Review of Australian Government Cyber Security Strategy

AIIA Response

April 2015

7-11 Barry Drive
Turner ACT 2617
Australia

T 61 2 6281 9400
E info@aiia.com.au
W www.aiia.comau

Contents

1. Introduction

1.1 About AIIA

The Australian Information Industry Association (AIIA) is the peak national body representing Australia's information and communications technology (ICT) industry. Since establishing 36 years ago, the AIIA has pursued activities aimed to stimulate and grow the ICT industry, to create a favourable business environment for our members and to contribute to the economic imperatives of our nation. Our goal is to "create a world class information, communications and technology industry delivering productivity, innovation and leadership for Australia".

We represent over 400 member organisations nationally including hardware, software, telecommunications, ICT service and professional services companies. Our membership includes global brands such as Apple, Avanade, EMC, Google, HP, IBM, Intel, Lenovo, Microsoft, PWC, Deloitte, and Oracle; international companies including Telstra and Optus; national companies including Data#3, SMS Management and Technology, Hills Limited, Technology One and Oakton Limited; and a large number of ICT SME's.

1.2 Overview

AIIA appreciates the opportunity to provide a submission to the Government's review of it's Cyber Security Strategy. As the peak industry body representing the views and opinions of the ICT industry, AIIA has worked in collaboration with our members to develop this submission.

The last two decades has been witness to the changing economic and social benefits that technology has brought to our way of working, interacting and our time at rest.

Open networks have made it easier to obtain and share information and have created untold opportunities for businesses and people to invent. As technologies become more pervasive, the costs of innovation are lowered empowering at consumers, small and medium-sized enterprises, and micro-enterprises to innovate on the same platform as large enterprises.

As technology continues to advance at such a rapid pace the gap between technology adoption and policy and regulations governing its use is widening. While there is a temptation to bridge this gap through increased regulation, this raises the risk of also stifling innovation.

Cyber security is increasingly a complex ecosystem. It is difficult for government alone to understand its full complexities. AIIA is strongly of the view that a holistic approach, involving industry, academia, universities and research organisations such as NICTA and CSIRO is required and that this needs to extend to the development of appropriate policy and regulation.

Clear accountability across government agencies with a single interface for industry will provide certainty and direction for Industry. Strengthened public/private partnerships will be fostered through existing structures and organizations, such as critical infrastructure sector networks. Cross sector mechanisms could also be established, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security.

Governments must invest in the education of our next generation of workers and citizens to grow a highly aware, security savvy culture. Government, industry, academia and research institutions need to work together to develop and best practices in cyber security. Understanding the new treats and vulnerabilities and working with global institutions in developing common knowledge that can then be shared must also be a priority.

Importantly, the Review needs to ensure that the outcomes of this current work does not simply amount to additional red tape as this will be counterproductive to all stakeholders with a genuine in addressing cyber security and building Australia's national resilience in this area.

In responding to the Review AIIA has therefore identified, and discusses in this submission six priority areas of action. These are:

1. The need to keep pace with rapid technology change;
2. Awareness of the increasing sophistication of cyber threats and risks;
3. Clarification of roles and responsibilities, including across government and between government and industry;
4. Improved reporting and information sharing mechanisms;
5. Appropriate legal and regulatory frameworks; and
6. Addressing the skills deficit.

This submission provides detailed recommendations in each of these areas and strongly encourages the Government to take these into account in development of its new Cyber Security Strategy.

2. Background

2.1 The digital ecosystem

Generating between $2 trillion and $3 trillion per annum[1] to the global economy the internet has become a fundamental 'utility' (like power and water), supporting the machinery of government, commercial organisations, and the well-being of citizens. Without its safe and effective operation, the gears of our increasing complex economy and society will grind to a halt.

Household and business use of the internet continues to rise.

The number of households with access to the internet reached 7.3 million in 2012–13 - some 83% of all households (up from 79% in 2010–11). Three quarters (77%) of these accessed the internet via a broadband connection, with four out of five households (81%) accessing it at home every day. Another 16% access the internet at home at least weekly.[2]

The Australian Bureau of Statistics (ABS) reports that some 92% of businesses access the internet, with the greatest increase being the proportion of businesses that place orders online - jumping 4 percentage points to 55% between 2010-11 and 2011-12.   Of businesses accessing the internet over 92% report using broadband.[3]

While the proportion of businesses that reported receiving orders online was steady between 2010-11 and 2011-12 (28%), the value of income derived from the sale of goods or services via the internet increased by 25%, from $189 billion in 2010-11 to $237 billion during this period.[4]

Concurrently average broadband downloads grew more than 33% from December 2013 to December 2014.[5]

As our reliance on the internet continues to grow, there is little doubt that high speed communication networks have become the indispensable infrastructure of modern societies and economies. Pervasive broadband, ubiquitous connectivity, cloud computing, social media, big data and data analytics, mobility, the Internet of Things (IOT) – to name a few, have coalesced to transform every aspect of our social, personal, economic and business lives and to expose every aspect of our life to cyber security risk.

Just as technology is being infused into all facets of society, making it impossible to separate business and technology strategy[6] so too it is impossible to separate cyber security risks.

2.2 Cyber security: Impacts and costs

While governments, Individuals, and industry are embracing the many advantages the internet offers, the reliance on online technologies is also exposing more of us, and our economies to cyber risks.

[1]The Telegraph, Cyber crime costs global economy $445 bn annually, article, 9 June 2014, http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html

[2] Australian Government, ABS, 8146.0 - Household Use of Information Technology, Australia, 2012-13, http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/8146.0Chapter12012-13

[33] Australian Government, ABS, 8129.0 - Business Use of Information Technology, 2011-12, http://www.abs.gov.au/ausstats/abs@.nsf/Products/4C4A170C572B354DCA257BCE0012316F?opendocument

[4] ACMA, Annual Report Key Indicators, 2013-14, http://www.acma.gov.au/theACMA/Library/Corporate-library/Corporate-publications/communications-report

[5] Australian Government, NBNCo, Internet downloads increase by 33 per cent – ABS, 2015, article, 1 April 2015, http://www.nbnco.com.au/corporate-information/media-centre/media-releases/internet-downloads-increase-by-33-per-cent-abs.html

[6] Deloitte, Tech trends 2015, The Fusion of Business and IT , 2015, http://landing.deloitte.com.au/rs/deloitteaus/images/Tech-Trends-2015_Report_FINAL.pdf?mkt_tok=3RkMMJWWfF9wsRons6XId%2B%2FhmjTEU5z16e8uWqKygYkz2EFye%2BLIHETpodcMTsRqNbzYDBceEJhqyQJxPr3CKtEN09dxRhLgAA%3D%3D

Australian businesses

Organisations experiencing cyber crime continues to rise. A recent PwC survey[7] reported that the total number of cyber security incidents detected in 2014 climbed to 42.8 million, representing an increase of some 48% from 2013. Significantly outstripping growth in global GDP at 21% (OECD, Economic outlook No. 95, May 2014).[8]

More worrying is PWCs estimate that some 71% of incidents go undetected and while large corporations are reporting a significant increase in incident detection, smaller companies advise a decrease (by 5%) of identified security incidents.[9] This is concerning in light of Symantec's latest finding that in 2014, 60 percent of all targeted attacks struck small- and medium-sized organisations.[10] These organisations often have fewer resources to invest in security, and many are still not adopting basic best practices like blocking executable files and screensaver email attachments. This puts not only the businesses, but also their business partners, at higher risk.

Despite the increase in security incidents, PwC also found that spending on security is declining – security spending stalled at 4% or less as a percentage of IT budgets for the last 5 years. While the report hypothesises the likely reasons for this, the fact remains that reliance on online technology, combined with its pace of change, means exposure to cyber risk is also rising.

The Australian economy

It is difficult to measure the financial impact of cyber crime. The cost of cybercrime is ultimately unknowable because many attacks are not reported and the value of certain types of information, such as intellectual property is difficult to calculate.

The cost to the Australian economy ranges from $1.06 billion[11] in 2013 to $4.3 million[12] in 2014. Globally McAfee estimates the cost at around $445 billion annually.[13] Verizon reports that a company that suffers a data breach involving just 100 records can expect a cost in the tens of thousands of dollars.[14] Whatever the figure, it is clear that the rise in cyber security incidents strongly indicates a correlating rise in costs.

Deloitte[15] identified specific industries as being at risk including high technology, online media, telecommunications, e-commerce, insurance, manufacturing, and retail. At a global level these risks compound to drive down economic growth and slow the pace of global innovation. Compromises to cyber security can result in far reaching individual, business, social and economic consequences.

Australian people

Australia is an increasingly popular target for cyber came. A recent report by Symantec[16] found Australia experienced a 1,300% increase of crypto malware – a scheme where users are sent emails

[7] PwC, Global State of Information Security Survey, 2015, http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

[8] PwC, Managing cyber risk in an interconnected word, Key findings from the global state of information security survey 2015, 2014, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[9] PwC, Managing cyber risk in an interconnected word, Key findings from the global state of information security survey 2015, 2014, http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf

[10] [10] Symantec, Internet Security threat Report, 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[11] Symantec, 2013 Norton Report: Total Cost of Cybercrime in Australia amounts to AU$1.06 billion, press release, 16 Oct 2013, http://www.symantec.com/en/au/about/news/release/article.jsp?prid=20131015_01

[12] Australian Security magazine, *HP Reveals Cost of Cybercrime in Australia Escalates 33 percent to $4.3 Million*, press release , 19 Dec 2014, available at https://www.australiansecuritymagazine.com.au/2014/12/hp-reveals-cost-cybercrime-australia-escalates-33-percent-4-3-million/

[13] The Telegraph, Cyber crime costs global economy $445 bn annually, article, 9 June 2014, http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html

[14] Verizon, Data Breach Investigations Report, 2015, http://www.verizonenterprise.com/DBIR/

[15] Deloitte, Global Cyber Executive brief, 2014, http://www2.deloitte.com/gz/en/pages/about-deloitte/articles/deloitte-releases-global-cyber-executive-briefing.html

[16] http://www.symantec.com/connect/blogs/australians-increasingly-hit-global-tide-cryptomalware

that typically appear as if they are from local companies. In 2013 38% of Australian mobile users – over a third, had experienced some form of cybercrime.[17]

Individuals are targeted by many means. While email remains the significant attack of choice, there is a clear movement toward social media platforms. In 2014, Symantec observed that 70% of social media scams were manually shared.[18] Mobile attacks is a growing concern, as many people only associate cyber threats with their PCs and neglect basic security precautions on their smartphones. The same report found that 17% of all Android apps (nearly one million) were malware in disguise. Risks to many IoT devices are exacerbated by the use of smartphones as a point of control. Some of this may reflect the attitudes of end users. The report found one in four admitted they did not know what they agreed to give access to on their phone when downloading an application and 68% were willing to trade their privacy for a free app.

Australian Government

Locally the Australian Signals Directorate (ASD) has responded to some 940 cyber incidents involving Government agencies over the last year - a 37% increase on the previous year. Based on industry experience, there is likely a large proportion of unreported incidents that are dealt with internally or discreetly.

In their 2013 Cyber Security Picture, ASD reported that socially engineered emails remain the most prevalent threat to the Australian government networks and that the techniques used by the hackers are evolving to appear even more legitimate to the receivers.[19]

[17] Symantec, Internet security threat report 2014, 2014, https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

[18] Symantec, Internet Security threat Report, 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

[19] Australian Government, Department of Defence, The Cyber Security Picture 2013, http://asd.gov.au/publications/protect/Cyber_Security_Picture_2013.pdf

3. Key considerations the Review must address

Cyber security is fundamentally a socioeconomic, not a technical issue. In discussions with Government agencies in this Review and more broadly, we think that this is generally understood by many but not all. Outlined below are a number of key areas we believe the Review should prioritise.

3.1 Responding to the pace of technology change

Technologies including the internet, computer systems, hardware, software, and services, ubiquitous devices, and digital information - change constantly. Devices to connect to the internet are continually updated and upgraded. Technology is disrupting business models and new service delivery models, mobile applications, social networking, and cloud computing capability are evolving and maturing.

Under the persistent pressure of technology change, companies are struggling to keep pace. According to Symantec[20]:

- Attackers are moving faster and defences are not. For example in 2014, it took 204 days, 22 days, and 53 days respectively, for vendors to provide a patch for the top three most exploited zero-day vulnerabilities (a hole in software that is unknown to the vendor). By comparison, the average time for a patch to be issued in 2013 was only four days.

- Attackers are streamlining and upgrading their techniques, while companies struggle to fight old tactics. For example attackers perfected watering hole techniques, making each attack more selective by infecting legitimate websites, monitoring site visitors and targeting only the companies they wanted to attack.

- Cyber attackers are leapfrogging defences in ways companies lack insight to anticipate. For example, in 2014 advanced attack trends include, building custom attack software inside their victim's network, on the victim's own servers and hiding inside software vendors' updates, in essence "Trojanizing" updates, to trick targeted companies into infecting themselves.

A 2014 Rand Corporation study on Markets for Cyber Crime Tools and Stolen Data[21] found the cyber black market has evolved from a varied landscape of discrete, ad hoc individuals into a network of highly organized groups, often connected with traditional crime groups (e.g., drug cartels, mafias, terrorist cells) and nation-states.

According to the study, black and grey markets for computer hacking tools, services and by-products such as stolen credit card numbers continue to expand, creating an increasing threat to businesses, governments and individuals.[22]

One dramatic example is the December 2013 breach of retail giant Target, in which data from approximately 40 million credit cards and 70 million user accounts was hijacked. Within days, that data appeared — available for purchase — on black market websites.

The growth in cybercrime has been assisted by sophisticated and specialized markets that freely deal in the tools and the spoils of cybercrime. These include items such as exploit kits (software tools that can help create, distribute, and manage attacks on systems), botnets (a group of

[20] Symantec, Internet Security Threat Report 2015, https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

21 Rand Corporation, Markets for Cyber Crime Tools and Stolen Data, 2014, http://www.rand.org/pubs/research_reports/RR610.html

[22] Rand Corporation, Markets for Cyber Crime Tools and Stolen Data, 2014, http://www.rand.org/pubs/research_reports/RR610.html

compromised computers remotely controlled by a central authority that can be used to send spam or flood websites), as-a-service models (hacking for hire) and the fruits of cybercrime, including stolen credit card numbers and compromised hosts.[23]

The Rand report found the evolution of the cyber black market mirrors the normal evolution of markets with both innovation and growth. Products can be highly customized, and players tend to be extremely specialized. For many, the cyber black market can be more profitable than the illegal drug trade.

In light of these advances, it is imperative that any cyber security strategy is dynamic and flexible.

Recommendation 3.1

To ensure cyber security approaches keep pace with the rapid development of technology products, services and capability it is recommended that:

a. *The refreshed Cyber Security Strategy is dynamic, with the capacity to adapt policies and actions to new technology developments/capabilities as they emerge.*

b. *Industry is proactively engaged by government to share intelligence on emerging technology developments, including potential cyber security implications.*

c. *Information about the benefits and risks of new technology is understood by all stakeholders.*

d. *The Cyber Security Strategy is subject to regular reviews, and this includes input from industry.*

3.2 Responding to lack of awareness in the sophistication of cyber crime

Security practices must keep pace with constantly evolving threats and security requirements. Doing so will require investments in the right processes and technologies. However many organisations are failing to make these investments.

Cyber security is a whole of business issue

Cyber security is a whole of business priority not simply an IT issue. For large businesses this means the Board must understand how the organization will defend against and respond to cyber risks. However according to the 2015 PwC survey, only 25% of respondents reported that their Board is involved in review of current security and privacy threats. Only 36% advised that their Board is involved in the development of security policies.[24]

Third party vendors are becoming a significant source of cyber risk. The PwC survey points out that as large companies tighten their security measures and become harder to breach, cybercriminals turn to smaller organisations as easier targets, using them as gateways in to their larger partners. Notwithstanding, the survey also revealed third party security weakened in the past year even as the number of incidents attributed to third parties increased. Only 50 % of respondents say they perform risk assessments on third party vendors (down from 53% in 2013), and just 50% say they have conducted an inventory of all third parties that handle personal data of employees and customers. Just over half (54%) of respondents say they have a formal policy requiring third parties to comply with their privacy policies, down from 58% in 2013.[25] This is despite privacy obligations under the Privacy Act and other legislation.

[23] Rand Corporation, Markets for Cyber Crime Tools and Stolen Data, 2014, http://www.rand.org/pubs/research_reports/RR610.html

[24] PwC, Global State of Information Security Survey, 2015, http://www.pwc.com/gx/en/consulting-services/information-security-survey/index.jhtml

[25] Ibid

To help stakeholders keep pace with constantly evolving cyber threats, AIIA considers education and awareness of security risks and threats is imperative.

Recommendation 3.2

Awareness raising, education and cultural change are an essential component of Australia's cyber defence system. This must be directed at all stakeholders: government, business and individuals. In emphasising the need for increased awareness raising and education it is recommended that:

a. *Awareness and education programs are developed to address the specific vulnerabilities of stakeholders including government, business and individuals. Particularly, ensuring stakeholders are aware of:*

    - *their legal obligation to protect information and the ramifications of failure to do so. Businesses should be made aware that consequences of damaged reputation may be higher than the costs associated with implementing best practice.*
    - *the range of security options available to them, including relevant technology, information sharing, risk management models, training and globally accepted security standards/guidelines.*

b. *Education for small and medium size businesses include security awareness training regarding the types of attacks they may face and the options available for the protection of both digital assets on premise and within cloud environments.*

    - *For operators of small IT service companies Government could consider the development of funded education programs focused on the cyber security fundamentals.*

c. *Government adopt a targeted approach to cyber security awareness within the general public. For example, leveraging training in schools to target students.*

d. *Large business and government education is provided through internal security awareness training programs. These programs should be premised on known best practice.*

e. *Awareness training for Australian government addresses cyber security issues on multiple fronts, i.e. that it is a department wide (not just IT) issue and cyber defence approaches are incorporated into all levels of policy and process.*

3.3 Clarifying roles and responsibilities

Roles and responsibilities in relation to cyber security and building Australia's cyber resilience must to be addressed at two levels: first in relation to the diversity of Government departments and agencies that have an apparent role relating to cyber security and second, clarification of the respective roles and responsibility of government and industry.

Roles and responsibilities across government

Across government, fragmentation of intelligence sources, cyber security policy and agency accountabilities mitigate our ability to manage cyber security holistically.

Responsibility for cyber security reporting, intelligence detection, cyber policy development, regulatory requirements, compliance and awareness and education programs both internal and external to Government, sit across a range of agencies. This includes across the Departments of Communications, Attorney General, Defence, Prime Minister and Cabinet and Finance.

AIIA appreciates the complexity of the Government operations but we are concerned that current arrangements lack a coordinated, consistent whole of Government approach. This creates the potential for gaps in messaging, communication and action across the system which potentially exposes unnecessary vulnerabilities in Australia's cyber security and resilience capabilities.

Notwithstanding the role of the Australian Signals Directorate (ASD) in developing and executing Government security policy, the level of expertise agencies have to identify and mitigate cyber intrusions in an increasingly dynamic digital environment is unclear. The ramifications of these weaknesses raise obvious concern for citizens who entrust government with their personal information and for the organisations and businesses that transact with Government.

AIIA members have expressed the view for:

- greater clarity in the roles, responsibilities and accountabilities of the Government's cyber security infrastructure;
- a rationalisation of efforts, with a corresponding consolidation of resources to ensure investment in cyber security resilience is appropriately robust and targeted; and
- a single cyber security reporting point, or at worst two reporting points; one for individuals and one for business and government agencies.

Role of Government

Both government and industry has an obligation in managing Australia's cyber security environment.

Government's role is threefold.

1. To develop and maintain a set of 'voluntary' guidelines for Best Practise.
2. To develop and implement an education and communication strategy for all stakeholder groups on how to identify, protect against, deter, respond and recover from a cyber-attack.
3. To mandate cyber security practices for Government Departments, Agencies and Government Contractors.

In terms of information provision to citizens and business, information needs to be easily accessible and should:

- promote the use of best practice;
- describe the protection that is both required as a minimum and recommended to ensure the likelihood of a breach or incident is minimised;
- provide alerts to business and citizens via websites and social media; and
- provide a single point for accessing information and reporting.

The provision of best practice information to citizens should be in a form that is accessible with information presented in a way that is easy to understand regardless of literacy level. Information should articulate how they identify, protect, deter, respond and recover from a cyber-attack.

Best practice information provided to business should articulate:

- requirements to protect information stipulated by any legislation;
- how this protection can be achieved; and
- what needs to be done in the event of a cyber-attack or data breach.

This information could be disseminated to businesses using existing touch points such as when a business is established, when a business registers for a domain name and through routine government/business transactions.

Role of Industry

Industry also has three specific obligations.

1. To adhere to best practice cyber security policy and process, including training.
2. To ensure it understands and meets its obligation in relation to the protection of digital assets and information of its customers.
3. Appropriate disclosure where security is compromised and information breached.

Businesses small and large are targets for both criminally motivated and state sponsored cyber-attacks where information is sought for either personal gain, economic advantage or espionage. As such businesses should be required to use best practice information to inform their risk management, security strategies and implementations.

Responsibilities of business should also include the sharing of information and the disclosure of incidents. Currently there are numerous points through which information on a cyber-security incident can be reported, including:

- CERT Australia (CERT): provided by the Attorney Generals Department for businesses;
- Australian Cyber Security Centre (ACSC): for business and government agency reporting;
- Australian Cyber-crime Online Reporting Network (ACORN) – specifically for reporting of information by individuals. Both CERT and the ACSC redirect individuals to this site.

Recommendation 3.3

Australia's cyber security defence must be founded on a solid understanding of the respective roles and responsibilities of Government and industry. It is recommended that the Cyber Security Review:

a. Require Government to collaborate with Industry to develop a shared responsibility approach to cyber security, having regard to the delineation of roles and responsibilities outlined in this response.

b. Recommend the rationalisation of cyber security roles and responsibilities across government, including the consolidation of investment to support a more coordinated national approach.

3.4 Better reporting and information sharing

In addition to the Cyber Security Strategy under review, current cyber security initiatives in Australia include:

- The Commonwealth Government March 2015 commitment[26] to enact a mandatory data breach notification scheme, which will apply to all Australian companies currently subject to the Privacy Act.
- The National Plan to Combat Cybercrime, 2013:[27] Commonwealth, state and territory governments commit to address the threat of cybercrime in six priority areas: education, partnering with industry, information sharing, improving government

[26] Joint Press Release, Senator the Hon George Brandis QC Attorney-General and the Hon Malcolm Turnbull MP Minister for Communications, Government response to the Committee report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, 3 March 2015.

[27] See Australian Government, Attorney General's Department, http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx

agencies including law enforcement, international engagement and effective criminal justice.

- Australian Cybercrime Online Reporting Network (ACORN) 2014:[28] a national online system that allows the public to securely report instances of cybercrime.

- Australian Cyber Security Centre (ACSC) 2014:[29] brings the Australian Government's cyber security law enforcement, defence, and security capabilities into a single location to ensure improved collaboration between these agencies.

- Computer Emergency Response Team (CERT Australia):[30] the point of contact in Government for cyber security issues affecting major Australian businesses.

- Trusted Information Sharing Network for Critical Infrastructure Resilience (TISN)[31], industry led initiative to provide an environment where business and government can share vital information on security issues relevant to the protection of critical infrastructure and the continuity of essential services.

- The Council of Registered Ethical Security Testers (CREST Australia)[32], originally funded by the Commonwealth Government, now a non for profit that provides accreditation and training to approved companies and certified staff as information security testing providers.

- Australian Signals Directorate's mitigation strategies[33]: a list of strategies to mitigate targeted cyber intrusions informed by its experience in operational cyber security.

There are a number of reporting mechanisms currently available (ACORN and CERT Australia) but sharing of information is limited to critical infrastructure (TISN).

There is insufficient detail to comment on the March 2015 commitment to enact a mandatory data breach notification scheme, however AIIA notes the lack of industry consultation.

AIIA supports the initiatives of ACORN and CERT Australia but believe there is room for improvement. AIIA considers that the 'missing link' in Australia's approach to building national cyber resilience is a mature information-sharing framework.

Notwithstanding some noted reservations[34], information sharing is critical to cyber resilience. It is a sure way to avoid wider damage and contribute to a deeper knowledge base aimed to detect, prevent and minimise the risk of future attacks. Continued threat intelligence and knowledge sharing would also facilitate real time threat detection and response.

What does a mature information-sharing framework look like?

Given the number of reporting mechanisms currently available (ACORN, CERT Australia, commitment to enact a mandatory data breach notification scheme) Government, in consultation with industry could develop an information sharing framework that considers:

- What information would be shared i.e. what would constitute an incident;

[28] See Australian Cybercrime Online Reporting Network, http://www.acorn.gov.au/

[29] See Australian Government, Department of Defence, http://www.asd.gov.au/infosec/acsc.htm

[30] See Australian Government, Attorney General's Department https://www.cert.gov.au/about

[31] See Trusted Information Sharing Network for Critical Infrastructure Resilience, http://www.tisn.gov.au/Pages/default.aspx

[32] See The Council of Registered Ethical Security Testers , http://www.crestaustralia.org/

[33] See Australian Government, Department of Defence, http://www.asd.gov.au/infosec/mitigationstrategies.htm

[34] Cyber security expert Martin C. Libicki, who provided testimony to US Homeland Security Committee noted that sharing information about threats is not necessarily a cyber security panacea. According to Libicki, usefulness of threat-based information-sharing rests on four assumptions about the nature of the threat itself. Such assumptions would have to be largely or totally true before the value of establishing an information-sharing apparatus can justify the effort to operate it, persuade organisations to contribute to it, and offset the residual risks to privacy that such information transfer may entail. See http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT425/RAND_CT425.pdf

- Who would share it (government, industry, individuals);
- How the information would be used; and
- If reporting is mandatory, and if so, the regulatory cost of reporting (this depends on what constitutes an incident), and proper incentives and penalties.

This information could be consolidated into a centralised repository of all information relating to cyber attacks, including cyber attacks on government, and could provide properly anonymous reports to interested stakeholders. These reports could outline the nature of incidents, the types of targets, the impacts/costs and be annually updated. Where the attack involves the release or theft of personal identity information or financial details, these events should be made public as soon as possible

A specific area of concern raised by AIIA members is the ability to ensure supply chain systems can quickly recover in the event of an incident. There is a need for better stakeholder understanding of global supply chain models, how these systems are interconnected, and the nature of cyber risk across systems. Information sharing in this instance relates to improving the understanding of data, location and vendor risks in order to develop practical mitigation plans.

An interesting example of one information sharing framework is new data security laws proposed by New York Attorney General Eric Schneiderman (see break out box).

In light of the increasing sophistication of cyber risk combined with the adaptive nature of cyber adversaries AIIA strongly advocates the need for a more systemic approach to cyber security. This requires the careful balance of compliance, incident disclosure, intelligence sharing and enforceable penalties. We anticipate that such a model will require a level of codification having regard to factors such as the sensitivity of the information breached; the nature and severity of the breach/attack/incident; and incident impact.

An example of balancing disclosure and ensuring accountability of organisations

Recognising the perverse incentive not to notify security breaches, new data security laws proposed by New York Attorney General Eric Schneiderman require companies to increase safeguards in the protection of personal information, while also providing a level of protection where data breaches are notified. The Bill, if passed, will broaden the scope of information that companies are required to protect, and mandate stronger administrative, technical and physical security measures to ensure information protection. These include:

- Administrative safeguards to assess risks, train employees and maintain safeguards;
- Technical safeguards to
    - identify risks in their respective network, software, and information processing
    - detect, prevent and respond to attacks
    - regularly test and monitor systems controls and procedures; and
- Physical safeguards to have special disposal procedures, detection and response to intrusions, and protect the physical areas where information is stored.

Organisations that undertake an annual, independent third-party audit certification process that reports compliance with the new requirements will have a rebuttable presumption of having reasonable data security measures in place should an incident result in litigation. The proposed law would also amend existing data breach notification law to include in the definition of "private information" the combination of an email address and password, the combination of an email address with a security question and answer, medical data, and health insurance information. Organisations are currently not required to notify consumers of a breach of any of these types of information.

Recommendation 3.4

The ability to share information regarding security incidents and breaches is essential to building a strong cyber defence system. It is recommended that:

a. In consultation with industry, Government establish an information sharing framework that is based on the agreement of:

   - what information would be shared i.e. what would constitute an incident;
   - who would share it (government, industry, individuals);

    - how the information would be used; and
    - if reporting is mandatory, and if so the regulatory cost of reporting (this depends on what constitutes an incident), and proper incentives and penalties.

b. This framework provide the basis for a centralised repository of all information relating to cyber attacks, including cyber attacks on government, and provide properly anonymous reports to interested stakeholders.

    - At a minimum these reports should outline the nature of incidents, the types of targets, the impacts/costs and be annually updated.
    - Where the attack involves the release or theft of personal identity information or financial details, these events should be made public as soon as possible.

c. Government should support the development of an industry led Legal and regulatory frameworks

3.5 Legal and regulatory frameworks

AIIA acknowledges the pros and cons of enforceable regulatory arrangements versus voluntary, self-regulation and industry guidelines to support improved control of cyber security.

Type of measure	Examples in force	Advantages	Disadvantages
Self-regulation	Content Classification Schemes	Bottom up - industry identifies viable solutions with limited government intervention	Limited oversight from government to ensure objectives
Industry guidelines	Office of Fair Trading, Guidelines for home building, clinical practice guidelines etc	Flexible guidance can evolve with technological progress	Redress mechanisms not always clear to consumers
Terms of service of platforms (filtering offensive / illegal content)	YouTube, Facebook, Google etc	Leverages collective power of user communities	Filtering decisions often not without controversy
Legislation/regulation	Privacy Act, Corporations Act, Consumer Protection legislations	Sets out expectations and consequences	Too inflexible for an evolving industry

In general industry is reluctant to support prescriptive legislation and regulation on the basis that such arrangements typically lack flexibility to respond to rapid technological change and the accompanying adeptness of cyber threats.

Even if government can be more agile (for example, by executing measures through conferred executive powers instead of legislation) the level of expertise required to deal with cyber security risks relating to industry aren’t readily available in government and threats that emerge are too decentralised for government to reliably mandate appropriate responses in a timely way.

Traditionally, the areas where prescriptive regulation has been successful are where there is a risk to loss of life for example, building codes, food safety standards and OH&S laws. This is not the case here.

There is strong support for set minimum standards, industry codes and guidelines. The issue is not that these require development but that business needs guidance in respect of which of these will meet their needs.

AIIA recommends the Australian Government release a comprehensive and easily accessible toolkit that provides advice on available options and how they should choose between them. The NIST Cyber security Framework and iCode are good examples of industry developed guidelines. The ASD *Strategies to Mitigate Targeted Cyber Intrusions*, is a good example of Government developed guidelines.

Encouraging an accreditation scheme to incentivise organisations to provide stakeholders with a level of assurance in their cyber protection strategies has also been suggested. The scheme could offer levels of accreditation depending on the level of information an organisation holds. This is different to the accreditation scheme provided by CREST Australia that provides accreditation or registration of security providers/professionals.

For consumers, secure user behaviour can be encouraged through both technical and non-technical tools. Overall, a review of the evidence suggests that there is need for more sophisticated security tools that give users greater control in managing the security of their devices.[35] Such tools may include more frequent patching and the potential of internet of things-specific protection software.

Non-technical tools may include privacy and security by design, the approach to systems engineering that takes privacy and security into consideration throughout the design process. Privacy and security can also be supported by 'nudges': strategies that aim to incentivise users to behave in more security-conscious ways, such as requiring updates before a program can continue to run.

By providing unified and centralised options for handling cyber security issues, the Government can play a pivotal role in helping strengthen and coordinate Australia's cyber security as a whole.

Recommendation 3.5

Given the lack of flexibility in legislation and regulation to respond to rapid technological change it is recommended that:

a. *Government adopt a light touch approach to cyber security regulation, such as self-regulation and industry guidelines including frameworks for protection.*

b. *In consultation with the ICT industry, Government develop a comprehensive and easily accessible cyber security toolkit. The toolkit should incorporate:*

    a. *training and awareness campaigns of available protective options such as guidelines, codes and standards and how to choose between them;*

    b. *information regarding relevant certification programs, and*

    c. *for individuals, a mix of technical and non-technical support tools and advice.*

3.6 Responding to the cyber security skills deficit

As cyber vulnerability increases the demand for professionals who have the skills to identify, analyse, manage and prevent cyber related attacks is increasing. But educating, recruiting, training and hiring cyber security professionals takes time and depends fundamentally on the right courses being available.

Despite increased industry demand for specific ICT skills, the take-up of ICT related tertiary course over the last decade has halved.[36] A 2014 analysis by the Australian Financial Review[37] of university course take-up by domestic undergraduate students since 2001 shows a 36% decline in students

[35] Rand Corporation, Living Room Connected Devices, (2014) p45

[36] Australian Computer Society, 2012 Australian ICT Statistical Compendium, 2012, http://www.acs.org.au/__data/assets/pdf_file/0014/13541/2012_Statcompendium_final_web.pdf

[37] The Financial Review, Shortage of IT graduates a critical threat, 7 Feb 2014, http://www.afr.com/news/policy/industrial-relations/shortage-of-it-graduates-a-critical-threat-20140206-iy4lx

starting IT degrees, and a 41% decline in students - graduating from those degrees in the same timeframe. Although there has been a slight recovery in commencement numbers since 2009, when Australian universities uncapped the number of students they enrolled in each course, the number of IT students still lags significantly behind an overall 39% increase in new undergraduate students since 2001.

Although ABS labour force data shows that employment of ICT professionals has grown strongly over the 10 years to May 2014 (notwithstanding the decline in student numbers taking up ICT courses), the feedback from employers is that the vast majority of graduating students were not suitable to the advertised positon.[38] Australian Industry Group's (AIG) 2015 *Progressing STEM Skills in Australia* report reinforced this gap – with 36% of business surveyed identifying the lack of tertiary qualifications relevant to the business and 34% the lack of employability skills and workplace experience a major barrier to ICT graduate employment.[39]

While the mismatch between the needs of industry and tertiary graduate qualifications is a general one impacting the whole of the ICT industry, it is particularly playing out in new and dynamic areas of technology capability where course pedagogy is not keeping pace with rapid technology developments. Cyber security is by its nature, one of these areas.

More broadly, building the pipeline of ICT graduates, in fact science, technology, engineering and mathematics (STEM) savvy graduates generally, must be a priority. With International research indicating that 75% of the fastest growing occupations require STEM skills and knowledge[40] government, industry and the tertiary sector must work together to ensure Australia keeps pace with rapid technological and scientific change.

In our recent (February, 2015) Digital Skills and Careers paper, the AIIA highlighted the need for increased Industry support and targeted youth engagement programs that harness and encourage young people to develop STEM based skills and specifically, pursue ICT based careers. While parents saw the value of their children pursuing a digital career few felt that this was a career of interest to them.

Program investment, Industry engagement and education agility are necessary to strengthen the pipeline of STEM and specifically ICT skilled graduates.

Recommendation 3.6

To ensure Australia has the skills and expertise to respond to the increasing threat of cyber risks and ability to build cyber resilience strategies, it is recommended that:

a. *The Government commit, as a matter of priority, to developing Australia's workforce of the future based on a foundation of increased STEM capability. For the purpose of this Review, this could include embedding cyber security into STEM education.*

b. *In consultation with the Department of Communications, the Review seek to expand the Government's Digital Careers program aimed to encourage young people to develop careers in ICT. Additional investment in the program could be targeted to meet the specific needs relating to strengthening Australia's cyber security capability.*

c. *The Government support industry efforts to increase engagement with the Australian tertiary sector to identify gaps, barriers and solutions to obtain job-ready graduates, including the development of best practice pedagogy and industry input into educational course and curriculum design*

[38] Australian Government, Department of Employment, Labour Market Research – Information and Telecommunications (ICT) Professions, http://docs.employment.gov.au/system/files/doc/other/ictclusterreportaus.pdf

[39]The Australian Industry Group, Progressing STEM Skills in Australia, 2015, http://www.aigroup.com.au/portal/binary/com.epicentric.contentmanagement.servlet.ContentDeliveryServlet/LIVE_CONTENT/Publications/Reports/2015/14571_STEM%2520Skills%2520Report%2520Final%2520-.pdf

40 Benchmarking Australian Science, Technology, Engineering and Mathematics, Office of the Chief Scientist, November 2014.

4. Implementation requirements

The weakness of the 2009 Cyber Security Strategy is that it failed to articulate a clear plan of action, accompanying accountabilities, outcome targets and success criteria, a measurement framework and a commitment to transparent reporting of progress. While it committed to a broad range of activities, it did not provide a clear execution path.

It is our view that the effectiveness of the revised Strategy will be determined by four core features.

a. The development of a Strategy premised on the understanding that cyber security is fundamentally a socioeconomic, not a technical issue. In discussions with Government agencies in this Review and more broadly, we think this is generally understood. Although, as noted in the previous section more is required to ensure priority is given to resourcing cyber resilience and in particular, developing the expertise necessary to keep pace with changing technology, potential vulnerabilities and the increasingly sophisticated and challenging cybercrime landscape.]

b. Shared responsibility, including shared intelligence. This requires Government and industry combining efforts to tackle increasingly pervasive cyber threats. While we believe there is intent to develop and execute a more holistic approach to mitigating cyber security and building cyber resilience, the Strategy will need to describe how this will translate to action.

c. The Strategy must be supported with a plan of action. This includes clarity of roles and responsibilities and accountabilities; milestones; targets; measures; investment commitments and reporting frameworks. Industry is committed is working with government in support of this Plan.

d. The Strategy must be dynamic and incorporate the principle of agility to reflect the environment in which it will operate. With the pace of change - both in technology and cyber risk sophistication – identified as a major challenge, the Strategy must have the ability to evolve and respond to the constantly changing environment in which it is applied.

5. Conclusion

As a priority we must look beyond cyber security as a cost of doing business and leverage our comparative advantage in highly specialised skills to become a world leader in identifying and managing cyber security threats as well as awareness and education campaigns from foundation education to the Boardroom.

Cyber security and the need to build national cyber resilience is a national issue that requires the cooperation and active participation of all stakeholders – individuals, businesses, governments, industry sectors and vendors. It requires a collaborative nation-wide approach in which all stakeholders understand that cyber vulnerability is not a simple technical issue but rather has much deep and potentially damaging social, economic and nation state ramifications.

In responding to this Review AIIA has strongly advocated for closer engagement between Government and industry, academia, universities and research organisations such as NICTA and CSIRO and that this needs to extend to the development of appropriate policy, regulation and information sharing frameworks. We believe this is imperative on an ongoing basis to ensure Australia is sufficiently agile to respond to the unpredictable but persistent landscape of cyber threats.

AIIA members have expressed a keen willingness to work with Government to refine and execute a new Cyber Security Strategy.