Afilias Australia
www.afilias.com.au

Australia's 2020 Cyber Security Strategy

A call for views

In response to Australia's 2020 Cyber Security Strategy, Afilias Australia Pty Ltd offer the below views:

2. Do you agree with our understanding of who is responsible for managing cyber risks in the economy?

Every internet user has a cyber security responsibility. While we agree that "End-users, such as individuals and small businesses, carry a high level of risk in managing their online activity and often bear the loss caused by malicious activity" we believe that this group must not bear the burden of the responsibility in mitigating threats. Each layer in internet delivery – communications, infrastructure, standards, applications and services – should take responsibility in protecting end-users.

Each internet delivery organisation should conduct the following:

(a) Plan and share: Evaluate their respective risks, collaborate on mitigation strategies and share relevant threat data.
(b) Utilise best practices: The internet is its safest when actors use agreed upon standards, norms and best practices.
(c) Communicate: Rapidly share breach information to impacted parties.

There are several existing global industry fora to complete these joint activities. For discrete goals, organisations should create pages within their websites or via social media to communicate with stakeholders.

The ideal role for Government at this time is to perform two functions – facilitator and educator. Creating many new and specific rules could create an overly regulated environment that limits opportunity for innovation, growth and fair market competition. The Government should focus on facilitating industry collaboration and have the flexibility to respond to and mitigate threats. The Government should also look to educate by developing campaigns to promote cyber safety among users, including youth users.

The Government should also focus on finding and promoting best practices for cyber security and cyber hygiene. Collaboration and the creation of a public-private partnership to educate and inform all participants in the cyber economy is an important task that only Government can perform.

+61 3 9021 6914
L35/360 Elizabeth Street
Melbourne VIC 3000
76 623 428 384

17. What changes can Government make to create a hostile environment for malicious cyber actors?

When seeking to cultivate a hostile environment for malicious cyber actors, there are several avenues a Government can consider in terms of their ccTLD space as well as the larger enforcement and judicial systems. Within their ccTLD, governments should encourage and empower the registry operator with the authority to promptly respond to and neutralise security threats using domains within their purview. This allows both the registry operator and domain registrars to take steps to reduce the uptime of malicious domains and other security threats, thus limiting the scope of potential harm. Even in relatively safe ccTLDs, these measures are essential to disrupting ill-intentioned players. However, many cyber threats come from outside a country's ccTLD for a variety of reasons and the consequence is that governments must look at additional steps to disrupt malicious actors.

Other changes that can increase the operating costs and develop a hostile environment include improving public-private interactions by facilitating interactions between industry, such as registry operators and registrars, and law enforcement or Government bodies, such as Australian Federal Police, ACSC, etc. A related element is working to streamline and refine court order and warrant requests coming from law enforcement to industry. When the public sector understands the capabilities and terminology of the companies' they are serving legal requests to, it can reduce the need for clarifying communications and expedite execution of the orders. Related to court orders is ensuring that there are mutual legal assistance treaties (MLATs) in place to allow law enforcement to reach cybercriminals beyond the nation's borders. MLATs and fostering trust between agencies can produce extremely effective joint operations to bring in the malicious cyber actors. Requiring transparency from businesses when they are the target of cyber attacks is a useful best practice to promote. Creating and releasing national cyber hygiene standards could go a long way in creating a safer environment for the users of the Internet in Australia.

As a final point, after investigations and any operations have been completed, punishments and consequences are another stick Government can wield. Having legislation crafted in a way to allow prosecutors to charge criminals to the fullest extent and having the ability to charge for all phases of the cyber-attack maximises the deterrent and removes ambiguity around whether particular techniques are covered within current law.

21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?

Information sharing is often problematic for two reasons. First, there is no baseline from which to require or build out more trusted and safer products and services. Second, there are always concerns

+61 3 9021 6914
L35/360 Elizabeth Street
Melbourne VIC 3000
76 623 428 384

about those end-users who don't keep up with changes and are thus at greater risk because bad actors know how to leverage vulnerabilities.

With the Government's roles being primarily facilitator and educator, information sharing could be set up as below:

- End-users have some responsibility to ensure they select products and services that offer the security they should have, including understanding the effectiveness of the various choices made by vendors. In addition, the basic education and resources that should be developed and evangelised, ensuring that end-users are notified of issues that need their attention. The FIRST organisation offers some globally accepted best practices to achieve this. The important element is to create a trusted system that is helpful and cooperative for all parties.
- Providers of products and services have a responsibility to ensure they are employing best practices and the Government can facilitate this by establishing a requirement to acquire only those products that mitigate cyber threats and vulnerabilities. As the largest procurement organisation, the Government would improve the options for its end-users with such a strategy. It is important to remain aware that even the best prepared may have the occasional issue. In addition to reporting out to end-users, a Government initiative that encourages organisations to report issues and concerns without prejudice, and facilitates the sharing of information between each affected organisation, will promote a more trusted and safer experience for everyone. This will ensure that investigative actions, e.g., with law enforcement, will also be enhanced.
- Absent a "safe space" for information sharing, data collection about cyber threats and vulnerabilities will remain fragmented. The Government could work alongside the aforementioned organisations to create a secure cyber data store where affected parties could upload information about attacks and vulnerabilities without concern about both legal and operational liabilities.

22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

Businesses and consumers are more comfortable using the internet for services if they view it to be comfortable and secure. Unfortunately, it is the breaches and negative security incidents that drive media, not the stories of success. Add to that the complexity of the cyber security topic, and users and businesses do not take the necessary steps out of intimidation and ignorance. Understanding what needs to be done and the tools that are available is a critical step.

Simply increasing awareness will not be sufficient to improve cyber hygiene. Just as in the public health space, awareness of the importance of hygiene led to behaviour changes, a similar mindset should be adopted with respect to cyber threats and vulnerabilities.

23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?

Targeted cyber awareness campaigns executed via the Government and businesses/associations are a logical vehicle for driving awareness. It is essential to show the simple measures to mitigate security risks – e.g., software patching, common sense password protocols, timely software and application updates - that non-technically savvy actors can take. By introducing relatively simple solutions, it will be easier to acclimate them to other actions.

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

In the United States, there is a public-private sector initiative called "Stop. Think. Connect" that provides tips and advice, organises national campaigns and provides resource material for users, businesses, and infrastructure providers. They host regular briefing sessions and actively distribute tips and information via social media. This initiative was organised by the National Cyber Security Alliance (NCSA), who also manage other cyber awareness activities. More information about their mission, scope of work and effectiveness can be found on their website.

On a global basis, there are several groups that develop, distribute and promote norms and best practices. These include:

- Global Commission on Stability of Cyber Space
- Internet Governance Forum (IGF) of the United Nations
- Global Forum on Cyber Expertise.

The Global Commission on the Stability of Cyberspace believes that fundamental cybersecurity defense through the widespread adoption of cyber hygiene has become essential to the responsible use and beneficial growth of the Internet. Security must be seen as a continuous process with responsibilities distributed among all actors with mechanisms in place, such as automated reporting and information sharing, to ensure appropriate accountability.

+61 3 9021 6914
L35/360 Elizabeth Street
Melbourne VIC 3000
76 623 428 384