**6 (a) Cyber security and data breaches in Australia**

Recently, there has been recent reforms in the law and a strategy implemented by the Australian Government to improve cyber security with the aim of minimising the number of breaches. In addition to leaking Australian’s personal information, cybercrime is having significant economic impacts with the cost on Australian businesses increasing by approximately 14% per annum.[[1]](#footnote-1)

**6(b) Mandatory data breach requirements**

National mandatory data breach requirements were first introduced in Australia in early 2017 as an amendment to the *Privacy Act 1988* (Cth). The amendments contain a notification scheme for certain types of data breaches involving unauthorised access and disclosure of personal information likely to lead to serious harm to individuals.

The requirements are binding on APP entities, credit reporting bodies, credit providers, tax file number recipients and internet service providers.

If an entity becomes aware of a data breach, it must inform the Office of the Australian Information Commissioner (**OAIC**) and the individuals whose data is affected when the data breach is likely to result in serious harm to the individuals involved. If directly contacting the affected individuals is not practical, the entity may publish a statement on their website and take reasonable steps to publicise the contents of the statement. If the data breach affects one or more entities, an entity is not required to complete these steps if another entity has already done so.

**6(c) Mandatory Notification of Data Breach Scheme (NSW)**

1. **Inception**

On 16 November 2022, the *Privacy and Personal Information Protection Amendment Bill* (NSW)passed both houses of NSW Parliament with agreement being reached on 28 November 2022. The Bill came into effect on 28 November 2023 with key changes including:

* The introduction of the Mandatory Notification of Data Breaches scheme (**MNDB scheme**). This includes notification requirements and relevant assessment being undertaken to assess the seriousness of harm suffered due to the breach occurring.
* Application of the *Privacy and Personal Information Protection Act 1998* (NSW)(**PPIP Act**) to all NSW state-owned corporations that are not covered under the *Privacy Act 1988* (Cth).
* Unifying public sector agencies by repealing s117C of the *Fines Act 1996* (NSW) to ensure all are covered under the MNDB scheme.

These key changes ensure a comprehensive framework for handling data breaches exists for both private organisations and federal bodies, as well as state-owned corporations in NSW.

1. **Examples of Breaches**

The Information and Privacy Commission (**IPC**) is the regulator within NSW for the MNDB scheme and they identify 3 areas to which public sector agencies (including NSW Police and local councils) experience data breaches. They include:

1. Human error – for example a letter or email is sent to the incorrect recipient or an employee loses their laptop in a public space.
2. System failure – for example no authentication is needed for systems containing confidential information or system automates workflows and redirects them to other users.
3. Malicious or criminal attack – for example malware, hacking and phishing.

Due to the MNDB scheme only being introduced 10 months ago, there are very few reported cases of eligible breaches and no annual data reportable by the IPC in terms of trends, recommendations or themes within the sector. Comparatively, the OAIC reported 67% of data breaches were criminal/malicious attacks for the last reported period (July-December 2023). Health service providers were the highest reporter of breaches with 104 being recorded, compared to the finance industry which was the next highest reporter with 49 breaches. Such data will assist state agencies in management processes and sector trends to safeguard against breaches.

1. **3-tier process in determining eligible breaches**

Not every data breach that occurs falls under the MNDB scheme, as s 59L(2) of PPIP Act provides that only eligible breaches are captured under this scheme. To determine an eligible breach, regard must be given to s 59D(1) in that:

1. Information held by a public sector agency has been unlawfully accessed, disclosed or lost (either internally or externally);
2. That information was/is considered personal information (s 59B); and
3. The data breach would likely result in serious harm for the individual to whom the information relates (s59D(1)(a) and s59D(1)(b)(ii)).

An agency that has a suspected eligible data breach reported to it has 30 days to conduct an assessment to determine if an eligible breach occurred. This is achieved by having an assessor appointed (s 59G) and relevant factors being considered (s 59H) such as to whom the information was released and how long they have had access to it.

If an eligible breach has occurred, agencies must notify the Information Commissioner immediately (s 59M) and the individual concerned (as soon as reasonably practical (s 59N)). Penalties could be up to $40,000 if the matter is decided in the NSW Civil and Administrative Tribunal.

1. **Who has responsibility under the NSW scheme?**

Agencies that hold personal information have a legislative responsibility to protect that information in accordance with the Information Protection Principles (**IPPs**) in Part 2 of the PPIP Act. As such, when an eligible breach occurs, all reasonable efforts must be made to contain the breach and mitigate the harm suffered.

Agencies are required to have a Data Breach Policy that outlines how they intend to address data breaches within their organisation as well as maintain both a public and internal register of eligible data breaches that have occurred within the agency. In addition to this, there is also a legislative onus on agencies to maintain a current Privacy Management Plan that not only outlines how personal information and privacy are reflected within the relevant organisation but the processes engaged when information is inadvertently released or unlawfully disclosed.

The Information Commissioner carries various enforcement powers, including:

* Directions can be issued in regard to providing specific information or making specific recommendations when reasonable suspicion is held that an eligible breach has occurred (s 59Y).
* Investigative powers and monitoring powers can be exercised to ensure systems, policies and procedures reflect the objectives of the Act and the agencies' requirements to uphold legislative requirements pertaining to personal information (s 59ZA).

Of particular note within the OIAC, civil penalty proceedings were instigated in November 2023 against Australian Clinical Labs Limited (**ACLL**) after an investigation into the privacy practices was conducted following a 2022 reported breach. Failure to conduct an expeditious assessment and notify the Commissioner are some of the allegations raised that demonstrates at the federal level there is an appetite to prosecute offences and disregard of the IPPs. Considering the MNDB scheme is modelled off the federal framework, it is not inappropriate to consider a similar stance being taken against NSW agencies who fail to adequately fulfil their obligations under the scheme.

1. **"Serious harm”**

For agencies subject to the MNDB scheme, little guidance is provided in terms of a legislative interpretation of “serious harm” but rather a collection of considerations is provided that does little to ensure a consistent application of the assessment process between agencies. There is no definition of “serious harm” prescribed within the PPIP Act. Naturally, each data breach case assessed would vary in severity and heavily depend on the case-specific factors including:

* individuals involved,
* the sensitivity of the information released,
* how the information was released,
* any known history concerning the individual, and
* the person to whom the information was released to.

The framework, although unifying, still lacks an underlying prescription of any form of what harm means or how it can be applied, without relying on cases to be tried within NCAT or through complaints lodged to the IPC.

**6 (d) Australia’s Data Breaches**

The Australian Signals Directorate (**ASD**) recorded 150 data breaches in 2022-2023, which was up from 81 breaches recorded in 2021-2022.[[2]](#footnote-2)

In September 2022, Optus became the target of a large cyber attack resulting in 9.8 million customer records being breached. This raised public concern about the information that telecommunication companies hold and their ability to protect this information from being exposed or exploited.

Following this, in October 2022, Medibank was the victim of a data breach where the hackers gained access to private medical records of approximately 9.7 million Australians. In response to this, the Australian Government has reformed the law surrounding cyber security to attempt to prevent these breaches from occurring again and come up with ways to minimise the impacts of data breaches.

These breaches resulted in reputational damage to these companies as well as individual concerns from the customers regarding potential identity theft and the misuse of their sensitive personal information.

Many of these companies were still using outdated encryption procedures and had insufficient monitoring systems. These breaches highlighted the need for the government to act swiftly and reform the law concerning cyber security to initiate stricter regulation and enforcement of cyber security measures.

**6 (e) Cyber security and data leaks**

Cyber security plays a fundamental role in protecting private information from being leaked in a data breach. Cyber attacks present a significant challenge to the sovereignty of states and personal data; these challenges being intensified due to the ongoing evolution of AI technology.[[3]](#footnote-3) The ASD has the authority to conduct cyber operations, information security and foreign communication. The Australian Cyber Security Centre forms part of the ASD and conducts threat assessments and incidence response services to cyber incidents and threats, forming a collaborative approach to cyber security in Australia.

**7 (f) The Cyber Security Strategy and Australian Security Legislation**

The Australian Government released the 2023-2030 Australian Cyber Security Strategy on 22 November 2023 which replaced Australia’s Cyber Security Strategy 2020. The strategy consists of six shields; strong businesses and citizens, safe technology, world-class threat sharing and blocking, protected critical infrastructure, sovereign capabilities, and resilient region and global leadership.

The strategy’s aim is preventative in nature but also seeks to achieve resilience and minimise the overall impacts that data breaches can have upon individual’s information as well as larger entities. The strategy also has a strong focus on collaboration between different departments to minimise the chance of a breach occurring through appropriate communication. To coincide with the introduction of this strategy, the Australian Government also appointed its first ever Executive Cyber Council. The role of the Council is to facilitate transparent co-management on key cyber security issues.

To facilitate this strategy the Australian Government also introduced the 2023-2030 Australian Cyber Security Action Plan which provides detail about how the strategy will be implemented across different stages. The action plan consists of multiple actions related to each of the six shields under the strategy. For example, one action under the ‘strong businesses’ shield is to support small and medium businesses to strengthen their cybersecurity.

The *Security of Critical Infrastructure Act 2018* (Cth)is one of the key pieces of legislation that governs cyber security in Australia. Relevant amendments include:

* The *Security Legislation Amendment (Critical Infrastructure) Act 2021* (Cth), which came into effect on 2 December 2022 and included introducing mandatory reporting of cyber incidents and the implementation of stringent security measures.
* The *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022* (**SLACIP Act**), which
  + added a new section 3(d): “imposing enhanced cyber security obligations on relevant entities for systems of national significance in order to improve their preparedness for, and ability to respond to, cyber security incidents;”
  + introduced a new risk management program requiring that a critical infrastructure risk management program is maintained by entities who hold one or more critical infrastructure assets (Part 2A);
  + introduced a requirement that the Minister to notify every reporting entity for assets that are declared to be of national significance, and the Minister also has the power to privately declare systems of national significance (Part 6A).

1. Australian Signals Directorate, Australian Government, *ASD Cyber Threat Report 2022-2023* (Report, 14 November 2023) <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>. [↑](#footnote-ref-1)
2. Australian Signals Directorate, Australian Government, *ASD Cyber Threat Report 2022-2023* (Report, 14 November 2023) <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>. [↑](#footnote-ref-2)
3. Robert Walters and Marko Novak, ‘Cyber security: In Cyber security, artificial intelligence, data protection & the law’(2008) Springer Singapore 5. [↑](#footnote-ref-3)