Cyber Security Industry Advisory Committee

Thursday 25 August 2022

MEDIA RELEASE

Authorised for release by Mr Andrew Penn, Chair of the Cyber Security Industry Advisory Committee

AUSTRALIA: GLOBAL CYBER THREAT LANDSCAPE WORSENS – NOW IS THE TIME TO EXPAND AUSTRALIA'S CYBER STRATEGY

The global cyber threat environment has intensified and Australia is an increasingly attractive target for malicious actors and cybercriminals, according to the Cyber Security Industry Advisory Committee (IAC) Annual Report 2022 launched yesterday.

IAC Chairman and Telstra CEO Andrew Penn said deteriorating geopolitical tensions, the expansion of hybrid work outside traditional corporate firewalls and adaptive offenders saw cybercrimes including ransomware, mobile malware and business email compromise (BEC) significantly increase this past year.

"New technologies and the move to more time being spent online as a result of COVID has created greater opportunities for cybercriminals," Mr Penn said.

"At the same time geopolitical tensions have grown following Russia's attack on Ukraine, and the risk of attacks on Australian networks – whether directly or inadvertently – has also increased.

"Cyber criminals do not show bias, with attacks affecting everyone from your neighbour working from home to multinationals.

"It is believed Australian SMEs lost more than $81 million to BEC in the 2020-21 financial year and alarmingly, there was a 15% increase in the number of ransomware cybercrime reports to the ACSC. The threats are real, so we have a lot more to do."

Mr Penn said the Australia Government's leadership through the development and implementation of the 2020 Australian Government Cyber Security Strategy had been critical but called for a continued focus on hardening Government IT systems, raising awareness and improving collaboration to combat increasingly common and sophisticated cyber-attacks.

"There has been considerable progress since the Cyber Security Strategy was launched two years ago and there has needed to be, because the environment continues to evolve at pace and malicious actors are becoming ever-more sophisticated, more targeted, more brazen and in that context, we need to keep improving," Mr Penn said.

"The Government's strong focus on cyber security as a national priority provides an excellent opportunity to enhance coordination across government on cyber policy, strategy and response mechanisms."

The IAC recommends seven pivotal areas of focus on over the next year:

- **Threat sharing:** Threat sharing, and Government and industry collaboration are both crucial to improving Australia's defences. The work of the Joint Cyber Security Centres plays an important role in this regard and they should be further scaled up.
- **Raising awareness:** Given the scale of the challenge and the extent to which increasing awareness can make a difference, more investment and resources should be committed to cyber awareness campaigns and initiatives.

- **Improved Evaluation and measurement:** A more universal and integrated fact base of Australia's cyber maturity should be established to measure the effectiveness of the initiatives being implemented under the Strategy, to enhance future policy decisions at all levels of government. This includes a recommendation of the development of a Cyber Security Maturity Index.
- **Best Practice Regulation Taskforce:** The Government should prioritise providing industry with feedback on the conclusions, including legal assessments of gaps in current legislation and any proposed initiatives or changes being considered.
- **Hardening Australian Government IT Systems:** The Government needs to be a role model in its own operations, while also improving the security of increasingly digital government service delivery.
- **Cyber skills:** We must increase our cyber awareness right the way across the spectrum from deep cyber expertise to basic cyber hygiene practices and this needs to be done through our schools and universities, governments and industry. Cyber needs to be a key topic at the Jobs and Skills summit next week and the Cyber Security Strategy needs to be expanded to embrace this challenge fully.
- **Protecting Critical Infrastructure and Systems of National Significance (CI-SONS) industry engagement:** Supporting regulations and any future amendments will need to be carefully designed and implemented in partnership with businesses to reflect the specific dynamics, technology and characteristics of each sector, ensuring a baseline uplift across all sectors.

Mr Penn said the security of the nation's digital infrastructure and platforms was critical to ensure Australia was able to benefit from the opportunities provided by the digital economy.

"Technology innovation offers Australia and Australians huge opportunities. However, the promise of the Digital Economy is not guaranteed – in fact while the security of our digital infrastructure and platforms has never been more important, it has also never been more fragile," said Mr Penn.

"Not only are they at risk from cyber-attack, but they are also exposed to other risks such as access to critical technologies, protecting interoperability of technology from the threat of the bifurcation of global technology standards, and the risk of the inadequacy of our skills base to meet these risks and capitalise on the opportunities.

"We look forward to working with the Minister to shape a broader National Cyber Strategy through this lens; a step which will be critical to building and protecting Australia's sovereign capability as Australia continues to navigate an increasingly complex cyber threat landscape, now is the appropriate time to refresh and expand from the 2020 Australian Cyber Security Strategy."

In relation to cyber skills, Mr Penn said if Australia wanted to meet all of these challenges and thrive in the accelerating digital world, the country would need to need to substantially uplift its cyber skills base.

"We must increase our cyber awareness right the way across the spectrum from deep cyber expertise to basic cyber hygiene practices and this needs to be done through our schools and universities, governments and industry, and we are going to need to it fast.

"Cyber needs to be a key topic at the Jobs and Skills summit next week and the Cyber Security Strategy needs to be expanded to more fully embrace this challenge," Mr Penn said.

A copy of the full report is available here: https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-IAC-annual-report-2022.pdf

Media Inquiries:
Steve Carey, +61 413 988 64