29-3-2023 - Sydney

How to make Australia the most cyber secure country by 2030 – Public Opinion Gathering Phase

From:

Devee P Maalampali

Senior Security Architect

Sydney

To:

Minister of Home Affairs

Dear Home Affairs Minister,

I want to start by congratulating you on your ongoing and thorough efforts to strengthen our country's robust cyberdefenses posture.

Second, I want to commend you for consulting the public on your national cyber resilience and defence program initiative.

I'd like to offer the ten key measures listed below to strengthen Australian National Cyber Defense programme.

1) Encourage and mandate that the top 20 critical industry organisations' business leaders (the Board, CEO, and CFO) allocate a portion of their annual budgets to their own internal cyber defence programmes and capability enhancements. Make the success of an organization's cyber defence just as important as its annual profit margin. At the same time, hold the Board, CEO, and CFO equally accountable for any cyberattacks or data breaches; this way, the CISO is not solely responsible for cybersecurity domain and business function. We must show that in any organization, cybersecurity is a team sport.

2) As the Human link is the weakest point in cybersecurity, promote cyber security, encourage, and mandate that every corporate employee take their company's Data Protection and Threat Protection policies seriously, just as they would typically take their own home security and family car/vehicle security seriously with alarms and locks, respectively. And to make compliance with these policy requirements a regular element of each organization's HR policies regarding expected cyber hygiene. To switch from the

traditional, unsuccessful methods of user awareness training, It is also possible to consider user coaching that is proactive and integrated (with the business application they are using).

Use cyber-hygiene coaching frequently and as needed, rather than just once only during the hiring process.

3) Promote and require every significant major corporate enterprise to implement a strong ransomware incident response plan. The end-to-end RACI Matrix in the Organization, covering who can make external communications and how to Regulators and Press & Fed Police on any breach situation should also be included in this. Also, a strategy for how to handle a breach when customer data has already been posted on the dark web for sale should be established.

4) Establish a formal structure for cyber insurance that includes both standard insurers and cyber-specific insurers. And create a Cyber Hygiene Baseline requirements for the Cyber Insurance Cover. For instance, The Org should have Identity and Privilege Access Control Management, 24/7 Network and Security Monitoring, Incident Response Capability, Secure Remote Access VPN, Data Leak Prevention capability, Endpoint detection and response control, and Network segmentation architecture to contain the breach. This can help align both the end user organizations and cyber insurance industry.

5) Create NASM/National Attack Surface Management and National SOC under DHA's purview, covering the nation's external attack surface threat intelligence and threat management capacity. Starting with continuous visibility and monitoring capability on all significant attack vectors and physical and logical data entry points into the nation, including subsea intercontinental fibre path transmission channel, satellite comms channel, 5G/6G cellular channel, global public cloud AU based data centres, and global DC connectivity path channel. These capabilities programme also conducts proactive research and keeps tabs on nation states and well-known international threat actors' movements throughout the world in real time. the National ASM and SOC Team/s to coordinate with all Federal Agencies, State Gov Agencies, and Critical Infrastructure Organizations in a single, coordinated national cyber threat grid.

6) To establish Cyber Governance and Security framework going-in Position paper on Emerging Tech such as BYOAI/Bring-Your-Own-AI, ChatGPT AI, Quantum Computing, 5G/6G, Digital Twins, Metaverse, Smart Cities/Buildings/Factories, and IT-OT Convergence. Critical infrastructure organisations and big businesses can use these principles to deploy these business-enabling developing technologies safely and securely within their own organisations.

7) Create a National Cyber Think Tank comprising the best 50 or 100 cyber experts in the nation, spanning a range of skill sets from governance, risk, and compliance (GRC) to security architecture, security operations, and security leadership. They can virtually work together once every quarter or so to assess the state of the nation and the world and provide the Minister of DHA with periodic recommendations.

8) Australia should adopt data privacy and protection regulations like to the GDPR in Europe. Alternately, you may add this particular Data Privacy/Protection regulation, which is exclusive to the Australian context and cyber jurisdiction, to the present ASD E8.

9) To have all Public Cloud providers in AU (Azure, AWS, Google, Oracle) reveal what data or metadata and to where they are sending from AU data centres to their USA or Europe or Asia on their DC-to-DC data automated replication for AI/ML/Data analytics/Remote Browser Isolation service objectives

10) With the following two steps, the outdated and ineffective government regulatory data handling process can be improved. Remove the requirement for 100–120 points of supporting KYC documents. Instead, give each citizen, ABN holders, and holder of a residential visa or study visa one national ID number. All the necessary supporting papers for the 120 points will only be gathered and stored during the National-ID-Card issuance process only. From that point forwards, this single national ID will be taken into account by every other government agency, bank, educational institution, or business that requires KYC. So, citizens do not have to provide tens of documents to tens of corporate entities in parallel, significantly increasing their own personal cyberattack surface. This suggested approach can help reduce the attack surface of every individual citizen. The second component of this strategy is to shorten businesses' data retention periods to a minimum of two years and a maximum of three years. Not five years or eight years of date retention regulatory requirements for the businesses.