Australian Catholic University

Feedback on *Australia's 2020 Cyber Security Strategy – A Call for Views*

October 2019

Feedback on *Australia's 2020 Cyber Security Strategy: A Call for Views*

Executive Summary

Australian Catholic University (ACU) welcomes the opportunity to comment on the Australian Government discussion paper *Australia's 2020 Cyber Security Strategy: A Call for Views* (Discussion Paper).

We also note that we support and are an active participant in the working group preparing the collaborative response from the Council of Australian Directors of Information Technology (CAUDIT).

ACU shares the Australian Government's view that a reassessment of the nation's approach to cyber security is warranted given the changing circumstances that Australia and Australians face. These circumstances include:

- greater national reliance on information technology (IT) enabled and controlled infrastructure;
- greater business and organisational reliance on a digitally enabled economy for survival and growth;
- greater reliance by individuals on a digital/online world to navigate their lives; and
- increased threats and more determined threat actors.

We understand the fundamental underlying question being asked is:

> How do we keep Australia and Australians safe, while taking advantage of new technology and the online world?

The Discussion Paper also has a particular focus on who should play what roles in keeping us safe, and singles out end-users, providers (organisations including business and not-for profit), and governments as the key entities. While the Discussion Paper contains 26 specific questions, we understood these to be prompts for consideration rather than requiring an individual answer to each. As such, we have chosen to respond to the paper by exploring our thoughts on three key questions:

- What are the cyber security needs of individuals and groups?
- What measures/recommendations could be effective and efficient in meeting those needs?
- Who is best placed to undertake these measures?

In answering these questions, we assume that the current landscape of measures and services exists and do not explicitly call these out except where we suggest that change is needed. In Section I, ACU seeks to distill the key cyber security needs of individuals and groups, including businesses and government. Section II makes recommendations, in line with these identified needs, on measures that could enhance the effectiveness of the nation's cyber security, and on who is best placed to enact these measures.

LIST OF RECOMMENDATIONS

ACU makes the recommendations below with respect to improving cyber security in Australia. However, ACU also notes that it is only through a national ecosystem, with multiple entities playing appropriate roles, that Australia will be able to improve the nation's cyber security posture and address the challenges we collectively face.

Recommendations

R1. Lead a national conversation through increased public education and awareness.
R2. Develop an online provider assurance/rating
R3. Stimulate Australian capability and skills development
R4. Further develop guidelines, including industry specific guidelines
R5. Package simple access to appropriate cyber security services
R6. Stop low level, high volume threats at a national level
R7. Share and encourage the timely sharing of threat intelligence
R8. Further increase government agency responses to threats to the nation

I. Cyber Security Needs of Individuals and Entities

INDIVIDUALS

There is no doubt that the actions of individuals are critical in ensuring a safe information security environment, within both private and employment contexts. However, individuals are currently the least empowered in fulfilling this role.

Individuals face a difficult task in understanding the risks that they face in the digital landscape. While the headlines frequently feature news of data breaches and cyber security related events more generally, little information is available to advise users of what that means for them. Campaigns by governments and other organisations to date have perhaps not broken through with their messages, and they certainly have not done so consistently.

In addition, while we typically talk about actions that business and government take, it is the actions of the individuals within them that make those organisations more, or less, safe. Creating awareness and a culture that recognises appropriate risks and actions as well as avoids blame in favour of lessons learnt, has the potential to significantly improve the wellbeing of organisations and the nation as a whole.

Once individuals are sufficiently aware, they also need to minimise their risks of obtaining goods and services online.

It is currently not clear to individuals how they can do so. Short of ceasing to use online goods and services, which is not practical in the modern world, people need to find ways of judging the appropriate risk tolerance for their circumstances and the cyber security stance of the service providers. This is a complex task that we cannot expect most individuals to undertake given the constantly changing cyber threat landscape and the limited information available to them.

SMALL AND MID-SIZED ORGANISATIONS

In some aspects, the needs of small and mid-sized organisations (hereafter "SMEs"), such as small business and not-for-profits, are similar to those of individuals in that they lack sufficient resources to understanding risks and evaluate the most appropriate responses.

In addition, most such organisations, in turn, face the prospect of needing to deliver services to individuals who will make judgements about the safety and attractiveness of the SMEs' online services. To do so, SMEs need to understand what actions they need to take to achieve and enhance their online reputation. This will tend to vary by sector and the service that is being provided.

SMEs also need to have easy and cost-effective access to the goods and services that they need in order to take the appropriate actions. Both this information, and the services, are not obvious nor easily accessible for SMEs. For example, it is not reasonable to expect such organisations to conduct a full evaluation of all the tools that help to protect from malware on the market and to select those that are most appropriate. Nor is it reasonable for them to know how to select the most appropriate skilled professionals.

LARGE ORGANISATIONS AND CRITICAL INDUSTRIES

Larger organisations and providers of critical infrastructure (LCOs) face a significantly increased range of threats, as they tend to be targeted by considerably more determined attackers, such as state actors, hacktivists, and large criminal gangs. There is also a greater burden on LCOs to provide assurance that they are in fact managing most threats. Typically, this is due to their larger cohort of stakeholders including other businesses, or in the case of some industries, the critical infrastructure they support and the need to assure government regarding threats to the nation.

In summary, in order to fulfil their roles, LCOs need to:

- keep themselves operating against determined and skilled attackers;
- provide assurance and maintain their reputation with governments and other stakeholders;
- obtain good industry specific advice on how to do these things; and
- have access to appropriate services to undertake the appropriate actions.

GOVERNMENT

Government's goals are no less than to assure a safer nation, safer people, and a safe and more productive economy. By the nature of these goals, government is required to look at the landscape much more broadly than any others and their needs are therefore on a larger and broader scale.

In order to fulfil their roles, government needs to:

- assure that critical national infrastructure is as safe as possible;
- assure that critical sectors of the economy are as safe as possible;
- minimise foreign interference;
- improve the economy through encouragement of growth and investment in a safe place; and
- keep individuals feeling secure.

SUMMARY OF NEEDS

Table 1 below provides a summary of the cyber security needs of individuals and groups, shown assembled by the type of need, as identified by ACU.

Table 1. Identified Needs

Need	Individual or group
N1. Understand/awareness of the risks	All
N2. Understand safety/quality of online providers	Individuals Small & Medium Organisations
N3. Obtain industry specific advice on actions to take	Small & Medium Organisations Large Organisations & Critical Industries
N4. Have good access to appropriate services to fulfil cyber security responsibilities	Small & Medium Organisations Large Organisations & Critical Industries
N5. Provide assurance and maintain their reputation with governments and other stakeholders	Large Organisations & Critical Industries
N6. Keep themselves operating against determined and skilled attackers (including foreign interference)	Large Organisations & Critical Industries Government
N7. Assure that critical national infrastructure is as safe as possible	Government
N8. Assure that critical sectors of the economy are as safe as possible	Government
N9. Improve the economy through encouragement of growth and investment in a safe place	Government
N10. Keep individuals feeling secure	Government

II. Cyber Security Improvement Recommendations (Measures)

This section outlines a range of measured that can make a difference to the nation's cyber security effectiveness in line with the needs outlined in the previous section. We also outline here which roles we believe are best placed to enact these measures.

At the outset, however, it is useful to first comment about the current state of the global cyber security environment. Cyber security is a known set of risks, with a range of frameworks, models, standards and research. However, there are elements of the "wild west" mentality around the landscape of services and capabilities offered to meet cyber security threats, not dissimilar to that seen around the time of the "dot com boom" (and subsequently, bust). Because of the rapidly changing risk landscape and threat actors, new and existing companies and consultancies offer constantly evolving services and capabilities, with often exaggerated claims of new methods and skills to counter the latest threats. In this somewhat immature market, it is often only actors such as governments that are sufficiently well-established, skilled, and resourced to assist in meeting the challenges.

This informs ACU's identification of the roles that we believe are best placed to perform the actions in the recommendations below. It is also the reason that we suggest cooperative industry specific groups could play a key role in the ecosystem. The industry groups would play a custodian role for the respective industry, assisting in developing guidelines and/or shared services, in partnership with relevant government agencies. CAUDIT, mentioned earlier, is one example of such a group that is beginning to undertake these roles. Such groups could be designated for each industry that is of particular concern to Australia - those important for national security (utilities, academia, etc) and the top industries that are critical for the economy.

Table 2 provides a summary of the recommendations made by ACU in this section, matched to the needs identified in Section I.

LEAD A NATIONAL CONVERSATION THROUGH INCREASED PUBLIC EDUCATION AND AWARENESS

Awareness and understanding of the risk of cyber security is crucial to Australia's ability to manage it. Government must lead a significant national conversation similar to other campaigns such as on alcohol consumption, sun safety, smoking, and workplace health and safety. Government is already providing a degree of education to individuals/citizens. This must be simplified, with clear messages in relation to the potential impact of these risks on individuals, as well as the minimum steps that people are advised to take in avoiding them. There is a need to evolve the culture to one that enables a much more informed conversation about risk tolerance, avoidance, and mitigation, as well as lessons learned from cyber security events. Communication must also be strengthened significantly to reach people wherever they are – social media, traditional media, the workplace, and so on. Government could seek to enable the learning at an early stage, by directing the embedding of cybersecurity awareness training in school curricula.

DEVELOP AN ONLINE PROVIDER ASSURANCE/RATING

The Government can seek to minimise individual (and businesses) risks of obtaining goods and services online through the provision of information about the cyber security stance of service providers and services. This could be achieved through the introduction of a recognisable rating or certification for services and equipment. It could take the form of an easy-to-interpret "star" rating or "tick" emblem, such as those provided for car safety, for the energy efficiency of appliances, or the heart health tick. This would establish a base level, or levels, of cyber protection that people and organisations could rely on. Furthermore, it would raise awareness within the community, and potentially increase competition amongst online providers regarding the quality of cyber security protection.

A challenge that would need to be overcome is that cybersecurity products and services can rapidly lose their effectiveness as new types of threats emerge or as new versions of those services and products are issued. Another challenge would be the potential cost of becoming certified, which could especially disadvantage SMEs. Some form of continuous and automated online certification could be investigated to assist with these challenges.

A similar scheme could be considered for cyber security products and services themselves, in order to make it simpler for SMEs and other organisations to make choices and to stimulate local cyber security development.

STIMULATE AUSTRALIAN CAPABILITY AND SKILLS DEVELOPMENT

There are already a range of Australian cyber security organisations providing products and services in the local and global marketplace. However, the incentives for cyber security professionals to join global companies and/or to migrate overseas is high, with significant demand and global shortages.

Economic incentives to encourage research and innovation in cybersecurity for local businesses and universities may tip the balance in favour of stimulating local cyber security work. As mentioned earlier, a scheme for recognition of high-quality cybersecurity providers could also be instituted.

In terms of skills, government could look at funding additional places for cyber security related qualifications at various levels, from micro credentials through to research degrees. Standards for cyber security qualifications could be created at a national level. Reaching a qualification level under these standards could make graduates immediately more recognisable for employment within Australia and thereby encourage them to stay in the local sector.

Certain higher levels of such qualifications, together with background checks, could be considered as a minimum standard for security roles that deal with sensitive information. These could, if developed, be made mandatory for people in such roles in all organisations, not only government.

FURTHER DEVELOP GUIDELINES, INCLUDING INDUSTRY SPECIFIC GUIDELINES

A key role that the government is well placed to undertake or in some cases to collaborate with others to play, is the provision of expected standards and guidelines for cyber security defences within the economy and within specific sectors.

The Australian Government already provides general guidelines including the Essential 8 and the Information Security Manual. It could seek to strengthen existing guidelines and look to potentially improve and better communicate some or all of these. Strengthening the privacy regime to a level similar or the same as that of EU General Data Protection Regulation (GDPR) guidelines, for more rapid reporting and effective action, could also be considered.

While the Australian Government could also seek to make some or all of the guidelines mandatory for both government and non-government organisations to follow, the compliance costs may prove prohibitive for many smaller organisations and perhaps uncompetitive with organisations in other jurisdictions that do not have the same costs. If the Australian Government was to make some guidelines mandatory, these could perhaps be stratified by the size of the organisation. For instance, SMEs could be asked to follow the most basic set such as privacy and essential 8 related guidelines, and larger organisations to follow a larger or full set of requirements.

In the first instance and given the level of maturity of the cyber security landscape, a better approach may be to work with industry groups to develop industry specific guidelines or minimum standards to better inform each sector. Such industry vertical organisations can be more responsive than the government to the specific risks and cyber security needs of industries – clearly health data held by local GP practices has a different sensitivity than data held by companies that sell homewares. The Australian Government could consider making such organisations, standards, and services mandatory for sectors that have an impact on national security and for the most important industry sectors for the Australian economy. Some such organisations (CAUDIT is given as an example earlier) have also begun to develop industry specific shared services and these could be encouraged and incentivised by government.

PACKAGE SIMPLE ACCESS TO APPROPRIATE CYBER SECURITY SERVICES

The landscape for services and capabilities offered to meet cyber security threats is currently fragmented and constantly changing. Larger organisations, providers of critical infrastructure, and key government agencies will often need to do their own due diligence on their needs, and purchase or develop appropriate tools. Such organisations have both more significant and specialised threats and the resources to undertake such work. However, this is not as simple for other organisations; particularly for SMEs.

Mechanisms to assist organisations towards achieving the recommendations laid out in guidelines or standards are important in order to lower the burden of compliance and to ensure a safer landscape for all. Education/awareness,

threat intelligence, and national blocking of low-level threats are covered elsewhere. However, it may also be useful to consider what can be done to provide services that are cost effective, and easy to understand, select, and consume. As mentioned earlier, it may be possible to encourage industry organisations to provide shared services. In addition, government negotiated panels with lower pricing already exist in various domains and may be useful.

Free or subsidised provision of resources by government may not be feasible. However, an alternative mechanism that may be considered as particularly helpful for SMEs, is the provision of some bundles of services by a government-run provider, operating as a market setter/leader. This could be seen as similar to, for example, how Medibank Private was originally set up in the health insurance market. Such a provider could select and bundle services that work well together in meeting a minimum level in a set of guidelines. It could also work in concert with the provider assurance/rating proposed earlier – for example, an SME that implements the "silver" bundle of services from this provider would be certified as meeting the "silver" assurance rating and could advertise this to the public. An alternative to a government-run provider would be to direct telecommunications/internet service providers (ISPs) to provide such packages of services as directed by government to meet these assurance ratings.

STOP LOW LEVEL, HIGH VOLUME THREATS AT A NATIONAL LEVEL

There is a large volume of relatively unsophisticated or known attacks that could, with appropriate guidance from government agencies, be blocked by telecommunications providers from reaching individuals and organisations. This could be part of filtering done at international entry points to Australia and within Australia, as a part of all telecommunications offerings. This would remove a lot of clutter from the data even reaching systems; ensuring that individuals and particularly organisations can target their efforts at more complex or targeted threats. There would need to be appropriate checks and balances, including reporting and review, to ensure that this action is not used inappropriately.

Another area where telecommunications companies could put some controls in place is around ensuring equipment connected to the nation's networks is up to date. Many individuals at home or in small businesses are operating with old technology that connects them to the internet, which doesn't meet or is not set up with minimum acceptable security standards. Government could assist individuals and SMEs to keep equipment up to date by dictating a minimum currency of versions/standards for connection to an ISP in terms of equipment and firmware. ISPs could then be asked to automatically exclude equipment that does not meet current versions/standards and to provide some guidance to subscribers to update it.

SHARE AND ENCOURAGING THE TIMELY SHARING OF THREAT INTELLIGENCE

Government agencies currently provide threat intelligence to organisations in some limited circumstances and particularly when a state actor is suspected. Such government agencies have much broader capabilities and access to intelligence than any other organisation or individuals in Australia. In addition, in many cases organisations currently pay for intelligence from private global companies, when it is already held by government. This is perhaps an inefficient use of limited cyber security resources by those organisations. Notwithstanding some circumstances where national security reasons dictate that the intelligence cannot be revealed, in most cases agencies should provide advice and automate cyber threat intelligence feeds to institutions and private enterprise rapidly, to enable appropriate response.

Government security and Defence agencies are also aware of a range of leaked credentials from organisations. These are sometimes but not always advised to the organisations. Agencies could be asked to play a stronger hand in providing information and advice on leaked credentials to organisations and individuals that are affected.

FURTHER INCREASE AGENCY RESPONSES TO THREATS TO THE NATION

As with threat intelligence, the capability to respond to sophisticated targeted attacks to national infrastructure, Defence assets, and commercial sectors that are critical to the economy is, for the foreseeable future, the domain of government security and Defence agencies. We recognise the efforts already made by such agencies in this regard and recommend that they continue and expand. Further, public recognition that this effort will be consistently undertaken, may in itself deter some threat actors.

SUMMARY OF RECOMMENDATIONS

Table 2 below provides a summary of ACU's cyber security improvement recommendations, which are listed alongside: 1) the entities that are best placed to provide them; and 2) the cyber security needs that they assist in meeting.

Table 2. Recommendations to improve cyber security in Australia

Recommendation	Provided by	Meets Needs
R1. Lead a National Conversation Through Increased Public Education and Awareness	Government	N1. Understand/Awareness of the risks N10. Keep individuals feeling secure
R2. Develop an Online Provider Assurance/Rating	Government	N1. Understand/Awareness of the risks N2. Understand safety/quality of online providers N10. Keep individuals feeling secure
R3. Stimulate Australian Capability and Skills Development	Government & Education Sector	N5. Provide assurance and maintain their reputation with governments and other stakeholders N6. Keep themselves operating against determined and skilled attackers (including foreign interference) N7. Assure that critical national infrastructure is as safe as possible N9. Improve the economy through encouragement of growth and investment in a safe place
R4. Further Develop Guidelines, Including Industry Specific Guidelines	Industry Groups with Government	N3. Obtain industry specific advice on actions to take N5. Provide assurance and maintain their reputation with governments and other stakeholders N7. Assure that critical national infrastructure is as safe as possible
R5. Package Simple Access to Appropriate Cyber Security Services	Government	N4. Have good access to appropriate services to fulfil cyber security responsibilities
R6. Stop Low Level, High Volume Threats at a National Level	Telecomms. Providers with Government	N4. Have good access to appropriate services to fulfil cyber security responsibilities N10. Keep individuals feeling secure
R7. Share and Encourage the Timely Sharing of Threat Intelligence	Government	N6. Keep themselves operating against determined and skilled attackers (including foreign interference) N8. Assure that critical sectors of the economy are as safe as possible
R8. Further Increase Agency Responses to Threats to the Nation	Government	N6. Keep themselves operating against determined and skilled attackers (including foreign interference) N7. Assure that critical national infrastructure is as safe as possible N8. Assure that critical sectors of the economy are as safe as possible

ATTACHMENT A

Australian Catholic University Profile

Australian Catholic University (ACU) is a publicly funded Catholic university, open to people of all faiths and of none, and with teaching, learning and research inspired by 2,000 years of Catholic intellectual tradition.

ACU operates as a multi-jurisdictional university with eight campuses, across four states, one territory, and overseas. ACU campuses are located in North Sydney (NSW), Strathfield (NSW), Canberra (ACT), Melbourne (Victoria), Ballarat (Victoria), Brisbane (QLD), Adelaide (SA), and Rome (Italy).

ACU is the largest Catholic university in the English-speaking world. Today, ACU has around 34,000 students and 2,000 staff.[1]

ACU graduates demonstrate high standards of professional excellence and are also socially responsible, highly employable and committed to active and responsive learning.

ACU has built its reputation in the areas of Health and Education. ACU produces more nursing and teaching graduates than any other university in Australia, serving to meet significant workforce needs in these areas.[2]

ACU has four faculties: Health Sciences; Education and Arts; Law and Business; and Theology and Philosophy. This consolidation of ACU's previous six faculties in 2014 has created a more efficient and competitive structure focused on the needs of industry and employment partners. ACU has also moved towards the adoption of a shared services model where suitable, to improve efficiencies, internal processes and better allocate resources.

ACU is committed to targeted and quality research. ACU's strategic plan focuses on areas that align with ACU's mission and reflect most of its learning and teaching: Education; Health and Wellbeing; Theology and Philosophy; and Social Justice and the Common Good. To underpin its research intensification efforts, ACU has appointed high profile leaders to assume the directorships, and work with high calibre members, in its research institutes.[3] ACU is a world-leading research university in its priority areas of education, health, and theology and philosophy.

[1] Student numbers refer to headcount figures while staff numbers refer to full-time equivalent (FTE).
[2] Department of Education and Training, '2017 Special Courses' in *Selected Higher Education Statistics – 2017 Student Data* (2018). Accessible via https://www.education.gov.au/selected-higher-education-statistics-2017-student-data.
[3] See Australian Catholic University, 'Research at ACU' via http://www.acu.edu.au/.