Murdock
Cheng
Legal Practice

Cyber Security Submission

Australia's 2020 Cyber Security Strategy — A Call for Views

Sydney Office
Level 10
50 Clarence Street
SYDNEY NSW 2000

T + 61 2 9262 5495
F + 61 2 9262 5496

Melbourne Office
Ground Floor
4-8 Osborne Street
SOUTH YARRA VIC 3141

T + 61 3 8899 7870
F + 61 3 9642 2008

mclp.com.au
ABN 35 161 110 014

TABLE OF CONTENTS

INTRODUCTION

This submission has been prepared in response to the Australia's 2020 Cyber Security Strategy – A Call for Views. This submission is prepared by Paul Cenoz of MurdockCheng Legal Practice (**MCLP**) and Rajesh Mathur of NFC Group Pty Ltd (**NFC**).

Mr Cenoz holds a bachelor's degree in political science and Juris Doctor degrees from Monash University and American University Washington College of Law. He is admitted as a barrister and solicitor in the State of Victoria, and as an attorney in the State of California and is employed as an Associate at MCLP in the information and technology department. MCLP is an incorporated legal practice with offices in Sydney and Melbourne.

Mr Mathur holds a master's degree in statistic and public administration. He is an experienced software developer. He is the director of NFC, a company specialising in organising and arranging test engineering and Agile conferences nationwide.

OVERVIEW OF THE CYBER THREAT ENVIRONMENT

Cyber theft, cyber sabotage by hacking, and cyber intrusion affect individuals, industries, and businesses. These crimes represent growing threats to the national economy, privacy of individuals, and viability of businesses. Recent intrusions and hacks of institutions, including the Department of Meteorology and Victorian public hospitals, demonstrate the need for a forward-thinking strategy, rather than the existing reactionary and fragmented policy responses.

GOVERNMENT ROLE

The Australian Government does not have the capacity to provide a panacea for cyber threats. Traditionally, government is reactive, and the executive, legislature, and judiciary are unable to act as quickly as needed in the cyber security landscape. The Australian Government should play the role of facilitator by:

(a) creating guidelines that assist private stakeholders in defending against cyber attacks and maintaining secure systems;

(b) providing financial incentives to individuals, agencies, institutions, and businesses to maintain and increase the security of their software and devices; and

(c) supporting certified trusted business partners, industry professionals, and software and hardware.

As the cyber threat grows, it is important for private and public institutions to receive incentives and guidance from the Australian Government to help protect their operations, users, and reputations. Healthcare providers,

financial institutions, energy producers, businesses, and government agencies are vulnerable targets with immense repositories of data, numerous users, and a myriad of different software and hardware.

Using a multipronged approach, the Australian Government should help the private sector—with the assistance of not-for-profits—conduct public awareness campaigns, enable private action and become a trusted partner for individuals and businesses.

There needs to be a shift to allow interested and capable private actors to carry a greater share of the responsibility of cyber security defence and offence, within the confines of government regulation, guidelines, guidance, and certification.

CALL TO ACTION

Trust of Government

The Australian Government's difficulties in safeguarding its own systems has likely had a negative impact on the public's trust in the Australian Government's ability to implement effective cyber security policies. The Australian Government should ensure that its own systems are protected first and foremost.

Additionally, in a legal environment following the decision of *Glencore International AG v Commissioner of Taxation* [2019] HCA 26—which determined that the Australian Government can use lawyer and client communications that are hacked and disclosed, thus undermining lawyer-client privilege—hacked parties may be unwilling to involve government actors for fear of confidential information being disclosed or used by the Australian Government.

To build trust, the Australian Government should consider providing the following:

(a) legal protection for end-to-end encryption;

(b) strict penalties for misuse of data by government employee and contractors;

(c) strong whistleblower protections that apply to government employees; and

(d) restricting the retention and use of data that it is provided or found during hacking investigations.

Legislative Changes

The Government can play a significant and effective role by removing barriers, incentivizing cyber agility, and strengthening vulnerable resources by taking early and focused action. The Australian Government's role should include education, law enforcement, international cooperation, creating guidelines for private actors, and incentivising individuals and businesses through tax deductions and exemptions.

Legislative changes are necessary to:

(a) protect personal privacy, personal liberty, freedom of speech, property rights, and procedural fairness;

(b) limit the liability for parties resulting from the disclosure of data hacks to authorities;

(c) protect personal privacy; and

(d) empower private actors.

The majority of technology and networks are held and administered by private companies. Allowing those assets to be more effectively and efficiently used to develop a cyber resilient Australia would be logical and efficient.

Guidelines for Private Actors

Some of the functions currently performed by the Australian Government should be safely devolved to the private sector. For example, the Australian Government can create a hostile environment for malicious cyber actors by allowing 'hack backs' by private, certified actors. The Australian Government can also facilitate the creation and monitoring of 'honeypots' within the networks of private businesses that can be used by internal and the Australian Government's forensic cyber analysts. While there are issues and risks facing the implementation of allowing hack backs by private actors (such as attribution and spoofing that can impact innocent parties and governments) we believe a well-developed strategic plan created through regulation, guidelines, and direct contact with relevant Australian Government actors can be effectively created and lead to beneficial outcomes.

The Australian Government should create:

(a) legal permission and limitation of liability for hack backs;

(b) regulatory guidelines;

(c) accessible direct contact with government officials to allow for immediate reporting, liaising, and facilitation;

(d) industry standards (discussed below); and

(e) trusted private certification of private actors.

Accreditation of professionals

The Australian Government, working with the assistance of private entities, can build a market of high-quality cyber security professionals in Australia through certification and education.

Certification of Hardware and Software

Lack of cyber awareness drives poor consumer choices. These choices can include the purchase of pirated, malware and/or virus-infected hardware that is installed to monitor users in phones, laptops, and accessories (for example, mobile phone charging cables).

Increasing consumer focus on cyber security can benefit Australian businesses that create secure products, helping them to expand their businesses, create jobs and grow the national economy.

The Australian Government can support the private sector through a government-facilitated accreditation process provided by government and private sector-funded independent private organisation. The result will be the increased quality and effectiveness of cyber security and digital offerings, and instilling better trust in ICT supply chains, including focusing on the provenance of the components.

Resource Centre

The largest constraints on information sharing between the Australian Government and industry on cyber threats and vulnerabilities is ease of access to Australian Government systems by small businesses and time.

We propose the creation of a government and private sector funded independent private organisation that is a resource for the public to contact regarding potential scams, hacks, and frauds related to cyber security. This organisation would work in collaboration with the Australian Cyber Security Centre; however, it would offer a more user friendly and robust option for individuals and businesses. Many people simply need an immediate confirmation that a letter, text, call, or email is a fraud or malicious.

High-volume, low-sophistication, malicious activity targeting Australians can be reduced by focusing on vulnerable people and regional residents through a range of mediums, including but not limited to telephone calls, written requests, emails or live chat. Furthermore, this new agency could employ youths, elderly and First Nations peoples to connect with those at most risk.

Government funding

The Australian Government should continue to incentivise and invest in cyber security. This can be accomplished through tax deductions and exemptions for investment in hardware and software upgrade directly related to cyber security, including updating old computer systems.

Additionally, the Australian Government should increase research funding, including through education, investment in next generation technologies such as Artificial Intelligence, quantum computing, and development of new encryption algorithms.

Standards

The Australian Government should create guidelines through regulation in collaboration with industry to achieve a vision and strategy to establish and implement government standards to support cyber security (e.g., metadata standards, confidentiality labelling standards, attribute-based access control standards, etc.) for data in the following sectors:

(a) financial services;

(b) healthcare;

(c) education;

(d) energy; and

(e) other sensitive personal data.

Employment

Employment laws should take into consideration insider threats and how employers monitor their employees, in consideration to data leakage, intellectual property theft, cyber security and espionage. Businesses and organisations should be encouraged to report cyber breaches caused by employees to relevant authorities.

Privacy

As people learn more about their cyber footprint and data being held by private and public actors, they have become more concerned regarding their right to privacy resulting in distinct privacy legislation in various jurisdictions, as can be seen in the European Union (EU), California, New Zealand, and Australia.

Privacy laws can be used to increase the perceived and actual privacy rights in relation to government and private entities. Additionally, privacy laws create incentives for businesses to increase cyber security capabilities through negative repercussion caused by data breaches, such as public disclosure and company and director liability for harm caused by the breach. However, any liability should be proportional and not heavy handed such as with the EU's General Data Protection Regulation. A tort for privacy could accomplish this by providing a private right of action by the individuals affected.

International coordination

The Australian Government should develop stronger co-operation mechanisms and co-ordination with international corporate and state actors to proactively prevent and stop cyber threats.

CONCLUSION

The Australian Government has an important role to play in cyber security, namely to play an active role in the development and implementation of guidelines and regulations, and to incentivise the efficient use of the private sector.

Should you have any questions in relation to the above matter, please contact Mr Cenoz on [redacted]

Yours faithfully,

MURDOCKCHENG LEGAL PRACTICE

MurdockCheng Legal Practice

PAUL CENOZ
ASSOCIATE
MURDOCKCHENG LEGAL PRACTICE
[redacted]

RAJESH MATHUR
DIRECTOR
NFC GROUP PTY LTD
[redacted]