GROUP OF EIGHT AUSTRALIA

The Group of Eight Limited
ABN 98 089 687 990

GPO Box 139
Canberra ACT 2601
Lvl 4, 10 Moore Street
Canberra ACT 2600
Australia

t: +61 (0)2 5123 6700
www.go8.edu.au

8 November 2019

Cyber Security Strategy & Governance Team
Strategy Governance & Industry Branch, Cyber Security Policy Division
Department of Home Affairs
E: cybersecuritystrategy@homeaffairs.gov.au

Go8 Submission to Australia's 2020 Cyber Security Strategy

The Group of Eight (Go8) thanks the Department of Home Affairs for the opportunity to submit to this important review of Australia's Cyber Security Strategy. Please note that this submission represents the views of the Go8 network. Member universities may also make their own, more detailed submissions.

The Go8 comprises Australia's world-leading, research-intensive universities, with:

- Seven of our members ranked in the top 100 universities in the world by the prestigious Academic Ranking of World Universities (2019);
- Ninety nine per cent of Go8 research rated as world class or above by the Excellence in Research Australia (ERA) exercise;
- The proportion of Go8 world-leading research being twice that of the rest of the sector; and
- Every dollar of Go8 research income being estimated by independent analysts London Economics to deliver close to ten dollars in benefits to the broader economy.

As noted above, the Go8 are Australia's leading research-intensive universities.

As such, we are deeply woven into the fabric of our successful, competitive economy.

We train the workforce of the future, we do the research that increasingly fuels industry and our economy, and we bring together the best and brightest minds from around the world in pursuit of national benefit. This makes us critical national assets in the prosperity of Australia, now and into the future.

This also makes us an attractive collaborative partner for other high-quality researchers and institutions around the world.

This is important. Research excellence is now a collaborative, international endeavour. The best and brightest minds need to work with the best and brightest minds in order to reach their full potential, regardless of where those minds are located. And advanced communications technologies now make that easier than ever before. It is no coincidence that the Go8, as Australia's highest performing research universities, also account for more than half of all Australian research papers with international collaborations.

However, along with greater opportunities, technologies bring an increased need to ensure certain protections are in place to maintain the integrity of the research that we do. This includes consideration of cyber security.

The key is to retain a balance between applying the necessary protections while maintaining the capacity of the sector to continue to engage in high quality collaborative partnerships.

It is essential that, in seeking to protect our assets, we do not inadvertently damage the very qualities that make them valuable in the first place, ie., the ability of our best minds to engage with, and learn from, their counterparts around the world.

The Go8 believes it is possible to balance these two competing needs. Universities have a long history of engaging on contract research with private industry or defence organisations, sometimes involving multinational partners, both of which have security or commercial in confidence requirements. The key is ensuring a scalable suite of measures that are proportionate to the degree of risk faced in each instance.

Recommendation: that Australia's cyber security strategies are designed to ensure a balance between providing the necessary protections while not impeding the relationships and exchanges that underpin Australia's social and economic prosperity.

Key elements of a risk-based approach

Universities have recently been working with Government on addressing cyber security risks to our sector. This work has been conducted as part of the University Foreign Interference Taskforce (UFIT) established by the Education Minister, Dan Tehan, and aimed at developing a set of best practice guidelines. [1]

The Taskforce has taken a risk-based approach, guided by a set of over riding principles, ie:

- Security must safeguard academic freedom, values and research collaboration;
- Research, collaboration and education activities are mindful of the national interest;
- Security is a collective responsibility with individual accountability;
- Security should be proportionate to organisational risk; and
- The safety of our university community is paramount.

These principles serve to confirm the broad values of the research and higher education sector, and are intended to underpin the development of individual measures.

A similar approach could also be taken at the national level, ie., what are the fundamental values of Australian society, and how should these underpin the development of the 2020 Cyber Security Strategy?

[1] https://www.education.gov.au/news/establishment-university-foreign-interference-taskforce

The Australian Values Statement, published on the Department of Home Affairs website, states that "Australian society values respect for the freedom and dignity of the individual, freedom of religion, commitment to the rule of law, Parliamentary democracy, equality of men and women and a spirit of egalitarianism that embraces mutual respect, tolerance, fair play and compassion for those in need and pursuit of the public good".[2]

Given this, the underpinning principles at a national level could include elements such as:

- The strategy must safeguard fundamental values such as the freedom and dignity of the individual, equality and the rule of law; and
- Security should be proportionate to degree of risk.

Elements such as these will help to ensure a degree of proportionality in any measures taken.

Recommendation: that the strategy adopt a risk-based approach, based on over riding principles based on fundamental national values.

Education and Training

Education and training must be a fundamental element of any cyber security strategy. The most sophisticated software in the world can be circumvented by a careless or naïve human action. A study conducted by researchers from the University of Illinois Urbana-Champaign, the University of Michigan and Google in 2016 found that 48% of 297 USB drives left scattered in a parking lot were picked up and plugged into a computer, some within minutes.[3]

Similarly, almost $1billion was lost to phishing scams in Australia in 2018, despite decades of public warnings not to click on links appearing in unsolicited emails or provide information during cold calls.[4]

This suggests that current approaches to public education are not yet sufficient. It could be useful to consider whether approaches taken in other countries could be applied to an Australian context. The "think before you link" campaign, for example, an Intel ® Security Digital Safety Program[5] aimed at promoting awareness and good practice in school children.

It is also essential that Australia foster a talent pool of highly skilled cybersecurity experts, a profession which is likely to be increasingly in demand.

In fact, investing in a suite of robust, extensive and high quality qualification offerings in this area could provide Australia with a valuable product that could be exported overseas.

[2] https://immi.homeaffairs.gov.au/support-subsite/files/life-in-australia/lia_english_full.pdf
[3] https://www.theregister.co.uk/2016/04/11/half_plug_in_found_drives/
[4] https://www.scamwatch.gov.au/about-scamwatch/scam-statistics?scamid=31&date=2018
[5] https://gtm-media-3.discoveryeducation.com/v3.3/CEP/CyberSafety_student/index.html#/

The Go8 acknowledges the recent announcement by Minister Coleman of the Global Talent – Independent Program, which will fast track the immigration into Australia of highly skilled individuals in key areas, including cybersecurity. This will help us to recruit the best minds in the world to boost our domestic capacity.

But this alone will not be sufficient. We urge the Government to consider how it might develop a whole of sector strategy to build cybersecurity competencies and skills across all levels of education, from primary school through to doctorate.

Recommendation: that government work with the higher education sector to develop a comprehensive awareness, education and training strategy to promote good practice across the Australian community, and to develop a suite of robust cyber security qualification options across all levels of education

Along with education and training, there is also the important principle of information sharing.

While the Go8 understands there are dangers in releasing too much information following a cyber-attack, this should not preclude the important role that information sharing can provide in promoting better knowledge and practices across Australian society.

In 2018 the Australian National University (ANU) was subject to a sophisticated cyber security attack. ANU's decision to publish the findings of their investigations – while avoiding the release of details that could enable a copycat attack – provided invaluable information to other organisations in designing or reviewing their own cyber security strategies. [6] If they had chosen not to share this information, this capacity to benefit from lessons learned would have been lost.

Government agencies, such as the Australian Cyber Security Centre (ACSC), are privy to information not accessible by most organisations. While this is often entirely appropriate, the ANU example shows that it is possible to use this type of knowledge to aid Australia's cyber security defenses, while maintaining security measures.

Recommendation: that the Government consider establishing reliable communication and information sharing channels between relevant agencies and Australian industry, including the higher education industry, which will help to ensure greater knowledge and understanding of the evolving threat environment, and possible mitigation strategies.

Yours sincerely

[redacted]

VICKI THOMSON
CHIEF EXECUTIVE

[6] https://imagedepot.anu.edu.au/scapa/Website/SCAPA190209_Public_report_web_2.pdf