Philip Nesci

Cyber & Risk

IBRS ALERT:

Australian Government unveils Australia's new Cyber Security Strategy

Background

The federal government has finally unveiled its cyber security strategy. The Australia's Cyber Security Strategy 2020, released on 6th August will see $1.67 billion invested in a number of already-known initiatives aimed at enhancing Australia's cyber security over the next decade.

Most of the funding for the Strategy 2020 is from July's announced $1.35 billion cyber enhanced situational awareness and response (CESAR) package much of the Strategy details will be contained in legislation to be put before parliament.

The Strategy's Key Elements

1. Enhanced Regulatory Framework

Proposed laws and an "enhanced regulatory framework" will enhance security of infrastructure which is deemed critical. The new framework will include "enforceable positive security obligations for designated critical infrastructure entities". The framework, which will be delivered through amendments to the Security of Critical Infrastructure Act, is expected to extend to beyond entities currently classified as critical to entities and systems of national significance.

Additionally the government will consider additional "legislative changes that set a minimum cyber security baseline across the economy".

2. Consolidated and more secure Agency networks

With departments and agencies continuing to struggle to implement rudimentary cyber security controls, the government has reversed its stance on leaving government departments *responsible for their own cybersecurity*. It will instead consolidate and centralise the management and operations of networks run by agencies, enabling greater focus on a smaller number of secure networks.

Standard cyber security clauses will also be introduced in to government IT contracts to avoid unnecessary risks.

3. Increased Funding for Law Enforcement

The government will also provide law enforcement agencies with $124.9 million to strengthen their ability to counter cyber crime, including $89.9 million for the Australian Federal Police.

The ACSC will also receive a further $31.6 million to improve its ability to counter cyber crime offshore and assist federal, state and territory law enforcement to identify and disrupt cyber criminals.

4. Uplifting SMEs

The Strategy outlines the government's $63.4 million plan to assist small and medium enterprises (SMEs) to uplift their cyber security capabilities. "The Australian government will work with large businesses and service providers to provide SMEs with cybersecurity information and tools as part of 'bundles' of secure services (such as threat blocking, antivirus, and cybersecurity awareness training)." "Integrating cybersecurity products into other service offerings will help protect SMEs at scale and recognises that many businesses cannot employ dedicated cybersecurity staff."

5. Cyber Skills and Situational Awareness

The Strategy also outlines:

- "Greater collaboration to build Australia's cyber skills pipeline, increased situational awareness and improved sharing of threat information".
- "Advice for small and medium enterprises to increase their cyber resilience, clear guidance for businesses and consumers about securing Internet of Things devices".

Key Takeaways

1. The Government recognises its role in cyber preparedness and in building a cyber resilient ecosystem with businesses and vendors.
2. Australian Government departments and agencies need to prepare for greater scrutiny and reporting on their cyber resilience and progress of their cyber plans. There will be consolidation and rationalisations of network and cyber operations across the government sector. Agencies will undertake regular cyber security incident exercise programs by the Australian Centre for Cyber Security (ACSC).
3. The number of organisations currently defined as critical infrastructure will expand. Critical infrastructure operators such as utilities will face additional legislative compliance and reporting against cyber security standards. This compliance and reporting will be given greater focus by directors and boards.

4. There will be additional government security support for cyber security awareness and cyber security attacks, particularly for SMEs
5. Demand for cyber security skills, already in short supply, will tighten further as the cyber security/resilience programs are implemented by both governments and businesses.

pnesci@ibrs.com.au

Submit and Inquiry