SUBMISSION TO AUSTRALIA'S 2020 CYBER SECURITY STRATEGY DISCUSSION PAPER

November 2019

Universities Australia (UA) welcomes the opportunity to make a submission to the Australia's 2020 Cyber Security Strategy discussion paper.

UA is the peak body for Australia's 39 comprehensive universities. Our members are spread across Australia, in both regional and metropolitan areas. They educate more than a million students each year and undertake research that adds to Australia's stock of knowledge, and to Australia's economic and social wellbeing.

UA thanks the Department of Home Affairs for working with UA to organise a higher education roundtable on 28 October to receive input from the university sector. The points below reflect in part the input provided at the roundtable.

KEY POINTS

Universities are both affected by cyber security and are active participants in managing the national response to cyber security readiness. Universities are involved in the education of the current and future cyber workforce, as well as at the forefront of cyber security research capability. Universities also contribute significantly to innovation in cyber security by developing products and services, and through industry engagement.

Cyber awareness

Universities understand that awareness of cyber threats and risks is a key aspect of preventing cyber security incidents. Work by the University Foreign Interference Taskforce is working actively to add to existing safeguards.

The potential for a community campaign on cyber security awareness has been raised. Whilst cyber security is a complex topic, there could be merit in examining such an initiative. Any initiative should be led by government, with the support of stakeholders, including universities, across the community.

Universities also understand their role in educating their staff and students in cyber safe practices. This cyber awareness has the potential to flow through into the community from those staff and students, thereby raising the overall level of community awareness and facilitating cultural change.

The experience of individual institutions is that the success of education programs is mixed, and a common finding is that the effects tend to be short lived. The effectiveness of programs needs to be measured over a number of years, given it takes time for cultural change to take hold. There may be benefit in the development of a common set of education materials by the appropriate government agencies that universities, as well as other education and community organisations, could draw on.

Education and skills development

A key difficulty in the provision of training and education for cyber security is the ill-defined nature of a 'cyber security professional'. Given the broad fields of education, skills and occupations involved, defining the key elements would enable the strategy to connect with the relevant stakeholders. A common view expressed at the higher education roundtable was that cyber security is not only about the training of cyber security specialists but involves a broad range of other occupational groups. For example, it is essential for an IT help desk operator to be familiar with aspects of cyber security.

Cyber security, and the required education and skills, are issues that cut across society and the economy. The strategy would benefit from an articulation of how the skills required map into education and training providers, as well as other relevant entities. These include universities, vocational education providers, third party providers and industry. Such an examination should also note the linkages and flows between these sectors. Industry, in particular, is both a significant source of, and consumer of, cyber security talent. An examination of the mechanisms through which industry could contribute to the education and training system would be worthwhile.

It was noted in the roundtable discussions that Australia may need a different model for the external accreditation of cyber security courses. A consideration of the current mechanisms against the scale of accreditation that may be needed in the future would be useful.

Research

Research is currently absent from the strategy. A rapidly evolving field like cyber security requires a responsive research ecosystem to both identify and understand current and emerging challenges. Research also enables the training of highly-skilled cyber specialists, and is an important input into commercial opportunities to support Australian industry. Universities are a primary agent in the research system and make a significant contribution in these areas.

Further work in mapping the cyber security research landscape, articulating the roles of universities, industry and government, and the efficiency of the connections between them would be worthwhile. In any such exercise, international collaboration should also be considered as a key input into the research process.

Roles and responsibilities

Cyber security is a broad issue that spans many areas of economic and societal activity. Government has leadership, facilitation and coordination roles in managing this complexity.

CONCLUSION

Universities can contribute to the cyber security of Australia in multiple ways, including:

- the education and training of the current and future workforce;
- as a key provider of research capability to enable the identification and management of current and emerging threats; and
- to assist in raising awareness of cyber security challenges.

UA encourages the Strategy Group to actively consider these contributions, and would welcome further discussions on the areas identified in the submission or any other matters.