PiperAlderman

Article Information

Author: Craig Subocz
Service: Cyber Security, Intellectual Property & Technology, Privacy & Data Protection
Sector: IT & Telecommunications

Australia has a new Cyber Security Strategy: What businesses need to know

In November 2023, the Commonwealth Government announced its 2023-2030 Cyber Security Strategy, focusing on six "cyber shields" to make Australia a "world leader in cyber security by 2030". The Government has flagged its intention to amend Australia's existing laws to increase cyber security. We review the possible changes and how businesses should prepare.

Overview of the Government's Strategy

The Commonwealth Government released its 2023-2030 Cyber Security Strategy (**Strategy**) on 22 November 2023. The Strategy outlines the Government's vision for making Australia a "world leader in cyber security by 2030" in order to make Australia a "hard target for cyber attacks".

To achieve this vision, the Government has set out six "cyber shields" to protect Australians:

- Shield 1: "Strong businesses and citizens";
- Shield 2: "Safe technology";
- Shield 3: "World-class threat sharing and blocking";
- Shield 4: "Protected critical infrastructure";
- Shield 5: "Sovereign capabilities"; and
- Shield 6: "Resilient region and global leadership".

The Government has also set three horizons for the implementation of the Strategy. In the first horizon (between 2023-2025), the Government will focus on strengthening the foundations of cyber resilience. Horizon 2 (between 2026-2028), the Government will focus on "scaling" cyber maturity across the whole economy. In Horizon 3 (between 2028-2030), it is intended that Australia will become a world leader in cyber security.

The Action Plan

The Government intends to support the Strategy by following its Action Plan, released simultaneously with the Strategy. The purpose of the Action Plan is to set out how the Government will achieve the strategic aims outlined in the Strategy and by naming the Government agencies that will be accountable for achieving the relevant strategic aim.

Key law reforms

The Strategy outlines several areas for law reform to achieve the goals set out in the Strategy.

A no-fault, no-liability obligation to report ransomware attacks

As part of the first "Shield" (Strong businesses and citizens"), the Government set out its intention to work with industry to break the ransomware model. In order to improve the visibility of the threat posed by ransomware, the Government will legislate a no-fault, no-liability ransomware reporting obligation. Under this scheme, in order to mitigate the current reluctance among businesses to disclose information about a ransomware attack in a timely fashion. Additionally, the Government will create a "ransomware playbook" to help businesses prepare for, deal with and recover from a ransomware or cyber-extortion attack.

The Strategy focuses on initiatives to assist small and medium enterprises deal with cyber threats. However, it is possible that the reporting obligation will apply to all businesses, regardless of size. We will provide further updates once the Government releases more detail about the proposed reporting obligation.

No specific ban on the payment of ransomware just yet

Although not specifically stated in the Strategy, the Government chose not to specifically ban ransomware payments at this stage. However, the responsible Minister, the Hon. Clare O'Neil MP, flagged that, in two years, the Government will review whether a ban is possible. Presumably, the Government will seek input from business and the community on the feasibility of a ban on the payment of ransomware, so there may be an opportunity to assist the Government in refining the law regarding the payment of ransomware in the future.

A mandatory cyber security standard for "IoT" devices

As part of the second "Shield" ("Safe Technology"), the Government has prioritised the legislation of a mandatory cyber security standard for Internet of Things devices. Additionally, the Government intends to implement a voluntary labelling scheme for consumer-grade smart devices. Businesses that specialise in the manufacture and sale of internet-enabled devices should monitor Government communications on the standard and scheme, and take the opportunity to participate in the development process.

Improving data governance standards and obligations

The Government is presently considering its approach to the reform of the *Privacy Act 1988* (Cth) (see our October article for more information).

Under Shield 2 ("Safe Technology") in the Strategy, the Government outlined an intention to review current legislative data retention requirements with a focus on "non-personal data" to determine whether existing provisions are "appropriately balanced".

The Government also intends to review the "data brokerage ecosystem" to assess whether action is needed to address risks associated with the transfer of data to malicious actors via data markets.

Extending the critical infrastructure regulation

Shield 4 ("Protected critical infrastructure") of the Strategy sets out the Government's strategy to upgrade and promote the cyber resilience of Australia's critical infrastructure. In the Strategy, the Government notes that the *Security of Critical Infrastructure Act 2018* (Cth) (**SOCI Act**) has been significantly revised in order to extend its operation to owners of "critical infrastructure assets" in a variety of sectors.

As part of its Strategy, the Government intends to further revise the *SOCI Act* to impose stringent obligations on telecommunications companies with respect to the reporting of cyber incidents.

The Government also intends to publish an overview of "corporate obligations" for critical infrastructure owners and operators.

More broadly, the Government signalled that the *SOCI Act* will be amended to clarify the obligations of managed service providers under the *SOCI Act*, with an emphasis on aligning those obligations with the data protection initiatives the Government will establish under the Second Shield. The Government also intends to amend the *SOCI Act* to clarify its application to ensure that operators of critical infrastructure assets are adequately protecting their data storage systems where vulnerabilities to those systems could impact the availability, integrity, reliability and/or confidentiality of such assets.

Further, the Government will amend the *SOCI Act* to introduce a so-called "consequence management power". If exercised, this power would allow the Government to direct an entity to take specific actions to manage the consequences of a "nationally significant incident", including cyber incidents and other hazards.

Conclusion

The Strategy represents a significant milestone in the Government's push to improve the nation's cyber resilience in the wake of several high-profile breaches that affected millions of Australians in the last 12 months.

As part of the implementation of the Strategy, the Government has flagged an intention to reform Australia's laws. The most wide-ranging reform under the Government's Strategy is the introduction of the no-fault, no-liability ransomware reporting obligation.

Those businesses that manufacture or sell internet-connected devices should take note of the Government's intention to introduce a mandatory cyber security standard and take advantage of any opportunity given by the Government to participate in the process for developing the standard.

Owners and operators of critical infrastructure assets, as well as providers of managed services to critical infrastructure owners and operators, should prepare for amendments to the *SOCI Act* to address the Government's strategic aim for improving the cyber resilience of Australia's critical infrastructure.