15 July 2021

AUSTRALIA UNDER CONSTANT CYBER ATTACK ANDREW PENN TELLS PRESS CLUB

A significant increase in malicious cyber activity by criminals and state actors mean Australia is now under constant cyber-attack so governments, businesses and Australians need to act urgently to protect themselves against cyber threats, Chair of the Australian Government Cyber Security Industry Advisory Committee and Telstra CEO Andrew Penn said today as he released the Committee's first annual report.

Speaking to the National Press Club, Mr Penn said ransomware attacks, gangs selling cybercrime as a service, increased hacking of business email, and the targeting of global supply chains meant cyber security had never been more important for Australia's economic prosperity and national security.

"Malicious cyber activity is happening all of the time. In the last year, the number and sophistication of attacks has grown with Australians losing more than $851 million in 2020 as scammers use the pandemic to con people according to the ACCC's latest Targeting Scams Report," Mr Penn said.

"Australia faces a complex cybercrime environment that targets everyone from the local fish and chip shop to ASX200 companies, the local primary school to global COVID vaccine supply chains."

Mr Penn said it was critical Australia's cyber defences were strong, flexible and built around a coordinated framework which was the aim of Australia's Cyber Security Strategy 2020.

"There has been considerable progress since the Strategy was launched just under a year ago and there needed to be because the environment continues to evolve rapidly and malicious actors are becoming more sophisticated, more targeted and more brazen.

"The Committee's first Annual Report updates on our progress and importantly includes six areas of key focus for the Cyber Security strategy in the coming period to accelerate how we shore up our cyber defences."

Raising awareness – most Australians and Australian businesses remain under-prepared for a cyber-attack and it is crucial more resources are invested in improving the level of knowledge so Australians can better protect themselves online. There is a need to commit further effort to raise awareness of threats and mitigations, this could be achieved through a mainstream and social media campaign, using one voice with a clear and simple call to action.

Continuing to enhance the capabilities of Australia's Joint Cyber Security Centres – accelerate JCSC programs which combine business, research and government resources to fight cyber threats including through threat sharing between industry and governments. Threat sharing is the key to threat blocking, which is the key to cleaner pipes.

Workplace readiness - As hybrid and remote working becomes widespread, organisations' cyber defences need to support increasing home-based workforces. Cyber security literacy and training should be built into work practices, in the same way that Workplace Health and Safety is now so both an organisation's decision-makers and its employees know how to put protections in place.

Ransomware - Ransomware attacks are increasing in number and sophistication, and businesses face tough decisions when they are victims of attacks. To better prepare, clearer advice on the payment of ransoms and consideration of the merits of cyber insurance regimes all need attention.

Improved evaluation - Developing metrics to assess the effectiveness of these initiatives and the overall level of maturity of our cyber defences. The bottom line is we need to be able to measure who is winning and where – the good guys or the bad guys?

Foster international dialogue - It is critical that Australia continues to work closely with like-minded international nations given vulnerabilities in key supply chains that underpin the digital world such as rare metals, silicon chip sets and telecommunications radio access technologies such as 5G.

Mr Penn said it was also important to understand how cryptocurrencies were being used to aid cybercrime as well as how over the longer term, in the wrong hands, supercomputing, advanced algorithms and AI could crack the encryption used to protect sensitive data, including financial data the world over.

“At a time when Australia aspires to be a world leading digital economy by 2030, it is a mission that is more important than ever before.”

Media enquiries:
Jonathan Larkin: +61 477310149