



Stephen Phillips

Vice-Principal, Operations

1 November 2019

Mr Greg Miller
First Assistant Secretary
Cyber Security Policy
Department of Home Affairs

By email: cybersecuritystrategy@homeaffairs.gov.au

Dear Mr Miller,

Australia's 2020 Cyber Security Strategy – call for views, September 2019

Thank you for your email to the Vice-Chancellor, Dr Michael Spence AC, inviting the University of Sydney to make a submission in response to the Department of Home Affairs' call for views about the design of *Australia's 2020 Cyber Security Strategy*. The Vice-Chancellor has asked me to respond on behalf of the University, given my responsibilities for the University's relevant strategies and activities.

The University of Sydney is very pleased to have the opportunity to be a part of these consultations to help renew and strengthen our national approach to cyber security.

The cyber threat environment has escalated as more economies globally have moved online. Cybercriminals have responded rapidly to digital adoption and low awareness of privacy and security risks, exploiting the Darknet, cryptocurrencies, real-time online banking transactions, and the ready availability of exploitation tools. Phishing, ransomware and business email compromise are common manifestations of this deterioration and the University is exposed to these threats along with the general population and other commercial enterprises. In parallel, the University's education and research missions also make us a target for entities and individuals that wish to influence the content of our teaching and the direction of our research, or who may wish to acquire protected student, staff and research data, or to gain access to intellectual property we are developing.

Responsibility for managing cyber risks is shared by governments, regulators, businesses and consumers of digital services, and in the absence of consistent standards of protection, this risk is substantially borne by the consumer. Changes to the statutory and regulatory obligations of organisations in respect of privacy and security have been intended to shift some of this burden away from the individual and on to organisations that are better resourced to understand and address the risks. However, the effectiveness of this strategy is compromised by the failure to impose material penalties for non-compliance.

Consumers, and small and medium-sized enterprises are poorly equipped to address the threat from cybercrime and expect providers of digital services to protect them from these threats wherever possible. For the most part, this has been acknowledged in Australia and there has been gradual improvement in consumer-focused cyber security controls, most noticeably in areas such as strong authentication of online payments, email protection, adoption of transport layer security (TLS), extended validation certificates, browser and operating system based security protection and mobile number porting procedures.

There is considerable scope for improvement on the part of telecommunications carriers and device manufacturers to protect consumers from high volume/automated scams and to patch software vulnerabilities.

We recommend that in developing Australia's new Cyber Security Strategy, the Government continues to play an important leadership, resourcing and coordinating role:

- managing threats arising from sophisticated threat actors targeting Australia's critical infrastructure (energy, water, telecommunications, banking, transport etc), democratic institutions, the judicial system and culturally important organisations such as universities;
- providing cyber security advice to the general community and businesses;
- supporting the prosecution of cyber criminals through the justice system; and
- engaging in international cooperation designed to disrupt sophisticated threat actors operating outside Australia.

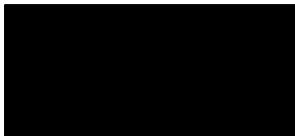
We further recommend that the Government consider:

- adopting an active cyber defence model of the type implemented by the UK Government, focused on blocking of Command-and-Control (C2) traffic and delivery of online services that support organisations to implement controls such as Domain-based Message Authentication Reporting and Conformance (DMARC), Protective Domain Name Systems and regular website checking for common vulnerabilities;
- cooperating with telecommunications carriers to block malicious telecommunications traffic; and
- working with the States and Territories to ensure that the primary and secondary education curriculum promotes an increased awareness of cyber security threats and safety across the Australian population.

We look forward to working with the Government as it develops and implements Australia's 2020 Cyber Security Strategy.

Should you require any further information from the University of Sydney, please contact Mr Derek Winter, Head of Cyber Security, [REDACTED]

Yours sincerely,



Stephen Phillips
Vice-Principal, Operations