Cyber incidents continue to embarrass

No week goes by without news about data discovered on the dark web pointing to a data breach by an Australian organisation. Recent data breaches serve as a reminder of major cybersecurity risks such as social engineering[1] and supply chain risks.[2] Perhaps rare but topical is the risk of unprotected public websites and APIs connecting to a database without layer security or an authentication requirement;[3] a rather critical oversight.

Australian businesses are being targeted by cyber criminals. Outsourcing, offshoring and digital transformation projects including the use of modern technologies such as artificial intelligence (**AI**) can give rise to information security risks which can be too great to handle even for well-resourced companies. Unfortunately, whenever a weakness in their defences is discovered by cyber criminals, Australian corporations suffer embarrassment in the press and in the boardroom.

Following data privacy reforms[4] which increased civil penalties for privacy interference and reduced the trigger thresholds, we expect to see more enforcement action going forward. The regulator's recent announcement about initiating civil penalty proceedings against Optus for its 2022 data breach,[5] which was the third largest in Australia, signals movement on the regulators to-do list.

What information security is required by law?

Organisations must take such steps as are reasonable in the circumstances to protect personal information. Following the recent data privacy reform, such steps include an obligation to implement technical and organisational information security measures.

Admittedly, the Privacy Act 1988 (Cth) only says as much as three sentences about this (which are repeated for credit information), but the actual legal requirements are dictated by good industry practice, which is reflected in various technical standards, the Guide to securing personal information[6] by the Office of the Australian Information Commissioner (**OAIC**) and other materials.

For example, supply chain information security risk is a complex area of compliance underpinned by complex risk mitigation practices. Some high-level compliance strategies to address supply chain risk could include, among others:

- Robust supply chain risk management framework that is operated by competent professionals with assigned responsibilities.
- Comprehensive due diligence on each service provider's information security maturity based on pre-determined criteria and consistent remediation requirements. Reviewing ISO 27001:2022[7] or SOC 2®[8] certificates alone will not be enough without further scrutiny.

[1] 19% of reports to the OAIC from July – December 2024 (link).
[2] Data breach report highlights supply chain risks (report for the period from July to December 2023), 22 February 2024 (link).
[3] Optus: How a massive data breach has exposed Australia, BBC, 29 September 2022 (link).
[4] Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022 (Cth) and Privacy and Other Legislation Amendment Act 2024 (Cth).
[5] Australian Information Commissioner takes civil penalty action against Optus, 8 August 2025 (link).
[6] Guide to securing personal information, updated 11 December 2024 (link).
[7] Information security, cybersecurity and privacy protection — Information security management systems — Requirements, International Organization for Standardization (ISO).
[8] Systems and Organization Controls 2, Association of International Certified Professional Accountants.

- Regular and effective information security audits best facilitated by a sophisticated Business System Control Assessment (BSCA) tool.
- Investigating and understanding the service provider's own supply chain (fourth-party) risk through a software bill of materials (SBOM) and vendor list.
- Secure data sharing protocols including cryptographic controls with at least TLS 1.3 for data in transit and AES-256 for data at rest, key rotation policies and secure key management.
- Service provider's access to personal information limited to what is necessary for its specific tasks, subject to least privilege - no one person should have sufficient privileges (and technical ability) to access and export large quantities data.
- Zero Trust Architecture (ZTA) principles implemented across supply chain, multifactor authentication, managed devices with Endpoint Detection and Response (EDR) solutions, and logging and monitoring.
- Only reliable and appropriately trained personnel should have access to data. Staff should be vetted, as is appropriate and lawful. Staff training should cover common risk of human error, including regular phishing simulations and preventing other risk of AI-enhanced infiltration attempts.
- Micro-segmentation to isolate systems and limit lateral movement in case of compromise.
- Data Loss Prevention (DLP) policies applied at endpoints, email gateways and cloud services to monitor and restrict unauthorised data transfers.
- Incident response, business continuity and disaster recovery plans and processes.
- Regular red team exercises and penetration tests focused on supply chain attack vectors including social engineering and phishing simulations targeting vendor personnel.
- The OAIC reiterates that "*Organisations need to proactively address privacy risks in contractual agreements with third-party service providers.*"[9] Based on the writer's experience, a service agreement should include:
    - a description of the personal information handled by the service provider with detail about which information is provided by the organisation and which is collected or generated by the provider for the organisation;
    - a restrictive data use licence;
    - specific rules about data minimisation and limited data retention;
    - detailed information security obligations including a substantive list of information security topics and measures informed by regular risk assessments;
    - visibility over supply chain changes;
    - event reporting obligations – there should be no delays hindering the organisation's reporting of a notifiable "eligible data breach"[10] to the OAIC;
    - obligations reflecting the Australian privacy principles where required for compliant cross-border data transfers between organisation and provider;
    - duties of cooperation, provision of information on request and audit rights;
    - review and intervention rights;
    - meaningful liability exposure of the provider commensurate to the handling of large volumes of personal information separate from commercial liability caps.

Much has changed over the last five years. Appointing a single head of data privacy without additional staff and resources might have worked in 2019 but it may not please the regulator in 2025. Today, most Australian organisations understand that managing data privacy and cyber risks does require a sizeable competent workforce and resources.

[9] Data breach report (07-12/2023) highlights supply chain risks, 22 February 2024 (link).
[10] As defined in the Privacy Act 1988 (Cth).

Consequences to be felt for years to come …

A data breach brings misery to the individual and the organisation. Authorities should gather intelligence and provide early warning and offer full support to affected organisations.

Infiltrated data can be used by criminals to build profiles about victims which are combined with other data available in the public domain and on the dark web. AI can be used to link identities in seconds. Customers of a breached organisation may be subject to scam campaigns at the time of the data breach, and at any time in future. With emerging AI-powered attacks such as phishing, vishing, smishing and whaling, consumers and businesses alike could be the next victim.

Breached organisations will likely suffer unfavourable media coverage and public debate. Recently, yet another cyber incident likely motivated the Attorney General to publicly comment about her continued effort to put forward "Tranche 2" of the data privacy reform.[11]

What might follow is a representative complaint to the OAIC and a class action lawsuit. The OAIC's determination of whether the law was breached or not could be critical for the early settlement of customer claims, but such determination might take some time (e.g. 3 years in the case of Optus). Meanwhile, the breached organisation might offer individual settlements to complainants in an attempt to start fixing its balance sheet.

It is unfortunate that a portion of what organisations hope to save by outsourcing and modernising their business infrastructure may later be used to deal with the aftermath of the cyber incident arising from those projects.

Conclusion

Business decisions concerning compliance and data privacy can have severe consequences. Digital transformation projects aimed at cost savings are legitimate business activities but they often come with a higher operational and compliance burden which must be met to avoid future liability.

Even well organised cyber defences which meet all legal standards could fail under the pressure of relentless attacks by increasingly organised and capable groups of cyber criminals. One key risk mitigation practice is data minimisation and limited data retention. Indeed, one of the OAIC's priorities for 2025/26 is rebalancing power and information asymmetries originating in excessive data collection and retention.[12]

The OAIC's enforcement is not specifically focused on larger organisations and we have seen regulatory action where it was most needed, particularly against smaller businesses engaging in serious privacy interference. However, large businesses have a role to play in getting data privacy right, particularly as they hold large volumes of personal information and many organisations will look to them for an example of how things should be done.

After the recent reform, the OAIC is well-equipped and ready to strike in a measured and strategic way to bring about a positive change in safeguarding the personal information of Australians.

Alexander Dittel is a Principal in **Data Privacy, Cyber and Digital** at KHQ Lawyers

[11] The 30-second statement triggered Australia's next privacy tranche – marketing, media and tech on notice, Mi3, 23 July 2025 (link).
[12] OAIC Regulatory priorities 2025/2026, 29 July 2025 (link).