IoT Security Adoption into Business Processes: A Socio-Technical View

Completed Research

Kavyashree G C
Lancaster University Management School
kavyashreegc@gmail.com

Forough Karimi-Alaghehband
HEC Montreal
forough.karimi-alaghehband@hec.ca

Desiree Özgün
Lancaster University Management School
desiree.oezguen@gmail.com

Abstract

Recently, the Internet of Things (IoT) has gained huge focus and has led to the generation of valuable data to create new value propositions for organisations. It is important to explore the impact these developments have on our society. IoT security is identified as the key issue amongst all the IoT applications and presents numerous social and technical challenges. We conducted interviews with IoT experts and the results illustrated how holistic security issues in IoT are undermined and to further emphasize the importance of addressing these issues by accommodating security into IoT business processes. This approach facilitated the assessment and identification of security threats from both social and technical perspectives. Our outcome highlights that IoT security must be implemented into IoT aware business processes to make the technology human centered, despite the challenges involved.

Keywords

Internet of Things, IoT aware business process, Socio-Technical approach, IoT security

Introduction

In recent years, technological developments have changed the way we live, learn and take actions. One of these developments is the Internet of Things (IoT). IoT has its roots in various industries like healthcare, retails, manufacturing, maintenance, utilities and more. IoT is an umbrella term, which represents the convergence of multiple domains, related visions and essential technologies. IoT can help businesses to anticipate customer needs and can be used to fulfil customer requirements effectively.

Applications of IoT can bring a great deal of convenience to people, however, the misuse of private information is a distinct possibility. One of the major challenges that must be tackled to integrate the IoT into the real world is security (Roman et al. 2013). Yet, IoT and its security challenges are mostly considered as technology-centric with much of the attention given to their technical features. There is need to consider social aspects in IoT development, and a redefinition of IoT to a human-centric system. A human-centric system is designed and developed based on human needs (Shin 2014).

While security is identified as a major challenge in most IoT studies, it lacks clear specifics on how security concerns from social and technical environments arise and what measures can be incorporated to avoid these. Using a sociotechnical approach (Mumford 1994), we highlight the importance of security incorporation in early stages of IoT business process design. Therefore we propose the following research question to highlight the importance of analysing security concerns in a holistic manner: “How does a socio-technical approach to IoT-aware business processes address IoT security concerns?” Based on the findings from this research question, we propose a model to address this issue and elaborate on the benefits of implementing this model.

This research highlights the need to consider security concerns as an important factor while designing an IoT business process. This highlights the need to revalidate the findings within more security-specific context and focus. Therefore, our study aims to contribute to IoT literature by using a socio-technical approach to gain a holistic view of security requirements in the design of IoT business processes.

Literature Review

IoT is defined as "the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (IBM 2014). IoT is built on three main pillars: First, the need for unique identifiers to establish relationships in a digital domain; Second, communication of a network of objects; Third, the ability to interact with the local environment through sensing capabilities (Miorandi et al. 2012). Through IoT, physical assets are becoming digitalized to create new products and business processes, which add value to the service provided (Bandyopadhyay et al. 2011). Notwithstanding the many benefits that are associated to IoT such as helping businesses to effectively anticipate and fulfil customer requirements, the challenges associated with using IoT need to be studied as well. In this study, we set out to examine the security challenges and how they could be addressed.

IoT Security

Security is one of the major challenges that must be tackled to integrate the IoT into the real world (Roman et al. 2013). IoT security is defined by Rouse (2015) as, "the area of endeavor concerned with safeguarding connected devices and network in Internet of things". IoT involves a wide range of security concerns that need to be addressed; some of them include the sensing infrastructure security, communication network security, application security and general system security (Keoh et al. 2014). Nevertheless, most of the literature on IoT security has mainly focused on *acknowledging* the security concerns associated with IoT. Although academic research on IoT security is still in its initial stages, many researchers analyse the existing challenges and provide potential protection mechanisms (Roman et al. 2013; Ning et al. 2011). However, there is a need for research to emphasis on the importance of gaining a holistic view of all the security issues associated with IoT.

A holistic view on security includes identifying concerns from both social and technical side of IoT. Security threat identified in one of the IoT application cannot be isolated from others since all these applications work collaboratively in an IoT system. The term "security" used throughout this research refers to cyber-security as opposed to physical security. International Telecommunication Union (2016) defines cyber-security as, "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user assets". Threats, vulnerabilities and safeguards are the pivotal elements, a threat can exploit an existing vulnerability to pose a risk to the organisation. Appropriate safeguards should be installed to mitigate an identified vulnerability and to protect assets (Goluch et al. 2008). A threat is "any circumstance or event with the potential to adversely impact organizational operations…, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability" (FIPS 2013). Even though a holistic view on security includes both social and technical factors, there is not one holistic concept of information privacy due to its dependency on context. Information privacy is being distinguished from other concepts like security and ethics. Social factors are referred to as privacy, trust, and awareness. Information privacy is stated as "one's control over personal information, particularly the secondary uses of this information" (Pavlou 2010, p. 978). People claim for control and influence on how information about themselves is being handled. Thereby, willingness to reveal personal information and trust are interrelated within information privacy (Pavlou 2010).

An Overview of IoT Aware Business Process

A business process is defined as "a set of logically related tasks performed to achieve a defined business outcome" (Davenport et al. 1990). As discussed by Haller & Magerkurth (2011), the integration of IoT with business processes is a complex scenario because of the challenges that come along: It is cumbersome to model adaptive and event driven IoT activities into the processes; data collected via sensors are unreliable and introduces uncertainty into the processes; devices often involve multiple actors which make it difficult to assess the compliance of the process. An IoT aware business process mainly includes technical aspects of an IoT system (Rouse 2015). IoT devices and native services can be expressed as potential resources in a business process environment, which are the sources that let in all process-relevant IoT

information (Haller & Magerkurth, 2011; Meyer et al.,2013). Figure 1 illustrates the relationships between the four major components of an IoT aware business process (Meyer et al. 2013): 1) An *IoT device* connects physical entities and establishes the IoT network. IoT devices possess capabilities such as monitoring, sensing and communication, and these devices are the technical process resources responsible for the execution of activities; 2) An *IoT service* refers to a set of activities within the process with well-defined and standardised interfaces. This provides access to other heterogeneous components and exposes their functionality as a unit of work to a business process. These process resources take over execution responsibility of the work; 3) A *Physical entity* refers to the identifiable parts of the physical environment which are of central interest to a user or an application, such as a business process. These are not processed resources but indirectly participate in the business process; 4) A *Native service* is a software component that is hosted on an IoT device, which allows users to gather information about physical entities and perform actions on them.

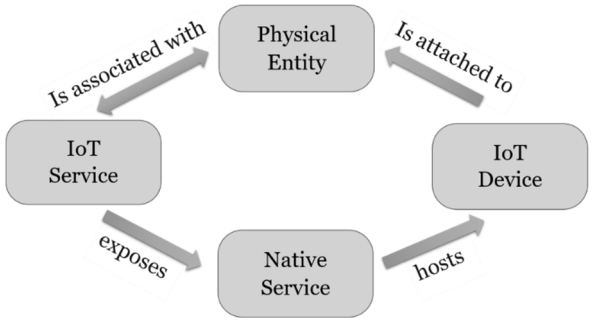

Figure 1: Components of IoT aware Business Process, adapted from Meyer et al.2013

While much of the attention is given to the actual technical implementation of IoT, little consideration is given to the integration of the IoT paradigm and its devices into IoT-aware business processes (Meyer et al. 2013). IoT comes with a lot of vulnerabilities and security issues, which pose potential risks to the IoT application and its network, which impacts the reputation as well as the competitive advantage of the organisation involved in the process. To address this issue, this research proposes to use the socio-technical approach. A business process should undergo a security analysis before the development of an IoT system to address security concerns. The socio-technical approach helps to assess and predict the development of Internet of Things.

Socio-Technical Approach

A socio-technical systems approach is a way of designing systems that consider both social and technical factors, which can contribute to the design of organisational structures, business processes and technical systems (Baxter et al. 2011).

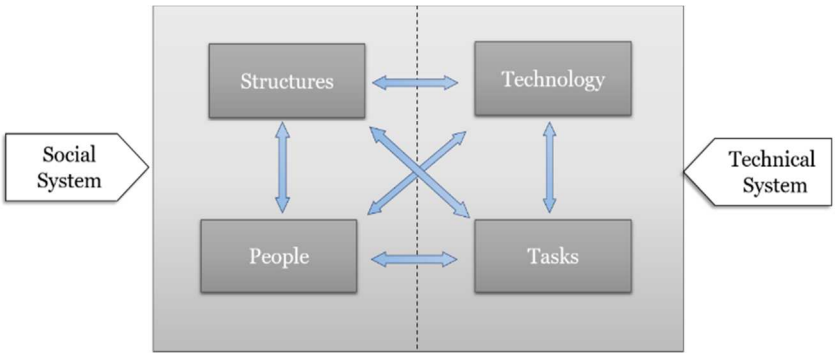

Figure 2: Socio-Technical Perspective, adapted from Bostrom and Heinen (1977 p.25)

Four key characteristics of a socio-technical system are proposed by Badham et al., 2000 (cited in Baxter & Sommerville, 2010): (1) Systems should have interdependent parts. (2) Systems should adapt to and pursue goals in external environments. (3) Systems have an internal environment containing separate but interdependent technical and social subsystems. (4) System goals can be achieved by more than one

means. According to socio-technical theory, technology and people involved in the system are interdependent where technology affects the behavior of people and behavior of people affects the working of the technology (Klien, 2013). As illustrated in figure 2, socio-technical approach expresses business process as a set of scenarios of sequential activities where the dependencies between actors, technological system and tasks are clearly defined, where the primary goal should always be the joint optimisation of social and technical systems (Mumford 1994). System performance relies on the joint optimisation of the technical and social subsystems. Focusing on one of these systems and excluding other will likely lead to a degraded system performance and utility. Many researchers have explored socio-technical design approach in different instances and illustrated the importance of considering both social and technical aspects of the systems in the process (Kettinger et al. 1997; Klein 2014). The socio-technical approach can help in gaining a clear understanding of how IoT will evolve and stabilise in the environment, this approach makes IoT more effective so that it can: 1) be accessible as a public tool; 2) be sustainable; 3) provide interoperability; 4) facilitate collaboration (Shin 2014). There are many challenging issues in IoT that still need to be addressed and it is crucial that both technological and social factors need to be united before the vision of IoT becomes a reality (Bandyopadhyay et al. 2011).

Research Methodology

Given the exploratory nature of this inquiry, a qualitative approach for our data collection and data analysis was chosen. The data collected in this study involves both primary data from in-depth interviews with experts and secondary data from documents, practitioners and journal articles. We used 'non-probability sampling' to identify interviewees. This technique uses subjective methods such as personal experience, convenience, and expert judgment to select the respondents in the sampling process. The interview participants were chosen based on their expertise and knowledge on the Internet of Things and business process design. We interviewed seven respondents in total. These interviews lasted an hour on average and resulted in approximately 80 pages of transcribed interviews. The interview guide used in this study was semi-structured, which involved the use of some pre-formulated questions with no strict adherence to them; therefore, new questions emerged while in conversation (Myers 2013). The list of interviewees, their organizational role as well as their affiliation are shown in table 1.

Interviewee Code	Role	Company
Interviewee A	Business and IT Security Manager	AXA PPP
Interviewee B	Solution Architect	SAP (UK)
Interviewee C	Chief Business Innovation Officer	TVH Group
Interviewee D	IoT Architect	SAP (UK)
Interviewee E	Head of Business Transformation	SAP (UK)
Interviewee F	Chief Solution Expert	SAP (UK)
Interviewee G	Consultant	Innovabee

Table 1: Interview Respondents List

The data analysis in this study was done through grounded theory approach, which helps to develop new concepts and theories of business-related phenomena, where these concepts and theories are firmly grounded in the qualitative data (Myers 2013). There are four important tools of grounded theory that were used in this study: 1) Coding: The data collected through interviews were transcribed and coded into conceptual constructs. Each of these represents a category, which speaks of the research question and objectives. 2) Theoretical Sampling: The interviews with SAP experts were conducted at first. After data analysis, the next interviewees were chosen based on respondent's expertise on IoT and its processes. 3) Theoretical Saturation: This stage was reached in the research study where at a stage the newly identified

codes related to already identified codes. 4) Constant Comparison: The codes generated in this research were constantly compared with previously identified codes throughout the coding process.

Research Findings

IoT from Socio-Technical Perspective

The primary objective of the socio-technical system is to consider both social and technical factors of the technology to make it more reliable, scalable and secure. These two aspects of technology should be given equal prominence in the system's design process. This holds true in IoT since human interaction in any context is an essential aspect of IoT applications. In addition to the explicit interaction between humans and devices, information that is human originated are highly valuable and are essential for many IoT applications. While considering human-technology interaction in IoT, it is essential to identify the potential security threats that could rise from the social environment. Social factors like trustworthiness, user privacy and user security awareness within any technological advancement are as important as its technical factors:

> "Users are not aware of the things that they use, we need to make sure that they ensure that this is not going to impact the brand and make it trustworthy to that user, I can't guarantee trustworthiness unless I know that the security of that device is fixed and sorted out before they receive it" - Interviewee A, Business and IT Security Manager.
>
> "Users in IoT need to go through the journey and it is essential that they are aware of all the challenges that they might be facing"- Interviewee B, Solution Architect.

An IoT aware business process functions based on the connectivity between several IoT devices:

> "It is said that there will be 50 gazillion connected devices by 2020. The key aspect is not only the number of devices, we already had devices; the only thing that has changed is connectivity…connectivity comes with a lot of vulnerabilities, security expert is needed more than the past." – Interviewee B, Solution Architect.

Connectivity leads to dynamic nature of an IoT business process, which should be acknowledged as part of the IoT system. Interviewee C, Chief Business Innovation Officer asserts that:

> "Building a sensing technology will help you to adapt your business process -and to take action per reality. That's the difference between real-time business process and static business process. Static business processes are built for static work, if not changing, all parameters are the same today and tomorrow…in dynamic business processes, you have to adapt your action as per the data that you are capturing and to valorising your business process out of the captured data."

IoT Security Incorporation into Business Process

The IoT brings a wide range of advantages to customers and businesses; however, it has implicit security concerns. Interviewee C, a Chief Business Innovation Officer, notes that "there are interesting solutions in the market but we need to have a solution in place to capture all kinds of security breaches and all kinds of problems related to the system…to increase the security level of the machine". Interviewee D, an IoT Architect, commented: "At this stage, there are concerns about security part, we start thinking about enhancing security through our architecture". "Security is a huge issue in IoT, the more we become dependent upon IT, the more emphasis we need to place on the security of the IT systems" - Interviewee E, Head of Business Transformation.

While dealing with IoT security concerns, having right security measures in place is crucial. Interviewee D, IoT Architect states that: "Risk assessment is carried out to get a clear understanding of the security threats and their impact-high, medium and low. When we are in the open environment, they have the minimal computing power and more exposure to security threats. These are the higher risk categories".

This research study emphasises the need for IoT security incorporation in business processes so that all security requirements are identified and addressed along with other application requirements. This can be done by defining activities to secure attack points in IoT as part of business objectives. By doing so, the right balance between providing customers with the convenience they expect from the application and security to keep an eye on their information privacy in an IoT application can be established in the early

stages of a business process. Interviewee F, Chief Solution Expert, elaborated the need for right balance between convenience and security in IoT applications with examples- "Security of the smart grid has the higher priority over convenience. If it comes to smart meters, customer themselves decide how much data they want to share. In other IoT areas, retail shops for example- security and privacy doesn't seem to be very prominent but convenience is much more important to customers".

Security incorporation into IoT business process facilitates revisiting of security requirements during every new release or sprint of the application. This can be done iteratively alongside other requirements of the business process:

> "Our system has evolved to build with things in place. Things being more agile now that means it become a continuous process. Each iteration at each agile sprint we go back and revisit all the requirements and make sure that they are built into the next sprint so we can't undermine the principles and assurances that should be in place as part of the evolution of the service, we need to maintain that assurance at whole times. The initial process before we proceed is to assure if the device is appropriate for the service we are providing" - Interviewee A, Business and IT Security Manager

The most challenging aspect in accommodating security into the business process is the cost of security. Interviewee G, Consultant asserts that- "Security is a big cost factor. By implementing new technology, for example creating a new system is already demanding by itself because it involves a lot of technologies. You have a lot of different topics you need to care about, and you're happy when it runs smoothly on mobile phones, on PCs and on laptops. I am happy so far, but to be honest now adding an additional step to make the whole thing secure, very secure, this is a cost topic."

Proposed Model, and Discussion

Our research findings suggest that contemporary organisations invest heavily in security but pay less attention to the social environment involved. Interviewees expressed concern regarding this separation of security from the actual business process and argued that security should be incorporated as an essential part of an IoT aware business process.

The model proposed in this research study is illustrated in figure 3. The model suggests perceiving IoT as a socio-technical system by considering the constant communication between social environment and technology involved in IoT systems. In addition to the explicit interaction between humans and devices, human originated information is highly valuable and are essential for many IoT applications.

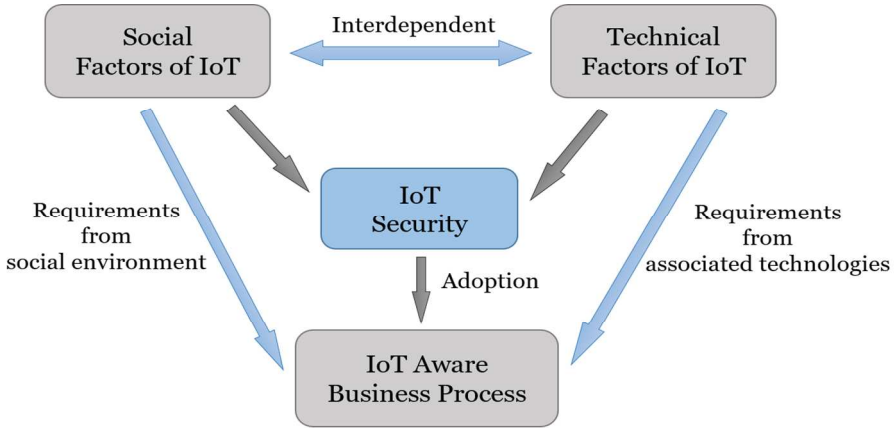

Figure 3: Proposed Security Model for IoT

We recommend that socio-technical approach should be used to study the security challenges in the IoT as it analyses the complex interaction between social and technical aspects of IoT by highlighting the co-

evolution, interaction, and interface, which constitute the potential network environment. IoT is a complex network of devices that makes it more vulnerable to malicious attacks than traditional systems.

An IoT device should possess capabilities to perform multiple functions at any given time. For example, a sensor should have the computing power, storage capacity along with sensing; There should be clear *boundaries* established for devices to know when to collect data from the user and when not to. These boundaries define the privacy element associated with user information; the data gathered by IoT devices should be transferred to *designated location* for further analysis. The analysis will help take necessary actions and create value for users. As demostrated in the model, the 4 main aspects that are prominent are- social factors of IoT, technical factors of IoT, IoT aware business process and IoT security.

Social Factors of IoT

Social factors of IoT functions alongside technical factors of IoT, which should be thoroughly examined to identify security concerns from social environment and further incorporating them into IoT aware business processes. Humans make IoT smarter and their interaction with the devices is the key for IoT to work; under certain circumstances, human interaction, judgment, and action can enhance the capabilities of IoT including data collection, analysis and behaviour (Luque 2014). *Compatibility* and reliability should be established between human agents and IoT devices. IoT users should have a complete understanding of the system and should participate in this interaction with a clear consensus; IoT devices gather an enormous amount of information from day-to-day activities of individuals. There should be clear *specification* about what information is essential to create value and how this information can be identified; The *social and technical* variances involved in the process should be identified; these variances include security and adoption challenges that are part of the technology.

While the technological aspect of IoT creates many advantages for businesses, the social factors are often overlooked. These factors are equally important because of the human involvement at some point in the IoT aware business processes. Three social factors are outlined: 1) *User Privacy* - Privacy is at the heart of trust, relationship building and data exchange. In all fields, users of IoT applications require the protection of their personal information, specifically their movements, habits and interactions with other people (Sicari et al. 2015). 2) *Trustworthiness* - This assures privacy and security to IoT users. Smart objects are usually human-related devices (e.g., carried by humans), which makes them exposed to public areas; and because these devices communicate wirelessly, they are vulnerable to malicious attacks (Shin 2014). 3) *User Awareness* - This awareness influences user technology adoption. User security awareness will impact the beneficial development of the IoT into society. IoT users should have access to knowledge that can help them keep their technology secure. Lack of this awareness negatively impacts IoT security.

Our research findings express that one of the benefits of considering social factors of IoT is that it helps establish the right balance between convenience and security: The number of connected devices in IoT is growing day by day. The connected devices bring added convenience in individuals' everyday activities. However, it is essential to understand what kind of security compromises are involved. Interviewees emphasised the importance of understanding the convenience of IoT and the security trade-off that it is involved. Wearable devices such as fitness trackers that stand out in IoT market in recent years generate a massive quantity of private data; businesses use this to create new opportunities, however, this holds potential user privacy concern since the data can be used down to every activity of the users including their location, time and behaviour. Finding a balance between convenience and security shows that companies should consider three sets of customers- those who prefer more convenience; those who prefer security, and those who are comfortable with the balance of convenience and security (Hasham et al. 2016).

Technical Factors of IoT

IoT technologies create value to the connected devices and support human activities; they further enhance the capabilities of the IoT network by cooperation and becoming the part of the total system (Yashiro et al., 2013). The essence of IoT lies in its connectivity. For successful functioning of IoT, reliability on connectivity is crucial. There are competing, incompatible connectivity for devices, for example, Bluetooth, LTE and ZigBee (Bauer et al. 2015). The data collected by one device is exchanged with other devices; and therefore, appropriate authentication mechanism should be in place for devices to be able to transfer data amongst themselves by trusting each other. The interviewees argued that the key problem is not about having an enormous number of devices but the connectivity between them. With connectivity, a

lot of new attack points and vulnerabilities are introduced into an IoT system. Identifying these vulnerabilities and having appropriate security measures to stop them from affecting the system is crucial.

There is a considerable amount of technical security issues that can emerge from an IoT system. Traditional IT systems have security isolated from the application, and security measures are only incorporated once the system is designed and developed. These traditional assumptions cannot be applied in the case of IoT. Security concerns should be tackled before the development of IoT application. Security threats may arise from various vulnerable attack points associated with IoT devices, technologies and networks: Security issues from associated technologies: IoT technologies like radio-frequency identification (RFID) and wireless sensor networks (WSN) are the non-contact automatic identification technologies and self-networks with dynamic network topology, which can automatically identify the target signal and obtain relevant data. They expose a lot of security problems (Jing et al. 2014). *Insufficient Authentication/Authorisation:* Identity authentication and access control can determine that the communication between two IoT devices and confirm each other's identity which can prevent malicious attacks to ensure authenticity and validity of the device in the network (Jing et al. 2014).

With the nature of connected devices, it is important to emphasis on the key aspects of data, data entry, data sharing, learning and decision-making. IoT is expected to ease and improve the decision-making responsibilities in any given context, organisations can make their decisions quickly, more efficiently by analysing the data in real-time. IoT devices dynamically make decisions and make changes in real-time given the constant monitoring of environment through sensors; To illustrate with an example from healthcare - smart pills - include microchips and is employed in individual's body, which can provide real-time information to be used in monitoring and communicating (Weinberg et al. 2015). However, what is the consequence if the smart pill compels individuals to take medications that they do not wish to take.

IoT Security

Companies developing an IoT system need to interact with the number of industries that supply one or the other essential component necessary for an IoT system development. To support this wide range of industry sectors and applications, it is essential to have standards that address common requirements (Bandyopadhyay et al. 2011). Currently, there are insufficient security capabilities in the emerging IoT standards; standards are slow moving but security standards need to be fixed faster (Ashford 2014). Interviewees agreed that new set of security standards should be in place for IoT because of IoT's nature-high network traffic, a large quantity of data and broad set of capabilities necessary in devices.

An IoT aware business process has a set of activities that need to be performed to fulfil business objectives. An IoT aware business process includes IoT devices and various technologies. Each of these elements poses a security risk. These can be threats to successful completion of the activities that can have a negative impact on the business process. Since IoT has a wide variety of devices and technologies involved, the kind of vulnerabilities they create is different from each other. Therefore, security analysis or risk assessment should be carried out on all the activities within the process. IoT devices should be highly sophisticated to incorporate security measures into it. Physical device security should be assured to reduce the risk factors associated with IoT by integrating physical barriers and technological tools. The devices should be designed with capabilities to authenticate, authorise their identity and encrypt the data they collect.

IoT Aware Business Process

The integration of IoT with business processes is a complex scenario because of the challenges that come along: It is cumbersome to model adaptive and event driven IoT activities into the processes; data collected via sensors are unreliable and introduces uncertainty into the processes; devices often involve multiple actors which make it difficult to assess the compliance of the process (Haller et al. 2011). Meyer et al., (2013) asserts that much attention is given to the actual technical implementation of IoT, little consideration is given to the integration of the IoT paradigm and its devices.

At any given time, an IoT device might be connected to a totally different set of devices than in another time. The growth of IoT depends on a range of sources including sensors, actuators, RFID and customer interaction in real-time. The dynamic nature of IoT would pose a greater challenge for organisations since it increases the pressure to ensure that the customers are provided with added value. Incorporating security requirements into IoT aware business processes will assure security despite all these dynamic

changes. Security requirements consideration into a business process should be an iterative/continuous process. In each iteration of the business process, it is necessary to revisit all the security requirements and make sure that the security measures designed at the beginning of the process are still valid in this iteration. One of the interviewees mentioned that by doing this, the principle of assurance will be part of the evolution of the IoT service and helps maintain assurance the whole time.

Cost of Security Adoption – Incorporating IoT security in a business process would mean secure IoT applications, organisations reputation and favours user adoption towards the technology. Despite the promise of user trust, security incorporation has cost factor involved. The cost of security is one of the major dimensions that the designer should always consider while incorporating security into a business process. Clear cost analysis should be carried out as part of security adoption. The security expert and domain expert should collaborate to weigh options around customer preference and work on the compromises that can be made in the system. The associated cost should be estimated for all the newly identified security concerns. In all cases, it comes down to the value of security. It is necessary to evaluate if the data and the process are valuable enough that it needs to be protected, it is also necessary to understand the consequences of not having security (Scherr 1993). Further analysis should be done on mitigating these costs.

Conclusion

This research study was aimed at exploring the cyber-security concerns associated with IoT, which affect both individuals using IoT applications and businesses that develop IoT applications. After a thorough analysis of interview findings, this paper first presented IoT as a socio-technical system due to its complex human-technology interaction. The study emphasised the importance of gaining a holistic view of security threats in IoT and therefore proposed a model using the socio-technical framework of system design approach in addressing the security challenges of IoT. Second, a security adoption into an IoT business process is recommended as an ideal solution to address a wide range of IoT security concerns. It is necessary to identify and incorporate security requirements alongside any other business requirement in the process. The study further identified the factors and challenges that need to be taken into consideration while integrating security as part of an IoT aware business process. These factors also facilitate in assuring a clear understanding of IoT functionalities and security measures. Having risk mitigation plans in IoT applications increases their credibility, reliability and efficiency. This research emphasises that security in IoT should evolve with its business processes. Since the security and business requirements for IoT applications vary across each industry, there is a need for further research to analyse industry-specific security requirements. This, in turn, will facilitate understanding of customer preference and helps businesses in creating added value to their service.

References

Ashford, W. 2014. Act now on IoT security, says Beecham Research. [online] Available at: http://www.computerweekly.com/news/2240230348/Act-now-on-IoT-security-says-Beecham-Research [Accessed 27 Aug 2016]

Bandyopadhyay, D. & Sen, J. 2011. Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Pers Commun,* 58(1), pp.49-69.

Bauer, H; Patel, M and Veira, J. (2015) Internet of Things: Opportunities and challenges for semiconductor companies. Available at: http://www.mckinsey.com/industries/semiconductors/our-insights/internet-of-things-opportunities-and-challenges-for-semiconductor-companies [Accessed 28 Aug 2016]

Baxter, G. and Sommerville, I. 2011. Socio- Technical Systems: From Design Methods to Systems Engineering. *Interacting with Computers,* 23(1), pp. 4-17.

Bostrom, R. P. & Heinen, J. S. 1977. Mis Problems and Failures: A Socio- Technical Perspective. Part I: The Causes. MIS Quarterly, 1(3), 17-32.

Davenport, T. & Short, J. 1990. The New Industrial Engineering - Information Technology and Business Process Redesign. Sloan management review, 31(4), pp. 11-27.

Federal Information Processing Standards (FIPS) 2013, Minimum Security Requirements for Federal Information and Information Systems. Carc.nist.gov. Retrieved 2013-11-05.

Goluch, G., Ekelhart, A., Fenz, S., Jakoubi, S., Tjoa, S. and Muck, T. 2008. Integration of an Ontological Information Security Concept in Risk Aware Business Process Management. *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, Waikoloa. 377-386.

Haller, S. and Magerkurth, C. 2011. The Real-time Enterprise: IoT-enabled Business Processes. *Workshop on Interconnecting Smart Objects with the Internet*. [online] Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.9881&rep=rep1&type=pdf [Accessed 8 Aug 2016]

Hasham, S., Rezek, C., Vancauwenberghe, M. and Weiner, J. 2016. Is cybersecurity incompatible with digital convenience? [online] Available at: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience [Accessed 27 Aug 2016]

IBM. 2014. Deriving business value from the Internet of Things. [online] Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=AZW03006USEN, p.2 [Accessed 31 July 2016]

ITU (2016) Overview of Cybersecurity. [online] Available at: http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx [Accessed 6 Aug 2016]

Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. and Qiu, D. 2014. Security of the Internet of Things: perspectives and challenges. Wireless Networks. 20 (8). pp. 2481-2501.

Keoh, S.L., Sandeep, S., Kumar, H. & Tschofenig, H. 2014. Securing the Internet of Things: A Standardisation Perspective. Internet of Things Journal, IEEE, 1(3), 265-275.

Kettinger, W. J. & Guha, S. 1997. Business Process Change: A Study of Methodologies, Techniques, and Tools. *MIS Quarterly,* 21(1), pp. 55-80.

Klein, L. 2014. What Do We Actually Mean by 'Sociotechnical'? On Values, Boundaries and the Problems of Language. *Applied Ergonomics,* 45(2), pp. 137-142.

Luque, C.M. 2014. Humans Can Make the Internet of Things Smarter. [online] Available at: https://hbr.org/2014/10/humans-can-make-the-internet-of-things-smarter [Accessed 26 Aug 2016]

Miorandi, D., Sicari, S., De Pellegrini, F. & Chlamtac, I. 2012. Internet of Things: Vision, Applications and Research Challenges. *Ad Hoc Networks,* 10(7), pp. 1497-1516.

Meyer.S, Ruppen.A, Magerkurth.C. 2013. Internet of Things-Aware Process Modelling: Integrating IoT Devices as Business Process Resources. [online] Available at: http://link.springer.com/chapter/10.1007/978-3-642-38709-8_6 [Accessed 6 Aug 2016]

Mumford, E. 1994. New Treatments or Old Remedies: Is Business Process Reengineering Really Socio-Technical Design? *Journal of Strategic Information Systems,* 3(4), pp. 313-326.

Murphy, M., 2015. 'There is confusion over Hana what we need to clarify' says SAP. [online] Available at: http://www.nbssap.com/there-is-confusion-over-hana-that-we-need-to-clarify-says-sap/ [Accessed 21 Aug 2016]

Myers, M. D. 2013. *Qualitative Research in Business & Management*: London: SAGE.

Ning, H. and Liu, H. 2011. Cyber-Physical-Social Based Security Architecture for Future Internet of Things. *Advances in Internet of Things*. 2. pp. 1-7.

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? MIS Quarterly, 35(4), 977-988

Roman, R., Zhou, J. & Lopez, J. 2013. On the Features and Challenges of Security and Privacy in Distributed Internet of Things. *Computer Networks,* 57(10), pp. 2266-2279.

Rouse, M. 2015. IoT security (Internet of Things security). [online] Available at: http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security [Accessed 10 Aug 2016]

SAP. 2014. SAP Brings You the Internet of Things for Business. [online] Available at: https://www.sap.com/bin/sapcom/en_us/downloadasset.2014-11-nov-12-17.sap-brings-you-the-internet-of-things-for-business-pdf.html [Accessed 20 Aug 2016]

Shin, D. 2014. A Socio- Technical Framework for Internet-of- Things Design: A Human-Centered Design for the Internet of Things. *Telematics and Informatics,* 31(4), pp. 519-531.

Sicari, S., Rizzardi, A., Grieco, L. A. & Coen-Porisini, A. 2015. Security, Privacy and Trust in Internet of Things: The Road Ahead. *Computer Networks,* 76, pp. 146-164.

Weinberg, B. D., Milne, G. R., Andonova, Y. G. & Hajjat, F. M. 2015. Internet of Things: Convenience Vs. Privacy and Secrecy. *Business Horizons,* 58(6), pp. 615-624.