drives, collaboration platforms and web applications to prevent accidental disclosures.
- Testing and configuration management: Apply robust change control and testing procedures for any system that collects or processes personal information.

Employee conduct

Approximately 19% of data breaches notified in the reporting period were the result of unauthorised employee access. The majority of which related to an employee or staff member accessing personal or health information without a legitimate purpose or for purposes beyond the scope of their function or role.

Government agencies hold a special position of trust in relation to the handling of personal information of the NSW community. That trust is fundamental to the delivery of government services and the effective operation of the public sector.

Access to personal information is a privilege that exists for the purpose of undertaking government functions and providing services to the public. This privilege should not be taken for granted, misused for personal curiosity, convenience or gain. Unauthorised access to personal information can cause distress to affected individuals, undermine confidence in public institutions and expose agencies and staff to legal, regulatory and reputational consequences. Just as importantly, it can erode the culture of integrity that agencies work hard to foster.

Agencies should set clear expectations and requirements for their employees. This should be embedded in procedures and policies which clearly explain what these practices look like on an agency and operational basis. Regular training can help ensure knowledge of procedures and consequences of not following procedures remains fresh.

Creating and maintaining a strong privacy culture also requires leaders at all levels to set clear expectations about appropriate access to information, reinforce those expectations regularly and model the behaviours they expect from others. Staff should understand not only what they can access, but why those access permissions have been granted and the responsibilities that accompany them.

Cybersecurity resilience

Cybersecurity risks remain a critical concern for public sector agencies, particularly when there is a dependence on third party vendors and supply chains. Investing in cybersecurity measures and managing cyber security risks are therefore essential to the protection of personal information. This is a consistent finding of the Auditor General of NSW in reports published during the reporting period. Some of the other reoccurring findings from across all sectors include[1]:

- inconsistent adoption of cyber security policies.
- adoption of essential eight preventative measures are lower than expected.
- weak management of supply chain risks.
- weak management of cyber security spending.

[1] Auditor General for NSW (17 June 2025), Cyber security insights 2025, Audit Office of NSW, NSW Government, page 3.

- operational goals are prioritised over cyber security.
- increase frequency of phishing simulation exercises as part of cybersecurity training.

Preventing cyber security breaches or reducing cyber security threats also involve properly managing data throughout its lifecycle. Information Protection Principle (IPP) 5 establishes obligations on agencies concerning the retention and security of personal information.[2] An analysis conducted by the Audit Office of NSW, captured in the Cyber Security Insights Report 2025, showed that the least progress was made in Cyber Security NSW's Mandatory policy requirements regarding 'identification, retention, and secure disposal of data'.

There is no room for doubt that security measures are vital to protecting personal information, which means embedding privacy controls on an administrative, organisational and technical level.

Supply chain risks

Every time an agency interacts with a supplier or service provider there is an inherent risk. Suppliers or service providers can affect the security of an agency's systems and their own services. If service providers can access valuable systems, operate with privileged access or have control over a large portion of a supply chain, they may represent a weakness that could be exploited by threat actors.

The MNDB Scheme does not generally apply to contracted service providers providing services to or on behalf of government. This is because personal information held by a contracted service provider are usually 'held' by the service provider and not by a public sector agency. However, there are some circumstances where personal information in the hands of a contracted service provider will be "held" by the agency. Under section 59C of the PPIP Act, an agency is taken to 'hold' personal information if the agency is in possession or control the information. Agencies should assess their current contractual arrangements and determine whether the service provider or agency itself is the holder of personal information. Further information is available in IPC's fact sheet on data breaches and contracted service providers.

Of the 116 breaches notified in the reporting period, at least 15 (13%) involved a contracted service provider. These breaches were primarily notified from the State Government sector.

Agencies should consider risks associated with outsourcing data handling, specifically personal information, from beginning to end of an engagement with the third party. Implementing a strong risk framework with privacy at the forefront at the time of procurement and contract negotiation is likely to minimise the harm and scale of a data breach.

Adoption of Artificial Intelligence

The public sector is increasingly integrating Artificial Intelligence (AI) to streamline operations and enhance services to the public. With this comes an elevated risk associated with the collection, storage, use of disclosure of personal information. Although there were no eligible data breaches notified involving the use of Artificial Intelligence (AI) in the reporting year, the use of AI, particularly unauthorised use of generative AI, has featured in a small number of suspected data breaches.

The use of AI tools in the public sector has the potential to improve operational efficiency, support more effective decision-making and enhance service delivery that centres the customer experience and improves the outcomes and experiences of individuals and communities. However, these tools also present a range of privacy risks when used to handle personal information.

[2] Section 5, PPIP Act

To assist and support public sector agencies to understand and comply with their privacy obligations in their use and adoption of generative AI, the IPC has published a number of resources, including:

- guidance on measures and compliance considerations that agencies should action to mitigate privacy risks that may arise through the adoption of generate AI tools
- guidance on undertaking Privacy Impact Assessments (PIAs) in relation to the use of AI systems and projects.

2. Snapshot of key findings

The findings are for the period 1 July 2024 – 30 June 2025.

116
eligible data breaches notified to the Privacy Commissioner

68%
of notifications were made by the Government Sector

84%
of notifications involved human error

36%
of notifications involved malicious or criminal attack

52%
of notifications to the Privacy Commissioner were made within 30 days

65%
of breaches affected 20 or fewer individuals

3. Sector snapshot of key findings

	Government	Local Government	University	State Owned Corporation
Number of notifications	79	21	15	1
% of data breaches caused by human error	87%	81%	73%	100%
% of data breaches caused by a criminal or malicious attack	38%	35%	40%	0%
Number of affected individuals	65,093	6,341	523,637	1
% of data breaches discovered within 10 days of occurrence	9%	38%	33%	100%
% of data breaches where assessment was completed within 30 days of discovery	41%	76%	73%	0%

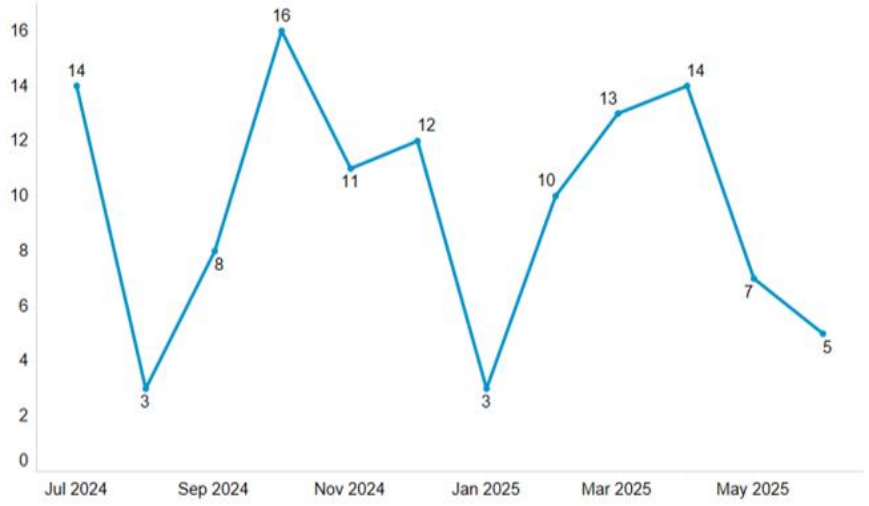
4. Analysis of key findings

4.1 Number of notifications

Number of notifications received

116 eligible data breaches were notified during the reporting period. In the prior seven-month reporting period, 52 notifications were received. The highest number of reported data breaches occurred in October 2024, with 16 notifications – the most reported since the scheme's inception. The lowest number of data breaches (3) occurred in August 2024 and Jan 2025, which remain consistent with the prior period.

Figure 2 – Number of notifications per month



Notifications by breach type

Figure 3 – Number of notifications by type of data breach

Type of Breach	Count
Unauthorised disclosure	66
Unauthorised access	36
Loss of personal information	13
Other	1

57% of breaches notified during the reporting period related to unauthorised disclosure of personal information, whilst 31% related to unauthorised access and 11% related to loss of personal information. In the prior year, the majority of breaches related to unauthorised disclosure (71%), however the number of breaches that is a result of unauthorised access (21%) has grown. Data breach notifications involving unauthorised access in this reporting period included where:

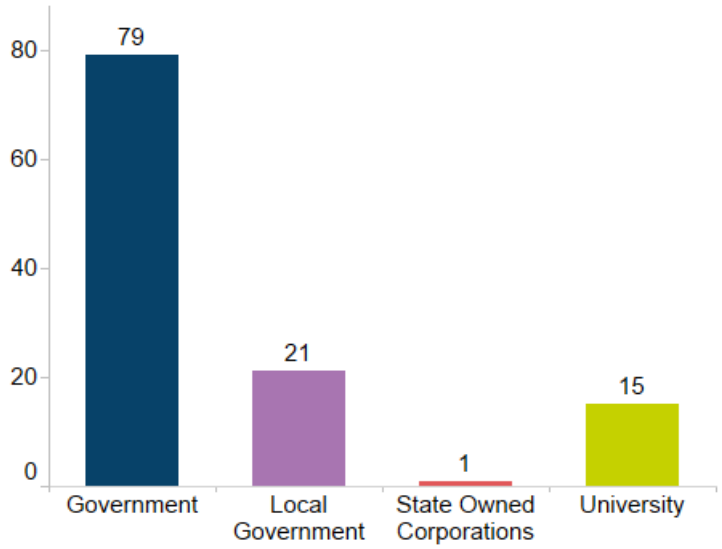
- an employee was the target of a phishing attack.
- an employee accessed sensitive information unrelated to their role.
- a threat actor obtained access to agency systems.

Further analysis on the above is detailed in section 4.2.

Notification by sector

Consistent with the prior period, the majority of notifications were received from the Government sector (68%), followed by the Local Government (18%) and University sectors (13%). This result is proportionate to the size of the Government sector in comparison to the other regulated sectors. One notification was received from the State Owned Corporation sector (SOC).

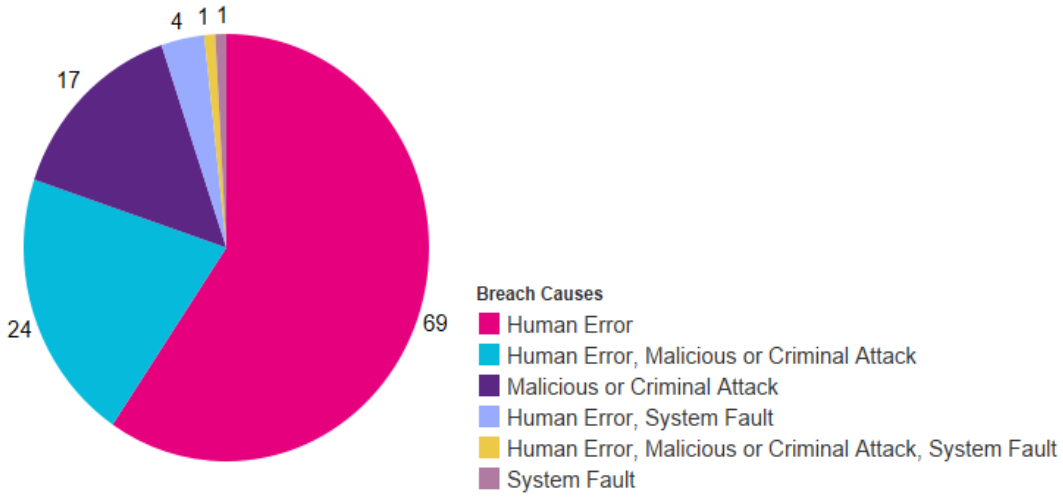
Figure 4 – Number of notifications by sector



4.2 Causes of data breaches

In the reporting period, the cause of the majority of data breaches was human error, (84%), followed by malicious or criminal attack (36%), and system fault (5%). This finding is consistent with the trend identified in the prior year where 79% of notifications involved a human error cause.

Figure 5 – Number of notifications by cause of breach

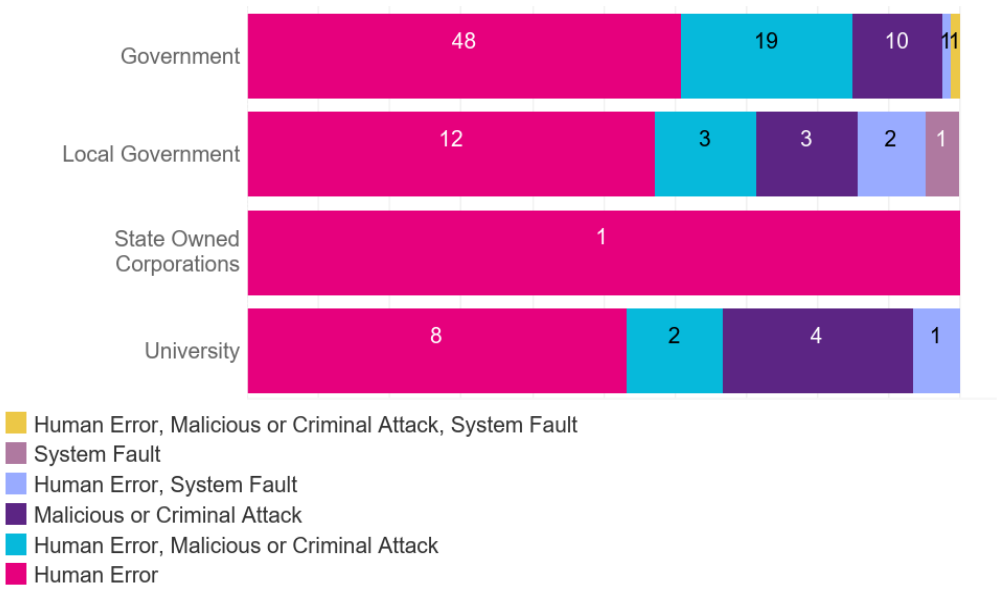


A key theme across the majority of notifications is that humans are centrally involved in most data breaches, whether it's a direct human error such as inadvertently sending an email containing personal information to an unauthorised recipient, or a cyber incident involving human compromise.

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

Causes by sector

Figure 6 – Number of notifications by cause of breach per sector



As shown in figure 6, human error remains the main cause of breaches notified by each sector, followed by criminal or malicious attack.

In the Government sector:

- 87% of notifications involved human error, a moderate increase from 79% recorded in the prior period.
- 38% of notifications involved criminal or malicious attack, a moderate increase from 26% reported in the prior period.
- 3% of notifications involved a system fault.

In the Local Government sector:

- 81% of notifications involved human error, consistent with 78% reported in prior period.
- 35% of notifications involved a criminal or malicious attack, a moderate increase from 22% reported in prior year.
- 14% of notifications involved a system fault, consistent with the 11% reported in prior period.

In the University sector:

- 73% of notifications involved human error, consistent with 78% reported in prior year.
- 40% of notifications involved a criminal or malicious attack, consistent with 44% reported in prior year.

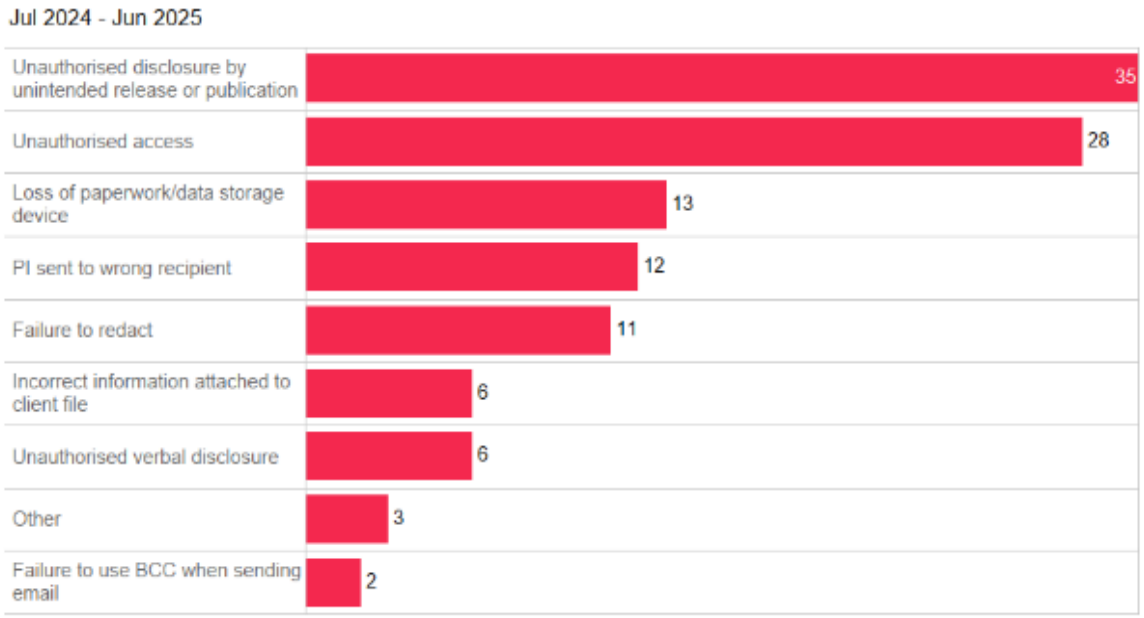
- 7% of notifications involved a system fault, consistent with the 11% reported in prior year.

Human error

The top three causes of human error data breaches were:

- unauthorised disclosure by unintended release of publication (30%)
- unauthorised access (28%
- loss of paperwork/data storage device (11%).

Figure 7 – Number of notifications by cause of breach (Human Error)



Similar to the prior reporting period, the most frequent type of human error breach was unauthorised disclosure by unintended release or publication of data. However, the data also indicates a growing number of breaches as a result of unauthorised access.

This is a common theme internationally. The UK Information Commissioner's Office (the ICO) reported in their 2025 financial year dashboard[3]:

- 76% of data breach incidents were related to non cyber causes
- the main non cyber incidents were emailing data to an incorrect recipient, phishing and unauthorised access.

The Office of the Privacy Commissioner of Canada (the OPC) reported in their annual report 2024–25 that of the breaches reported by the Federal Government, mishandling of information (e.g. data entry error, misdirected correspondence, labelling error) was the main cause of breaches, followed by cyber incidents and employee misconduct[4].

Section 12 of the PIPP Act provides that an agency must ensure that personal information is protected by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification to information or disclosure and all other misuse.

[3] UK Information Commissioner's Office, Data Security Incident Trends Dashboard

[4] Privacy Commissioner of Canda (5 June 2025), Prioritising Privacy in a Data Driven World, Office of the Privacy Commissioner of Canada, page 30.

Although unauthorised access may reflect the actions and intent of an individual, the responsibility and accountability for protecting personal information ultimately rests with the agency. This starts with embedding a culture of privacy, by establishing clear expectations and requirements for employees. This should be captured and documented in privacy policies, which re-enforce the importance of respecting privacy, and outline the consequences of not complying with privacy obligations. It should also be accompanied by periodic reminders, and training of employees, particularly those who have direct access to personal or health information.

Agencies should ensure employee access to information is restricted and commensurate with their role. Agencies should monitor and audit access logs to proactively detect unauthorised access and reactively investigate incidents. When staff have the knowledge and are reminded of the repercussions of accessing information that is not aligned with the requirements of the role, this will reduce incidents based on impulsiveness, misunderstanding or curiosity.

Case study – Employee use of shadow IT tools

An employee uploaded personal information to an unauthorised generative AI tool. The data uploaded included the individual's name, address, date of birth, contact information, driver's licence and signature.

This case demonstrates the following privacy risks:

- unauthorised use and disclosure of personal information which may be inconsistent with the agency's purpose of collection.
- unauthorised use and disclosure of personal information leading to a data breach which exposes individuals to serious harm such as identity theft.
- inability to completely erase content the tool has digested leading to extended retention of personal information by the provider.

This is a reminder that employees should only use approved agency tools.

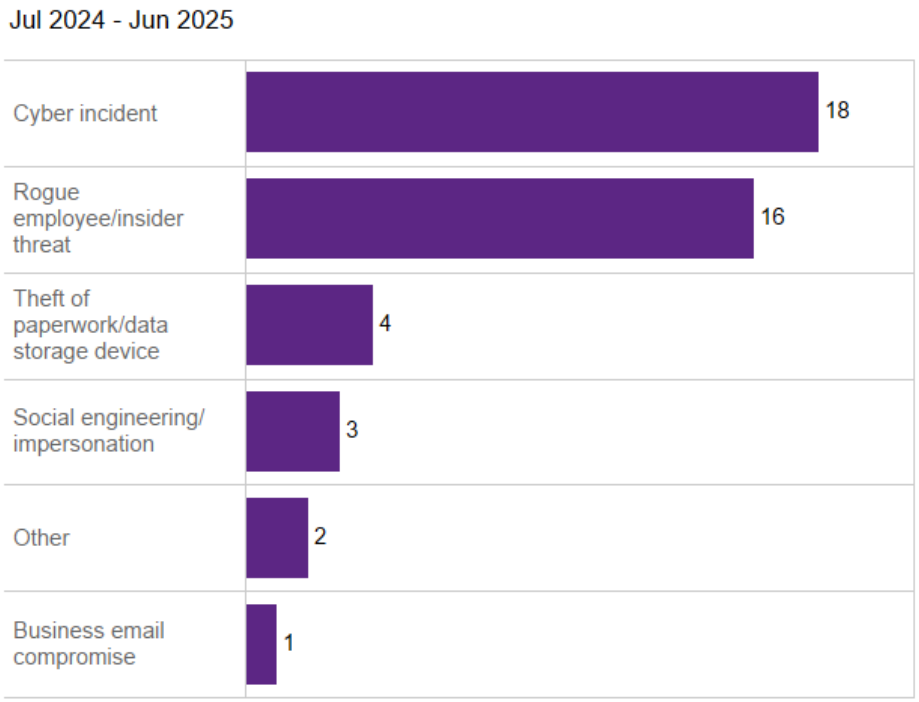
Individual employees may seek to adopt shadow IT tools to increase productivity, convenience or efficiency gains. These tools may be used because the individual felt it offered better functionality than the alternative presented by the agency. The use of the tools may seem harmless such as an employee sending a government document through an unsanctioned file sharing platform to another employee or agency. However, as the shadow IT tool is not authorised or monitored by the agency's IT team, this may expose the agency to privacy and security risks.

Agencies should be clear and specific about the use of shadow tools within their environments. Any authorised use of AI should be supported by a clear and comprehensive governance framework or policy that clearly sets the boundaries of acceptable use and approval processes for employee use of tools including generative AI tools at work. Complementary procedures should cover, or be updated to address, issues arising from potential noncompliance or breaches.

For further information refer to the IPC's Guide Privacy risks associated with the use of generative AI tools Guide.

Malicious or criminal attack

Figure 8 – Number of notifications by cause of breach (Malicious or Criminal Attack)



Similar to the results of the prior period, most breaches caused by malicious or criminal attack during the reporting period was a breach involving a cyber incident (41% in 2024/25 compared to 87% in the prior period). This is closely followed up by rogue employee or insider threat (36%).

Cyber incidents

Most cyber incidents in this reporting period involved phishing (33% or 6 notifications) and hacking (28% or 5 notifications).

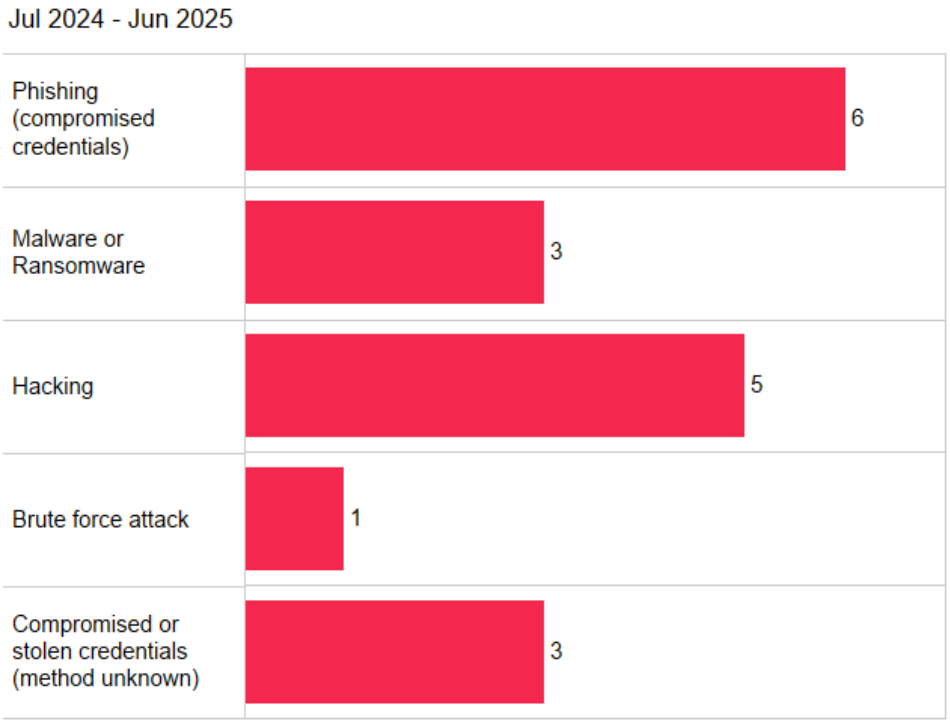
Phishing attacks being the leading cause of cyber incidents are consistent with reports nationally. The Office of the Australian Information Commissioner (OAIC) reported for 2024-2025, that 32% of all cyber incidents involved phishing attacks. Whilst in 2023–24, 30% of cyber incident breaches involved phishing attacks[5].

An increase in phishing attacks is observed despite continuing cyber security training and awareness efforts. This may be driven by multiple factors:

- growing sophistication of phishing attacks,
- persistent influence of human error,
- improvement in detection of attacks, and reporting processes due to expansion and accessibility to digital tools.

[5] Office of the Australian Information Commissioner, Notifiable Data Breach statistics dashboard

Figure 9 – Cyber incidents breakdown



Case study – Data breaches involving contracted service providers (CSP)

An agency notified a data breach involving a CSP engaged to provide services to the public on the agency's behalf.

The CSP advised the agency that it had been notified of a data breach by its IT service provider. As a result of the breach the CSP's email system had been compromised, and an unknown individual had obtained access to client files.

The agency advised that it had experienced delays in obtaining information from the CSP and that it had only limited information concerning:

- the sequence of events resulting in the data breach occurring
- the remediations being adopted by the CSP and IT service provider
- the number of individuals who were affected by the breach.

The contract between the CSP and the agency required the CSP to comply with the NSW information protection principles but did not include provisions regarding the management of data breaches.

The CSP disagreed with the agency's assessment of the data breach and objected to the CSP making notifications to the affected individuals. The agency and the CSP eventually reached agreement on these matters and notifications were made by the agency to affected individuals. However, the utility of the notifications in enabling individuals to take steps to protect their personal information was reduced (or impacted?) due to the time between the breach occurring and the notifications being made.

Learnings

Agencies should ensure their procurement contracts contain explicit provisions concerning notification of data breach occurring, how data breaches will be managed, including detailing the relevant responsibilities of the parties and an obligation to provide the agency with access to sufficient information to undertake a data breach assessment. Agencies should also maintain a data asset register that details the scope, nature, location of the data accessed or provided to its CSPs.

Agencies should undertake an adequate level of privacy due diligence prior to entering contracts with a CSP. An agency should take the necessary steps to satisfy itself as to the maturity of the CSP's privacy governance and adequacy of its data breach policy and response plans.

Employee Conduct - Rogue employee/insider threat

The data shows there's been an increase in notifications that is attributed to rogue employees and insider threats in the reporting period. Of these cases the majority were related to unauthorised access. A review of the cases involving unauthorised access caused by rogue employee or insider threats indicates these breaches were related to:

- accessing information that is unrelated to the employee's role
- accessing information to which an employee has legitimate access for personal reasons.

Although these notifications were assigned as a malicious or criminal attack, there is also a human factor to these breaches that is incompatible with acceptable employee conduct. This is consistent with data breaches on a national level, with the OAIC reporting in their 2025 dashboard, that the health sector contained the most breaches involving rogue employee/insider threat[6].

[6] Office of the Australian Information Commissioner, Notifiable Data Breach statistics dashboard

This reinforces the need to not only uphold good governance through adopting policies, and delivery of privacy training but highlights the importance of promoting and embedding a pro privacy culture from top down.

Good practice tips – Performing a root cause analysis

The IPC has observed that agencies are assigning both "human error" and "malicious or criminal attack" as the cause of a breach that is attributed to unauthorised employee conduct. It is important to note that human error, which generally involves accidental or inadvertent actions, is distinguishable from conduct that is deliberate and intentional.

While both causes may be a contributing factor in some incidents, it is still important that agencies perform a root cause analysis to detect the primary or leading cause of the breach. This is critical as it enables agencies to:

- implement targeted and effective remediation measures.
- address systemic issues rather than surface level symptom.
- reduce the likelihood of similar incidents occurring in the future.

When preparing a data breach notification, agencies should refer to the Glossary (prepared by the IPC) and carefully consider which category best reflects the root cause of the incident.

Where there are breaches that involve multiple contributing factors, the agency should identify and notify the primary contributing cause of the breach. Agencies should also distinguish between human error that arises from an accident or mistake and conduct which involves a deliberate and intentional action by an employee to access and/or disclose information that there is no lawful or legitimate purpose to have accessed or disclosed.

System fault

In the current period, 5% (or 6 notifications) of all breaches involved a system fault. There were only 2 notifications received during the prior reporting period. The data is not sufficient to draw insights concerning this category of data breach.

Case Study – Insider threat

Example 1

A senior employee accessed personal information without authorisation. The unauthorised access was identified through a periodic audit. The audit identified that the employee accessed health information of individuals in its record's system. Further investigation found that the employee accessed this information simply out of curiosity.

Although the systems access assigned to the senior employee was appropriate, this case stresses the importance of safeguarding against access of personal information that has no function or purpose to an employee's role and work. It is important to put in place regular role-based training and knowledge-based testing to ensure employees are aware of the seriousness and the consequences of accessing personal information without function or purpose.

This case additionally highlights the necessity of performing regular proactive audits on access logs to deter and detect inappropriate access to personal information. Any anomalies identified should be investigated immediately and timely corrective action should be implemented to prevent reoccurrence.

Example 2

An employee circumvented system controls to facilitate access to records without authorisation and for their own purposes unrelated to their role. Furthermore, the employee had printed the accessed materials and left these materials in an area that was accessible to other staff.

This case highlights the importance of establishing effective controls that protect against unauthorised access or disclosure of personal information. This means:

- having an up-to-date access control policy including a process to establish and maintain employee access privileges. Access must be kept to a minimum required for an employee to perform their responsibilities.
- periodic review of access logs to ensure access is appropriate and commensurate with roles and responsibilities. Agencies should understand baseline access patterns to identify anomalies and report findings including corrective actions to leadership.

4.3 Type of personal information involved

Figure 10 shows the number of notifications by type of personal information. The total number in figure 10 will not equal the total notifications reported in section 5.1. This is because some notifications involved more than one type of personal information.

Consistent with the previous report, contact information was the most common type of personal information involved in data breaches (72%) in 2024/25 compared with 69% in the previous period. This category includes information such as name, residential address, phone number or email address.

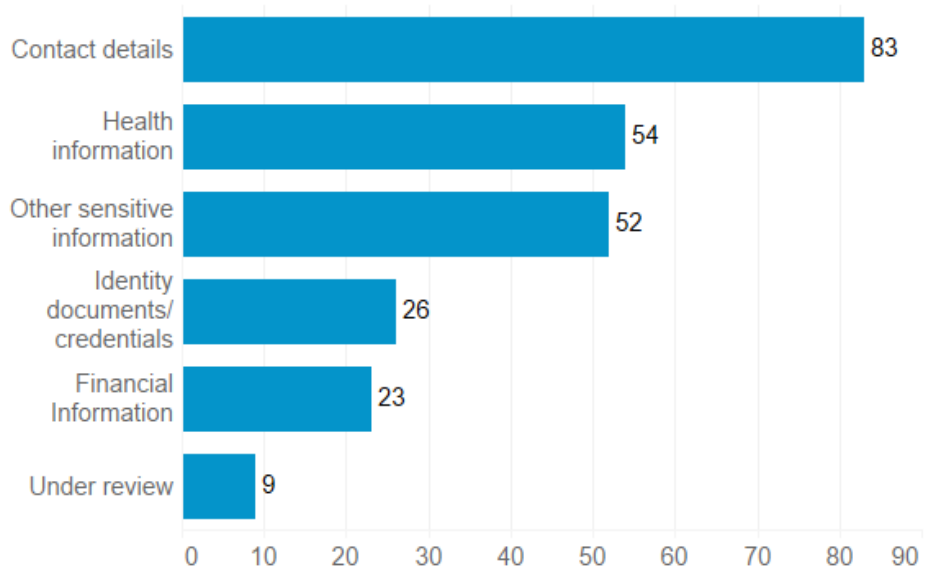
Following contact information, the other major breaches include:

- Health information (47%) a moderate increase from the 37% reported in prior period.
- Other sensitive information (45%), consistent with the 42% reported in prior period.
- Identity documents/credentials (22%), a moderate decrease from the 29% reported in prior period.

This data is consistent with data reported at the national level, with the OAIC reporting that contact information was the leading type of personal information involved in a breach during 2024/25[7].

The consequences of a breach involving contact information may not be as immediate as a breach involving financial or identity information, however it creates a gateway to other follow up attacks such as social engineering and personalised phishing attacks. This is a trend noted by IDCARE who reported that following major data breaches, scammers are using leaked personal information to tailor attacks and increase believability of their communications[8].

Figure 10 – 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 is revised following updates to the Privacy Commissioner as the agency completes its investigation.

4.4 Impacts of breach

Number of individuals affected by eligible data breach

Eligible data breaches notified during this reporting period affected 595,072 individuals.

This represents a significant increase from the 71,178 affected individuals reported in the prior period. This increase is attributed to two factors:

- the prior period did not represent a full 12 months; and
- more significantly, the increase was driven by one large scale breach in the University sector.

The majority of breaches reported in all sectors (65%) impacted ten or fewer individuals. Most of the breaches reported which impacted ten or fewer individuals arose from the Government Sector (50%). This is consistent with the previous reporting period.

[7] Office of the Australian Information Commissioner, Notifiable Data Breach statistics dashboard

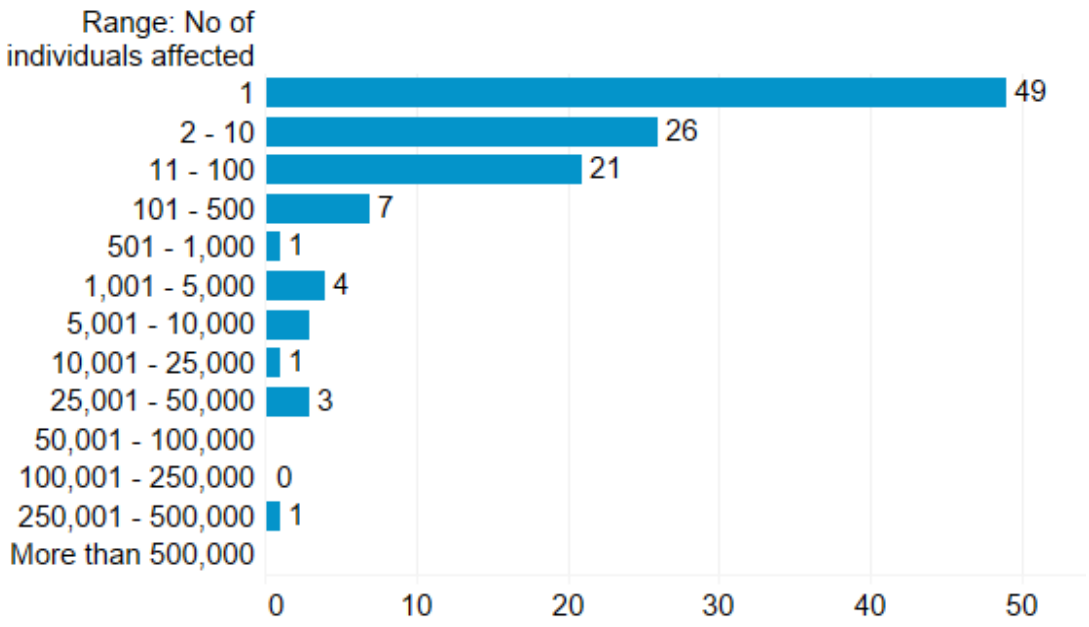
[8] IDCARE, "looking back at 2025 and what's next" newsletter

In the reporting period, only one notification was recorded where impacted individuals were between 250,001-500,000 individuals. To date this is the largest reported data breach impacting individuals under the MNDB Scheme.

This trend of observing a smaller number of large-scale breaches with a high number of affected individuals is consistent with trends observed at the national level.[9]

The findings in this section of the report, are consistent with the findings at section 4.2 concerning the cause of data breaches. Gaps in operational practices and procedures may be contributing to smaller scale breaches and re-enforces the need to embed stronger practices at an operational level for governing and protecting information.

Figure 11 – Notifications by number of individuals affected



[9] Office of the Australian Information Commissioner, Notifiable Data Breach statistics dashboard

Good practice tip – Supporting individuals after a breach

In the NSW Community Attitudes Survey towards Privacy 2026, the public reported inconsistencies in the provision of support to individuals following a data breach. This means individuals that use the services of an agency may lose confidence or trust in the agency to hold and protect personal information. It may amplify the reputational damage caused by the data breach and can worsen public perception of the public sector.

Responsibility does not end when a data breach is resolved. It extends to how an agency responds and manages the breach. Strong remediation shows the public and those impacted that the agency is committed to supporting affected individuals and safeguarding personal information. This is supported by the survey results which show that majority of those who have received support from the relevant agency were satisfied with the results.

To best support those affected by a breach:

Take a people first approach – Remember that depending on the size or nature of a data breach, consequences for individuals can be significant. Keeping affected individuals front of mind throughout the process can lead to better outcomes for them and your agency.

Communicate and notify – As soon as practicable, take reasonable steps to notify affected individuals (unless an exemption applies). If an agency is unable to directly notify any or all affected individuals, the agency must issue and publicise a public notification.

Provide clear messages – provide affected individuals with clear information on what has occurred, the type of personal information affected, any actions agency is taking in response to the breach and how the individual can contact the agency for further information.

Offer practical support – Mitigation should focus on steps that genuinely help affected people protect themselves. This may include guidance on securing accounts, replacing compromised information, or offering tailored advice for those at higher risk. Where relevant this may also include providing information on support services the individual can access for further assistance

Notify transparently – Timely and easy to understand notifications help individuals act quickly. Clear communication demonstrates accountability and reinforces confidence in your breach response.

Number of individuals affected by an eligible data breach by sector

Figure 12 below sets out the number of individuals affected by data breaches during this period across different sectors.

Government sector

73% of breaches notified by the Government sector impacted 10 or fewer individuals during this reporting period. This is a moderate decrease compared to prior period. Most data breaches observed in this sector was a result of human error relating to poor email hygiene, therefore the number of individuals impacted are expected to be low.

Local Government sector

76% of breaches notified by the Local Government sector impacted 100 or fewer individuals. This trend is consistent with the prior period. Of the 21 notifications in this sector:

- 8% of breaches impacted 10 or fewer individuals
- 33% of breached impacted 11-100 individuals.

Consistent with the prior period, the main cause for breaches was human error.

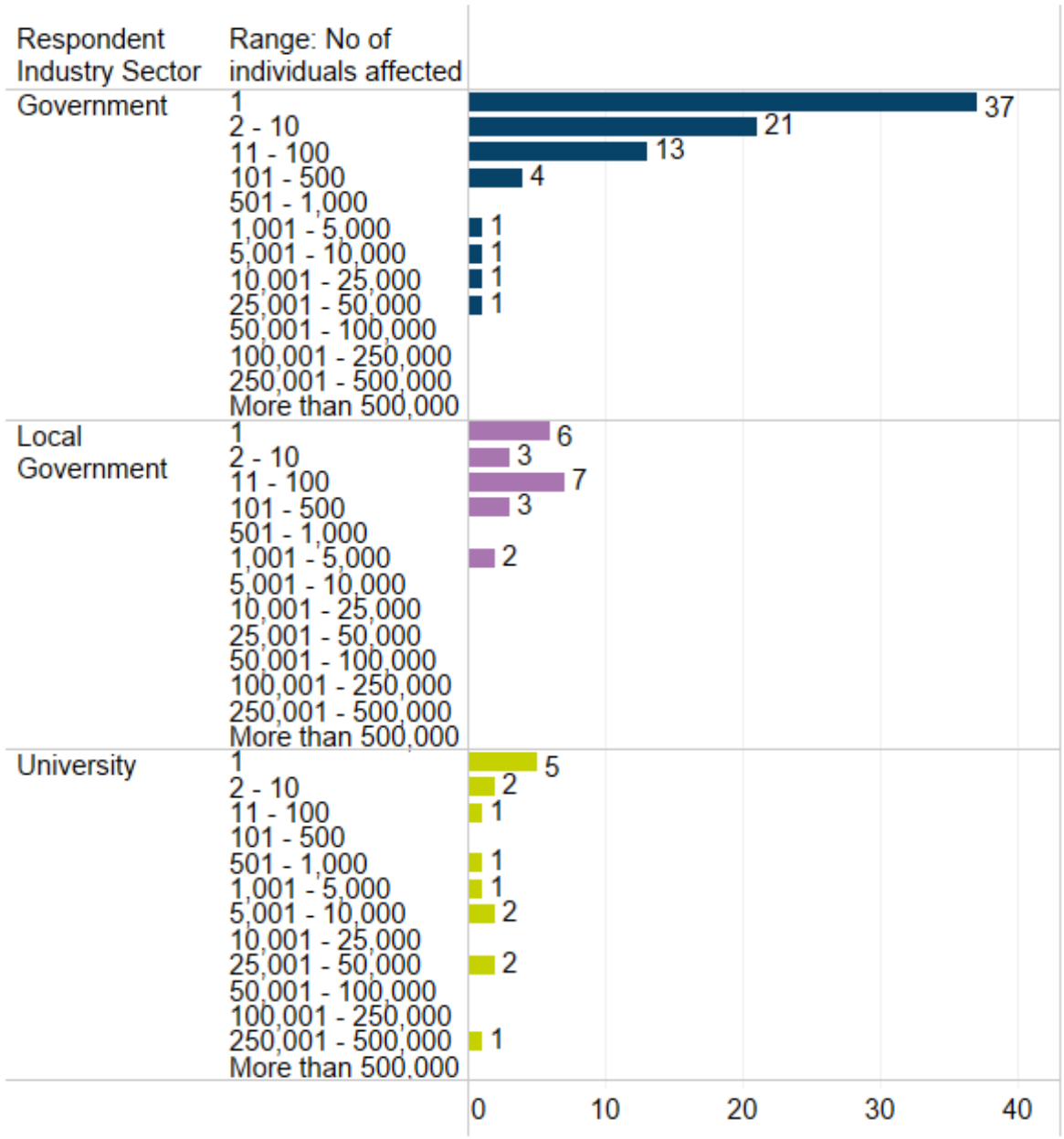
University sector

This sector has recorded most of the larger scale data breaches in this reporting period which is a similar trend to the prior period. One notification impacted 250,001-500,000 individuals. This is reported as the largest wide scale breach impacting the most individuals since the inception of the scheme.

State Owned Corporations sector

Figure 12 does not show results from the State Owned Corporation sector as only one notification was reported which impacted one individual.

Figure 12 – Number of individuals affected by sector



Case Study – Systems and Practices

Human error is the leading cause of data breaches. The data illustrates that strong systems can easily be undermined by inconsistent staff practices. It is important that staff undergo regular training that is just in time, role based and not reactive, so that staff are reminded of correct procedures when it matters the most. A small error that may be inadvertent in nature could have the ability to impact a high volume of individuals. The case below demonstrates the importance of layering security controls to avoid a single point of failure.

Example

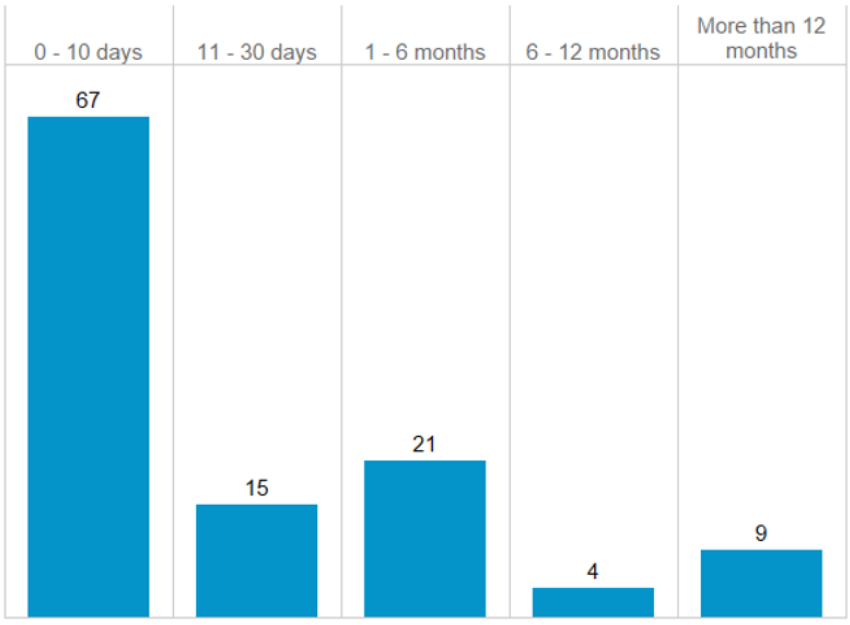
During a large event, a printed list of data containing personal information of over 30,000 people went unaccounted for and misplaced. The data set is recognised as one of the most important data sets held by this agency. In response, the agency:

- improved scanning in and scanning out of materials from manager and office
- reviewed procedures, roles and responsibility for packing materials in venues and return of materials to managers
- reviewed officer training and procedures around escalation.

4.5 Timeframes

Time taken to identify data breaches

Figure 13 – Number of days between breach occurring and breach discovered



Over half of all data breaches (58%) were identified within 10 days of occurring, compared to 67% in the prior period. 13% were identified within 11-30 days, whilst 18% were identified within 6 months. This suggests that the majority of breaches were discovered rapidly, which is a positive result considering timely action is important for mitigating the harm caused by data breaches. The OAIC has reported a similar trend, whereby on average 55% of breaches were discovered within ten days of the breach occurring during 2024/25[10].

[10] Office of the Australian Information Commissioner, Notifiable Data Breach statistics dashboard

During the reporting period 29% of breaches were discovered over 30 days of the breach occurring, which is the same result reported by the OAIC during 2024/25 (29%). The reporting period result is also consistent with the prior period, where 28% of data breaches were discovered over 30 days of the breach occurring.

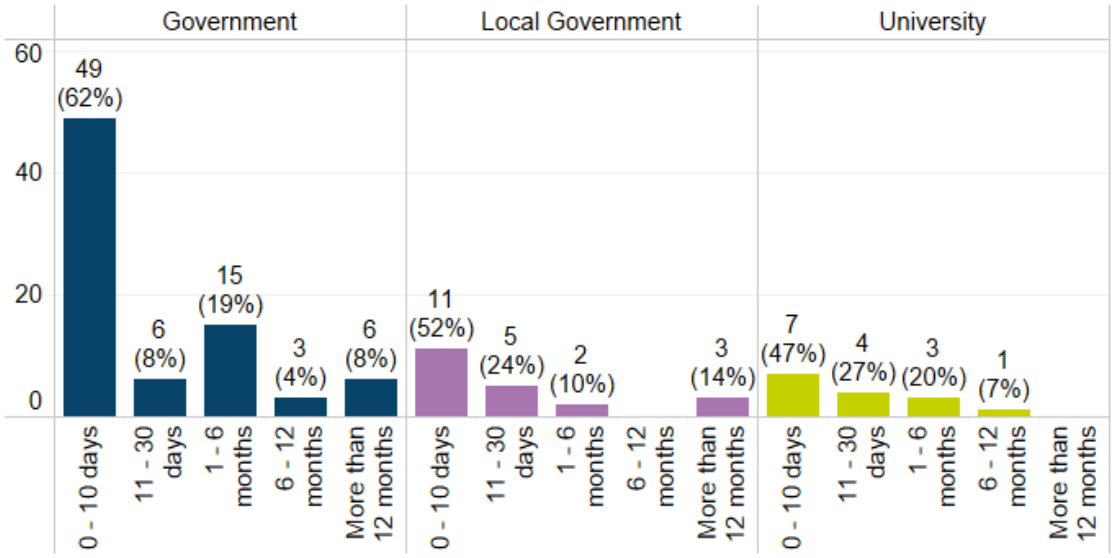
Time taken to identify data breaches by sector

The majority of breaches in all sectors were identified in 10 days or less of the breach occurring:

- Government sector – 62% (a moderate decrease from 71% reported in prior period)
- Local Government sector – 52% (a significant decrease from the 78% reported in prior period)
- University sector – 47% (no change from the 47% reported in prior period).

Human error is the leading cause in each of these sectors. The time to identify human error after it has occurred is typically immediate, or within a short period of time, compared to a cyber or malicious attack. As noted above, this report has observed an increase in cyber-attacks compared to the prior period particularly from the Government and Council sector, which may account for the decrease in identifying breaches within ten days or less of the breach occurring.

Table 14 – Number of days between breach occurring and breach discovered by sector



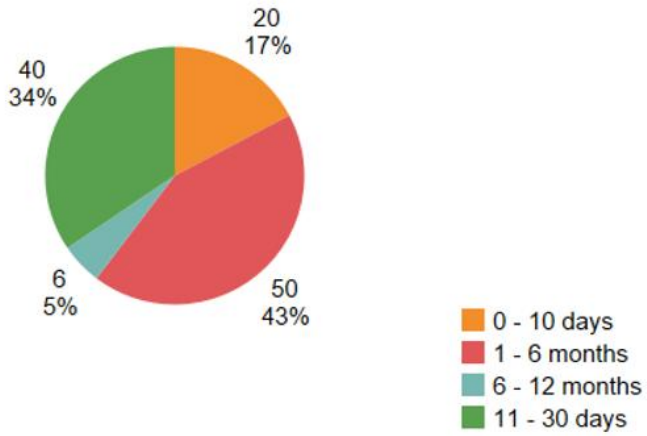
Time taken to notify the Privacy Commissioner

Section 59E of the PIPP Act requires an agency to carry out an assessment of whether a data breach is an eligible data breach within 30 calendar days after the agency becomes aware of a breach occurring.

52% of agencies notified within 30 days of becoming aware of a data breach. The result is consistent with the increase seen in cyber incidents, which traditionally takes a longer time to assess compared to human error causes such as a misdirected email.

48% of agencies notified of an eligible data breach after 30 days of becoming aware of a data breach. This likely reflects agencies' use of section 59K to extend the assessment period where it was not reasonably possible to complete it within the 30 days. Section 59K provide that the head of an agency may approve an extension of the assessment period where satisfied that an assessment cannot reasonably be completed within 30 days.

Table 15 – Number of days between breach discovered and Privacy Commissioner notified



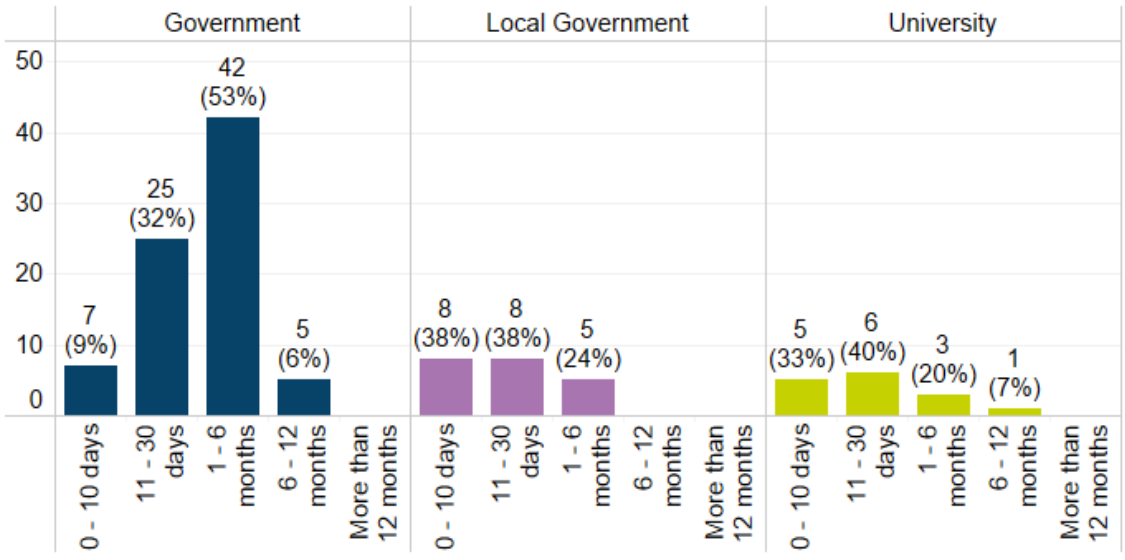
Time taken to notify the Privacy Commissioner by sector

In the Government sector 41% of notifications were made within 30 days, whilst the remaining 59% of notifications reported the data breach to the Privacy Commissioner after 30 days of the data breach discovery.

Whilst, in the local government sector 76% of the notifications were made within 30 days of becoming aware of the data breach.

In the University sector, 73% of the notifications were made within 30 days of becoming aware of the data breach.

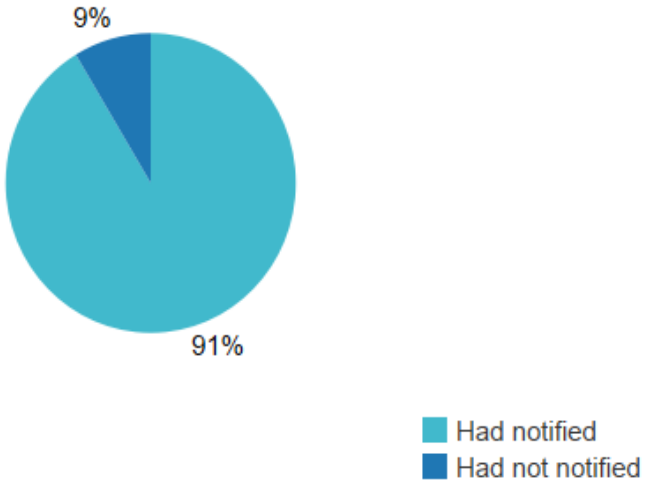
Table 16 – Notifications grouped by days between breach discovered and Privacy Commissioner notified by sector



Timing of notifications made to affected individuals

Figure 17 shows 91% of agencies notified affected individuals before making a notification to the Privacy Commissioner, a moderate increase from the 85% reported in prior period.

Figure 17 – Percentages of agencies that had notified affected individuals



5. Abbreviations

Acronyms or abbreviation	Explanation
ICO	Information Commissioner's Office (UK)
OPC	Privacy Commissioner of Canada
IPC	Information Privacy Commission
OAIC	Office of the Australian Information Commissioner
PIPP Act	*Privacy and Personal Information Protection Act 1988*
HIRP Act	*Health Records and Information Privacy Act 2002*

6. Glossary

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 or other government issued identifier.
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 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.
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.
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

Information and Privacy Commission NSW
T 1800 IPC NSW (1800 472 679)
www.ipc.nsw.gov.au

Information and Privacy Commission NSW