AIIA feedback: threat blocking at the network level

Prime Minister's Advisory Council on Cyber Security Industry Working group

September 2017

Ground Suite B
7-11 Barry Drive
Turner ACT 2612

GPO Box 573
Canberra ACT 2601

61 2 6281 9400
info@aiia.com.au
www.aiia.com.au

About AIIA

The Australian Information Industry Association (AIIA) is the peak national body representing Australia's information technology and communications (ICT) industry. Since establishing 35 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, EMC, Google, HP, IBM, Intel, Microsoft, PWC, Deloitte, EY and Oracle; international companies including Telstra, Optus; national companies including Data#3, SMS Management and Technology, TechnologyOne and Oakton Limited; and a large number of ICT SME's.

Focus questions:

Can we deploy technical solutions at the border gateways or other high-traffic chokepoints?

This Working Group will consider the feasibility, implications and options for blocking threats before they can spread across Australia's domestic networks. The goal is to reduce cybercrime targeting businesses – particularly SMEs – communities and individuals. Consideration may need to be given to making a form of 'safe harbour' for companies in the event that measures necessary to counter or nullify cyber attacks – eg gateway blocking – result in temporary disruption or network connectivity of some customers.

Comments

Cyber security is a whole of economy issue and any solution to effectively counter cybercrime or 'threat block' must address all levels of the economy; government, industry and citizens.

At the government level

Traditional approaches to security needs to be questioned

The cyber world does not respect traditional approaches to borders, gateways and "perimeter" security for the physical environment.

Cyber security is not 'static'. Addressing the modern cyber challenge cannot rely on existing approaches to security, legislation, and policy.

Using a Law Enforcement example, to prosecute someone for a criminal action in the physical world would require police to capture physical and electronic evidence in the form of witness statements, video surveillance, DNA, etc. In the cyber world, the criminal action may not occur in Australia - for instance, an Australian-based server could have been compromised by an overseas actor and used to carry out an attack that appears to be from an onshore action, and thus the police may not have jurisdiction to arrest them. This means we cannot use a traditional law enforcement approach, and instead may require a diplomatic or counter-attack approach. If the criminal actions were from an onshore actor, then the approach to collecting evidence is fundamentally different. This means traditional evidence requirements for a crime are no longer suitable, making it difficult (or impossible) for police to prosecute.

New defence techniques that are not constrained by legislation designed for the physical world (and IT security approaches designed to support it) are required to identify and protect against these new types of attacks.

Improve threat intel sharing by having a 'One Australian Cyber Central View'

By having cyber security roles span across many Government departments, it is difficult for Industry to provide holistic support. Each agency is more interested in protecting their own needs than supporting the needs of the ecosystem. This siloed approach results in agencies being protective of their systems and information, and results in a fragmented view of the cyber eco-system. Government needs to move to a single consolidated data and analytics platform to become more agile and responsive to cyber-security threats.

Current funding is spread too thinly across too many agencies. This results in wastage, lack of reuse (i.e. all agencies trying to build their own system), and limited information sharing. The centralisation of all money Government has for cyber security will result in the establishment of far more advanced capabilities, versus lots of the same constrained and limited capabilities.

It perpetuates the interdepartmental silos that have slowed down the progression of free flowing ideas and activities. A more holistic, national cyber security structure under a single agency, supported by clear direction and strong leadership is required in response to the issues raised above.

AIIA recommends the establishment of a single cyber security focussed department/agency (or division) to amalgamate and replace current bespoke functions, responsibilities and funding arrangements. This must be supported by a Cyber 360 approach incorporating a focus on government, business and citizen. Ideally, the structure sits under a single minister with a single focus on cyber security. The UK model under a senior Cabinet Minister would be optimal.

Establish New Separate Entity

Recognising various political and practical constraints, we suggest consideration of the following options.

The objective is to build specific cyber core competencies through a centralised national function that is culturally open and receptive to stakeholder engagement and industry consultation.

The core aim of the agency would be to develop a threat intelligence sharing platform that, using readily available technology, could collect and consolidate multiple 'local (banks) and global (vendors)' sources of security data (including both structured and unstructured) combined with data already accessible to government.

The agency could utilise this central repository of security intelligence data from all around the globe to have a complete picture on how best to respond to threats. (See also 5-eyes commentary below).

An option is to drive ICT consolidation to eliminate system duplication and remove information silos, and establish divisional forces i.e. Australian Border Force, Australian Cyber Force (i.e. new force), Australian Police Force (i.e. AFP), Australian Counter-Terrorism Force (i.e. AFP), Australian Organised Crime Force (i.e. ACIC), Australian Fraud Force (i.e. AUSTRAC). All these agencies collect similar information and a centralised ICT platform will facilitate improved intelligence sharing.

Advantages:

- Distinct entity that the federal government can task with all matters related to cyber security that are in the broad national interest
- True single point of contact for state and local governments, industry and citizens
- Broadens focus from cyber-defence to holistic, national cyber-security
- Allows government and industry to contribute without barriers raised by existing security clearance requirements
- More efficient – reduces duplication, consolidates funding and roles

Disadvantages:

- Costly and potentially disruptive to establish
- Vulnerable to budget changes/resourcing issues
- Depending on relationship with PM&C may need to build out support and administrative structures
- Need to establish new WOG relationships

Recognising various political and practical constraints, we also suggest consideration of:

Centralised Cyber Function Within Existing Structure

There are a few ways to do this.

First, expand the role of an existing agency, such as the ASCS (Aus CS Centre) or Australian Criminal

Intelligence Commission (ACIC) and consolidate key cyber security functions and responsibilities.

- In the case of the ACIC, the organisation is developing as a whole of government data hub (via the National Criminal Intelligence System): it provides business/citizen services (i.e. ACORN) for cyber-security and has ties with all law enforcement organisations across Australia. With this underway, they would be well placed to expand their efforts to support a consolidated cyber security approach, particularly if functions and funding was centralised into them. Consolidation could be done in several phases i.e. AUSTRAC first (as per Commission of Audit recommendation), then AFP, etc.
- In terms of the ACSC, it should at the very least, be its own organisation, not a blend of various departments, each with their own masters. The functions of the ACSC could be separated out from the ASD/AG, effectively setting it up as an independent authority (e.g. statutory authority) with representatives from all major stakeholders.

Alternatively, create a heads of agreement between all agencies who have portfolio responsibility over cyber security and consolidate key cyber security functions and responsibilities under this agreement.

- A chair and secretariat will need to be nominated by the parties. The chair and secretariat should be rotated periodically to ensure all agencies have responsibility over the agreement. Decision making can be by group consensus across the agencies.
- This approach is similar to a COAG agreement but at the federal level only. This type of approach worked well in streamlining the Australian consumer law and also in dealing with environmental regulations that span a number of regulators in different jurisdictions. There are similar issues for cyber security in terms of many different actors working in the same pace with different agendas but ultimately working towards a common goal.

An important component of the above approaches would be to establish an Industry representative panel including consumer groups. This would have representatives from all aspects of Industry, and the education sector. It would have an advisory charter but also provide an interface into awareness and shared threat intelligence. It would rotate members regularly to ensure no one group dominated and help establish and measure the effectiveness of the ongoing policies and approaches. It could help establish common qualifications / certifications and approaches for the different market places such as government, business, SMEs and citizens.

Similar to the Option 1 above, the aim would be to develop a threat intelligence sharing platform that, using readily available technology, could collect and consolidate multiple sources of security data for a 360 view of the entire ecosystem (including both structured and unstructured).

Advantages:

- Actual and/or logical centralisation of cyber security responsibilities with clear mandate to oversight national cyber security posture.
- More efficient – reduces duplication, consolidates funding and roles and less expensive than creating a totally new structure
- A familiar model to most bureaucrats and ministers

Disadvantages:

- Potential tensions in amalgamating 'cultures' of different agencies with potential for fall out because some agencies will lose 'control'
- New structure would need to establish new WOG relationships
- A Heads of Agreement will likely result in very slow decision making

Functional infrastructure for an online digital ID

Identity and authentication is core to any security system. This is true for your traditional parameter security and is also true for online security.

There are a number of benefits:

The majority of cyber attacks on an individual is by and large to do with sealing identity.

By having a provider that can authenticate your real identity with your online ID and link to all your other online IDs, it means that in the event of an attack you can ideally just go back and report once to your provider. Who can than suspend your linked actions. This addresses the issue of the weakest link (particularly around SMEs), where currently an individual interacts with 100s if not 1000s of websites with varying levels of security.

It also makes the hackers jobs harder because it means to do anything important you'll have to acquire a more rigorous form of authentication. And it reduces the space that doggy people can operate in.

For more information see AIIA's Guiding Principles for an online trust framework at Attachment A.

AIIA is currently working closely with the DTA on this issue and is happy to share any updated material.

Cooperation between Industry and Government on threat blocking

Minimum standards, industry codes and guidelines supported by easily accessible toolkit

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 has already recommended in various forums that 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.
- Efforts to identify and set requirements via international standards, as opposed to creating localised one would streamline procurement and help enable government and other Australian businesses to adopt leading security solutions.

- Whatever guidelines/codes are agreed, a simple online tool could be developed to assist businesses assess their cyber security status and resilience. The tool could identify both vulnerabilities and risks as well as remedial strategies.

Cyber security can be improved exponentially by taking some very simple, low cost and common sense steps, such as those recommended by the **UK Cabinet Office Cyber Essentials scheme** - a Government led initiative to improve basic cyber security awareness and measures across UK government and industry. This allows public and private sector organisations to demonstrate their cyber security commitment and capability, increasing citizen and consumer confidence.

Secondment and Exchanges

The UK's approach for its new National Cyber Security Centre recognises that government "cannot protect businesses and the general public from the risks of cyber-attack on its own". In response it has put in place the Industry 100 initiative which will facilitate 100 temporary places given to private sector staff to work in the centre.

The industry 100 approach aims to capture the collective knowledge and experience from many domain experts, and leverage these to develop appropriate cyber security policies, tools and techniques. It facilities Government implementing more practical cyber security measures that businesses and citizens can use/apply. It would also ensure that the views/challenges of business and citizens are captured and contribute to cyber defence processes.

At the Industry level

Critically, ensure that: (1) there are clearly defined security roles, responsibilities and accountabilities within the organisation and supply chain (e.g. someone responsible for maintaining contact with cyber security interest groups to understand emerging threats); and, (2) staff are trained or made aware of basic 'cyber hygiene'.

Conduct and maintain an assessment of cyber security risks and actions that can be taken to mitigate these risks.

All businesses should have a documented security policy that clearly sets out the organisations context, position and expectations with respect to cyber security.

Security doesn't stop when an IT solution has been delivered; it is an ongoing concern. Support arrangements must make provision for (ideally automated) security patching and security monitoring (e.g. scanning for viruses and network intrusions).

At the citizen level

At the citizens-at-large level, the first stage should be to understand what industry currently offers to the citizens at large and whether those offerings are appropriate. We need to understand where the real issue lies; where the real gap is between what is being done and what needs to be done by the individual.

More generally, 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. Such tools may include more frequent patching and the potential of internet of things-specific protection software and security behaviour '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.

ATTACHMENT A

1.1 Guiding Principles: Online Trust Framework

AIIA supports an online environment where individuals and organisations are able to trust each other because they follow agreed upon standards, policies and process to obtain and authenticate their digital identity and the digital identity of devices.

AIIA believes this online trust environment must be founded on the following guiding principles. *These principles are not listed in order of importance, as many are interdependent, and all play an instrumental role in the development of a trust framework.*

1. **Multiplicity of identities:** Online identity solutions must take into account the multiplicity of user identities that must be managed; such as for individuals, devices, groups and businesses.

2. **User centric**: Online identity solutions must be user centric. They must be based on technology that is easy to understand and use; provide convenience for individuals; and offer choice so individuals can choose the service providers from whom they will receive credentials. Solutions must, by design, ensure a positive user experience.

3. **Privacy enhancing:** The online identity system will use privacy enhancing technology, policy and processes to ensure the integrity of individual privacy and civil liberties.

4. ***User-owned identity:*** The online identity trust framework must ensure user(s) can own and control their identity in an online environment.

5. **Secure and Resilient:** Online identity solutions must be secure and resilient. This requires technical robustness in the form of platform, network and software security and a commitment to driving awareness across individuals and organisations of their respective security obligations to support the integrity of the system.

6. **Whole of Economy:** Development of an online identity system must be architectured to support secure transactions across the whole economy, including transactions that range from anonymous to fully authenticated and from low to high value.

7. **Future-proofing framework:** The digital identity framework must be appropriately adaptable to ensure it can evolve in alignment with changing technology trends.

8. **Policy and Technology Interoperability:** Policy and technology interoperability is required to ensure service providers can accept a variety of credential and identification media types; provide choice and convenience to users; support identity portability; and facilitate a whole of economy digital identity ecosystem.

9. **Leverage Existing Standards and Frameworks:** Existing standards and frameworks should be considered for their relevance and application in the broader online identity system rather than models that start from first principles.

10. **Foster a Competitive Marketplace:** A competitive marketplace of highly reputable credential providers is necessary to ensure choice and convenience for users.