# Australia's 2020 Cyber Security Strategy – A call for views

The University of Western Australia (UWA) welcomes the Australian Government's 2020 Cyber Security Strategy and provides the following submission.

UWA's response focuses on:

- Responsibilities for cyber security and the Government's role;
- A trusted marketplace with skilled professionals; and
- A hostile environment for malicious cyber actors.

In particular, UWA's response highlights the need for greater support for cyber security across the higher education sector and other sectors of the Australian economy, specifically focusing on the resourcing of skilled professionals and sharing of cybersecurity services to protect the sector.

## Responsibilities for cyber security and the Government's role

UWA recognizes the importance of the Government's role in protecting the nation against Cyber related attacks and focusing its efforts on Australian businesses that provide essential services including energy, water, telecommunications and transport.

However, UWA believes that more focus is required on assisting Australia's higher-education institutions to ensure they have the necessary cyber security controls and practices in place to protect against cyber-attacks.

The targeting of the networks of Australian universities continues to increase. The Australian National University has been the target of 2 cyber-attacks that resulted in gaining access to sensitive confidential data of staff and students and the attacks reportedly originated from state actor(s).

Universities are an attractive target given their research across a range of fields and the intellectual property this research is likely to generate. In addition, universities often have a number of interlinked networks that connect to other organizations including hospitals, government, and defense organizations, providing a vector for cyber attackers to gain access. Higher education institutions often hold larger and more sensitive data sets than private sector organizations, however often with fewer resources and defenses in place to monitor and protect against cyber-attacks.

Whilst not considered "critical infrastructure", the compromise of national higher-education networks can present a risk to national security and the exposure of volumes of personally identifiable information that can result in significant harm to the community.

UWA believes that the Government should concentrate its efforts on addressing high impact, advanced and targeted cyber threats and events that would likely require substantial time to assess, respond to and recover from. This level of sophistication is often beyond the level most organizations are resourced or equipped to deal with. These types of threats could cause significant harm if targeted at critical infrastructure, and the higher education sector could be included within this scope and considered a "critical system" that potentially requires stronger cyber defenses.

UWA supports the Government's efforts in establishing industry standards and monitoring for cyber threats. UWA envisages an opportunity for greater participation from industry, both vendors and asset owners, in driving industry standards and dealing with "commoditized" high-volume/low-impact cyber threats.

UWA suggests that the Government might consider strengthening the accountability of executives in the private and public sectors for cyber security. A requirement for defined responsibilities for cyber security in organizations of certain criteria (size, revenue), similar to that adopted by other nations such as Singapore's Monetary Authority of Singapore (MAS) and the United States' sector-specific regulations, will establish cyber risk as a board-level agenda and be treated as a business-wide risk rather than a technology issue.

UWA believes the challenge in managing cyber risk facing Australian businesses and orgranisations, including higher education institutions, primarily involves sourcing skilled cyber professionals and providing the necessary resources to manage the risk. UWA believes that the government could assist in this national shortage of cyber security resources through the provision of shared services that could be shared across verticals. Examples could include a national security operation center (SOC), staffed by experts that could help institutions to monitor, prepare for, and respond to cyber-attacks. These shared cyber-security services could be provided at a national federal level or through regional state agencies.

## A trusted marketplace with skilled professionals

UWA believes that the Government has a leading role in the establishment of a trusted marketplace that is the first point of call for the community for products, services, and advice on cyber issues. A Government initiated and established a trusted marketplace will elevate the importance of cyber resilience within the community.

UWA believes that a marketplace which is well represented by a diverse range of cyber services spreading across different regional/geographical boundaries will provide the greatest benefit to the community. While cyber threats may be originated from different part of the globe, a localized response is often required to achieve optimum outcomes.

While the "top-end" of town is often able to have access to and afford cyber security service providers, small businesses typically rely on their technology retailer that may not have any competence to deal with cyber threats. In addition, there are monetary thresholds that have to be made before the law enforcment system is involved. As a result, the consequences of a major cyber incident to a small business can be financially crippling.

The marketplace would need to be supported by a national framework for the accreditation and/or registration of service providers and professionals providing cyber security services. The framework will include a core set of capabilities and delivered outcomes that are expected of a competent service provider.

The framework and/or registration process needs to be accessible and inclusive to different types of service providers, including small business operators and/or skilled professionals that may only specialize in a particular cyber domain.

A trusted marketplace that is integrated into existing Government's instruments such as the Australian Cyber Security Centre (ACSC) will be crucial for the continued maturity and sustainability of the marketplace. The continued resilience of the Australian economy relies on the ability to disseminate threat intelligence and mobilize the service providers that are appropriately skilled to minimize business disruptions.

UWA believes that the ACSC regional centers have a strong role in the delivery of framework competencies in the maturing of the marketplace at large. With the shortage in cyber security skills being felt across industries, the ability to establish "first-responders" to contain and mitigate cyber threats become more important.

## A hostile environment for malicious cyber actors

UWA believes that in order for Australia community to remain resilient within an increasingly hostile cyber threat environment, it requires the Government to drive a "cyber" agenda at a national level and involve the collaborations of both public and private organizations.

UWA believes that the Government should consider the pros and cons of introducing a set of cyber hygiene obligations that is based on industry standards and best practices, that is suitable for different business structures. By embedding these obligations within business licensing process, it could put cyber at the forefront of business viability.

The role of Internet Service Providers (ISPs) in the protection of the Australia community in the face of increased cyber hostility, either in sophistication and/or quantitatively, needs to be revisited. The ISPs will need to be able to offer affordable cyber-related services and/or products that can be bundled into existing business offerings. Cybersecurity services such as "basic malware detection" are a necessity in email offerings and not an "add-on".

## Next steps

We understand that the consultation process includes a series of roundtables in capital cities, and we look forward to participating in these.