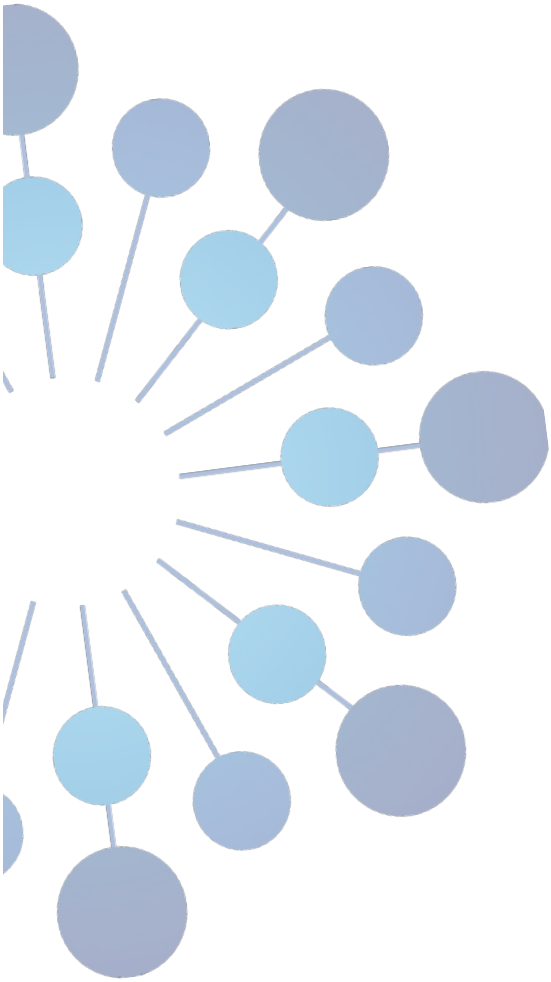
IoT Alliance Australia

Strategic Plan to Strengthen IoT Security in Australia



Strategic Plan to Strengthen IoT in Australia v4
September 2017

This Strategic Plan was developed by Workstream 5: Security and Network Resilience of IoTAA, (the Internet of Things Alliance Australia)

www.iot.org.au

Disclaimers

1) Notwithstanding anything contained in this *Strategic Plan*:

a) Internet of Things Alliance Australia, (IoTAA) disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for any direct or indirect loss, damage, claim or liability any person may incur as a result of any:

i) reliance on or compliance with this *Strategic Plan*;

ii) inaccuracy or inappropriateness of this *Strategic Plan*; or

iii) inconsistency of this *Strategic Plan* with any law; and

b) IoTAA disclaims responsibility (including where IoTAA or any of its officers, agents or contractors has been negligent) for ensuring compliance by any person with this *Strategic Plan*.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Introduction

IoTAA Workstream 5 (WS5): Cyber Security & Network Resilience formed a sub group led by Patrick Fair and resourced by: Geoff Gerrand, Telstra; Tim Miller, IBM; Andreas Dannert, Deloitte; and Matt Tett, Enex. This sub group was chartered with developing a strategy document which describes the key security issues facing IoT globally and sets the IoTAA WS5 position on those issues. A security strategy document was created, and this was reviewed by the wider WS5 members; over 100 members representing 65 organisations across Australia.

Purpose

The strategy aims to achieve industry good practice in cyber security for IoT in Australia, and set an agenda to communicate and collaborate with governments, industry and peers on IoT security globally.

Matt Tett
Chair
Workstream 5: Cyber Security and Network Resilience

Summary

The IoT security strategy identifies eight key items and describes proposed policy, stakeholders and steps required to implement. Four of those have been identified for priority focus and action in 2017/18. The eight items are as follows with the four priority focus areas in **bold**:

1. Identify, reconcile, publish and promote IoT security guidelines and standards – including collecting, collating and reviewing current global activities in this area ensuring good practice is promoted.

2. **Develop, implement and promote an IoT product security certification program: an independent IoT product security claims-testing, evaluation and certification "trust mark" program for demand-side assurance.**

3. Draft an IoT network protection framework: based on the iCode, expand the remit to cover which additional network characteristics, information and practices should be included to cover security of IoT networks.

4. **Develop and promote IoT supply-side security awareness and education programs. Many IoT developers/manufacturers/suppliers are not aware of basic IoT/network security risks and requirements to integrate security in their design, development, manufacturing and supply chain processes. IoTAA will take the lead in Australia setting a global good practice program in this area.**

5. **Develop and promote IoT demand-side security awareness and education programs. Many on the IoT demand-side are not aware of basic security requirements when procuring and implementing IoT products. IoTAA will take the lead in Australia setting a global good practice program in this area.**

6. Draft guidelines for IoT network security breach/incident investigation and remediation. The guidelines will include the need for network operators to consider how they might respond in the case of a cyber-attack. In particular, how they can develop and maintain capabilities such as detection, quarantining, response (notification/reporting) and remediation.

7. **Establish and maintain relationships with government, industry and international bodies related to IoT security; enabling national and international IoT security focused collaboration, communication, information and good practice sharing.**

8. Adopt and promote the IoTAA security strategy as an administrative framework. The cornerstone of the IoT security regulatory framework should be IoTAA itself. As the established industry association for the IoT in Australia it should use its structure to adopt this strategy as a policy and use its administrative and financial resources to carry out the various steps described with reliable persistence.

Strategy in Detail

Item	Proposed Policy	Stakeholders	Steps to implementation
1	**Approve, develop and publish guidelines and standards** Current standards are fractured yet evolving. The appropriate level of security controls will vary widely, depending on the role / function of the IoT environment as a whole (endpoint, gateway, network and back-end / cloud / server). Option to evolve the security principles in the existing IoTAA Security Guideline into a 'soft' certification / self-regulation approach - allowing the industry to state that a base level of security has been implemented. This is more suitable for lower risk IoT ecosystems, where basic security is all that is required, and the customer is the consumer.	**Primarily:** Device manufacturers, Importers and distributors **Also interested** Network owners Retailers Consumers	a) Identify relevant security standards and guidelines in existence and under development. b) Develop a system for classification based on functionality/ purpose of the product to ensure adequate coverage: I. should the requirements be different depending on the whether there is an open or closed network or based on other features of the network management? II. is it endpoint, gateway, network, back-end? Is there a distinction between a hardware and software? III. should the requirements be different where the data needs to remain confidential or is of high/critical importance (for example monitoring an elderly person living at home) or integrity? (for example health monitoring systems). c) Reconcile between competing security standards covering same subject matter. d) Identify any gaps in coverage and process. e) Produce a guide listing relevant standard bodies, relevant security standards and suggesting where Australia might: I. adopt a security standard; II. seek participation in the modification or setting of new security standards; III. develop its own security standard.

Item	Proposed Policy	Stakeholders	Steps to implementation
2	**IoT product certification** For IoT environments with moderate security requirements (wearables, ICS environments etc.), a more detailed certification approach could be defined, once again extending on existing security principles. This could continue to be opt-in, however could have some degree of independent testing / validation / assurance behind it. For IoT environments with the highest security requirements (medical devices etc.) the existing security principles could be used, however they should be linked into other IoT security standards as they are developed and become recognised (GSMA, OWASP etc). This would require a formal testing mechanism. A testing and certification scheme would require the development of applicable programs. The testing could also involve testing of manufacturer security claims (Security Claims Testing). The program specified could involve assessment of features such as the ability to update an operating system, maintenance of online monitoring and how vendors manage the product lifecycle. To be meaningful the certification scheme should be associated with a system of certification mark and a rating that can be promoted in the marketplace.	**In relation to testing:** Device manufacturers, Importers and distributors Network owners Consumers **In relation to certification mark recognition** Corporate customers Retailers Consumers	a) Development and PoC I. develop an evaluation and certification program that is suitable for use in a security claims tested scheme. The certification program should be consistent with any international standards and guidelines identified in item 1 above; II. conduct lab testing in accordance with the certification program issued; III. develop a certification mark and rating system consistent with adopted certification scheme. Protect the intellectual property of the proposed mark and any associated logo by registering them with IP Australia. b) Develop a financial model for maintenance and operation of the certification scheme. If the program is to be owned by IoTAA it might charge a royalty for the certification/re-certification and sub-contract the testing to a Testing Authority (TA) while remaining the technical Decision Authority (DA). If the program is to be developed by a Lead Testing Authority (LTA), IoTAA might permit that body to charge a fee to other certifiers (Accredited Test Facilities (ATFs) wishing to use it and the LTA is also the program DA. IoTAA might require licensing of any program in order to ensure there is sufficient certification capacity and competition in the market for certification. c) Develop a marketing plan to promote the certification scheme. In particular, a key list of device manufacturers expected to support the scheme needs to be identified and involved in development. Considering the very large number of devices at a consumer and industrial level, it may be necessary to identify a particular market segment to use as a testbed. Device manufacturers should see real value in having an independent

	An important challenge in establishing a certification scheme is stability and consistency over time. To be worthwhile and meaningful the scheme would need to stay in place delivering a consistent service over many years and promoting its mark consistently so that recognition and value builds over time. A key part of setting up a certification system is to have the support of all stakeholders and design a well-funded scheme that can be maintained as a reliable institutional service. There is an issue regarding whether we should aim for a single scheme or a set of industry specific schemes. On the one hand, there could be benefits in going industry by industry. On the other hand, such an approach would add complexity and inconsistencies.		security certification in order to encourage customer acceptance.

Item	Proposed Policy	Stakeholders	Steps to implementation
3	**Network protection framework** In setting up guidelines and a certification scheme, the IoTAA should avoid creating "red tape" that imposes requirements on services and facilities that do not pose a risk to the public or third party networks. If a device uses only a private communications framework or will function only on a closed network, it could perhaps be exempt from more detailed technical security standards. It is noted that there are very few truly closed networks and networks that start closed often become connected over time. IoTAA should explore the characteristics of an isolated or restricted device and if thought realistic/valid, create an exception for the operation of such a device when it cannot create a risk to third parties. Network characteristics are also an important element of delivering IoT security. For example, the ability of the network operator to detect compromised devices on the network, the network operators policy/ability to respond and remediate and/or shut down compromised devices all contribute to the overall security of the network.	**In relation to development and use of the framework:** Network owners Service operators **In relation to understanding and use of the framework** Device manufacturers, importers and vendors Corporate customers Retailers Consumers	a) Starting with the iCode, consider what additional network characteristics, information and practices should be encouraged in order to take advantage of and/or support the security features recommended in relation to IT devices from international standards and guidelines. b) To the extent that network characteristics and features stand independently of the devices but remain relevant to security characteristics of the network, develop a standard and/or guidelines for network operators to improve and maintain secure networks. c) Consider whether this should be a certification scheme or part of a certification scheme.

Item	Proposed Policy	Stakeholders	Steps to implementation
4	**Vendor/ Supplier Security Awareness/Education** Education for the consumer on why security is important and how they can use the security principles to guide their decision making process (think Heart Foundation tick). We need to specify who will be responsible for this. This could be device manufacturer (e.g., Fitbit, home security device manufacturer), or, could be platform operator (e.g., ISP or other service provider), or, could be government/industry body (e.g., Dept. PM&C, IoTAA). By identifying who should be responsible, we articulate the standards that need to be met. Education for the vendor / supplier / manufacturer to consider security end-to-end when developing / selling their IoT systems. This education should also highlight the legal obligations inherent within the sale of IoT devices (such as privacy legislation. For example. the Optus enforceable undertaking, which was partially due to default passwords being set on modems supplied to customers enabling attackers to readily compromise those where the passwords had not been changed after installation). In implementing this strategy it would be advisable to start with this item in conjunction with Item # 1. Security awareness among original equipment manufacturers,	Vendors Suppliers	a) The vendor/supplier education can take many forms. IoTAA should consider developing a plan that works with other aspects of this strategy to communicate the importance of IoT security and the opportunities and benefits of participating in and supporting the standards guidelines certification and training programs developed by IoTAA. b) IoTAA strategy should expand as other work in the strategy document is completed. A stepped rollout of education and information might involve: I. Development of a website containing standards and information regarding the certification program; II. Appointment of training officer or officers to speak at industry events, explain and direct stakeholders to industry resources; III. Creation of multimedia material giving case studies and examples of guidelines standards and certification at work; IV. Appointment of a media officer to speak to the press regarding developments in IoT and IT security with reference to IoTAA initiatives.

	device manufacturers etc. is low and many are unwilling to take responsibility. Engagement may prompt this sector to either seek out what is happening specific to their industry, or advise IoTAA what they are already doing themselves. This feedback could be incorporated into item #1.		

Item	Proposed Policy	Stakeholders	Steps to implementation
5	**Consumer Security Awareness/Education** Only some IoT devices will be sold to consumers. However consumer products pose a particular risk because they are usually low-cost, they may not be sourced from reputable manufacturers and they may be used long after the technology that was used to make them has become obsolete. Consider whether products should have a "use by" date and/or be marked with date of manufacture as an indicator of compliance. An important dimension of a certification scheme would be to educate consumers regarding the importance of considering security when buying IoT devices and encouraging consumers to buy certified devices thereby both improving security and adding value to manufacturers and importers that have their devices certified.	Consumers Retailers	A consumer education scheme might involve the following steps: a) general public education regarding the importance of Internet security; b) marketing of the certification scheme and the mark associated with certification to consumers; c) publication of information and media engagement regarding cases of identified weakness in IoT devices and the fallout from cyber-attacks.

Item	Proposed Policy	Stakeholders	Steps to implementation
6	**Investigation and remediation** Linking back to the existing security guideline, establishing standards based on risk would be appropriate, i.e. for your lowest risk systems, a low effort mechanism. As the risk rises, a more structured approach could be defined.	Device owners Network operators Service operators	a) IoTAA should develop guidelines for investigation and remediation. b) The guidelines should include the need for offenders and network operators to consider how they might respond in the case of a cyber-attack. In particular how they can develop and maintain capabilities such as: I. detection - looking for compromised devices and/or attacks originated from compromised devices; II. quarantining – isolating compromised devices; and III. notification/reporting – somehow notifying owners of compromised devices. c) IoTAA might consider that the ability of a vendor or network operator to demonstrate a capacity in this area might lead to, for example, a six star rating rather than a five star rating for a relevant device or service. d) IoTAA might consider whether it should maintain an advisor or contracted service advisor to step in in cases where a significant IoT installation is compromised to provide assistance and guidance in implementing appropriate remediation.

Item	Proposed Policy	Stakeholders	Steps to implementation
7	**Liaison with government and international bodies** A key question for industry in the delivery of IoT security is the extent to which it wishes to seek regulatory support from government. It is clearly in Australia's interests to have a secure and safe Internet. The development of the IoT promises real economic and social benefit. On this basis, it is realistic to hope for and expect policy and possibly financial support from government. This may be by issue of a grant or other indirect means. For example, the government might support the IoTAA security certification scheme by requiring that all government IoT devices be certified to an acceptable level in accordance with the scheme. It is also important to bear in mind the potential for and perhaps the advantages of more aggressive government intervention. For example, possible government interventions include: • seeking to give industry standards and codes of practice legislative force; • imposing a requirement that devices meet certain basic security standards before they can be manufactured, imported or sold in Australia; • imposing a requirement on importers/venders to maintain remediation capabilities and implement them in cases	IoTAA Federal and state governments	a) IoTAA should develop a position on the balance between regulatory intervention by government and voluntary industry supported schemes. b) In developing this policy IoTAA should consider the extent to which: I. government funding might be available to support the development of various aspects of the strategy outlined in this document; II. Commonwealth and state government policies, as major customers for IT devices could help support the initiatives of IoTAA in IT security; III. regulatory support perhaps by registering guidelines or cooperating with the Australian cyber security centre and other cyber security initiatives might help support IoTAA security initiatives. IV. Whether there are regulatory interventions that might be of general benefit, even though they represent a regulatory or cost imposition, because they create a level playing field.

	where a device they have sold causes third-party loss; • introducing a liability scheme where negligence in relation to online security can give rise to legal responsibility to third parties who suffer damage or loss. The working party does not recommend that IoTAA go to the government seeking the creation of new rules and requirements. However IoTAA should consider if there are cases where industry would prefer a level playing field imposed by consistent legal regulation over a voluntary system where some industry participants do not participate or provide support. We should also ensure engagement with the relevant industry bodies, such as the Information Sharing and Analysis Centres (x-ISAC)		

Item	Proposed Policy	Stakeholders	Steps to implementation
8	**Administrative framework for IoT security** The cornerstone of the IoT security regulatory framework should be IoTAA itself. As the established industry association for the IoT in Australia it should use its structure adopt this strategy as a policy and use its administrative and financial resources to carry out the various steps described with reliable persistence. IoTAA might appoint a special working group, or indeed the existing working party, to carry out policy-making and deliver recommendations for the implementation of various stages of this strategy. Each standard and guideline should be subject to a review process that involves collection of information regarding feedback, practical difficulties and a call for public comments on a regular basis. The organisation with responsibility for the standard should suggest changes and publish proposed changes according to a regular cycle. Such a process could apply to this strategy: a 24-month review cycle including written submissions, a formal review by members plus a session with all industry participants / government.	IoTAA	a) IoTAA should: I. formally adopt a strategy (this strategy) aimed to achieve industry best practice in cyber security for IoT devices in Australia; II. formally appoint the Working Group or others as a subcommittee of the board to make recommendations for delivery of the strategy and allocate a budget for carrying out each of the steps described above; and III. the chairman of the security working party should work closely with the Chief Executive Officer of IoTAA to liaise with stakeholders, government, contractors and the public at large to ensure effective implementation. b) The cyber security strategy should be reviewed on an annual basis with changes and amendments submitted to the IoTAA board for consideration and adoption as opportunities present, the market changes and elements of the strategy are successfully implemented.