IMDA CONSULTATION

ON

IOT CYBER SECURITY GUIDE

COMMENTS

FROM

BSA | THE SOFTWARE ALLIANCE

8 MARCH 2019

Contact:
Darryn Lim,
Director, Policy - APAC
darrynl@bsa.org
300 Beach Road, #25-08 The Concourse, Singapore 199555

IMDA CONSULTATION ON IOT CYBER SECURITY GUIDE – COMMENTS FROM BSA | THE SOFTWARE ALLIANCE

Table of Contents

Introduction and Summary of Comments

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to provide comments in response to the consultation by the Infocomm Media Development Authority of Singapore (**IMDA**) on a proposed Internet of Things (**IoT**) Cyber Security Guide (**Guide**).[2]

BSA applauds IMDA's leadership in addressing IoT cybersecurity, which represents an important and urgent priority for creating a more secure and trusted digital ecosystem. In summary, BSA offers the following feedback:

- BSA commends IMDA for producing a technically sound, coherent, and adaptable approach to IoT security that aligns closely with internationally recognized standards and best practices.
- BSA recommends that IMDA clarify each of the recommendations in the Guide to identify its intended audience (IoT developers, providers, or users) and avoid confusion.
- BSA recommends that IMDA introduce new "Security-by-Design" principles (and related recommendations) in the Guide to strengthen security throughout IoT product lifecycles.
- BSA recommends that IMDA make modest clarifying changes to the Vendor Checklist in order to ensure its applicability and clarity as a tool for assessing and advancing security in the IoT marketplace.
- BSA recommends that IMDA refrain from introducing a certification scheme for IoT devices at this juncture.

Statement of Interest

As the leading advocate for the global software industry, BSA works closely with governments and regulators around the world to help foster a policy environment that is conducive to digital transformation. Our member companies create cutting edge technologies, including IoT devices and

[1] BSA is the leading advocate for the global software industry before governments and in the international marketplace. Headquartered in Washington, DC, and with operations in more than 60 countries. BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy. BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

[2] As published at: https://www.imda.gov.sg/regulations-licensing-and-consultations/consultations/consultation-papers/2019/consultation-for-iot-cyber-security-guide

services, that drive the digital economy and partner with organizations across all sectors. They recognize that the benefits of the digital economy can be realized only through robust cybersecurity.

Comments

A. Comments on the Guide

(*BSA's comments and recommendations in this section relate to questions 1, 3, and 6 of IMDA's consultation paper*[3] (***Consultation Paper***).)

BSA recognizes the importance of the task IMDA has undertaken in promoting best practices for implementing security for IoT devices and networks, and in encouraging awareness that security must be built in during the design phase. IMDA's Guide represents a thoughtful and comprehensive approach to securing the IoT and improving the quality and resilience of IoT devices. BSA applauds the Guide's flexibility and alignment with internationally recognized standards and best practices.

As IMDA seeks to further refine the Guide, BSA appreciates the opportunity to recommend the following modest changes to improve its clarity and precision.

A.1. Clarify the intended target audience for each recommendation

(*Relating to questions 1 and 6 of the Consultation Paper*)

The Guide offers recommendations with three identified target audiences: IoT developers, IoT providers, and IoT users. Each set of stakeholders occupies different roles and has different responsibilities with regard to IoT security. These differences should be made clear in the Guide.

For example, section 7.3.1 of the Guide advises the use of network segmentation to ensure IoT devices belonging to different networks can be appropriately isolated from one another and from other enterprise systems. This suggestion may be most applicable to IoT providers or corporate IoT users that manage and configure networks or services hosting IoT devices. Similarly, the proposal in section 7.5.2 of the Guide to regularly back up system data is most applicable to IoT users. Neither recommendation is necessarily relevant to IoT developers.

To ensure that each set of stakeholders has a clear understanding of the respective recommendations that apply to them, **BSA recommends that IMDA should clarify, in the Guide, the intended party or parties to whom each recommendation applies.**

A.2. Introduce "Security-by-Design" principles

(*Relating to questions 1 and 6 of the Consultation Paper*)

As a representative of companies that pioneers many of the leading software security best practices, BSA strongly supports the adoption of "security-by-design" principles as a basis for ensuring that software products are securely developed and securely maintained. "Security-by-design" principles guide developers to build security considerations into the entire software development process. It is generally considered to be distinct from "security-by-default", which entails ensuring that the product or service in question is configured to default settings that are as secure as possible. Both categories of principles are important, and both should be highlighted in the Guide.

Accordingly, **BSA strongly recommends that IMDA should include, in the Guide, "security-by-design" principles for software development**. Relating to this:

- several of the Guide's suggestions, such as strong encryption (section 6.2.1 of the Guide) and threat modeling (section 6.3.1 of the Guide), would appropriately be listed in a new "*Secure by design*" heading; and IMDA should consider incorporating additional recommendations under such a heading, including that developers should:
    - validate input and output to mitigate common vulnerabilities;

[3] IMDA, *Consultation Paper Issued by the Infocomm Media Development Authority on IoT Cyber Security Guide*, 25 January 2019, available at: https://www.imda.gov.sg/-/media/imda/files/regulation-licensing-and-consultations/consultations/open-for-public-comments/consultation-for-iot-cyber-security-guide/imda-consultation-paper-for-iot-cyber-security-guide.pdf

  - subject products to robust security testing prior to release; and
  - vet and test third-party components for security issues prior to and during their integration into a product; and

- the recommendations under the "*Secure by default*" heading in the Guide should be adjusted to address configuration issues, to include ensuring that access control settings, security event log settings, and data protection settings are configured to the most secure settings possible upon deployment.

A.3. Make clarifying changes to the vendor checklist

(*Relating to question 3 of the Consultation Paper*)

BSA appreciates IMDA's effort to draft a vendor checklist in support of the Guide. A vendor checklist can provide a valuable starting point for customers seeking to vet (and vendors seeking to make assurances of) the security of products prior to their acquisition.

However, given the diverse circumstances in which customers acquire, integrate, and use IoT devices, **BSA recommends that IMDA should clarify, in the Guide, that the checklist should be best considered as a template of example questions that should be tailored to the circumstances of a given customer and acquisition according to risk**.

In addition, BSA recommends two modest modifications to improve the vendor checklist:

(1) First, **question CK-LP-03 should be edited to read as follows**:

> "*Do you implement and maintain the system with components from a secure supply chain, with no known**, unmitigated** vulnerabilities?*"

Known vulnerabilities can be mitigated to minimize their negative effects. For example, in certain instances, software developers may use components that call on libraries with a known vulnerability, but do not use the functions within the library that introduce vulnerability; or they may develop a specific mitigation against the known vulnerability to render it harmless. In such instances, a lack of precision in the vendor checklist question could open the door to confusion between vendors and customers. The proposed edit would help minimize such confusion.

(2) Second, **the checklist should be reviewed to ensure that the questions are indeed applicable to IoT vendors**. If the checklist is to help enterprise customers select IoT devices, then questions not applying to IoT device vendors should be removed; and if the checklist is intended to help customers select both IoT devices and network management or related enterprise services for managing IoT devices, then the checklist should be re-organized to clarify and disaggregate these two distinct objectives. In relation to this, IMDA should consider removing or re-organizing those questions that are more appropriately targeted to providers (network administrators) rather than developers/vendors. Examples of questions that should be re-examined include:
   - CK-NP-03, relating to secure connectivity;
   - CK-NP-04, relating to segregated communication channels;
   - CK-MT-02, relating to access controls;
   - CK-RS-02, relating to denial of service mitigation; and
   - CK-LP-06, relating to network inventory management.

Finally, BSA is working to develop a Software Security Framework (**Framework**) to serve as a benchmark for software security considerations across a software product's lifecycle. While the Framework will not address hardware-specific or other non-software considerations, it has the potential to dramatically simplify customer assessment of security for software-centric products. BSA would welcome the opportunity to discuss the Framework with IMDA as it reaches maturity.

B. Other Comments

(*BSA's comments and recommendations in this section relate to question 7 of the Consultation Paper.*)

B.1. It would be premature to introduce a certification scheme for IoT devices

BSA again commends IMDA's intent to promote best practices and cultivate awareness in relation to IoT security. However, beyond the Guide, it would be premature to introduce a certification scheme in Singapore for IoT devices. Considering that the international community is still engaged in developing international standards in this fast-evolving area, the adoption of such a certification scheme in Singapore could hinder the availability and adoption of new IoT technologies in the country.

To avoid inadvertently creating confusion in the industry and undermining the benefits of interoperability, **BSA recommends that IMDA should refrain from introducing a certification scheme for IoT devices in Singapore at this juncture, and instead:**

- **look to participate in international efforts to develop IoT standards and to promote IoT security** (e.g., in the United States, the European Union, and elsewhere); and
- **continually revisit the Guide to ensure maximum alignment with emerging internationally-recognized standards and best practices in IoT security**.

Conclusion

BSA appreciates IMDA's consultative process for the recommendations in the Guide. We hope that our comments will support IMDA's efforts to promote internationally-recognized standards and best practices for IoT security in Singapore.

Please do not hesitate to contact us if you have any questions or comments regarding our suggestions. We remain open to further discussion, and look forward to further opportunities to work with IMDA, on the development of the Guide as well as the broader IoT security policy regime in Singapore.

BSA | The Software Alliance