Australian Government Cyber Security Review

The Cisco Response

Today, governments are almost universally pursuing a development and modernisation agenda to nurture their society into the digital age, and Australia is no exception. As an early adopter of cloud, the Internet of Things (IoT), and other new technologies, Australia is well placed to become a hub of innovation and digital development that will drive Australia's future economic prosperity. For this opportunity to be realised however, cyber security must be recognised in all aspects of national strategy.

Cisco is recognised as a trusted, world-class technology partner to the public and private sectors globally. In Australia, Cisco provides extensive government and private IT infrastructure to support critical services. We are well placed to help cyber security become a reality for Australia, and were invited to provide industry insights to inform the Australian Prime Minister's 2015 Cyber Security Policy & Strategy Review.

This review considered the responsibilities of government, industry, research, academia and the community. A partnership between these groups is critical if we are to meet the cyber security challenges of today and the future.

Cisco supports the development of a bi-partisan national cyber security strategy to provide a robust structure for Australia's digital future. Cisco's input into the review highlights the following considerations for the Government:

1. The future of Australia's national economy is to be 'cyber-enabled.'
2. Put simply, cyber insecurity is taxing Australia's economic growth.
3. The formation of a national level cyber strategy is critical for a strong economy today and in the future. It's an opportunity for Australia to be a global leader as the world economy enters the next wave of digital enablement.
4. For a positive cyber security environment in Australia, we need to focus on a partnership between government, public and private entities that addresses the following priorities: uplifting cyber security leadership; implementing state-based Cyber Security Centres; building and maintaining trust; enabling a greater level of information sharing; incentivising innovation and positive cyber security behaviours; and creating a national cyber security curriculum 'engine.'

Cyber security: a national priority

With the increase in the number and sophistication of cyber security incidents, and our growing dependence on the internet to live, work and learn, there is now an urgent need for cyber security to be one of Australia's top national priorities.

Cyber security incidents are varied, and the implications of successful attacks are well documented. Incidents range from identity theft, fraud, and stealing customer data, to activities that could cause massive disruption to essential services.

Cyber security incidents erode trust in Australian organisations and the Australian Government which can then lower investment and business confidence.

This impacts industry, and especially small businesses which make up 97% of all Australian businesses.[1]

As a trusted technology partner, Cisco is well positioned to help minimise the impact of cyber security incidents in Australia, and to provide advice on the implementation of effective practices to enhance our country's cyber security maturity. This is critical to Australia's economic prosperity.

Cisco submitted a series of recommendations to the Prime Minister's Cyber Security Review, which are summarised here. We've also outlined the opportunities and challenges that Australia needs to consider as the national strategy evolves.

Cyber insecurity is taxing Australia's growth potential

The number one cyber challenge for Australia is the increasing number of incidents that are causing harm to the economy and society. From breaches, crimes and disruption of essential services, to the destruction of corporate and national assets – the frequency of these incidents needs to be addressed.

A further risk to the future cyber landscape is the erosion of trust. We're seeing that some governments are turning to legislation and regulation to manage the risks to their infrastructures, while other governments are turning to protectionist policies to limit market access and position national champions. The free flow of data, goods, and services across borders is being degraded electronically. At the same time, governments are trying to explore expanded bilateral trade arrangements – trade and the digital delivery of that trade, can no longer be dealt with separately. We risk fragmentation and regionalisation of the internet, all of which will diminish the potential of the internet economy.

The threats to a connected society are outpacing the defences, and GDP growth is being eroded every day.

Put simply, cyber **insecurity** is a tax on growth. Globally, national losses from cyber security incidents are estimated to be as high as 1% of GDP, which for Australia, could be as much as $17 billion dollars per year. It is also estimated that the Group of Twenty (G20) economies have lost 2.5 million jobs to counterfeiting and piracy.[2]

The frequency of cyber security threats is increasing at the same pace, or even faster than, the technology development cycle, which, in turn, is moving much faster than the currently complex compliance and policy vehicles. Initiatives that address these differences through simplicity and scale are critical if the internet and IT systems in general, are to deliver maximum benefit.

There is already a global shortage of approximately one million cyber security professionals, and this number continues to grow. This problem extends to Australia, as most organisations do not have the people or the systems to continuously monitor extended networks and detect infiltrations.

[1] ABS media release 'The number of Australian businesses have increased', 2 March 2015.

[2] Cyber Security Readiness Index 1.0, by Melissa Hathaway, Hathaway Global Strategies, October 2013. Melissa Hathaway is a Cyber Security Advisor to the Obama and Bush Administrations.

The future of Australia's economy is to be 'cyber-enabled'

The greatest cyber opportunity for Australia is to maximise the value of the internet as the world enters the next wave of digital enablement. That's when technology begins to connect everything from people, processes and data to things. In fact, estimates are that by 2020, 75% of businesses will be digital businesses or preparing to become one.[3]

As the move to a digital economy accelerates, cutting-edge infrastructure will increase national GDP, reduce spending and create jobs. It will allow governments to extend the reach and impact of public services by converting insights into action. It will foster new and diverse businesses that shape the world.

And it will ensure that countries become more globally competitive.

Australia's future is digital, hyper-connected and critically dependent on technology, making a strong cyber security capability crucial to navigating the associated risks and opportunities ahead. Cyber security incidents can lower investment and confidence in Australia. This is a long-term national campaign to reposition Australia in the world economy, where cyber security will be a key differentiator.

The future of Australia's national economy must be 'cyber-enabled'.

Creating Australia's National Cyber Security Strategy

As economic development powered by the internet touches on nearly all aspects of Australian life, our digital opportunity can only be realised if cyber security is a key component of national strategy.

The creation of a national cyber security strategy is one of the most important tasks Australia will undertake. To be successful, the strategy must recognise and appreciate the link between national security and economic prosperity.

A national cyber security strategy will accelerate and increase economic prosperity for generations to come. To achieve this, an accountable and mutually invested partnership between government, private, and public entities is required. The Australian Government can play a key role in coordination and leading by example, as well as incentivising private and public organisations to invest in improving Australia's cyber security capabilities. Equally, in the near future, Australian citizens will need to be as well educated in cyber security as they are in Mathematics or English.

The strategy should include:

- Affirmation that cyber security is of strategic importance for both national security and national prosperity
- The creation of a multi-year strategy which builds the capacity, talent, and workforce for the cyber future
- The goal that Australia becomes the safest online place to do business. This could be met through targets such as having:
  - The world's "cleanest" cyber infrastructure, measured through the lowest malware infection rates
  - The strongest penalties for cybercrimes
  - Accountability and education for Board members and CEOs on cyber security
  - Minimal disruption to essential citizen services because of cyber security vulnerabilities
  - Increased citizen confidence in their use of, and dependence on, internet services.

[3] http://www.forbes.com/sites/gartnergroup/2014/08/26/where-are-you-on-the-digital-business-development-path/

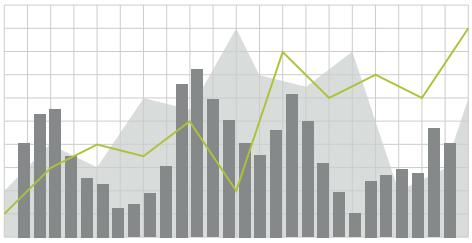
Cisco's recommendations for a secure cyber future in Australia

Australia must address the current threat landscape and put mechanisms in place to keep up with the changes in the next decade. The actions required to address Australia's cyber security challenges are:

A NATIONAL CYBER SECURITY STRATEGY

A national cyber security strategy with a ten year outlook and a twenty year view for skill building should be created. This should be reviewed every one to two years. The strategy must take a bipartisan approach that allows a coherent strategy to be implemented beyond election cycles. This should include:

- A "big picture" view that creates a framework to define the cyber security roles and responsibilities for government and private, public, and citizen entities.
- Formalising the role for all stakeholders within the Australian Cyber Security Centre (ACSC), including greater collaboration and information sharing to maximise the value these partnerships bring.
- Defining interactions and information flows, and informing incident response capabilities to address national resilience across a range of industries.
- Focusing on and aligning resources to identify and drive research and other initiatives where Australia can lead the world, and attract multinational investment. This should include the creation of interlinked cyber security Centres of Excellence (COEs). Building on Australia's global leadership in the adoption of cloud and the Internet of Everything (IoE), these Centres should focus on market sectors such as resources, agriculture, health, and financial services, and include small to medium sized enterprises (SMEs), start-ups and incubators.



Offering the cleanest, safest and most versatile digital infrastructure will support trade and investment in Australia.

UPLIFTING CYBER SECURITY LEADERSHIP

Cyber security leadership needs to play a greater role in corporations and institutions. Executive committees and boards need to lead this transformation, whether this is in government or in business. This could include CEO level accountability for the integrity, confidentiality, and assured availability of data, systems and services. The government should also integrate cyber security requirements into their procurement and acquisition processes, to drive the market toward greater cyber security maturity.

Cyber security leadership needs to play a greater role in corporations and institutions.

BUILDING AND MAINTAINING TRUST

The government must invest in its ability to shape multilateral and bilateral frameworks, international and regional forums, and trade outcomes that differentiate Australia as offering the cleanest, safest and most versatile digital infrastructure. This will support trade and investment in Australia.

POSITIONING AUSTRALIA TO MAXIMISE THE ADVANTAGE OF DIGITAL MARKET TRANSITIONS

With Australia assuming the position of a world-leading adopter of digital market transitions, there's an opportunity to position our nation as a global leader in cyber security operational excellence. For example, the growth of the number of 'things' connected to the internet is fundamentally changing the landscape for cyber security and a minimum standard for connected devices needs to be established and enforced. Australia could lead the world in setting and testing these standards.

There's an opportunity to position our nation as a global leader in cyber security operational excellence.

ENABLING GREATER INFORMATION SHARING

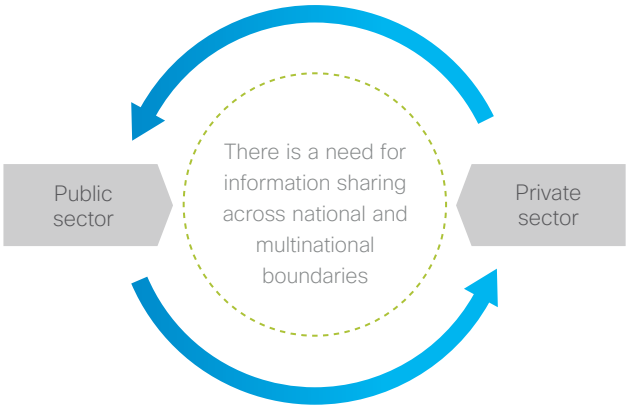
There is a need for information sharing across national and multinational boundaries, including between government and the private sector. This needs to include support for machine-speed solutions. It should be guided by the principles that information sharing is bidirectional, voluntary, increases trust, is actionable and relevant, and doesn't cause conflict with other regulations. Furthermore, there needs to be a regime that offers protection from, or is compliant with, privacy, data protection, and corporate reporting requirements.

IMPLEMENTING NEW STATE-BASED CYBER SECURITY CENTRES

The formation of the Australian Cyber Security Centre (ACSC) is a positive step in enhancing Australia's cyber security framework. However, there is a need to expand its reach to better influence the Australian states, as well as to widen access to skilled personnel. This should be done through lower classification areas within the ACSC, as well as virtualisation of the ACSC to include state-based centres. New cyber security Centres of Excellence will create a hub for learning, as well as create local liaison centres for state and local government, and industry.

ACCELERATING INNOVATION AND POSITIVE CYBER SECURITY BEHAVIOURS AND OUTCOMES

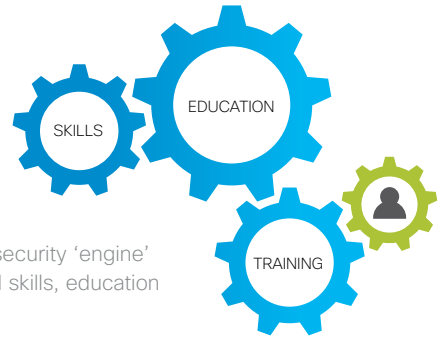
Appropriate incentives for investing in research and development, including the formation of incubators, must be introduced to accelerate innovation and skill development. Incentives should also be introduced to accelerate preferred behaviours and outcomes for cyber security by Australian government agencies and business.



BUILDING SKILLS, EDUCATION AND TRAINING

From a skills perspective, the key priority is to define the national cyber security curriculum 'engine', including a program that maps skills, and is accountable for hiring, education and training. This initiative must include:

- A twenty-five year outlook, to address the creation of the next generation of cyber security experts and cyber security-aware personnel.
- The expanded role of government and industry in growing cadetships that increase cyber security skills across all market sectors and domains.
- The alignment of key research and teaching resources, similar to the activities of the Australian Cyber Security Research Institute (ACSRI), which has a goal of creating an additional 40 PhD students in cyber security by 2025.
- Education and training that extends beyond traditional computer and IT higher-education courses, to non-traditional streams such as law and business. We should also develop a new stream of skilled personnel through TAFEs.
- A pedagogical view that cyber security should be treated no differently to Maths or English in that it will be a fundamental skill for future generations.
- Initiatives that empower females to study science, technology, engineering and maths subjects from primary school. We also need to encourage, retain and create growth opportunities for women in IT and cyber security, including board-level opportunities.



A national cyber security 'engine' is needed to build skills, education and training.

Helping Australia reach its economic potential

As an early stage adopter in cloud and other new technologies, Australia is well placed to become a hub of innovation and digital development. Accordingly, the future of Australia's economy is to be cyber-enabled. A bi-partisan Australian cyber security strategy is critical for a strong economy and future prosperity.

A national cyber security plan will help secure Australia's economic future and address national priorities that include uplifting cyber security leadership, implementing state-based Cyber Security Centres; building trust; enabling a greater level of information sharing; incentivising innovation and positive cyber security behaviours; and increasing education and training for Australians in cyber security related areas.

Cisco looks forward to an ongoing partnership with the Australian Government in helping Australia, its citizens and its partners, to reach their economic potential on the foundation of a secure digital economy.

Cisco would like to acknowledge key contributions to this report by Melissa E. Hathaway.

Cisco Australia and New Zealand | Head Office, Level 10, 80 Pacific Highway, North Sydney 2060, Australia | Contact