Strengthening Australia's cyber security regulations and incentives

ioXt is an Alliance of leading technology manufacturers, service and platform providers, silicon manufacturers, and retailers working together to increase the confidence of consumers around the security of connected products and services. The Alliance has over 500 member companies supporting Smart Home, Smart Building, Cellular, and mobile application markets. It is our goal to promote a set of harmonized security standards which are testable, scalable, and impactful to the end consumer. We have certified over 160 products ranging from connected dog collars to smartphones, building controllers to mobile applications such as VPNs. We provide security transparency to the end consumer through our certification mark and live label which allows consumers to see the latest security stance of any certified product before purchase.

The ioXt Alliance supports the establishment of baseline security requirements for connected consumer products as this helps drive adoption and provides direction for manufacturers. We do caution against fragmentation of standards and, especially, certification programs as this leads to a reduction in consumer choice with higher development and resale product cost, while creating confusion in the global markets.

The following is the ioXt Alliance's response to the call for views. Please note that we are not responding to all questions in the call for views as many items were specific to the Australian market or were in regards to existing Australian regulations. A lack of response should not be interpreted as a position for or against the questions being asked.

Chapter 2: Why should the government take action?

1. What are the factors preventing the adoption of cyber security best practice in Australia?

There are several factors which are slowing the adoption of cyber security best practices. Until recently, there has been a lack of security standards which address the consumer IoT market. Standards must be scalable to address the wide range of products and services. Further, the standards must provide clear acceptance criteria for the manufacturers, while being flexible enough for the wide variance in protocols, interfaces, and business models of consumer product companies.

Currently, there is a mismatch in market incentives for manufacturers selling connected products. Between the race to launch new products and services in ever shorter timelines and the competitive pricing pressures, many companies find it difficult to justify the budget to staff and build sufficient security controls into their products. Further, the lack of recurring revenue models for many device manufacturers do not encourage long term security support periods. The market pull towards low-cost, throw-away products puts consumers at risk. Baseline security regulations, with security transparency would greatly help change these dynamics.

Chapter 4: Governance standards for large businesses

6. What cyber security support, if any, should be provided to directors of small and medium companies?

Baseline cybersecurity must be adopted by all companies who manufacture connected products, no matter the size of the organization. We believe baseline cybersecurity can be set at a level which protects the consumer from large scale remote attacks, while not being too burdensome for the manufacturer or service provider.

Directors and product managers need to be educated that the controls required to meet baseline security is easily achievable without increasing development and product costs. Actionable guidance would help directors such that they do not feel the need to hire outside consultants or greatly increase staffing to understand what changes they need to make to their products or processes. High level security best practices often do not make it to the decision makers and are often written for security professionals, not business leaders.

A simplified list of baseline requirements and the actions (or example policies) which may be used by the manufacturer will greatly increase adoption. Further, market data which helps to build a business justification would greatly help this group of stakeholders.

7. Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

Explaining the importance and steps to be taken in securing connected products should always be targeted to the audience receiving the message. Messaging to a security engineer would not be the same message given to an end consumer. The same applies to senior business leaders.

Messaging to business leaders should focus on high level regulatory requirements, reductions in liabilities, and potential increases in revenue through increased sales or higher profit margins. The message should be balanced with increases in product security that does not necessarily greatly increase product cost and can be offset by the items previously listed.

Chapter 6: Standards for smart devices

11. What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

The Australian government should adopt a baseline set of security controls in which all connected products must meet. Penalties for failure to comply, reduction in liabilities for those who do, or limiting access to market places can help to drive adoption. Further, there should be transparency as to the security controls supported by connected products such that companies can compete in the marketplace and be rewarded for their security investments.

Baseline security does help set the minimum level of security for any connected device. However, different devices have different threats and risks to the consumer. For example, a Zigbee enabled light bulb has very limited code space and network bandwidth. Further, it will be connected to a gateway, which limits the connection of the device to the wider network. However, a Linux based camera may have a large amount of code space, high bandwidth, and a direct connection to the Internet. Many of the controls which make sense for the camera are overkill for the light bulb.

This is where Security Profiles per device type is critical. While standards such as ETSI EN 303 645 provide a baseline of requirements, they may not be enough for some IoT devices, software, or service. Further, consumer labeling must be simple to understand and use by all consumers. The ioXt Alliance recommends a live label without printed levels. The label should indicate that the device is secured for its use, and include a QR code which allows a consumer to see the latest compliance information regarding the product. Light bulbs will have lower security controls than cameras. However, a 1-star light bulb may be perfectly suited for the consumer while a 1-star camera may not.

The ioXt Alliance provides a safe and level playing field for device manufacturers of the same type of device to get a room together and set the minimum and optional requirements of the

type of device they are manufacturing. Other stakeholders, such as network operators and retailers are also in the room to help balance the security concerns from each of their perspectives. Profiles further define the devices which must certify under the profile. Thus, a single stamp is used for all devices, but the minimum security levels may change based on the device. Thus, the consumer simply needs to understand that a product with the certification mark has been secured.

12. Would ETSI EN 303 645 be an appropriate international standard for Australia to adopt as a standard for smart devices?

ETSI EN 303 645 is a standard, not a conformance program. A standard simply defines the requirements which devices must follow. A conformance program operationalizes a standard. For example, a standard does not include the means to engage and manage lab assessments of conformance of products against the requirements nor authorize and audit labs such that all labs provide consistent results against the standard. Further, a standard does not provide a means for dispute resolution when the general baseline requirements do not fit the unique security situation that a new device may bring to the market. A standard also doesn't build cross recognition programs with other standards to harmonize and reduce the overall testing that a global manufacturer may face.

All of these things are addressed through conformance programs such as ioXt. Selecting a baseline is important, but is only the first step down the road of consumer product security.

a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

The top three requirements address the most egregious issues and does provide a channel for researchers to report issues. Though the security support period does imply that the researcher submitted issues will be addressed, this area may need further definition.

However, many issues are not addressed by the top three. Most importantly, the top three does not require products to communicate securely, or provide other basic protections from large scale remote attacks. Thus, there is a danger that a program based on the top three will cause a large drop in consumer confidence once the first attack occurs for a device which has only met the top three.

b. If not, what standard should be considered?

ioXt recommends cross recognition with multiple standards for the baseline requirements and a method in which SDOs, trade alliances, and conformance programs can work together to address unique device or market security requirements.

14. What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

For the top three, the primary cost driver is the security support period. This will require companies to make an upfront commitment to the support period if the top three is implemented as a date vs an end of life policy. This expense may be difficult for companies who only sell hardware and do not have a recurring revenue stream associated with the product.

Further, the full EN 303 645 standard does require the addition of hardware protections and the use of secure processors and storage. We would recommend a regulatory framework which focuses on reducing a large-scale remote attack and providing a framework in which companies which opt to increase their hardware protections can make this apparent to consumers and then let the market reward those companies.

15. Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

It is critical that governments work together to prevent fragmentation when mandating standards. Further, custom packaging or product markings should be avoided when possible as this creates special versions of products for the Australian market, which would increase costs and reduce consumer choice.

Chapter 7: Labelling for smart devices

16. What is the best approach to encouraging consumers to purchase secure smart devices? Why?

Consumer labels are useful when consumers are aware of the label and they have a clear action they should take. The wide range of connected products present challenges to any labeling scheme. Using the Singapore labeling program, is a 1-star Zigbee lightbulb safe to use. How about a 1-star WiFi video camera?

We strongly recommend Security Profiles be adopted to make sure devices have the right level of security for the type of device and risks it presents to the consumer. If the consumer is assured that the device has the right level of security and that they are not overpaying for security they don't need, they are more likely to trust a simple label that means "right security guaranteed… no thinking required". This paradigm is what the consumer is used to and expects from the UL and CE certifications for Electrical Devices. The consumer just knows when they

see the stamp that the appliance will not burn their house down, not what conditions were used to test and verify the appliance.

Setting minimum security standards which must be met in order to be placed on store shelves is a far more effective means to drive compliance. This method can also be applied to deployment of devices into any system (Commercial, Industrial, Governmental) which receives any form of government funding.

17. Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

Labeling does create a market incentive for companies to compete on higher security levels for products. However, this is only effective if consumers understand the mark, and it truly improves the security of the devices and systems the device connects into.

18. Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not?
    a. If so, which existing labelling scheme should Australia seek to follow?

Voluntary labeling will have limited success. The companies which produce secure products will participate in the program. However, the companies who really need to improve their security will ignore the program. Companies in the middle will be forced to perform a cost/benefit analysis.

19. Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

A printed expiration date will create major issues for retailers who hold inventory as every product sitting on the shelf now has a limited shelf life. Further, companies will be forced to set an expiration date at the time a product is launched, which may be difficult. Instead, we recommend an end of life policy in which manufacturers will give a user X years notice before discontinuing support of a device.

20. Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

Labeling programs should be applied to all connected products. More web traffic comes from mobile devices and consumers interact with mobile devices more than most other consumer electronics in their lives. However, there is little guidance to consumers with regards to the security embedded into the device or the length of time a manufacturer will continue to support the device. For low cost devices, it is common for the operating life to far exceed the security support period. However, consumers are not aware of this risk at the time of purchase.

21. Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

Yes, both digital and physical labels should be used. Retailers have often expressed concern that many of their customers simply want to know that the device has met the baseline security requirements. Many consumers do not want to use their phone when selecting products on the store floor.

However, smart labels provide further information which more advanced consumers may care about when selecting products. The added information can easily be displayed on a mobile device without complicating the product packaging. Further, the latest information or compliance changes could be reflected through the digital label.

Chapter 8: Responsible disclosure policies

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

It is critical that all companies who produce connected products and services implement a vulnerability disclosure program such that researchers and consumers have a means to report potential security vulnerabilities. If a product does not automatically receive security updates, then there should be a means for the manufacturer to inform users of critical security patches such that they can deploy the update themselves. The ioXt Alliance highly recommends all manufacturers implement an inbound vulnerability disclosure program, implement automatic updates, and provide a means to inform impacted users when further action may be required.

Conclusion

The ioXt Alliance has an active compliance and security labeling program for Smart Home, Smart Building, Cellular Devices, and Mobile Applications. We believe that manufacturers should be transparent around the security provided by their products or services. This allows consumers to make informed decisions. However, we warn against fragmentation as it creates undue burden and overhead for manufacturers. Further, consumer labeling must provide clear messaging to the consumer as to what is "**good**" versus what is "**great**" and what actions they should take. A product with a one star rating may be better than one with no rating. However, consumers will avoid the one star products if they are sitting next to a three star product. The labeling scheme must reflect that the product has the "right" level of security for that type of device agreed upon by industry experts which is why a security scheme based on industry agreed Security Profiles is crucial for the success of any security labeling program. Finally, the label must actually mean basic security controls are in place. The entire effort will fail if labeled products are repeatedly demonstrated to be vulnerable to large scale attacks.