Key Insights from the OAIC's 2024 Half-Year Report

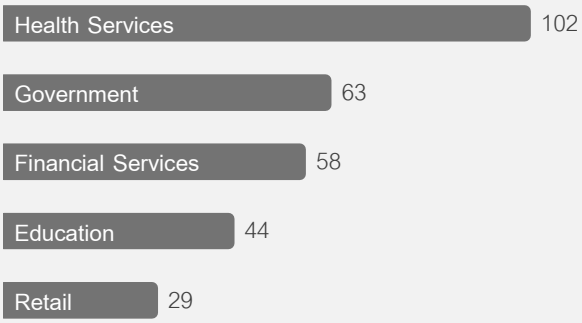
Who is the OAIC?

The Office of the Australian Information Commissioner (OAIC) is an independent national regulator whose purpose is to promote and uphold individuals' rights to privacy under the *Privacy Act 1988* and information under the *Freedom of Information Act 1982*.

What are Notifiable Data Breaches?

Under the aforementioned legislation, organisations and agencies are required to inform the affected individuals and the OAIC if a data breach is likely to result in serious harm to anyone whose personal information is involved.

Top Five Sectors to Notify of a Data Breach (Jan-Jun, 2024)



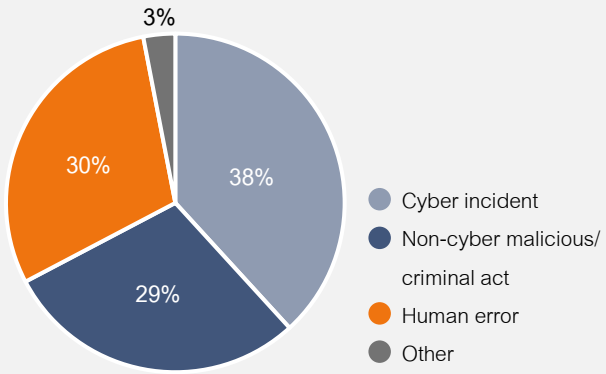
Data Breaches in FY2024

1010
notifications in FY2024

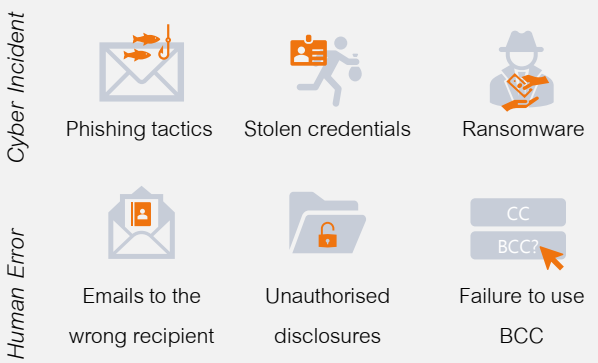
11%
From **906 notifications** in FY2023

2024 statistics indicate a notable **9%** increase in notifications from January to June, highlighting a significant upward trend during this latest 6-month period.

Key Sources of Data Breaches



Breakdown of Causes



How to strengthen your organisation against a data breach

The OAIC issued a report this year, outlining six key themes and recommendations for public and private organisations to strategically safeguard personal information. The below outlines Amstelveen's view of the key Preventative, Detective and Corrective controls that help protect organisations against common themes that can compromise personal information.

	Mitigating Cyber Threats	Extended Supply Chain Risk	Addressing the Human Factor
Preventative	Adopt the **Principle of Least Privilege**. Provide users the minimum level of permissions to perform their roles.	Execute **secondary approvals for critical transactions** with suppliers within well-defined rules on data sharing requirements.	Regularly **train staff on the latest tactics** used by threat actors, spotting sophisticated phishing attempts.
Detective	**Invest in tools** that help identify data breaches such as e-mail filtering when sensitive documents are attached.	**Carry out audits** on a regular cadence to test compliance with security standards and contractual obligations.	Establish **monitoring tools and thresholds** for potentially malicious activities like large data transfers.
Corrective	Review and **minimise the scope of personal information** required to complete a process/service, reducing the retention period.	Maintain **incident response plans** that include steps to deal with breaches involving third-parties.	Recognise human error is not always preventable – implement robust **backup and recovery processes**.

	Misconfiguration of Cloud-based Data Holdings	Relevance of a Threat Actor's Motivation	Lessons Learnt in Australian Government
Preventative	Require **multi-factor authentication** for administrative access, remote network access and any high-risk activities.	Automate **deprovisioning access immediately** upon termination, rights revocation, or role change of a user.	Complete a **privacy impact assessment** for new projects to consider privacy risks early.
Detective	Ensure **users and information assets are uniquely identified**, so activity can be logged against individuals.	Develop a **penetration testing program** (authorised simulation of attacks to evaluate system vulnerabilities).	Delineate programs for **general and privileged user access reviews**, so permissions are based on duties.
Corrective	Include **contractual obligations through Service-Level Agreements** (SLAs) relating to performance expectations and outages.	Create **supplementary crisis management documents** like tactical procedures and playbooks e.g. for ransom payments.	Establish end-to-end **escalation protocols** in incident response plans with distinct handover points.

Data breaches are only increasing in frequency, complexity and impact for organisations of all sizes and sectors. A proactive risk management approach is therefore crucial to guide resilient cyber security to keep personal and confidential information safe. Amstelveen is well positioned to support clients prepare themselves against data breaches, with extensive experience in the development and assessment of preventative, detective and corrective controls. Contact us at info@amstelveen.com to discuss how we can help.

References

OAIC. (2024). *Notifiable Data Breaches Report: January to June 2024. Available at:* https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2024 (Accessed: October 2024)

Amstelveen

Amstelveen equips organisations to identify, assess and mitigate their most significant risks. Our risk, compliance and technology professionals support clients to improve the governance of their organisations. We provide specialist support to the largest public and private organisations in Australia and New Zealand.