Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2016 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-10-2016

Defining Objectives For Securing The Internet Of Things: A Value-Focused Thinking Approach

Gurpreet Dhillon
Virginia Commonwealth University, gdhillon@vcu.edu

Lemuria Carter
Virginia Commonwealth University, ldcarter@vcu.edu

Javad Abed
Virginia Commonwealth University, abedj@vcu.edu

Defining Objectives For Securing The Internet Of Things: A Value-Focused Thinking Approach

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu
Lemuria Carter
Virginia Commonwealth University
Javad Abed
Virginia Commonwealth University
Ramandeep Sandhu
Virginia Commonwealth University

ABSTRACT

Over the past few years Internet of Things (IoT) has touched most people. Companies have been competing with each other in inventing new IoT based products and services. It has become a real business opportunity for various companies and a luxury for end users. Yet, the research on securing the Internet of Things (IoT) is in its infancy. In this study, we use the "value-focused thinking" approach to systematically identify IoT security values and objectives from 58 IT professionals. This study provides a foundation for strategically planning and thinking about IoT security. We present four fundamental objectives and thirteen means objectives. The results of this qualitative study will help researchers and practitioners identify and prioritize key IoT security issues.

Keywords: Internet of things, Internet of things security, value thinking, Security objectives, Consumer values

INTRODUCTION

With Internet of Things (IoT), we have entered a new era of ubiquity. Tan et al. (2013) define IoT as "things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environment and user contexts." In 2015, there were 25 billion connected devices; this number is expected to reach 50 billion by 2020. The

FTC (FTC, 2015) indicates "IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety (p. ii)". Researchers have argued that IoT security and privacy should not be an afterthought (Sicker and Lookabaugh, 2004). It is important to consider all security aspects at the design state of IoT products and services. Gubbi et al. identify IoT security as a fundamental challenge for security in the cloud (Gubbi et al. 2013). Similar calls have been made by many other scholars including Xia et al. (2012), who note "security remains one of the most important issues that baffle the development and applications of IoT." Hence, there would be several security challenges in IOT. The main reasons would be: a) Extension of the 'internet' through the traditional network, sensor network and the mobile network b) Internet connecting everything c) The things communicating with each other.

There are several technical challenges for IoT security in application layer, perception layer, network layer and physical layer (Kumar et al., 2016). Several studies investigate these technical challenges in order to secure IoT (Hui et al., 2012). However, studies addressing the human perspective of IoT are rare. Most existing studies in IoT security consider only the technical perspective. According to Dhillon and Torkzadeh (2006) understanding users' expectations, values and beliefs is very important to achieve success in technological implementations or management of security. They assert that users' assumptions and values should be considered alongside with the technical perspective in order to have successful information systems outcomes and successful security management.

Since IoT is a very active and new research field, research on securing IoT is in its infancy. Therefore, more attention should be paid on issues such as confidentiality, authenticity and integrity of the IoT data. In this paper we undertake an extensive study to define objectives for securing IoT. The objectives form the basis for organizational strategic planning with respect to IoT security.

UNDERSTANDING IOT SECURITY

Agarwal and Dey (2016) note, "a safe and secure world enabled by IoT promises to lead to truly connected environments, where people and things collaborate to improve the overall quality of life. Indeed IoT will give us actionable information at our fingertips, without us having to ask for

it or even recognizing that it might be needed (p.88)." According to Vermesan et al. (2016), the Internet of Things is "a dynamic global network infrastructure with self-configuring capabilities based on a standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities, use intelligent interfaces and are seamlessly integrated into the information network (p.10)."

With regards to securing IoT, Vermesan et al. (2016), state "In this context the information pump of the real world of interest is represented across billions of 'things,' many of which are updating in real-time and a transaction or data change is updated across hundreds or thousands of 'things' with differing update policies, opens up for many security challenges and security techniques across multiple policies. In order to prevent the unauthorized use of private information, research is needed in the area of dynamic trust, security and privacy management (p. 41)." Agarwal and Dey (2016) also not "security in IoT means providing access control mechanisms and policies and being able to enforce them, particularly in the face of the tremendous number of heterogeneous devices (p.90)."

The concept of security of IoT needs some elaboration. There is no doubt that human interactions with technology have evolved from the pre-internet era to accessing content (e.g. email and information) to services (e.g. e-commerce) to social interactions (e.g. social media) to automatic tracking and monitoring (e.g. various IoT devices). The word *thing* in Internet of Things is rather interesting. It relates to smart sensors which join various aspects of the network. Research into security IoT and its security aspects is at a nascent stage. This is because of the newness of the technology and its adoption in diverse domains - e-Health, e-Commerce, e-Trafficking, among others. Many researchers have explored security aspects of IoT, there is still a lack of a systematic understanding. IoT security research largely identifies problems and privacy challenges.

The privacy for individuals, confidentiality of business processes and third party dependability are the three core issues with IoT. There are four interconnected, interacting components in IoT settings, that communicate over the untrusted public networks. These components are people, objects, software and hardware and are bound to be confronted with privacy, security and open trust problems. The previous vulnerabilities in the conventional networks leading to IoT face the passive and active attacks, hindering its functionality and nullifying its benefits of using its services (Abomhara, & Koein, 2014).

Since IoT devices are by design resource constrained, employing conventional security mechanisms is problematic, let alone consumer requirements that should dictate security choices. At a technological level, there are three classes of security constraints - hardware limitations, software limitations and network inadequacies. All three inform the manner in which security can be designed for IoT devices. The constraints also form the backdrop for users and organizations to strategically decide about IoT security objectives.

Hardware constraints for IoT security are significant (Babal et al., 2010). Since IoT devices are battery driven, it is challenging to port computationally expensive encryption algorithms. Memory constraints also cause a significant problem. Traditional security algorithms assume significant RAM and hard drive space. This is not true in case of IoT devices. IoT devices also run the risk of being tampered with because of the small size and remote deployment, which in itself is a security threat (Abie and Balasingham, 2012)). At a software level, the smallness of the devices is a cause of some concern in terms of defining security. IoT devices have thin network protocol stacks and hence security needs to be adequately configured yet retaining the robustness and fault tolerance characteristics. IoT devices also have an issue with remote reprogramming and hence patching can be difficult if not impossible. From a networking perspective there are some concerns with respect to mobility and scalability. Since the IoT devices are by nature mobile, the need for mobility resilient mechanisms to ensure security becomes important. Traditional security mechanisms for accessing networks have a hard time coping with network topological changes.

Given the nature of IoT and security challenges, conventional security requirements and technology use is problematic. OWASP (2015) identified several vulnerabilities, which are specific to IoT. These include - ability to collect usernames by interacting with authentication mechanisms and the pervasiveness of weak passwords. Username enumeration coupled with weak passwords can be a cause of a security nightmare. Additionally, unencrypted services and missing update mechanisms can also add to the security problems.

METHODOLOGY

To identify IoT security objectives, we utilize the value-focused thinking methodology proposed by Keeney (1992). Keeney (1999) uses this approach to identity customer values associated with Internet commerce. He states:

> *The best way to find out what customers value is to ask them. It is useful to ask many prospective customers because different people have different values and they express them differently. When values are elicited, they are not naturally combined into cohesive groups with a clear understanding of which values relate to which others and why. This organization is important to provide a basis for reasonable thinking through company decisions about Internet commerce (p. 534).*

In this study, we use the value-focused thinking approach to elicit IoT security values and objectives from IT professionals that focus on maximizing IoT security.

According to Keeney (1992), alternative thinking practices are used as the basis for most decision making methods. Within the literature, number of the individuals to be interviewed varies. Pythan and King (1992) interviewed two expert managers, who were involved in assessing tender enquiries to identify, what are the key factors and rules that would influence tender decisions. However, Hunter (1997), interviewed 53 individuals in two organization and elicited the individual conceptions through conducting a content analysis. Keeney (1999), conducts interviews and discussions with more than 100 individuals about their values with regard to internet purchases.

In this study, w conducted 40 – 50 minute interviews with 58 IT professionals of varying backgrounds and experience to obtain their perceptions of IoT security. All participants have significant experience using the internet of things on a day-to-day basis. Respondents represented the following sectors: transportation and logistics, health care, retail, finance and banking. We used a three-step process to identify and organize the values, which an individual possess with respect to IoT security (Keeney, 1999). These steps included:

- Developing a consumer value list, which involves asking the concerned people what they value with respect to IoT security.
- Converting each value statement into a common form and then adding directional preference to create an objective.
- Organizing objectives to define the means-end relationships to achieve the end benefit (fundamental) objectives.

Developing a consumer value list: This process starts with interviewing individuals. At the start of the interview, it is very important to clarify the purpose and the scope of the interview. With regard to this research, the overall objective is to maximize the security of IoT. While setting the

decision context, it is also very important to clarify that the scope of the values is only limited to the use of IoT by the individuals, not the organizations. In order to avoid the misunderstanding, the individuals are provided with the explanation of what IoT means and what security related issues exist with respect to IoT. In our research IoT is defined as "the system of interrelated computing devices, mechanical and digital machines, objects, and people that are provided with unique identifiers and the ability to transfer data over a network without requiring human to human or human to computer interaction." The interview proceeded where the interviewer asked the respondents what their values were with respect to IoT security. Suitable probes were used because of the inherent latency of the values.

Further, the individual's thoughts were stimulated by bringing up some concerns related to access controls, ethicality, privacy etc. Once, the discussion stopped stimulating more values, individual wish lists were combined. The wish list included cases where the same value was stated in different ways. Keeney (1999) suggests that when the intent is to get the comprehensive list of all the values necessary to describe any individual's values, redundancy is not a shortcoming.

Converting each value to a common form: The initial list of the values includes many concepts such as: awareness programs, increased training and educational programs to inform public, anonymity of the data for the non-users and use of token-based IDs. In order to achieve consistency, these expressions were converted into corresponding objectives. The first step in converting the wish list into objectives is removing the duplication and then considering each value and converting it into sub objectives. For example: "awareness programs, increased training and educational programs to inform public" above become "educate consumers on IoT security", "use of token based ids" becomes "define token based authentication for IoT".

Organizing objectives: At this stage we had a long list of objectives. The first step was to combine similar objectives into categories. For instance, the objective "maximize user's autonomy" had many components such as, "self-determination right for IoT users; users responsible for their data; use of opt in/opt out policies." All of these are categorized under the general objective "Maximize user's autonomy". Keeney (1999) suggests, "it is useful to relate categories by means- end relationships. For each of the generated objective, one has to consider "why is this important". This is appropriately termed as the WITI test. In considering each of the objectives, the researchers evaluate the importance of each objective relative to the other. If an

objective suggests that it is important because it leads to another objective, then it is a candidate for a *means* objective. If the objective is important in its own right, then it is a candidate for a *fundamental* objective. Systematic application of the WITI test helps in defining a complete set of means and fundamental objectives.

Considering the example from this study, the objectives maximize security of awareness of IoT. Why is this objective important? Because maximizing the security awareness helps to "use the IoT responsibly." Why it is important to "use the IoT responsibly", because using IoT responsibly helps "protection of the personal information on devices." Why it is important to "protect the personal information on devices," because doing so "ensures the security of the personal data on the public databases." Given our decision context of maximizing IoT security, it is important to ensure the security of personal data on public data bases, which is fundamental for the decision context.

4. IoT Security Objectives

The four fundamental objectives identified in this study include: *Ensuring security of personal data on public databases*; *Develop and sustain ethicality*; *Maximize IoT Data integrity*; *Maximize IoT access control*. These fundamental objectives resonate well with what it has been defined in literature and the main characteristics of IoT things such as intelligence, connectivity, sensing, expressing, energy, safety. In paragraphs below we discuss the objectives in more detail.

FUNDAMENTAL OBJECTIVES FOR IOT SECURITY

FO1: Ensuring security of personal data on public databases: Interviews with our respondents suggested that there was a lot of concern with respect to two important issues. The first issue is unnecessary storage of private data on public forums. Many of the IoT devices and applications constantly stream data to other devices and servers. And this data never gets deleted. Rather it is aggregated and used for trend analysis or evaluation of browsing histories. Second issue is indefinite availability of search histories. Given that any search performed on any of the IoT linked devices and platforms stays for long time, there is growing concern among individuals interviewed that their search patterns are indefinitely logged and are available. One respondent noted:

> *I wish my search history is not saved and available for sale. I want my browsing to be private and don't want it to be linked across all my devices.*

In the privacy literature there is significant concern with respect to ensuring security of personal information on public databases Geo-location is the privacy sensitive information and its leakage can tremendously damage the privacy of user. In an interesting article, (Jia et al., 2015) discuss how geo-inference attacks can sniff location data that has been left behind by several location oriented websites such as google, google maps, craigslist. Sometimes, these websites leave the location sensitive information in the browser cache. The other websites use the timing side channels to sniff the user's geo locations from the browser cache to infer the user's location. On the other hand, the web attackers use the victims' geo locations for social engineering, personally targeted advertisements or spear phishing.

FO2: Develop and Sustain Ethicality: Respondents in our study identified two aspects with respect to sustaining ethicality in an IoT environment – consideration of ethics and responsible use. The extant literature has considered responsible use and ethics to be important as well, particularly because of the pervasiveness of technologies. As (Michael and Michael, 2015) notes, "The four themes underpinning socio-ethical studies include the investigation of what the human purpose is, what is moral, how justice is upheld and the principles that guide the usage of a given technique. Participants; their interactions with systems; people concerns and behavioral expectations; cultural and religious belief; structures, rules and norms; and fairness, personal benefits and personal harms are all areas of interest in a socio-ethical approach." (pg. 65).

One of our respondents also noted:

> *Advances in technology use come with increased responsibility. I wish we all use our IoT devices with care. It is very easy to get carried away and we soon end up responding to issues even before we understand them.*

F03: Maximize data integrity: Data integrity emerges as a fundamental issue in IoT. This is because there is a constant transmission of data from one device to the other. And there is an increased change of unauthorized changes and the accuracy of the data that is received. It is therefore paramount that technologies that enhance integrity be integrated into IoT. One of the respondents in our study noted:

> *I am always worried that the message I receive through apps such as snapchat is from the person who claims to be the sender. Since reaction time is so quick, I always feel stressed that I am responding quickly without appropriate authentication.*

A sentiment such as the one voiced above is genuine and is increasingly becoming a concern for many individuals.

FO4: Maximize IoT Access control: This fundamental objective is somewhat related to the fundamental objective of maintaining the data integrity. Organizations may possess a wealth of sensitive data, but that data is typically not available to everybody. Given the IoT related to a large number of connected devices, it also means that there are more attack vectors and hence an increased possibility of an attack. An unauthorized access might exploit the security vulnerabilities, which may create risks to physical safety (FTC 2015). One of the participants in our study stated that:

> *I am worried that intruder would remotely access my data about my energy usage from the smart meters to determine whether I am away from my house or not.*

Table 1 provides an overview of fundamental objectives for maximizing IOT security.

MEANS OBJECTIVES FOR SECURING IOT

MO1: Ensure IoT trust mechanisms: This objective pertains to organizations responsible for creating, maintaining IoT. Trust is the huge factor. These organizations have a fundamental and moral obligation to ensure the IoT products are well protected and trust building technologies are used properly. The security measures must be supplemented with the continuous monitoring and constant upgrades of the system, so that the IoT devices are protected against the latest form of attacks.

Table1. Fundamental objectives

Fundamental objectives
Ensure security of personal data on public data bases ➢ *Eradicate unnecessary storage of private data on public forums.* ➢ *Minimize indefinite availability of search histories.*
Develop and Sustain Ethicality ➢ *Promote IoT usage ethics.* ➢ *Encourage responsible use of IoT.*
Maximize IOT Data integrity ➢ *Minimize unauthorized changes to IoT information.* ➢ *Increase data accuracy.* ➢ *Enhance use of data integrity technologies.*

Maximize IOT access control
- *Minimize unauthorized access to IOT.*
- *Ensure fine grained access policies for efficiency and security of IOT.*
- *Provide several levels of user access.*

At the advent of the Internet Commerce era, several trust building mechanisms were established. In particular, these took the form of web assurance seals. Today similar developments are necessary. Some progress has been made in the cloud computing arena. Latest addition is the Amazon Web Services Certificate Manager[1].

M02: Maximize security awareness of IoT: While security awareness has always been a vital issue to consider, its importance is elevated in an IoT environment. This objective deals with the increasing awareness of IoT and educating the consumers on IoT security. In a survey conducted by AT&T, it has been concluded that only 10 percent of respondents are fully confident with that their devices are fully secure. About 68 percent of respondents say that their companies are planning to invest IOT security in 2016.Many organizations deploy IOT devices, but in some of them the IOT devices are deployed without proper security measures. The reason is because shop floor equipment, vehicles, and many other IOT enabled devices were not built with requisite security or internet connectivity in mind. Many organizations are unaware of it (2) Thus, the behavior of the users with the access to data on IoT devices affects IoT security. It is important to inform consumers about IoT security issues so they remain alert about the threats.

M03: Increase responsible use of IoT: This objective addresses how consumers act responsibly in their use of IoT devices. Unfortunately, IoT devices place access to data at the finger-tips of consumers and the reaction time to think before acting gets significantly reduced. Hence, it is important to inculcate a 'responsible use' culture, which lays out the principles and fundamental issues related to IoT use.

M04: Enhanced protection of personal information on devices: This objective emphases the importance of placing reasonable limits on the collection and retention of data by IoT. When a large amount of data is stored, it is more likely at the risk of being hacked by the intruders, thus increasing the potential harm to the personal information on the devices. Therefore, there is a need to develop policies and practices that impose reasonable limits on collection and retention

1.www.amazontrust.com)
2.https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf

of the consumer data. The data should be disposed of once the purpose for which it is collected is met. In the literature, the problem of protecting personal information in the context of IoT has been well recognized. Zhou and Piramuthu (2015) propose a privacy model where issues of differentiation and mass customization are addressed. They note:

> *We argue that consumes with low demand for privacy protection should not be forced to bear the cost of the fraction of the population with demand for high privacy protection. On the other hand, the high demand consumers should be allowed the flexibility to enjoy their desired high level privacy protection, at a cost. (pg. 20)*

M05: Maximize user autonomy: This objective emphasis the importance of consumer consent in collecting the IoT enabled data. The objective stresses that a notice and choice is necessary for individual control over sensitive data and thus enhanced privacy. Not all data require choice. When data use is inconsistent with the context of interactions, individuals should be offered clear and easy to read choices. In the literature, similar arguments have been made. In terms of giving autonomy to individuals, particularly in terms of IoT privacy protection (Kounelis et al., 2014), argue:

> *The overall system of interactions can sustain confidence and trust only if the human-and- artefact mix relate to each other in a way that preserves the potential for intentional human choices and decisions within the architectures, as well as awareness and alertness towards unintended changes and threats. (pg. 75)*

Table 2 provides an overview of the means objectives for maximizing IoT security.

Table 2. Means objectives

Ensure IOT trust mechanisms
➢ Increase consumer trust in IoT usage ➢ Enhance security of IoT solutions ➢ Increase use of trust building technologies ➢ Ensure trust in IoT products Design formal security mechanisms for IoT solutions ➢ Enhance IoT security governance
Maximize security awareness of IOT
➢ Educate consumers on the IoT security ➢ Develop awareness of IoT security ➢ Update consumers on the threats and security issues ➢ Provide government official training on privacy issues
Increase responsible use of IOT
➢ Increase protection of confidential consumer data ➢ Encourage responsible use of IoT ➢ Increase individual accountability
Enhanced protection of personal information
➢ Ensure IOT use only relevant personal data ➢ Define relevant usage periods for IoT data ➢ Increased individual control over data

Maximize user autonomy ➢ Enforcing self-determination for the IoT users ➢ Ensure users are made responsible of their data ➢ Increase use of opt in / opt out policies
Ensure user authentication ➢ Ensure social media authentication processes ➢ Define token-based authentication for IoT ➢ Increase use of biometrics ➢ Ensure user identity check mechanisms ➢ Minimize authentication misrepresentations
Ensure Physical Security ➢ Increase physical indications ➢ Ensure virtual safety
Ensure Safe Connectivity ➢ Ensure safe connections between different devices ➢ Prevent brute force mitigation attacks
Ensure Ecosystem Security ➢ Enhance security of specific IoT ecosystems ➢ Ensure monitoring of individual devices ➢ Enhance integrity of IoT ecosystem
Adequate incident response plan ➢ Ensure self-data destruction programs after the breach ➢ Ensure consumer support ➢ Define IoT security breach incident reporting
Maximize Auditing ➢ Ensure auditing ➢ Ensure definition of automated auditing of IoT use
Ensure Legal Compliance ➢ Develop self-regulatory programs ➢ Define baseline IoT security standards ➢ Monitor compliance with enterprise policies
Ensure Data Anonymity ➢ Increase data anonymity for non-users. ➢ Minimize digital footprint

M06: Ensure user authentication: This objective deals with the importance of building authentication mechanisms such that IoT security could be enhanced. Authentication mechanisms, such as passwords, are inherently insecure and inefficient. The hardware tokens used in two factor authentication are necessarily best suited for IoT authentication. Hence the 2FA software based-solutions should be introduced to enhance the user authentication. Enhanced use of the biometrics may also prove to be logical and a conclusive way to prove IoT user identity. It is possible to replicate the password or the hardware token, but it is not possible to replicate the fingerprint with the descent sensor. The social media sites also have the fundamental and moral obligation to ensure the user authentication processes.

M07: Ensure physical security: This objective lays emphasis on requiring manufacturers and developers to work together in establishing the baseline standards allowing the physical security systems to work with IoT devices in such a way that the physical security goes beyond the confines of the industry, albeit without losing security. Devices built by different vendors are

incompatible, because they differ from each other in technologies and services. All the devices connect through internet. Hence, there is need to readdress the standardization to provide the interoperability among various objects and senor nodes within the network, ensuring physical safety (Matharu et al., 2014). In this study, respondents stated that physical security along with virtual safety is really important.

M08: Ensure safe connectivity: This objective deals with safe connectivity between different IoT devices to mitigate the threats. When the individuals privately access the data and applications anywhere and anytime, they expect to be fully secure. Data flows freely between countless applications and platforms. Hence, implementation of secured socket layer/TLS to ensure the safe connectivity between different devices is fundamental.

M09: Ensure ecosystem security: This objective highlights the need for the industry to focus on providing the safe, reliable interoperable access to the information and services irrespective of the vendor (Lofgren, 2015). There are various challenges posed by growing IoT ecosystems. With the new eco systems appearing every day, maintaining the security of them is a big challenge. Regarding the increase in number of IoT devices, privacy ensuring technologies must form the core of IoT design. As data travels across diverse devices, establishing the contextual integrity of data becomes fundamental issue.

MO10: Adequate incident response plan: This objective deals with the adequate incident response plan after the breach or occurrence of the incident. It is a common saying that prevention is better than cure. No matter how much you are familiar with the network environment, there are always risks of being hacked or attacked. The IoT devices are at the greater risk of being attacked. The systems should have inbuilt security sub-systems, which consist of self-data destruction programs, so that the impact of the breach is minimized. The incident response teams should act as the central communication points in order to receive the reports for the breach incidents and getting the consumer report through the advices and solutions after the breach. It should be ensured that all the emergency system information is available offline too .This was echoed in the survey responses as “I wish the companies should make quick response from the cyber security breaches to the individuals by giving advice and solutions to recover from these incidents “.

M011: Maximize Auditing: This objective deals with maximization of the auditing process. Auditing processes are very critical to check the performance and utilization of the devices. IoT devices consist of high vulnerabilities. IoT devices should have the automated auditing features to routinely assess the vulnerabilities in them and ensure that the latest patches are installed and devices operate in a reliable manner. One of the respondents said that:

"I wish the smart office could provide the means of real time auditing and the used security levels of application and the space itself.

M012: Ensure legal compliance: This objective deals with the government organizations monitoring the IoT devices and determining the rules and regulation to be undertaken for the IoT security. Massive new reservoirs of data about individual personal information is being restored and shared, thus reinforcing global society compliance on data security is vital. Hence it becomes imperative to make such laws which protect the data privacy and the limitation of the data usage .There should be laws which would focus on providing the baseline security standards for different classes of IoT. Unwanted processing of the personal data should be regulated. In United States, there is the law under section 5 of FTC act, which calls the lack of reasonable security measures to protect the consumer rights as success in security management focusing on technical issues is not enough and addressing human issues is necessary for successful security. For securing IoT the same gape exists in the literature. Most of studies that investigate security of IoT do not consider social and people perspective for securing IoT.

M013: Ensure data anonymity: This objective addresses the need for the data to be made anonymous for the non-users. This is the most common way of protecting the confidentiality of the data on IoT. Potential damage to the sources of data can result in the absence of anonymity, but there should be a balance between making the data anonymous for the non-users and making it non-anonymous for the users, in order to avoid the undesirable consequences of both.

Each individual carry a digital footprint that enables their uniqueness-aspects about them. IoT data draws on aspects of individual's work life, study life, social life, home life to make assumptions that are beyond typical market segmentations. The IOT devices supply the organizations with the intimate details of an individual's personhood- like what clothes one wears, how much power and energy is used in one's homes, when the pulse rate begins to race etc. The digital footprint will have some implications resulting into potential harm to an

individual (Michael et al 2014). The digital footprint should also be minimized in order to avoid the potential harm to individual identity.

DISCUSSION

It is obvious that for desirable IoT outcomes security plays an important role. There are several technical challenges for IOT security in the application layer, perception layer, network layer and physical layer (Kumar et al., 2016). Several studies investigate these technical challenges in order to secure IoT (Hui et al., 2012; Dhillon and Torkzadeh, 2006). On the other hand, studies addressing the socio-technical perspective of IoT are rare and existing studies in IoT security mostly consider technical perspective. It is obvious that complexity in human behavior and expectations and the role that people play in IoT requires further investigation. In addition, according to several research works (Hitchings, 1998; Armstrong, 1999; Dhillon 2001; Karyda et al., 2003) for achieving success in security management focusing on technical issues is not enough and addressing human issues is necessary for successful security. For securing IoT the same gape exists in the literature. Most studies that investigate security of IoT do not consider the social and behavioral perspective for securing IoT. Several behavioral concerns emerged in this study, including ethics and trust.

One of the fundamental objectives that emerged from this study is promoting the ethical use of IoT. In particular, participants highlight the need for organizations to promote IoT usage ethics and to encourage the responsible use of IoT. To achieve this objective, organizations should invest significant resources in IoT security, education, training and awareness (SETA) campaigns. Future research is needed to identity unique approaches that will effectively train users on IoT security. In particular, SETA initiatives and studies around the ethical challenges associated with IoT property, accessibility, accuracy and private use will be an integral part of the emerging IoT security research stream.

In addition to ethics, trust of IoT also emerged as a significant means objective. Participants emphasized the need for organizations to increase consumer trust in IoT usage and ensure trust in IoT products. Trust has been explored extensively in diverse disciplines. The information systems community is replete with studies on trust in an online environment. However, given the proliferation of IoT, additional research is needed on the role of trust in this domain. The results of this study indicate the need for future research to explore ways to increase the use of trust

building technologies, design formal security mechanisms for IoT solutions and enhance IoT security governance.

The qualitative study presented in this paper has two limitations. First, the process of identifying values from the interview data was largely subjective and interpretive. Walsham (24) also have mentioned this issue as one limitation of research of this kind. He suggests "the choice should be consciously made by the researcher dependent on the assessment of . . . merits and demerits in each particular case" (p. 5).

Second, our research may have had difficulty in considering manager/subordinate or gender values.

CONCLUSION

This paper utilizes the value-focused thinking approach to provide objectives for securing IoT. According to Keeney (1999) "values to consciousness allows you to uncover hidden objectives, objectives you didn't realize you had" (p. 24). Some studies (Dhillon and Torkzadeh, 2006) have utilized Keeney's value focused methodology in order to understand objectives and their relationships based on people values. For instance, May et al, define value-based objectives in order to assess ERP systems planning. The value focused thinking approach has not been utilized to define security objectives of IoT from the user perspective. Extracting IoT objectives from user's values can help managers and practitioners maximize IoT security based on comprehensive list of objectives.

This study contributes to extent literature, by introducing fundamental objectives and means objectives for securing IoT. This study investigates the relatively unexplored area of IoT security. We conduct a qualitative investigation using value-focused thinking that helped to extract 17 objectives, grouped into four fundamental and 13 means objectives, essential for securing IoT from user perspective. The objectives developed in this study employ a socio-technical perspective and provide a way forward for developing IoT security measures. The findings of this research show that confidentiality, integrity and availability should be considered within the broader scheme of things in IoT security.

REFERENCES

Abbas, R., Michael, K., & Michael, M. G. (2015). Using a Social-Ethical Framework to Evaluate Location-Based Services in an Internet of Things World. International Review of Information Ethics, 22(12).

Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on (pp. 1-8). IEEE.

Abie, H., & Balasingham, I. (2012, February). Risk-based adaptive security for smart IoT in eHealth. In Proceedings of the 7th International Conference on Body Area Networks (pp. 269-275). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Agarwal, Y., & Dey, A. K. (2016). Toward Building a Safe, Secure, and Easy-to-Use Internet of Things Infrastructure. Computer, 49(4), 88-91.

Armstrong, H. (1999). A soft approach to management of information security.

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010, July). Proposed security model and threat taxonomy for the Internet of Things (IoT). In International Conference on Network Security and Applications (pp. 420-429). Springer Berlin Heidelberg.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. Computers & Security, 20(2), 165-172.

Dhillon, G., & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. Information Systems Journal, 16(3), 293-314.

Guo, B., Zhang, D., Wang, Z., Yu, Z., & Zhou, X. (2013). Opportunistic IoT: Exploring the harmonious interaction between human and the internet of things. Journal of Network and Computer Applications, 36(6), 1531-1539.

Gusmeroli, H. Sundmaeker, A. Bassi, et al., Internet of Things: Global Technological and Societal Trends, 1, 9-52.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions.*Future Generation Computer Systems*, *29*(7), 1645-1660.

Hitchings, J. (1996). A practical solution to the complex human issues of information security design. In Information systems security (pp. 3-12). Springer US.

Hunter, M. G. (1997). The use of RepGrids to gather interview data about information systems analysts. *Information systems journal*, *7*(1), 67-81.

Jia, Y., Dong, X., Liang, Z., & Saxena, P. (2015). I know where you've been: Geo-inference attacks via the browser cache. IEEE Internet Computing, 19(1), 44-53.

Karyda, M., Kokolakis, S., & Kiountouzis, E. (2003). Content, context, process analysis of IS security policy formation. In Security and Privacy in the Age of Uncertainty (pp. 145-156). Springer US.

Keeney, R. L., & McDaniels, T. L. (1992). Value-focused thinking about strategic decisions at BC Hydro. Interfaces, 22(6), 94-109.

Keeney, R. L. (1999). The value of Internet commerce to the customer.*Management science*, *45*(4), 533-542.

Kounelis, I., Baldini, G., Neisse, R., Steri, G., Tallacchini, M., & Pereira, A. G. (2014). Building trust in the human? Internet of things relationship.*IEEE Technology and Society Magazine*, *33*(4), 73-80.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016, January). Security in Internet of Things: Challenges, Solutions and Future Directions. In 2016 49th Hawaii International Conference on System Sciences (HICSS) (pp. 5772-5781). IEEE.
May, J., Dhillon, G., & Caldeira, M. (2013). Defining value-based objectives for ERP systems planning. Decision Support Systems, 55(1), 98-109.
Matharu, G. S., Upadhyay, P., & Chaudhary, L. (2014, December). The Internet of Things: Challenges & security issues. In Emerging Technologies (ICET), 2014 International Conference on (pp. 54-59). IEEE.
Michael, M. G., Michael, K., & Perakslis, C. (2014, November). Uberveillance and the Internet of Things and People. In Contemporary Computing and Informatics (IC3I), 2014 International Conference on (pp. 1381-1386). IEEE.
Sicker, D. C., & Lookabaugh, T. (2004). VoIP security: Not an afterthought. Queue, 2(6), 56.
Tan, L., & Wang, N. (2010, August). Future internet: The internet of things. In2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) (Vol. 5, pp. V5-376). IEEE.
Staff, F. T. C. (2015). Internet of Things: Privacy and Security in a Connected World. Technical report, Federal Trade Commission.
Suo, H., Wan, J., Zou, C., & Liu, J. (2012, March). Security in the internet of things: a review. In Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol. 3, pp. 648-651). IEEE.
Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A. ... & Doody, P. (2011). Internet of things strategic research roadmap. O. Vermesan, P. Friess, P. Guillemin, S.
Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A & Doody, P. (2011). Internet of things strategic research roadmap.
Vermesan. O, Friess. P, Guillemin. P, Gusmeroli. S, Sundmaeker. H, Bassi. A, Internet of Things: Global Technological and Societal Trends, 1, 9-52.
Walsham, G. (1995). Interpretive case studies in IS research: nature and method. European Journal of information systems, 4(2), 74-81.
Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things.International Journal of Communication Systems, 25(9), 1101.
Zhou, W., & Piramuthu, S. (2015). Information Relevance Model of Customized Privacy for IoT. Journal of Business Ethics, 131(1), 19-30.