Prime Minister's Advisory Council on Cyber Security - Industry Working Group on "IoT"

AIIA feedback

October 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".*

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.

Overview

The industry working group was tasked to address the following:

"Security has been a low priority for IoT developers. Can we make the IoT devices more secure? This Working Group will consider cyber security standards / certification for IoT devices to provide greater assurance for home users and on a national level. Could be usefully developed in cooperation with the IoT Alliance group".

Comments

Ensuring security of IoT devices is an ongoing concern.

Generally speaking there are 3 elements/layers to the problem:

1. The design and manufacturer level
2. The user level and
3. The government level

At the design and manufacturer level

In principle we support the work of the IoTAA around their best practice guidelines. And we encourage others to provide their comments during the consultation stage. Taking a principles based approach we think some key things any such guide should consider includes:

- Taking a balanced approach for IoT manufacturers vis a vis consumer protection. At its most basic level, IoT exists to exploit the data economy - maximally collect, store, and process data and this needs to be taken into account in how a guide is drafted and presented. Otherwise it runs the risk of being ignored by manufacturers
- Although you want the guidelines to be high level to take into account the evolving nature of technology, they also need to be detailed enough to be practicable for developers. To this end we think a guide should cover the full life cycle of an IoT i.e. from inception to adoption, including design, build, code, etc.

More generally, should a standard approach be adopted, AIIA recommends **any standard be developed based on an agreed risk matrix**. Noting that risk can never be fully eliminated and should be managed proportionately. Dealing with risk is not a matter of eliminating all uncertainties, but of setting clear limits upon the scope for accidents, attacks and errors. In thinking about IoT security, we need to decide how much risk is acceptable based on the relative trade-offs. The answer does not lie in an absolutist rejection of risk, but a clear policy about where on the spectrum of risks one decides to draw a line. This risk matrix should be developed in the first instance and the standard to fall out from that.

We also support **encouraging an accreditation scheme to incentivise organisations** to provide a level of assurance in their cyber protection strategies. 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 (he Council of Registered Ethical Security Testers) that provides accreditation or registration of security providers/professionals.

At the citizen level

The first stage should be to understand what industry currently offers to the citizens at large and whether those offerings are appropriate in the IoT context. We need to understand where the real gap is between what is being done and what needs to be done.

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.

At the government level

Breach and related compliance regulations will need to evolve – factoring in the new ways cyber-attacks may occur. While AIIA does not typically endorse increased regulation it may be necessary to increase penalties for companies if they are deemed negligent in having the right cyber security assurance and safety information/awareness arrangements.

To this end, having the right incentives in place for businesses to provide cyber secure products is key. Businesses currently don't bare the direct cost. Some suggestions from members include:

- Make security incidents, costs, losses, and mitigation expenses a mandatory reporting requirement on shareholder annual reports.
- Mandate that ASX listed organisations appoint a named Executive to act as an accountable authority for cyber security.

At the government level there are also broader issues that goes beyond security when it comes to the IoT:

- The Federal Government needs a strategy on how to leverage IoT or Australia risk falling behind the rest of the world. The time to act is now. We need a strategy that can keep pace with change, addresses the implications of 'disruptive' technology and ensures secure collection and sharing of data
- A clear definition of IoT is required along with a greater awareness of its nature and application. Understanding and addressing the implications of this new way of using technology, including its 'disruptive' nature, will allow Australia to capitalise on IoT while minimising shocks as industries adjust.
- **The real value of IoT are the insights and actions driven by the data that's collected and shared. Data collection and sharing must therefore be useful to decision makers. Interoperability of systems, data formats, and cost effective access to the data is key to achieving this.**
- As data becomes more prevalent through adoption of IoT, the impact of the IoT on storage infrastructure, particularly the increasing demand for more storage capacity will have to be addressed.

More details on our IoT policy position in Attachment A

Attachment A
see next page

AIIA position statement: the internet of things

Position

The Internet of Things (IoT) promises to deliver a healthier, more convenient and more efficient future for Australia and its citizens.

The time to act is now. The Federal Government needs a strategy on how to leverage IoT or Australia risk falling behind the rest of the world.

Privacy and security are critical features of IoT and have to be addressed to maintain long term viability.

A clear definition of IoT is required along with a greater awareness of its nature and application. Understanding and addressing the implications of this new way of using technology, including its 'disruptive' nature, will allow Australia to capitalise on IoT while minimising shocks as industries adjust.

The real value of IoT are the insights and actions driven by the data that's collected and shared. Data collection and sharing must therefore be useful to decision makers. Interoperability of systems, data formats, and cost effective access to the data is key to achieving this.

As data becomes more prevalent through adoption of IoT, the impact of the IoT on storage infrastructure, particularly the increasing demand for more storage capacity will have to be addressed.

Moreover, the National Innovation and Science Agenda articulates a vision premised on technology led innovation but it is hard to imagine how Australia's global competitiveness can keep pace unless all Australians have access to fast, ubiquitous, affordable connectivity infrastructure.

Key policy principles:

- 'Flexible by design' IoT policies that are able to keep pace with change
- Interoperability of systems and data formats to ensure data is useful, timely and cost effective
- Clear communication and understanding of what IoT means
- Getting the balance right between privacy and security
- Data storage

Rationale

IoT is upon us now. Australia must be IoT ready otherwise, uncertainty on the 'road rules' will hold Australian IoT applications back and others will take their place.

The potential global annual GDP value of IoT is estimated to be around $11 trillion: some $120b per annum for the Australian economy by 2025. *Communications Alliance April 2016 (14)*

Data use in Australia is growing exponentially. Some 2.5 exabytes of data were generated in any given day in 2015 – more data than was generated in total since the dawn of time until 2014. *CSIRO, Tomorrows Digitally Enabled Workforce 2015 (13)*

In 2015, 73% of connections in Australia are LESS than 4mpbs. This compares with South Korea with 81% of connections higher than 10mpbs. *2015 Quarter 4 Akamai Report*

Priority Action Required

1. An IoT strategy that can keep pace with change, addresses the implications of 'disruptive' technology and ensures secure collection and sharing of data
2. Clear communication and better understanding of IoT: this involves a clear definition of IoT and a greater awareness of its nature and application
3. Identification and alignment of standards that ensure interoperability of systems and data formats
4. Fast-tracking the rollout of the NBN to ensure Australia is a nation of digital exemplars, placed to exploit the economic and social opportunities available through digital technology and technology led innovation.
5. Working with industry to allow for the continuous flow of sufficient, adequate, and new spectrum, to support the expansion of Australia's wireless market in 5G, LPWAN and beyond.
6. Government cooperation with industry to deliver innovation and growth as set out in the National Innovation and Science Agenda

AIIA will...

- Help to highlight the changes that must take place if the benefits of IoT are to be realised
- Support information campaigns for State and Federal MPs aimed at educating them around technological disruption and the opportunities/risks for Australia
- Contribute to body of knowledge to be used to educate businesses, promote IoT to member organisations and other organisations such as the IoT Alliance Australia
- Participate in Impact Studies to assess the potential implications of IoT on Government
- Support pilots of IoT and IoT initiatives