



Australian Government  
Department of the Prime Minister and Cabinet



CYBER SECURITY

## OFFICE OF THE CYBER SECURITY SPECIAL ADVISER

### Joint Standing Committee on Trade and Investment Growth

#### DEPARTMENT OF THE PRIME MINISTER AND CABINET – TRADE SYSTEM AND THE DIGITAL ECONOMY

The Department of the Prime Minister and Cabinet appeared before the Joint Standing Committee on Trade and Investment Growth on 14 September 2017 and provided evidence. This submission outlines Australia's efforts to improve the cyber resilience of the business sector and provides a response to the question the Committee asked in relation to the trade sector and what kind of cyber attacks are most likely. We have also provided two case studies to assist the Committee. Further case studies will be in the Australian Cyber Security Centre 2017 Threat Report, to be released in mid October.

#### Overview

##### *Opportunities*

Our society is rapidly undergoing a digital transformation. We estimate that 90% of Australians are already online with that proportion continuing to grow. Similarly, 84% of Australian small and medium-sized businesses already have online presences, with half receiving payments online.

As the Prime Minister said when he launched Australia's Cyber Security Strategy in April 2016, "there is no global institution or infrastructure more important to the future prosperity and freedom of our global community than the Internet itself." As the majority of Australian businesses have done, the Australian Government has embraced the opportunities the Internet offers in the provision of services to the Australian people. This is being pursued with the Digital Transformation and National Innovation and Science agendas. But the potential of digital transformation depends on the extent to which we can trust cyberspace.

##### *Threats*

Alongside the vast opportunity of the Internet comes a degree of risk. We are not immune from threats to our systems posed by cyber criminals and state-sponsored actors. As people and systems become increasingly interconnected, the quantity and value of information held online has increased and so have efforts to steal and exploit that information.

Australian and overseas organisations across both the public and private sectors have been compromised by either criminal or state-sponsored intrusions. A substantial amount of sensitive commercial and personal information has been lost and significant damage has been incurred to businesses and reputations. Figures vary, but cybercrime is estimated to cost Australians over \$1 billion each year and by some estimates the real impact of cybercrime to Australia could be around \$17 billion annually.

The Australian Cyber Security Centre's Threat Report 2016 advises that Australian government networks are regularly targeted by the full breadth of cyber adversaries, from foreign states through to criminals and issue-motivated hacktivists. Foreign states represent the greatest level of threat,

but cybercriminals pose a threat to government-held information and provision of services through both targeted and inadvertent compromises of government networks with ransomware.

### **Threat to the private sector**

Australian industry is persistently targeted by a broad range of malicious cyber activity, risking the profitability, competitiveness and reputation of Australian businesses. The spectrum of malicious cyber activity ranges from online vandalism and cybercrime through to the theft of commercially sensitive intellectual property and negotiation strategies.

The ongoing theft of intellectual property from Australian companies continues to pose challenges to the future competitiveness of Australia's economy. In particular, intellectual property theft impedes Australia's competitive advantages in exclusive and profitable areas of research and development – including intellectual property generated within our universities, public and private research firms and government sectors – and provides advantage to foreign competitors.

The current threat environment and case studies that have been published can be found in the Australian Cyber Security Centre's 2016 Threat Report ([Attachment A](#)). The 2017 Threat Report will be released on 10 October 2017 and will contain an updated threat environment analysis and new case studies.

The remainder of this submission sets out the Government's measures to improve the cyber security and cyber resilience of Australia's trade focused business sector. As outlined at the hearing on 14 September 2017, our submission defines cyber resilience as the 'ability to continue to operate or quickly resume operations in the wake of a cyber incident'.

### **Measures to improve the cyber security of Australian businesses**

The Government, through the Australia's Cyber Security Strategy, is undertaking a range of activities to improve the cyber security of all Australian businesses. Excellent progress has been made against the Strategy's 33 initiatives, with many delivered and others well in train. Additional and emerging bodies of work have also been identified and captured with a view to ensuring that the Strategy is constantly evolving with the rapid rate of technological and social change.

The Strategy has already proven to have been a catalyst for cultural change across the country, generating momentum and stimulating more direct and richer conversations between government, business and the public. Leaders in business and government are now more attuned to cyber security risks and opportunities, which has allowed the incubation of new ideas and initiatives beyond and above those originally identified.

The ASX 100 Health Check has brought cyber security into our top boardrooms, highlighted by the launch of the industry-led report on the state of cyber security governance in our top companies. Establishment of Joint Cyber Security Centres in key capital cities, including Brisbane, Melbourne and soon to be in Sydney.

The Department of the Prime Minister and Cabinet is developing strategies to ensure our economy is able to quickly respond to cyber security incidents such as the recent global ransomware campaigns. We are working with telecommunications providers to better protect Australia core networks from malicious actors and cyber threats. The raised public profile of cyber security and increased collaboration between the Australian Government, the States and Territories and the private sector has revealed that threats are increasing, vulnerabilities are being exposed and a serious step change is required to improve our security.

### **Making Australian cyber security businesses more competitive**

The Government, through the Australian Cyber Security Growth Network (now AustCyber), is actively working to make Australian cyber security businesses more competitive in the global marketplace.

There are three main priorities:

*1. Growing an Australian cyber security ecosystem.*

AustCyber is growing the cyber security ecosystem by helping cyber security start-ups find their first customers; improving research focus and collaboration to assist commercialisation; making access to seed and early stage capital easier and simplify government and private sector procurement processes.

*2. Exporting Australia's cyber security to the world*

AustCyber is supporting Australian firms to develop scalable service delivery models, develop cyber security as an educational export and attract multinational corporations to use Australia as an export base for the region.

*3. Making Australia the leading centre for cyber education*

AustCyber is also working to attract and retain the best and brightest to cyber security, creating vibrant, industry led professional pathways and introducing initiatives to dramatically ramp up cyber security education and training.

### **Partnering with the private sector to improve cyber security and cyber resilience.**

The Government is working more closely with the private sector than ever before to improve the nation's cyber security and cyber resilience. The Government recognises we cannot ensure Australia's cyber security alone. Governments, business and individuals must work together to share information and strengthen our defences against cyber threats.

The Government has actively engaged the private sector on cyber security, hosting regular dialogues with industry. These have included:

- In July 2017, Minister Tehan led a roundtable with leaders from across the private, educational and government sectors to explore ways to enable more Australians to pursue a career in cyber security.
- In May 2017, Prime Minister Turnbull hosted a roundtable with leaders of Australia's telecommunications companies and web-based platforms that discussed the new frontier of threats to Australia cyber security.
- In April 2017, Prime Minister Turnbull hosted an industry roundtable that canvassed technological advances that will potentially disrupt Australia's cyber security ecosystem and strategies to get ahead.
- Minister Tehan hosted dialogues in late 2016 and early 2017 focused on cyber security incident response and improving the cyber security capacity of small to medium enterprises.

To further enhance cooperation with industry partners, the Government is also relocating the Australian Cyber Security Centre to enable greater collaboration with the private sector and academia.

### **Targeted work to enhance Australia's cyber resilience**

The Government is also undertaking targeted work to enhance Australia's cyber resilience. In July 2017, the Prime Minister announced that his Department would undertake work to strengthen

our national cyber incident response capability and resilience in the event of a significant cyber incident.

The Department is bringing a unified, whole of economy focus to education, prevention, prediction and response to cyber threats and shaping the cyber ecosystem to deliver a cohesive national narrative and capability for cyber resilience.

The Australian Government has also published a Stay Smart Online Small Business Guide and Stay Smart Online My Guide for individuals. These guides provide advice on vital areas of online security including: privacy, passwords, suspicious messaging, browsing safely, online finances and payments, tablets and mobiles, security software and reporting and can be downloaded from the Stay Smart Online website.

**Domestic initiatives are complemented by our international engagement**

Australia's Cyber Security Strategy recognised the need for Australia to partner internationally on cyber affairs to improve our cyber security.

On 4 October 2017, the Government launched Australia's first International Cyber Engagement Strategy which prioritises and coordinates Australia's whole-of-Government approach to international engagement across the full spectrum of cyber affairs.

The Strategy outlines the principles, interests and goals that guide Australia's international engagement on cyber issues, including our plans to partner in the Indo-Pacific region to maximise opportunities for economic growth and prosperity through digital trade. The International Cyber Engagement Strategy can be found online at: <http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html> .