COMMUNICATIONS
ALLIANCE LTD

Department of the Prime Minister and Cabinet
Consultation Paper

Cyber Security Review

COMMUNICATIONS ALLIANCE SUBMISSION
2 APRIL 2015

EXECUTIVE SUMMARY

Communications Alliance appreciates the opportunity to provide this submission in response to the Cyber Security Review (the Review) undertaken by the Department of the Prime Minister and Cabinet.

Industry welcomes a review of Australia's cyber security strategy. It appears that historic developments and an, at times, piecemeal approach have left Australia with a very large number of Government departments and agencies with partly overlapping and intersecting cyber security-related responsibilities. A better coordination of the current spread of agencies and programs and the creation of a single national point of access to Government's cyber security agencies is likely to increase efficiencies and to deliver a clearer message to all stakeholders.

Industry notes that the Review and any resulting framework must link in with other Government security related initiatives such as the Telecommunications Security Sector Reform (TSSR), data retention legislation, copyright and website blocking legislation etc. Currently, these initiatives appear to run in parallel and without a clearly formulated overall strategy. Industry also raises its concerns over the perception that all Industry players ought to and are able to fund these initiatives.

Importantly, any cyber security framework ought to centre around the creation of a cyber literate nation. Individuals and businesses alike must understand the continuously changing requirements of the cyber world and adopt cyber security measures as part of their daily routine, lifestyle and business practices. Equally, industry and academia must ensure that cyber security specialist resources are meeting national demand (in quality and quantity).

Given the nature of cyber security and the fast moving environment in which it operates, it is imperative that the framework remains flexible and allows for rapid adaptability to accommodate technological change.

Industry sees the need for industry-developed codes, standards or guidelines that do not interfere with global efforts towards a standardised security development and solution design. Industry highlights the importance of cooperation of all stakeholders to set common and open security standards that specify the object of protection rather than the technology used to do so.

Consequently, Industry supports an independent process compliance scheme, as opposed to various national certification schemes for devices and IT systems, etc. Industry contends that an industry-led codes/standards-based approach, combined with a framework of protected sharing (e.g. through a legal framework similar to the US Cyber Intelligence Sharing and Protection Act) and a regular and open exchange with all relevant Government stakeholders will provide a more effective strategy to deal with cyber security in Australia.

While cyber security poses challenges for Australia, it also offers opportunities for Australia to become a world leader in identifying and managing cyber security threats and executing education campaigns. Seizing these opportunities not only requires a coherent and efficient national approach to cyber security but also an active Government involvement at an international level with the objective of leading collective action against the source of cyber threats, and the development and enhancement of effective (yet balanced) enforcement mechanisms for Australians adversely affected by foreign cyber threats.

1. Introduction

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

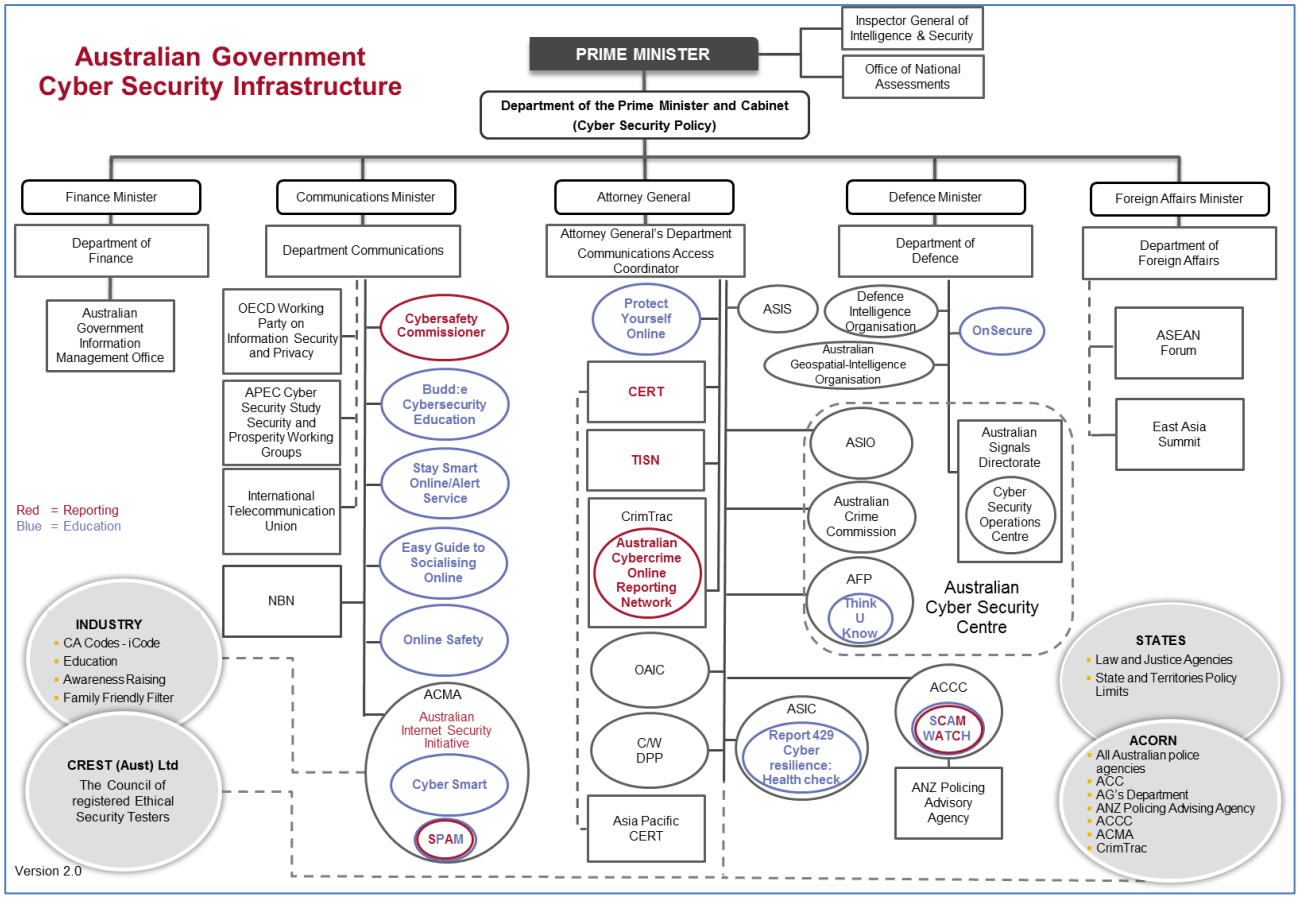
Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance. For more details about Communications Alliance, see http://www.commsalliance.com.au.

In this submission Communications Alliance provides views of its members on a national Cyber Security Strategy. The issues addressed in this submission are guided by the questions raised in the Department of the Prime Minister and Cabinet's consultation paper.

2. The Australian Government Cyber Security Infrastructure

Industry believes that Government's strategy on cyber security ought to focus on coordination, optimisation and efficiency in the use of Government resources to fight cybercrime. In this regard, Industry would like to raise the following points:

As the below diagram highlights, the Australian cyber security landscape is characterised by a wide diversity of Government departments and agencies with an interest in or portfolio responsibilities relating to cyber security. These departments/agencies cover a large array of security related issues and address a multitude of different stakeholders, e.g. telecommunications network operators, businesses across all sectors, the general public, etc.



Source: Baker & McKenzie

Industry seeks to gain a better understanding of the precise roles and responsibilities of each of the involved departments/agencies, and where their responsibilities intersect and overlap. Industry would support a better coordination of the current spread of agencies and programs and more focussed spending on a single national point of access as it is likely to be more effective than the current approach.

Until such an approach is defined, there remains the question of who is the arbiter of security risk within the current landscape. Industry believes that there ought to be a unified directory (or 'single point of truth')of information regarding cyber threats and responses where relevant professionals and members of the public can subscribe to receiving further targeted awareness information (and alerts depending on criticality).

Looking at a wider policy context, Industry is keen to understand the relationship between the Cyber Security Review and the Telecommunications Security Sector Reform (TSSR) currently also being undertaken by Government. It appears that the logical chronological

order of actions has been reversed, i.e. elements (TSSR) of a larger strategy are being considered before the strategy itself (Cyber Security Review) has even been defined.

Industry is also unsure of how the proposed funding model for the TSSR (i.e. full cost-recovery from industry via a levy) fits into a cyber security model and it remains unclear what benefits Industry and consumers will receive from either framework. As set out above Industry recommends a single point of access to a cyber-security framework. Given that such a single point currently does not exist, Industry notes that allocation of any funds (irrespective of their origin) to only one body/agency does not appear to be consistent with the current framework. Industry further comments that, in their view, ASIO may not necessarily be the most appropriate single point of access for a future cyber security framework.

Moreover, Industry reiterates its concerns about the ease with which incremental costs appear to be applied to Industry through legislation and/or regulation (i.e. data retention legislation, copyright regulation and website blocking legislation, TSSR and cyber security reform) – all without a clearly formulated view from Government on an overall strategy or a discussion on a sensible funding contribution model.

3. Challenges and Opportunities

Cyber security specialist resources

One of the biggest challenges posed by cyber security for many organisations, and Australia in general, is the constant need for expert resources to cope with the evolving scope of cyber security threats. This demand for cyber security specialists is not met with an equal supply available to all Australian businesses. The shortage of supply may be partly a result of lacking tertiary (and other) education opportunities in this field. As matters stand today, telecommunications industry members have highlighted a shortage of supply of specialist resources in various areas, e.g. in forensics, penetration testing, incident management and risk assessment.

Against this background, Industry urges Government to develop a cyber security strategy that includes a targeted program to develop and retain Australia's expertise in this area to ensure that local resources are available to all industries and all players within those industries. Given the fast pace of evolution in the cyber security arena combined with the level of technical expertise required for practical industry application, educational institutions/academia and industry from all sectors must cooperate very closely to ensure that education remains relevant and meets demand as technology evolves. Consequently, any education program ought to include mentoring initiatives, graduate programs (including substantial work experience), and grant schemes aimed at fostering innovation and creativity in this space.

Cyber security literacy of individuals and businesses.

As social engineering is a key element of cybercrime, it is essential that individuals and particularly small businesses are being educated on the basics of IT security. A concerted coordinated effort is required to achieve high levels of awareness, education and implementation of security measures. Industry contends that the diverse array of education and awareness initiatives across federal and state agencies is not conducive to achieving this aim. It is recommended that a strategy be developed that analyses the key targets of educational initiatives, focuses the messaging and activities of each program accordingly and ensures a coordinated delivery.

As we rapidly move closer toward an environment of Internet of Everything, the challenge of good cyber awareness, literacy and ultimately security equally moves from being a must for businesses to being imperative for all individuals in Australia who will own or operate an ever increasing number and variety of smart devices, computers, consumer electronics, etc.

Industry contends that a coordinated Government-led education campaign is required to push and actively promote the safe(er) use of social media, email and the internet. Currently, Government initiatives like SCAM and the Stay Smart Online Alert Service go in this direction, however, they require individuals to actively search for information and subscribe rather than pushing information out to the general public. There is a role for Government to foster an instinctive understanding of the general public that cyber security is part of daily life and routine as much as road safety, environmental consciousness and healthy lifestyles ought to be.

While larger Australian businesses are likely to have access to more financial resources to provide attractive employment packages for cyber security professionals, smaller businesses may not be able to compete with cyber security experts' expectations of remuneration. Importantly, smaller businesses may not understand the need for investment in this area in the first place as they may fail to adequately perceive the risk posed by cybercrime.

In any case (for small and large businesses alike), resourcing for the risk of cybercrime always competes with resourcing for other business priorities that are being perceived of delivering more certain and tangible benefits to the company, e.g. the evolution of existing products, innovation of new products, network expansion (in a telecommunications environment) and the general commercial requirement to satisfy customer needs.

It may be worth considering if programs similar to CitySwitch[1] which include the use of awards and certification levels might be used to encourage (particularly small and medium sized) businesses to implement cyber security measures.

Opportunities

While cybersecurity poses challenges for Australia, Industry can see opportunities for Australia to become best-in-class and a world leader in identifying and managing cyber security threats and education campaigns. However, as indicated above such opportunities will only arise on the back of a single cohesive, collaborative nation-wide approach to cyber security that is embraced by Government, industry and the public. Given the fragmented and at times uncoordinated and piecemeal approach to cyber security Industry fears that Australia is not positioning itself to fulfil aspirations of best-practice and becoming an exporter of cyber security related goods and services. Quite to the contrary, it currently appears that Australia is losing qualified professionals to overseas locations without necessarily repatriating the expertise that those individuals have gained abroad.

From a more technical perspective, Industry suggests exploring the potential of a 'secure cloud' to improve personal and small business systems.

4. Legal and Self-Regulatory Framework

Industry believes that the use of a prescriptive legislative framework and stiff regulation in a fast moving environment such as cyber security is inappropriate as they lack flexibility and rapid adaptability to accommodate technological change. However, Industry sees a need for industry codes, standards and guidelines. The NIST Guideline and the iCode serve as good examples of industry documents that have been designed for 'real world' application by industry players of varying sizes. Such codes, standards and guidelines are helpful to ensure that all providers have access to a set of minimum standards to implement in their businesses in a way that suits their business models and their business activities. This is

[1] CitySwitch is a program that supports commercial office tenants/building managers to improve office energy efficiency through the provision of a range of services, with the ultimate aim of achieving a 4 star or higher NABERS energy rating. It helps participants to use a structured approach to planning and implementing energy efficiency projects with the aim of saving time and money and helping to build participants' own capacity to embed sustainability within their corporate structure.

particularly important for key assets that require protection, e.g. the protection of credit card details on the basis of the PCI-DSS standards.

Furthermore, Industry supports global efforts towards a standardised security development and solution design, referred to as Security Assurance Methodology (SECAM)[2]. There is a real risk that uncoordinated global efforts in this area will lead to a diverging set of security requirements, which would jeopardise not only interoperability, but make security that much more complex to guarantee. Global standards and best practices are therefore fundamental to the efficient handling of threats – especially those that originate across national borders – as well as to building economies of scale, avoiding fragmentation and ensuring interoperability. Therefore, it is essential that stakeholders, including operators, vendors, regulators, policymakers and IT-focused companies as well as players from other industries, work together to set common and open security standards that specify what needs to be secure and protected, rather than mandate the use of a particular technology, i.e. Industry supports an independent process compliance/validation scheme rather than fragmented, national certification schemes for devices and IT systems, or expensive, time consuming certifications like the Defence level Common Criteria (CC). The provision of an independent validation for vendor product security claims, similar to the UK Government's Independent CESG Claims Tested Mark (CCTM) could be investigated. This validation essentially paralleled the CC EAL2 (claims test) – but at a realistic Industry/eGov/CNI level, rather than having to apply Defence criteria. Another part of this validation is the Certified Product Assurance (CPA) which paralleled the CC EAL3 (incorporating design, production, supply evaluation criteria).

Key requirements of such validation programs are clear and trusted independence, effective costing for vendors and efficient and reliable turnaround times.

5. Cooperation and Information Sharing

Beyond standards, collaboration among relevant stakeholders can encompass a number of practical areas, including information exchange, threat analysis, performance analysis, sharing of best practices and encouraging cutting-edge research. Given the proliferation of the Internet of Things, cooperation with other connected infrastructures such as energy, transport, health care, resources, automated manufacturing etc. will be of increasing importance.

Within the telecommunications sector, Industry would prefer a single framework of protected sharing to a mandatory data breach notification approach. Industry feels that Government ought to consider creating a legal framework of the kind proposed in the US *Cyber Intelligence Sharing and Protection Act*. This legislation creates protection and immunities for the sharing in good faith of cyber intelligence and would be an advance to the informal arrangements in place for the Trusted Information Sharing Network (TISN). Industry contends that information sharing of this nature is overdue and is necessary to ensure consistent high level protection of critical infrastructure. However, under any approach (legislated or informal) the benefits, communication channels and scope (terms of reference) of information sharing must be clear to all stakeholders to ensure their ongoing engagement and commitment to established processes. Regular working groups and fora to bring Industry and Government together to discuss cyber security issues would assist, especially if Government can offer expertise or advice to business on the current threats and work together to identify future areas of focus. Industry also believes that information about security breaches suffered by Government agencies and information related to espionage

[2] Security Assurance Methodology (SECAM) establishes security requirements not just for products but also for product development processes. According to proposed SECAM rules, accreditors will verify a 3GPP manufacturer's overall capability to produce products that meet a given set of security requirements, which will eliminate the need for explicit certification on a per product basis, while also encouraging a solution based view.

related cyber attacks should be shared by Government with relevant Industry stakeholders subject to protected sharing.

With regards to supply chains, Industry believes that cooperation could be improved to better understand global supply chain models and their interconnections, to understand the nature of threats and risks and the extent to which these can be mitigated, and to ensure supply chain systems can quickly recover in the event of a cyber incident. Industry requires a better approach to the definition of risks and urges Government to adopt an approach similar to that adopted with the development of the iCode where Industry has taken the lead. For example, data, location and vendor risks must be understood in order to develop practical mitigation plans. In practical terms, it would be useful to have a forum facilitated to specifically address security risks for supply chain management and continuity, in addition to ensuring that a standard approach (e.g. ISO27K/ISM, The Open Group Technology Provider Standard, etc.) to security risks is identified and is being followed by all participating entities or industries.

Finally, the overall Cyber Security Strategy itself should be subject to discussion and review in a public forum involving Government and Industry at yearly intervals and expressly be subject to updating in three yearly intervals.

In this context, Industry notes that the Attorney-General's Department Expert Panel has not met in recent times. (Industry understands that the current 'Experts Group' discussing data retention related matters is separate to the AGD Expert Panel.) Industry would welcome the opportunity to continue these forums to discuss at a senior level cyber security issues.

4 Conclusion

Communications Alliance, on behalf of its members, would welcome the opportunity to engage in further dialogue with the Department of the Prime Minister and Cabinet to discuss the views proposed in this submission and the ongoing development of Australia's cyber security strategy.

For any questions relating to this submission please contact Craig Purdon on 02 9959 9124 or at c.purdon@commsalliance.com.au.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507