RESPONSE TO AUSTRALIAN CYBER SECURITY STRATEGY

20 April 2023

INTRODUCTION

Monash University is pleased to respond to the Minister for Cyber Security's consultation on the development of an Australian Cyber Security Strategy. We draw on our academic expertise as well as our experience as a large complex organisation which has made a significant commitment to provide effective, adaptable and risk appetite aligned management of cyber risks to support the University in its mission of excellent research and education.

INVESTING IN THE CYBER SECURITY ECOSYSTEM AND WORKFORCE CAPABILITY

Monash University supports the multi-stakeholder approach and the coordination across Commonwealth and State/Territory governments, and acknowledgement of the need to build Australia's cyber security workforce and skills pipeline. This pipeline forms the foundation from which to capture the three sets of opportunities and also to reduce the risk and mitigate the impact of cyber threats.

The creation of this skilled workforce requires greater discussion and deeper understanding of the benefits of a university education in building genuine and sophisticated cyber capability. For new entrants to the field and for professional upskilling, at undergraduate and postgraduate level, university programs enable a comprehensive understanding of cyber security, including industry trends and tools, and existing and emerging technologies. It also requires preparing for the future as technologies and attacks become more sophisticated.

At Monash we understand that cyber security requires interdisciplinary training and that there is a range of cyber security pathways for students.

Monash has undergraduate and postgraduate coursework and research opportunities in cyber security, balancing practical skills with leading research in the field and augmented with capstone projects and work integrated learning experiences that allow them to immediately contribute to keeping the data and systems of Australian organisations resilient to cyber attacks.

These benefits of a comprehensive education in cyber are widely acknowledged and should be supported via greater investment in program development to create the next generation of academics, particularly in key fields such as cryptography, quantum computing, software security, human factors in cyber security, and cyber crime investigation.

Further, as the paper acknowledges, future workforce requires more than technical skills. A well-rounded understanding of security is required - including understanding the human. Social engineering attacks, for example, are only successful when the criminal can tap into the vulnerabilities of people. In addition, critical thinking is the most important strategic capability to develop nationally, particularly as it relates to risk management, problem identification, and solution assessment.

Recommendations

- Formalise the tripartite partnership model across government, industry and academia to develop and translate cyber technologies and practices.
- Offer targeted funding opportunities for cyber academics, for large multi-institution projects and also support early- and mid-career researchers, to develop and trial innovative technologies, and strategies to deal with attacks (prevention, disruption, detection) and the aftermath of an attack.
- Adopt a broad view on workforce capability and engage with industry and academia on a set of cyber strategy skills beyond the technical core, including critical thinking, risk and behavioural analytics.

MONASH University

RESPONSES TO SELECTED QUESTIONS

2b Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

Personal information on corporate systems is protected by the Privacy Act and other legislation. To avoid overlap and to ensure appropriate focus on Australia's most critical infrastructure, we do not recommend further reform of the definitions of critical assets.

2c Should the obligations of company directors specifically address cyber security risks and consequences?

There should be no safe harbours. The obligations of company directors, and their equivalents, should specifically address cyber security risks and consequences.

The Government may care to mirror non-executive director responsibilities under the *Work Health and Safety Act 2011* (Cth) (WHS Act), where company directors have a legal duty to ensure the health and safety of workers and others affected by their business operations. If a company director fails to meet their individual responsibilities under the WHS Act, they may be held personally liable and face penalties, including fines and imprisonment.

2e How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

The intent of legislation should be tested for application and consequence across all sectors. For example, universities were not meant to be in scope of the Data Retention Implementation Plan within the Telecommunications (Interception and Access) Amendment 2015, but were included as a result of operating as carriage service providers to students and other entities.

2f Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cyber crime; and/or (b) insurers? If so, under what circumstances?

The government should discourage ransomware payments but should not outlaw it. Prohibition will not stop payments being made. Instead, they will go underground and this will result in reduced reporting of extortion demands. Keeping them legal will promote transparency of the scale of the problem.

Analysis and communication about the benefits and detriments of paying an attack is required.

7 What can Government do to improve information sharing with industry on cyber threats?

As a first step, Government agencies such as the Australian Signals Directorate and the Australian Cyber Security Centre should reconsider the requirement in some cases to hold a security clearance to access threat intelligence.

As well as providing information about what is happening, Government can provide "actionable" intelligence with industry to advise them on appropriate and best practice courses of action. They need to be able to effectively communicate this information in a way that all businesses (including SMEs) can comprehend the real risks and the steps to secure their businesses (with the understanding that not all industry can afford the state of the art security).

15a What assistance do small businesses need from Government to manage their cyber security risks to keep their data and their customers' data safe?

Government information campaigns should target the broader Australian public and cover relatable, simple and effective good practices, for example multi-factor authentication and the use of unique passwords. Raising awareness about scams is less effective than training and education that can significantly change behaviour.

17 How should we approach future proofing for cyber security technologies out to 2030?
and
19 How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?

As a principle, the development of cyber security technologies should follow best practice for substitution and replaceability, rather than embedding customisations that limit the adoption of new technologies.

Minimum security standards for devices and services sold in Australia should be developed and enforced, potentially including a simple cyber-secure star rating system.

21 What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Visibility of expenditure to enable public understanding about effectiveness of investment and metrics that capture behaviour change in individuals and community.

Multi-stakeholder expert and community working groups could be established to help identify areas that require greater attention?