Australian
National
University

Canberra, Friday 1 November 2019

Antony L. Hosking, PhD (Professor)
Director, RSCS
T: [redacted]
F:
E:
108 North Road, Acton, ACT 2601
www.anu.edu.au
CRICOS Provider No. 00120C

Department of Home Affairs
re: Australia's 2020 Cyber Security Strategy

To whom it may concern,

I write on behalf the Research School of Computer Science at the Australian National University, to respond to the Department of Home Affairs call for views on Australia's 2020 Cyber Security Strategy, as documented in the Discussion Paper for this call.[1]

The Discussion Paper provides a balanced view of various aspects of cyber security, with an excellent list of important questions to address.

Here, we respond to some of these questions that are addressed by our expertise, as a research school in one of the main technical disciplines aligned with cyber security.

Our response focuses on two main aspects that are most relevant to the higher-education sector: research and education.

We are a strong proponent of the concept of "building security in" and are in favour of a cyber security education with emphases on strong hands-on technical skills, grounded in solid foundations in core disciplines of computer science. These drive our education and research agenda and underly our approaches to addressing the questions below.[2]

Question 12: What needs to be done so that cyber security is 'built in' to digital goods and services?

There are obviously many factors that may contribute to ensuring that security is built-in, ranging from regulations, training skilled professionals to providing better tools (to build security-related or security-enhanced products and services). Our response falls in the latter two categories:

We advocate an approach to computer science and IT education where security is taught as an integral part of technical fields relevant to cyber space, such as software, operating systems, hardware, databases, web applications, and so on.

The majority of products and services were built or provided to serve certain business functions that are unrelated to security. So, they tend to be built by builders or developers without security skills, but with expertise in various other domains. This leads to a situation where security is 'added in' after the fact rather than 'built-in' from the beginning, which potentially adds to the costs of development and the costs of deployment. To achieve the latter, the builders themselves need to be aware of potential security issues from an early stage of development, prior to deployment. As products and services are more and more interconnected, security should become an essential requirement for development of any product or service. It thus makes sense to require basic security skills as a mandatory part of education of our IT workforce.

A recent survey of the state of cyber security hiring contains the following key finding:

[1] https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-strategy-2020-discussion-paper.pdf

[2] We use the same numbering of questions as in the Discussion Paper.

> "Cybersecurity is a specialty, but most of the workers who practice it are not specialists. In many organizations, cybersecurity is a task built into other IT jobs, such as network administrators. Overall, these 'cyber- enabled' jobs form the majority (56%) of all cybersecurity-related openings."[3]

By making all IT/CS graduates "cyber-enabled," we can potentially address the majority of the cyber security skills shortage in the long run, while at the same time improving the state of security of products and services.

We advocate strong support for both fundamental research that enables engineering of secure systems and practical vulnerability research.
The importance of vulnerability research is obvious, so there is no need for explanation. Fundamental research that may not be directly related to security is just as important but may not appear obvious. Many security issues, in particular those related to operating systems and hardware, have roots in "bugs" resulting from poor constructions of the affected hardware and software. Some of these bugs are security-critical, others are not, and in many cases, the distinction between security-critical and non-security critical bugs are only the context in which they appear—the bugs are the same. Improvement in research into bug detection tools in support of mainstream programming languages, for example, is not necessarily driven by security needs, but can have great impact on the security of products developed in that language. Similarly, improvements in the design and implementation of a provably correct operating system can potentially eliminate a large class of security issues, even if it was not explicitly targeted at eliminating those issues.[4]

Question 14: How can Australian governments and private entities build a market of high quality cyber secu

Private entities and governments need to be clear about the roles these cyber security professionals need to fulfil, and what particular skills are in shortage.
The roles of a cyber security professional can be quite diverse, and the skill sets required for different roles can be very different. The NIST NICE framework provides an example of capturing security professional work roles via sets of knowledge, skills and tasks required, that can serve as a good starting point. A similar analysis was done, for example, by the US Department of Homeland security.[5]

We advocate a greater emphasis on hands-on practical technical skills in all cyber security training.
Various sources of market research, such as the report by Burning Glass Technologies (see page 2, footnote 3) and the analysis done by the US DHS Cyberskills Task Force, identify a severe shortage of technically skilled professionals in various mission-critical areas. The DHS Cyberskills Task Force, for example, noted that:

> ". . . the Task Force found that the national security imperative arising from the current shortage of hands-on technical skills is sufficient to warrant focusing the entire DHS-sponsored community college program on hands-on, advanced mission-critical cybersecurity skills."[6]

We caution against on relying on cyber security certifications that do not include hands-on practical technical skills as part of their training and examination processes, an opinion shared by security professionals.[7]

Promote regular cyber security competitions (for example, 'capture the flag' competitions such as Cyber Challenge Australia).
This is an excellent way to attract and develop talent in cyber security skills.

[3] Recruiting Watchers for the Virtual Walls: The State of Cybersecurity Hiring. Burning Glass Technologies. June 2019. https://www.burning-glass.com/wp-content/uploads/recruiting_watchers_cybersecurity_hiring.pdf

[4] See for example, CSIRO Data61 secure operating system seL4. https://sel4.systems

[5] Homeland Security Advisory Council: Cyberskills Task Force Report. Fall 2012.

[6] Homeland Security Advisory Council: Cyberskills Task Force Report. Fall 2012. Page 19.

[7] See for example: https://arstechnica.com/information-technology/2016/07/cissp-certification-how-to-hire-infosec-pros/

Question 11: What specific market incentives or regulatory changes should Government consider?

A critically important aspect of cyber security is vulnerability research and disclosure. Governments and private entities should consider the creation of an ecosystem that provides incentives for a timely and regulated vulnerability disclosure. This is in line with a key finding in a recent report by the European Union Agency For Network and Information Security (ENISA) which stresses the importance of coordinated vulnerability disclosure (CVD). In particular, the report mentions:

> "Most prominently, there are opportunities to improve finder wellbeing and the overall CVD ecosystem by ensuring safe harbour practices and legal safeguards for security researchers working to identify and report vulnerabilities.'[8]

Yours sincerely,

[redacted]

Professor Antony L. Hosking, PhD
Director, RSCS

cc: Dr. Alwen Tiu, Senior Lecturer, RSCS (coauthor of this response)

[8] Economics of Vulnerability Disclosure. December 2018. European Union Agency for Network and Information Security. http://www.enisa.europa.eu/