Gai Brodtmann MP

MEMBER FOR CANBERRA

Senator Arthur Sinodinos
Minister for Industry, Innovation and Science
Digital Economy Strategy Team
GPO Box 2013
Canberra ACT 2601
Email: digitaleconomy@industry.gov.au

Dear Minister

As Shadow Assistant Minister for Cyber Security and Defence I welcome the opportunity to comment on the consultation paper *Digital Economy: Opening up the conversation* produced by the Department of Industry, Innovation and Science.

Any serious effort towards improving our nation's cyber security must involve everyone. It must focus on educating the community about the risks of this rapidly changing environment, and it must empower the community to mitigate these risks to realise the benefits and potential of the digital economy.

Internet of Things

By 2019, it is estimated the average Australian household will have 24 devices connected online.

With the proliferation of the Internet of Things, the threat potential will only grow and expand as devices increase the number of attack vectors into our homes and businesses.

Technology producers and developers need to continue to innovate and improve the safety, security and cost effectiveness of the products they create. Australia has the opportunity to lead the way in standards development to ensure these devices cannot be leveraged for cyber attack.

Small business

In the 2016 financial year, more than 90 percent of Australian organisations faced some form of cyber security compromise. in the first six months of this year, there were almost 24,000 incidents of cybercrime reported to the Australian Cybercrime Online Reporting Network. And that is just what gets reported.

Between denial-of-service extortion, data ransoming and sophisticated spear-phishing campaigns, Australia is facing threats on multiple fronts.

WannaCry hit around 200,000 companies and organisations in 150 countries. In Australia we were fortunate to escape the brunt of the attack, but at least 12 Australian businesses were victims. And it is understood most of these 12 were small businesses.

By 2020, Australia's 'internet economy' is estimated to be worth $139 billion, growing at twice the rate of the rest of the economy.

However, a Norton Small Business report released earlier this year showed almost a quarter of Australian small and medium businesses do not have any form of security software on their systems. A survey of more than 1000 New South Wales small and medium businesses found only one had a cyber incidence response plan.

Given 97 percent of all businesses in Australia are categorised as small or medium enterprises, the risk posed to our economy by cyber attacks cannot be underestimated. Around 60 percent of small businesses don't have a shop on the high street — most of them are micros operating from their own home.

If we are to keep our nation and economy safe, government must urgently develop strategies to improve the cyber security practices of small and medium business.

Skills development

Forecasts suggest that by 2019 there will be 6 million jobs in cyber security globally, and only 4.5 million people with the skills to fill them.

Unfortunately, our approach to addressing this challenge is ad hoc and piecemeal. We need a whole of government, national approach to cyber security knowledge and skills development. The approach must acknowledge the continuum of education and be developed in close consultation with industry and every level of the sector.

Currently, there are no clear pathways to a cyber security career from secondary school, through to vocational education or university. Nor does our education system adequately address Recognition of Prior Learning.

Development of new course and pathway offerings must ensure meaningful and practical work experience.

Education marketing for cyber security is currently geared towards careers for technicians, when ethicists, communicators, psychologists, behavioural scientists and creative minds are also needed.

Penetration testers, systems administrators, policy makers and many other cyber security roles all have different educational requirements. We therefore need to encourage universities to ensure cyber security professional courses and pathways tailor for the needs of generalists and specialists. In much the same way we view engineering and medicine disciplines, generalist skills should be the foundation, not the outcome.

Now is the time to put in place initiatives that will improve educational outcomes to deliver the skills and knowledge we need to ensure our nation's security and prosperity. And these initiatives must be inclusive and must encourage diversity.

Critical infrastructure

Disruption of critical infrastructure from physical or cyber threats can have a serious impact on our national and economic security. The evolving threat environment means Australia needs to constantly assess how we can best protect our critical infrastructure.

My recent submission to the Attorney-General Department's consultation process on the exposure draft of the Security of Critical Infrastructure Bill noted the Bill's scope was limited. The draft Bill identifies electricity, water and ports as the "highest-risk sectors". Yet there are other equally important critical infrastructure sectors overlooked by the draft Bill.

The Trusted Information Sharing Network identified eight critical infrastructure sectors as "vital to Australia's social cohesion, economic prosperity and public safety".

These are:

- Banking and finance
- Communication
- Energy
- Food and grocery
- Health
- Transport
- Water services
- Commonwealth Government.

Each of the eight TISN sectors has experienced some form of cyber threat in the past 12 months, at the national or international level. Given the importance of these sectors to our nation's security and economy, consideration should be given to including all eight sectors in our security framework.

We should also consider extending coverage for critical infrastructure to other important industry sectors. This would be consistent with international approaches.

The United States critical infrastructure security and resilience strategy identifies 16 sectors. The United Kingdom identifies 13 sectors. Canada identifies 10 sectors. Singapore identifies 11 sectors. The sectors recognised by these nations, but not currently included in the TISN, include:

- Emergency services
- Information technology infrastructure
- Chemicals
- Manufacturing.

In this digital era we need all Australians to understand they have a role in keeping our nation and economy safe and secure.

This will ensure we are empowered and resilient enough to reap the rewards of the myriad opportunities offered by this new environment.

Once again, I welcome the opportunity to contribute to the development of the digital economy strategy.

Yours sincerely

G.M. B

Gai Brodtmann MP
Member for Canberra
Shadow Assistant Minister for Cyber Security and Defence

30 November 2017