Bulletin of Networking, Computing, Systems, and Software – www.bncss.org, ISSN 2186-5140
Volume 9, Number 1, pages 40–42, January 2020

A Preliminary Study of Multi-viewpoint Risk Assessment of IoT

Sonam Wangyal
Faculty of Social System Science
Chiba Institute of Technology, Chiba, Japan
s1891301cb@s.chibakoudai.jp

Tenzin Dechen
Faculty of Social System Science
Chiba Institute of Technology, Chiba, Japan
s1891302bd@s.chibakoudai.jp

Shigeaki Tanimoto
Faculty of Social System Science
Chiba Institute of Technology, Chiba, Japan
shigeaki.tanimoto@it-chiba.ac.jp

Hiroyuki Sato
Information Technology Center
The University of Tokyo, Tokyo, Japan
schuko@satolab.itc.u-tokyo.ac.jp

Atsushi Kanai
Faculty of Science and Engineering
Hosei University, Tokyo, Japan
yoikana@hosei.ac.jp

***Abstract*— With current global businesses extensively depending on data, Internet of Things (IoT) sensors have become the primary source of the real-time data that enable the digital transformation. According to Bain's Insight, the market for the IoT will grow to more than $520 billion by 2021. The technology has been significantly adopted with an array of use cases, but due to the ever-expanding threat landscape, many customers show that security remains the primary barrier when it comes to acceptance of IoT. The current security risk management methodologies focus mostly on the cyber view. This paper identifies 29 risk factors that are extracted using the risk breakdown structure method by expanding the traditional view to include other views such as physical and psychological ones, which are critical to business operations. These, in turn, will help clarify the IoT security and the relation of non-cyber risk for proper implementation of IoT systems.**

Keywords*— Internet of Things, risk breakdown structure, non-cyber aspect, psychological aspect

I. Introduction

With current global businesses extensively data-driven, IoT systems have become a primary source of the data that facilitate smarter systems and better decision analytics. IoT disrupts almost every industry from improving agricultural farm yields to predictive maintenance in aircraft engines. Particularly in Japan, IoT plays a key role in achieving a super-smart society (Society 5.0) that makes people's lives more comfortable and sustainable [1].

According to Bain's Insight, the combined market for the Internet of Things will more than double by 2021, with a market size of $520 billion [2]. Although the technology has been significantly adopted with an array of use cases such as smart grids, healthcare, smart homes, connected cars, and smart cities, among others, many customers still feel that security remains the primary barrier when it comes to the acceptance of IoT due to the ever-expanding threat landscape. Around 84% of IoT adopters have experienced a security breach [3]. These considerations highlight the importance of fully understanding the associated risks and determining how to enforce a security policy to take full advantage of IoT systems.

Generally, in an IoT system, Things are ubiquitous and inexpensive. This brings new risks that do not exist in the traditionally connected computer network. Indeed, Things are highly resource-constrained in terms of computing capacity, memory, and energy use. The sheer volume of devices and the complexity of the system makes the existing risk assessment methodologies inapplicable. Existing risk assessment methodologies such as the National Institute of Standards and Technology (NIST) SP800-30 [4] and the Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) [5] mostly focus on the cyber view. We feel, the IoT risk assessment method should expand the view of the traditional methods to include non-cyber views such as physical and psychological ones, which are critical to business operations. The current assessment of non-cyber aspects is inadequate.

In this paper, using the risk breakdown structure [6], both cyber and non-cyber risks are extracted. These will help to clarify the IoT security and the relation of non-cyber risk for proper implementation of the IoT systems

II. Current Status and Issues

A. Explosion of IoT

With the recent exponential growth of IoT systems, IDC projects that there will be 41.6 billion connected devices generating 79.4 zettabytes (ZB) of data by 2025 [7]. Many businesses have made strategic alignments to exploit the rapid growth of IoT by moving from legacy systems to a complete IoT solution.

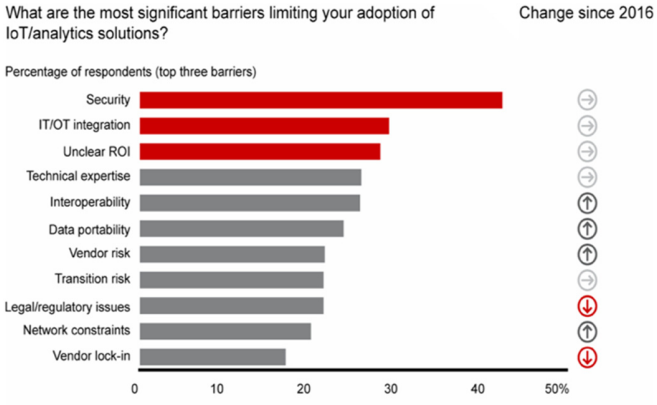

Fig. 1Most significant barriers to IoT adoption [2].

B. *Security in IoT*

As IoT moves towards the core business strategy, integrating new security solutions is imperative. Businesses should also consider the potential risk of IoT-based business models, such as disruption to the information flow, theft of sensitive information, damage to critical information, and even loss of life. Considering the array of use cases and the resources-constrained nature of IoT devices, the security of these devices is critical for the success of intended use. Bain's customer survey [2] shows that security is still the primary barrier to the adoption of IoT enabling analytic solutions (Fig. 1). Therefore, identifying potential risks and vulnerabilities should be prioritized as a critical business objective.

III. Risk Assessment of IoT

In general, risk assessment in project management is conducted in three steps: (1) risk specification, (2) risk analysis, and (3) risk evaluation [6]. This paper only conducts risk specification using the Risk breakdown structure (RBS). The latter two will be explored further in future works.

A. *Risk specification of IoT*

Here, the risk factor of the Internet of Things (IoT) is systematically extracted through a literature survey from the multi-viewpoint with the RBS method.

Since IoT sensors and actuators highly interact with the physical environment, the risk factors are divided into cyber, physical, and psychological categories as the first hierarchy of RBS. As a result, as shown in Table I, 29 risk factors were extracted.

TABLE I. Risk specification of Internet of Things.

No	First Level	Second Level	Risk Factors	Contents
1	1. Cyber	1.1 Communication	1.1.1 Lack of fog security policy	Lack of standard practices for fog computing compared to cloud security
2			1.1.2 Quality of services constraint	Latency and throughput constraint from IoT device to cloud
3			1.1.3 Edge devices communication vulnerability	Security vulnerability in gateway and edge devices
4			1.1.4 Heterogeneity of communication protocol	Lack of standard protocol and agreement on best practices
5			1.1.5 Lack of efficient encryption algorithm	Most of the standard secure encryption algorithms are resource-intensive
6			1.1.6 Lack of efficient network management	Lack of standard practices managing IoT scale network
7		1.2 Hardware	2.1.1 Low capacity and memory	Ubiquitous devices with low memory and capacity
8			2.1.2 Low energy constraint	Need to use energy efficiently without constant power supply
9			2.1.3 Lack of standard practices	Lack of standard practices for manufacturing of the products
10			2.1.4 Compromise gateway	Attack on gateway will cripple the whole IoT system
11		1.3 Software	1.3.1 Vulnerability in middleware	A vulnerable legacy system that is connected to IoT via middleware
12			1.3.2 Vulnerability in API	Poorly secured Application Program Interface (API)
13			1.3.3 Remote updates and patches	Inability to easily update and send security patches
14			1.3.4 Malicious code injection	Malicious code injection leads to compromised device part of botnet
15	2. Physical	2.1 Things Location	2.1.1 Sensor data manipulation	Physical manipulation of sensor data
16			2.1.2 Theft and sabotage	Theft of IoT devices or intentionally sabotaging the function of IoT system
17			2.1.3 Sensitivity of location	Location and use of IoT in life critical environment
18			2.1.4 Breakage and out-of-services	Identifying and serving malfunctioning IoT devices
19			2.1.5 Management of things	Physical management and securing of IoT devices
20			2.1.6 Mobility	Constant of movement of IoT devices as in vehicular IoT system
21			2.1.7 Safety in an industries	Risk of safety in industries by using IoT in a safety-critical environment
22		2.2 Data Location	2.2.1 Natural disaster	Risk of cloud data center under natural disaster
23			2.2.2 Theft, sabotage, and manipulation	Theft, sabotage and manipulation of data by services provider
24			2.2.3 Cloud and fog data center location	European Union's GDPR, and other laws that restrict data's location
25	3. Psychological	3.1 Privacy violation		Lack of standard practices for managing individual privacy
26		3.2 Security fatigue		Risk of being overwhelmed by constantly changing security practices
27		3.3 Lack of education		Lack of education regarding the security of IoT system
28		3.4 Unauthorized redistribution of confidential information		Redistribution of confidential information to an intruder
29		3.5 Social engineering		Intruder exploiting the psychology of people working within IoT system

IV. Related works

In the current literature, numerous published papers focus largely on the cyber risk aspect of the Internet of Things and correspond to specific use cases. Djamel et al. reported a top-down security survey of the Internet of Things for different use cases. They also introduced the benefit of new approaches such as Blockchain and Software-Defined Networking [8].

Bako Ali et al. applied the Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), known as OCTAVE allegro, which assessed the risk of IoT-based smart homes. They identified ten threats corresponding to ten different assets in the home environment and proposed possible mitigation approaches [9].

Jason et al. raised a strong argument about the need for new risk assessment methods that address the complexity of the new security landscape. They also showed where the current risk assessment methods fail when applied to IoT systems, since most of those methodologies were established before the widespread use of dynamic IoT systems [10].

Each of these studies either shows risk associated with the IoT system or the need for better risk assessment that considers the dynamic and resource-constrained nature of the IoT. However, despite the various studies, the non-cyber risk of the IoT has remained largely understudied or unexplored.

V. Conclusion and Future Work

In this paper, we conducted a risk assessment of the Internet of Things to clarify the cyber and non-cyber risks when it comes to proper implementation of IoT systems. Although the risks are extracted comprehensively, this is not exhaustive, as other views such as the economic view and the operational view are part of future work.

This future work will also involve risk analysis and risk evaluation of extracted risk and will suggest corresponding countermeasures.

Acknowledgment

This work was supported by JSPS KAKENHI Grant Number JP 19H04098.

References

[1] Government of Japan, The 5th Science and Technology Basic Plan, https://www8.cao.go.jp/cstp/english/society5_0/index.html

[2] Bain & Company, Unlocking Opportunities in the Internet of Things, https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/

[3] KPMG, Risk or reward: What lurks within your IoT?, https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/04/risk-or-reward-what-lurks-within-your-IoT.pdf pp. 7

[4] NIST (National Institute of Standards and Technology) SP800-30 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[5] operational critical threat, asset, and vulnerability evaluation (OCTAVE) https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

[6] Projecet Management Institute, "A guide to the procjet management body of knowledge PMBOK Guide", Sixth Edition

[7] International Data Corporation (IDC), "The Growth in Connected IoT Devices", https://www.idc.com/getdoc.jsp?containerId=prUS45213219

[8] Djamel Eddine Kouicem, Abdelmadjid Bouabdallah and Hicham Lakhlef, "Internet of Things security: A top-down survey", ScienceDirect

[9] Bako Ali and Ali Ismail Awad, "Cyber and Physiccal Security Vulnerability Assessment for IoT-Based Smart Homes", MDPI.

[10] Jason R.C Nurse, Sadie Creese, David De Roure, "Security risk assessment in Internet of Things systems", IT professional (IT Pro), 2017