THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

The University of Queensland’s submission to Australia’s Cyber Security Strategy 2020

Contents

Executive summary

- Cyber security should be treated holistically by both the public and private sector in a manner similar to a public health issue.
- Include appropriate cyber security and cybercrime awareness messaging at all levels of education.
- There is a critical need to promote guidelines for cyber security curricula across all levels, but not in an overly-prescriptive manner.
- To support quality teaching of cyber security there needs to be a scheme to help the university sector to match the remuneration of cyber security lecturers to close-to-market rates.
- Provide intelligence on cyber security events and data breaches to researchers.
- Effective and timely sharing of cyber security intelligence is critical to supporting the hardening of Australia as a target against cybercrime.
- Enhance the JCSC initiative further to better facilitate the formalised development of platforms and trusted networks for the Government to share intelligence in a timely manner.
- There are limitations on how timely and openly the ACSC shares cyber security intelligence with private sector stakeholders.
- Consider options for a Cyber Security "Civil Defence" capability.
- Consider if an intelligence agency (ASD) the best place for the Government’s national CERT capability (ACSC).
- Consider the development and adoption of a consumer-friendly cyber security product rating.
- To support the creation of standards for IoT devices, a network of device security testing labs could be established.
- Government should prioritise the development of external assurance frameworks for software development.
- Consideration should be given to creating cyber security guidelines for the higher education sector

Introduction

The University of Queensland (UQ) is in the world’s top 50 universities and is renowned for the quality of its teaching and research, it also hosts the national not-for-profit security group, the Australian Cyber Emergency Response Team (AusCERT). AusCERT is Australia’s pioneer cyber emergency response team and it helps members prevent, detect, respond to and mitigate cyber security incidents. UQ appreciates the opportunity to contribute to Australia’s 2020 Cyber Security Strategy and the collaborative nature of the Government’s engagement in this important area.

Cyber security should be treated like a public health issue

With the all-pervasive nature of the ever interconnected economy and the exponential nature of cybercrime, there is a growing need for cyber security to be treated holistically, by both the public and private sector, in a similar fashion to public health issues. This requires a diverse range of responses from fundamentals taught to children through to deep discipline-specific actions. Just as children are taught to wash their hands and look before crossing the road, cyber security fundamentals and cybercrime awareness should be taught from a young age and become embedded in the culture of future generations. This necessitates changes to national, state and territory school and higher education curricula to ensure appropriate and consistent cyber security messaging is included at all levels of education. Additionally, as with public health campaigns, cyber security and cybercrime awareness strategies should also include ongoing campaigns using various media.

Cyber Security Skills

There are several key challenges in the uplifting of cyber security skills across different levels of knowledge, and across different stakeholder needs in Australia. There is a need to map the skills pipeline from K-12, and then to vocational institutions (e.g. TAFE) and universities. Alongside the mapping of the skills pipeline would be the mapping of the professional development and certification options available to professionals seeking skills upgrading or technical knowledge. There is a critical need to promote guidelines for curricula across all levels, but not in an overly-prescriptive manner. For example, the skills required for K-12 would differ strongly from the needs of vocational training. UQ would be happy to contribute to the development of draft curricula with other stakeholders in the skills pipeline.

There is also a lack of support for the training of teachers within the education sector. It is common to find teachers randomly allocated with the responsibility to teach digital technologies or to teach cyber security without much time or professional development. We encourage the government to consider a strategy to address this gap, as it will have the potential to introduce generational change through schools.

Cyber Security Teaching Talent Attraction and Retention

Within the university sector, it is extremely difficult to hire the right people to teach and research cyber security. There are many factors influencing this, including (1) the relative lack of skilled high-tech individuals willing to join the academic sector, (2) higher remuneration in the private sector, and (3) for overseas candidates, the time it takes for the visas to be issued. Many universities have to re-advertise positions and the process to hire the candidate meeting our selection criteria takes at least nine months and sometimes up to a year – from the time of advertising the position. It would be ideal if the Government introduced grants or schemes which would enable the university sector to match the remuneration of cyber security lecturers to close-to-market rates. Such grants were recently introduced by the Japanese government with great success, with their ability to hire more experts from overseas to fill in their positions. Similarly, the government could introduce schemes which incentivises industry to second skilled professionals to teach in universities as adjuncts or as part-time lecturers to fill the gap.

Government cyber security information sharing

Sharing information for research

Much valuable information on breaches and cyber security events are inaccessible for research, yet they can provide valuable insights into how Australia's cyber security posture could be strengthened. For example, notifications under the Mandatory Data Breach Notification scheme are confidential, and only published in broad, sectoral aggregate form. Appropriate, secure access to details of the reports would allow researchers to identify systemic sectoral and organisational weakness, which in turn can drive policy and regulatory change. More broadly, stronger linkages should be developed with the University sector to allow impactful research that meaningfully contributes to the challenge, beyond traditional technology research.

Timely intelligence sharing

Effective sharing of cyber security intelligence is critical to supporting the hardening of Australia as a target against cybercrime. Sharing of cyber security intelligence must be timely and content described at a level of detail that supports the following purposes.

Generally, intelligence is used:

- First, to identify new threats and risks to inform proactive security measures; and
- Second, to identify and respond to current threats.

The Australian Government should participate as openly as possible in both forms of intelligence sharing for the benefit of all organisations and the broader community. While the JCSC model is starting to show some benefit, as it becomes part of the information security industry culture, it would be beneficial if the Government enhanced the JCSC initiative further to better facilitate the formalised development of platforms and trusted networks for the Government itself to share sensitive cyber security intelligence in a timely manner.

A way is also needed to anonymously report indicators of compromise (IoC) to a central agency which is then disseminated out freely so businesses and Government can inform the wider community of cyber security threats and not just limit intelligence to the agencies that the Government identifies as relevant for them to partner with.

Re-Assessing the Government National CERT/ACSC

The current structure of having a Government CERT function, the Australian Cyber Security Centre (ACSC) under an intelligence agency, the Australia Signals Directorate (ASD), creates limitations on how timely and openly the ACSC shares cyber security intelligence with private sector stakeholders.

It may be of benefit for the Australian Government to consider options for a Cyber Security "Civil Defence" capability, under appropriate supervision which broadens the reach of public outreach and education, and can be mobilised in response to cyber events outside the remit of existing agencies. Such a concept has been around since at least the 1990's internationally, however they have tended to focus more on critical infrastructure than the broader society and economy.

The most recent Government cyber security strategy in 2016 allowed a department dealing with trade and foreign affairs to financially assist in the creation of National CERTs in the Pacific Island nations. The existence and persistence of these CERTs depends on the interaction with other like mandated CERTs and free information sharing between international governments. Without Australia’s ability to freely share IoC with other National CERTs as these newly formed cyber security groups may not be able to continue due to lack of support.

With intelligence sharing constraints from ASD impacting the ACSC, insurance organisations may also lack quality actuarial information required to make their cost of participation and policies reflect the need of the market. Actuaries make calculations on statistical information and a lack of information translates to higher safety margins, resulting in a swath of Australian businesses discounting entering such cover. A lack of event and impact information also skews the design of policies in a manner that a legal out-clause is made in favour of the insurer even if criminal behaviour in the cyber space has been long standing. The funding model for a National CERT/ ACSC, with economy-wide responsibility, should not be limited temporarily and distributed as project work, from project funding. Setting up an effective CERT operation is a significant project in itself, including gathering critical knowledge to provide consistent service, and establishing national and international points of contact.

Increase the security of cyber security and digital offerings

Standards for IoT Devices

It would be beneficial for Australia if the Government developed and adopted a consumer-friendly cyber security product rating, similar to the Health Star Rating for food products, and the Energy Star system for electrical devices. Such concepts have been considered elsewhere, such as the 2018 NIST Interagency Report (NISTIR) 8200 which contemplated IoT Cyber security standards, however this suggestion is specifically focused on giving consumers access to digestible information that can inform purchasing decisions. Such a system would require significant support both in development and execution, and universities would be well placed to contribute to this. Further, widespread public information campaigns, as part of broader cyber security public outreach, would also be essential for adoption and impact. Clear guidelines would be developed that indicate the expected benchmarks to be met for a product to receive a certain rating or accreditation.

To support the creation of standards for IoT devices, a network of device security testing labs should be established, for example within the University sector, adequately resourced by public funding as well as levies on manufacturers and importers, whose purpose is the assess and accredit the security of devices destined for the Australian market.

Cloud services

Like many businesses, universities are increasing their use of cloud-based services for which contractual controls are required to mitigate cyber security risk. As cloud-based vendors have captured greater market share it has become more difficult for even large customers to negotiate sufficient contractual controls. The Government should consider strategies to leverage the combined purchasing power of agencies to raise the general standard of security offerings by cloud vendors, specifically in relation to SaaS, by strengthening security clauses in contractual frameworks used by government.

The deployment of cyber security controls is now a significant cost of business. Software vulnerabilities are a major cause of security incidents, however it is difficult for customers to identify software vendors with adequate secure software development practises. As a result, the software industry is driven by features and innovation far more than adequate security quality. Government should prioritise the development of external assurance frameworks for software development, to ultimately improve the quality of software and manage the escalating cost of incidents resulting from software vulnerabilities.

Higher education guidelines

UQ applauds the recent initiative to create cyber security guidelines for the higher education sector. Guidelines which are well grounded in the reality and experience of the higher education sector will raise standards whilst supporting existing efforts and provide needed assurance to consumers.

Summary

The challenges that an ever increasingly interconnected world brings in relation to cybercrime means that there is a growing need for cyber security to be treated holistically. Approaching cyber security in the same way a national health issue is addressed from fundamentals taught to children through to deep discipline-specific actions and public information campaigns can support cyber security messaging. There is also a critical need to promote guidelines for cyber security curricula across all levels, but not in an overly-prescriptive manner. To attract quality educators into the cyber security space, consideration needs to be made on how remuneration for teachers and lecturers can be improved. The Government needs to consider whether ASD is the best place to house the national CERT function and also improve intelligence sharing to make it timely and widely distributed. A civil defence capability could support the ACSC and help private sector organisations in a way that the ASD led organisation cannot. The JCSC model is starting to show some benefits, however it needs to be enhanced to facilitate the formalised development of platforms and trusted networks for the Government to share intelligence to all sectors in a timely manner. Standards should be considered for IoT devices and the Government should prioritise the development of external assurance frameworks for software development. It is appreciated that the Australian Government is seeking wide ranging responses to consider for Australia’s 2020 Cyber Security Strategy.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

www.uq.edu.au

CRICOS Provider Number 00025B