Author: Muhammad Tariq Ahmed Khan, Head of Cyber Security Audit in a Bank
ISO 22301 BCM LA, ISO 27001:2013 ISMS LA, CISA, CISM, CRISC, CISSP, CDPSE, CEH, PMP, CDFE

I am not an Australian Citizen nor do I belong to any Australian Organization. I am not sure my submission will be accepted by Australian Government or not. However, when I noted that Australia is seeking submissions on Cyber Security Strategy, I decided to provide my feedback which might add some value to Australia's Cyber Security Strategy 2020 as I am currently working on a Company Profile (Scope of Work) to establish a Cyber Security Audit Firm/ Company (either a sub-company under one registered company in Australia or an independent Sole Proprietary Company).

I understand that role and importance of Cyber Security. Usually, cybercriminals target organizations with weak cyber security to access, tamper, or destroying sensitive information; extorting money from users; or interrupting normal business operations resulting regulatory sanction and penalties.

But one should not overlook the role of "Cyber Security Audit".

Why "Cyber Security Audit"?
We know that a false sense of cybersecurity implementation is ubiquitous in the world and it is one of the main root-causes why cybercriminals are so successful in their ill objectives by targeting the weakest links of the organization such as people, processes and procedures. In reality, most organizations are breached due to false sense of security and assurances provided by IT management that their organization is protected from cyber-risk due to implementation of number of cyber security controls (technologies and vendor products) and documentation of several cyber security policies and procedures.

So I recommend that Australia's Cyber Security Strategy should consider integrating Cyber Security Audit in the strategy as I believe that integrating the requirement of Cyber Security Audit earlier in the strategy and ensuring that it provides governing rule, is proactive rather than reactive, is one of the most reliable ways to strengthen the security posture of any organization in Australia.

***What is* "Cyber Security Audit"?**
The role of "Cyber Security Audit" is to provide a reasonable assurance to senior management that how effectively and efficiently cyber security controls, standards, guidelines and procedures are implemented in an organization. It has become vital to keep pace with the drastically changing cybersecurity risks.

So, in my opinion, the Cyber Security Strategy should consider including the following requirements:

- *Cyber Security Strategy should be aligned with organization's business strategy*.
- *The Audit Committee should have oversight responsibility on cybersecurity risks in the organization. Generally, Audit Committee members are financial savvy and they lack the knowledge of cybersecurity. They, therefore, may want to bring in someone onto audit committee with expertise in cybersecurity and they should ensure that right cybersecurity management personals with right processes are available in the organization.*
- *Internal Audit should consider conducting cybersecurity risk assessment based on latest cybersecurity trends/ threats and devise a risk-based cybersecurity internal audit plan. Internal Audit should also ensure that the plan is aligned with the organization's strategic plan as cybersecurity has become a business issue these days.*

In a nutshell, strategy should clearly state the requirement of mandating internal audit to provide an objective assurance that cybersecurity controls are effectively implemented and operating well. Further, internal audit should recommend for improvement opportunities to protect the organization's goals and objectives.