2017

Exploring Security, Privacy, and Reliability Strategies to Enable the Adoption of IoT

Daud Alyas Kamin
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Daud Kamin

has been found to be complete and satisfactory in all respects,
and that any and all revisions required by
the review committee have been made.

Review Committee
Dr. Jon McKeeby, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Exploring Security, Privacy, and Reliability Strategies to Enable the Adoption of IoT

by

Daud A. Kamin

MS, Walden University, 2013

BS, San Diego State University, 2003

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2017

Abstract

The Internet of things (IoT) is a technology that will enable machine-to-machine communication and eventually set the stage for self-driving cars, smart cities, and remote care for patients. However, some barriers that organizations face prevent them from the adoption of IoT. The purpose of this qualitative exploratory case study was to explore strategies that organization information technology (IT) leaders use for security, privacy, and reliability to enable the adoption of IoT devices. The study population included organization IT leaders who had knowledge or perceptions of security, privacy, and reliability strategies to adopt IoT at an organization in the eastern region of the United States. The diffusion of innovations theory, developed by Rogers, was used as the conceptual framework for the study. The data collection process included interviews with organization IT leaders (n = 8) and company documents and procedures (n = 15). Coding from the interviews and member checking were triangulated with company documents to produce major themes. Through methodological triangulation, 4 major themes emerged during my analysis: securing IoT devices is critical for IoT adoption, separating private and confidential data from analytical data, focusing on customer satisfaction goes beyond reliability, and using IoT to retrofit products. The findings from this study may benefit organization IT leaders by enhancing their security, privacy, and reliability practices and better protect their organization's data. Improved data security practices may contribute to social change by reducing risk in security and privacy vulnerabilities while also contributing to new knowledge and insights that may lead to new discoveries such as a cure for a disease.

Exploring Security, Privacy, and Reliability Strategies to Enable the Adoption of IoT

by

Daud A. Kamin

MS, Walden University, 2013

BS, San Diego State University, 2003

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

November 2017

Dedication

I dedicate this work to my wife Mariam and children (Laila and Eli) for their unconditional love, support, and motivation while I was a working student and a parent. This is proof that you can achieve anything if you work hard at it. Do not let failures slow you down; they are clues set to help you reach your goals. I also want to dedicate this to my parents, who gave up everything to bring their children to a place where they could flourish. I will never forget, and I hope this accomplishment makes you proud.

Acknowledgments

I want to thank so many people for their support throughout my studies for their involvement throughout my studies all these years, including my grade school and high school teachers who inspired and encouraged me to reach for the sky. I want to thank my committee chair, Dr. Jon McKeeby, and all of my committee members, Dr. Bob Duhainy and Dr. Steven Case. This undertaking has challenged me academically, emotionally, and physically. Thank you, all, for your support, encouragement, and understanding. In addition, thank you to Walden's chief academic officer, Dr. Karlyn Barilovits and all of the other faculty members and classmates at Walden University that I have worked and studied with these past few years. I want to also thank all of those who participated in this research for your dedication to my project in the midst of a your day-to-day responsibilities. Your participation in my study is very much appreciated. Finally, I especially want to thank my wife and children for putting up with my odd hours and sleepless nights, missed family nights, dance classes, soccer practices, and general time together. I love you all. Thank you for your support, understanding, and motivation.

Table of Contents

List of Tables v

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 2

Nature of the Study 3

Research Question 4

Interview Questions 4

Conceptual Framework 5

Definition of Terms 6

Assumptions, Limitations, and Delimitations 6

Assumptions 6

Limitations 7

Delimitations 7

Significance of the Study 8

Contribution to Information Technology Practice 8

Implications for Social Change 9

A Review of the Professional and Academic Literature 9

IoT Defined 10

Organizational Benefits of IoT Adoption 14

IoT Security Issues 16

IoT Privacy Issues 21
IoT Reliability Issues 28
Diffusion of Innovations: Five Characteristics 34
Diffusion of Innovations Theory 34
Compatibility 36
Relative Advantage 39
Trialability 44
Observability 49
Complexity 54
Analysis of Related Theories 58
Limitations of Diffusion of Innovations Theory 59
Usage of Diffusion of Innovations Theory in Research 60
Transition and Summary 63
Section 2: The Project 65
Purpose Statement 65
Role of the Researcher 66
Participants 69
Research Method and Design 72
Method 72
Research Design 74
Population and Sampling 78
Ethical Research 81

Data Collection 84
Instruments 84
Data Collection Technique 90
Data Organization Techniques 93
Data Analysis Technique 94
Reliability and Validity 98
Dependability 100
Credibility 101
Transferability 102
Confirmability 102
Transition and Summary 103
Section 3: Application to Professional Practice and Implications for Change 105
Overview of Study 105
Presentation of the Findings 106
Theme 1: Securing IoT Devices is Critical for IoT Adoption 106
Theme 2: Separating Private and Confidential Data From Analytical Data 114
Theme 3: Focusing on Customer Satisfaction Goes Beyond Reliability 120
Theme 4: Using IoT to Retrofit Products 127
Applications to Professional Practice 134
Implications for Social Change 137
Recommendations for Action 139
Recommendations for Further Study 141

Reflections 142

Summary and Study Conclusions 143

References 145

Appendix A: Human Subject Research Certificate of Completion 186

Appendix B: Interview Protocol 187

Appendix C: Participant Invitation 189

List of Tables

Table 1. Frequency of First Major Theme 107

Table 2. Frequency of Second Major Theme.....115

Table 3. Frequency of Third Major Theme 121

Table 4. Frequency of Fourth Major Theme.....128

Section 1: Foundation of the Study

Background of the Problem

The diffusion of Internet-connected devices, such as smartphones, has improved quality of life for many people (Ju, Kim, & Ahn, 2016). A similar solution is necessary to solve a complex problem of the dynamic detection of toxic gasses to ensure the safety of people working in coal mines, petroleum industries, and gas storage plants (Yuanfang, Gyu, Lei & Crespi, 2016). Home automation is another necessity for many people who wish to manage the room temperature or set a home alarm remotely (Gonnot, Yi, Monsef, & Saniie, 2015). In the healthcare industry, experts look to proactively manage wellness rather than illness, focusing on the prevention and early detection of diseases (Su, Wang, & An, 2013). It is likely that patients will eventually carry sensors to monitor their body temperature, blood pressure, and breathing activity (Miorandi, Sicari, Pellegrini, & Chlamtac, 2012). The Internet of Things (IoT) is a technology that connects any device with an on and off switch to the Internet and to each other (Andersson & Mattsson, 2015). Thus, IoT may be a suitable technology solution to address all the challenges presented above and meet the wellness requirements of the healthcare industry.

However, IoT presents disadvantages that prevent organizations from implementing and distributing the technology. These disadvantages include security, privacy, and reliability challenges in IoT devices (Roman, Zhou, & Lopez, 2013). In this study, I explore strategies organization information technology (IT) leaders use for security, privacy, and reliability to enable the adoption of IoT devices.

Problem Statement

IoT security, privacy, and reliability remain critical issues that prevent the development of applications to use IoT across industries (Kim, Lim, & Lee, 2015). Meanwhile, IoT will help grow the number of connecting devices from billions to hundreds of billions of devices (Brody & Pureswaran, 2015). As a result, IoT will require standardization to help advance security, privacy, reliability, and processes for organizational leaders to adopt the technology. The general IT problem is that there is a shortage of knowledge to strategize adoption of IoT devices. The specific IT problem is that some organization IT leaders lack security, privacy, and reliability strategies to enable the adoption of IoT devices.

Purpose Statement

The purpose of this qualitative exploratory case study was to explore strategies that organization IT leaders use for security, privacy, and reliability to enable the adoption of IoT devices. The population consisted of organization IT leaders including the chief information officer (CIO), chief information security officer (CISO), enterprise architect, data center manager, and IT director from an IT organization in Stamford, Connecticut who have implemented IoT strategies. The IT leadership team participated in semistructured interviews to explore the security, privacy, and reliability strategies used at the organization to enable the adoption of IoT. The implications for positive social change include the potential for improvement to IT practices as the IoT devices have sensors that make routine decisions and perform common tasks based on human tendencies. There is also the potential to contribute to new knowledge and insights that

may lead to discovery, such as the prevention of chronic traumatic encephalopathy (CTE). If athletes wore sensors to detect the impact of objects to their head, athletic officials may be able to implement preventative measures based on the number of concussions for an athlete as a solution to prevent CTE.

Nature of the Study

The intent of this qualitative exploratory case study was to explore organizational security, privacy, and reliability strategies to enable the adoption of IoT devices. According to Stake (1995), case studies offer a deeper understanding of a phenomenon. During this study, I provided depth in understanding the strategies of security, privacy, and reliability that affected the decision to adopt IoT. A qualitative research method was suitable for this study because I focused on one organization and its successful implementation of IoT. Qualitative research enabled the generation of detailed responses to complex subjects, and there were no numerical data to measure as there would have been with quantitative studies. Quantitative researchers test hypotheses and evaluate the numeric outcomes identified in the research while the methods lack the flexibility to explore the depth of the study (Rennie, 2012). Therefore, quantitative research was not appropriate for this study.

A case study was the best design choice for this study as I focused on the successful adoption of IoT at one organization while offering details from multiple sources through the method of triangulation. A case study offers authenticity due to the true representation of the data and the participants' views and their experiences (Cronin, 2014). Moustakas (1994) posited that a phenomenology study contains lived experiences

and events from the phenomenon. While a phenomenology study was valuable, it would not have addressed the specific details about an organization's strategy and the impact security, privacy, and reliability had on the adoption of IoT. An ethnographic study focuses on a culture's characteristics (Cunliffe & Karunanayake, 2013), which was also outside of the scope of this study. Finally, a narrative study entails gathering artifacts and life experiences for storytelling about how humans experience the world (Wolgemuth, 2014). Since I focused on an organization's strategy, a narrative study was not applicable to this study.

Research Question

What are security, privacy, and reliability strategies used by organization IT leaders to adopt IoT devices?

Interview Questions

1. What security, privacy, and reliability strategies have you used to adopt IoT devices?
2. How did you determine to use security, privacy, and reliability strategies to adopt IoT devices?
3. What methods worked best in the security, privacy, and reliability strategies to adopt IoT devices?
4. What strategies did you use to ensure IoT compatibility issues were addressed?
5. What strategies do IoT provide to gain a relative advantage over existing technologies?

6. How did you test or pilot IoT to ensure meeting organizational objectives?
7. How did the visibility of IoT enable its adoption at your organization?
8. How did your strategies address the complexity of IoT adoption?

Conceptual Framework

Rogers established the diffusion of innovations (DOI) theory in 1962. Rogers (1962) described five characteristics of innovation, which include compatibility, relative advantage, trialability, observability, and complexity. Compatibility refers to the new technology adapting to the current systems (Sanni, Ngah, Karim, Abdullah, & Waheed, 2013). Relative advantage addresses the benefits gained from the new technology compared to the existing technology (Yung-Ming, 2015). Trialability is short for the ability to test or pilot the new technology (McMullen, Griffiths, Leber, & Greenhalgh, 2015). Observability refers to the effects or implications of adopting the new technology (Penjor & Zander, 2016). Finally, complexity addresses the difficulty of learning the new technology (Sugarhood, Wherton, Procter, Hinder, & Greenhalgh, 2014).

I selected the DOI theory as the conceptual framework for this study because it aligned particularly well with the adoption of IoT devices. The basis for the adoption of IoT was the ability for IoT to provide a relative advantage to existing technologies. As such, organization IT leaders must be able to experiment using trials and observe the technology's use. Also, IoT must be compatible with the organization's existing technologies. In addition, IoT complexity must be limited to allow organizations to adopt it. An integral part of adopting IoT is to ensure that the devices are secure, that they do not breach privacy, and that the devices are reliable for organizations to adopt them. The

objective of the study was to understand the security, privacy, and reliability strategies that enabled the adoption of IoT devices. Therefore, a theory was used to understand the motivation of organization IT leaders when adopting IoT devices.

The DOI theory is often used for new technology adoption across multiple industries (Sáenz-Royo, Gracia-Lázaro, & Moreno, 2015). In healthcare, patients are members of the community where IoT devices are the innovative technology for doctors to provide better care. Thus, patients will gain access to improved health monitoring thanks to the benefits of IoT devices. Meanwhile, the types of patients and end users for these devices vary drastically. Doctors may benefit from IoT technology to notify them when their patient needs their advice. The diffusion of the IoT automation process will benefit healthcare facilities as it enables process improvement, process efficiency, and doctors and nurses to be more effective in the day-to-day activities.

Definition of Terms

Organization IT leader is a person serving in an IT position such as a CIO, executive vice president, vice president, director, senior application developer, or senior project manager (Alimo-Metcalfe, 2010).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are issues that researchers take for granted or accept in faith without verification (Kirkwood & Price, 2013). One assumption about this study's participants was that they understood and responded to interview questions to the best of their

knowledge and ability. The second assumption was that participants responded to interview questions honestly and accurately.

Limitations

Kirkwood and Price (2013) characterized limitations as unavoidable shortcomings surrounding the study leading researchers to confine their conclusions. One limitation of this exploratory case study was that participant interview data were based on a single IT organization, which may have led to participant bias based on their experiences in the company. The next limitation was the industry of the organization, as the responses to interview questions may not align with other industries such as manufacturing or transportation. Finally, the interview participants only included organization IT leaders. As a result, perceptions of business users or individual contributors using or supporting IoT was excluded from this study.

Delimitations

Delimitations are restrictions or boundaries that researchers impose to focus the scope of the study (Svensson & Doumas, 2013). Participants of the study included organization IT leaders who had knowledge or experience using security, privacy, and reliability strategies to adopt IoT at their organization. The data collection instruments included interviews with organization IT leaders and a review of company documents. The interview questions were semistructured and open-ended to enable participants to share their experiences and perceptions about security, privacy, and reliability strategies to adopt IoT devices. I selected the study participants based on a census sample and

included all participants who met the eligibility criteria. I conducted the study at an IT organization in Stamford, Connecticut.

Significance of the Study

Contribution to Information Technology Practice

IoT is still a new technology for most organizations, and not enough organizations have implemented it for others to learn from the lessons of adoption (Ahsan, Talib, Sarwar, Khan, & Sarwar, 2016). The results from this study may provide much-needed insights into the strategies by which organization IT leadership must implement about security, privacy, and reliability to adopt IoT devices. Insights from this study may aid organizations to consider the factors for their organization to adopt IoT. The focus of this study was to understand the security, privacy, and reliability strategies needed to adopt IoT devices.

The purpose of IoT is for users to share information on a network in real-time (Yang, Yang, & Plotnick, 2013). Technology drives many organizational processes, and consumers highly depend on it in their lives (Andersson & Mattsson, 2015). As technology continues to advance, organization IT leaders must take the necessary steps to ensure they have a strategy to implement innovations. Before doing so, they must first consider the security, privacy, and reliability risks presented by the adoption of IoT. The leadership adopting the technology must consider security, privacy, and reliability strategies to include IoT into the organization.

Implications for Social Change

The implication for social change is that IT organizations may increase the ability to develop tools for detection, prevention, and monitoring of issues. IoT may also make doctors productive and efficient while improving patient lives because of the real-time access to information. IoT may equip researchers with information to help create new drugs or prevent a disease such as CTE (Maroon et al., 2015). Organizations such as the National Football League (NFL) can be proactive in adopting IoT medical devices because the trend of CTE seems to be a great concern to many players and families. Breslow (2014) referred to a statistic where 101 out of 128 football players who passed away tested positive for CTE. The players' families may argue that the NFL can use an innovative way to measure the impact of a collision to address this issue proactively and protect the players after they retire from the game. Veena, Devaraj, Rajasree, and Oberoi (2014) proposed a prototype sensor that may address the need for detecting the impact to helmets. The prototype is an innovative way of enabling doctors to use technology to protect players from further brain damage. As similar issues arise from different organizations, communities will speak up and ask for change.

A Review of the Professional and Academic Literature

The purpose of this qualitative case study was to explore strategies that organization IT leaders use for security, privacy, and reliability to enable the adoption of IoT devices. The focus of the literature review was the research question: What are security, privacy, and reliability strategies used by organization IT leaders to adopt IoT devices? I explored the current security issues, privacy issues, and reliability issues across

multiple industries, while focusing on the healthcare industry as a leading example. Next, I explored strategies researchers have studied to address security, privacy, and reliability issues using the five characteristics of the DOI theory as a framework.

This literature review contains references from 141 articles, journals, and conference proceedings. The primary research libraries and databases included the ACM Digital Library, EBSCOhost Computers and Applied Sciences Complete, IEEE Xplore Digital Library, ScienceDirect, Google Scholar, ProQuest Computing, and ProQuest Dissertations and Theses Global. I identified the peer-review status of articles using Ulrich's Global Serials Directory and individual journal websites. I reviewed 141 articles, of which 129 (91%) were peer-reviewed and 128 (91%) were published within 5 years of my anticipated graduation date.

The literature focused on four key areas: (a) the five characteristics of the DOI theory, (b) security issues and strategies, (c) privacy issues and strategies, and (d) reliability issues and strategies. The review of the five characteristics of DOI focused on tenets that influence IoT adoption. The characteristics included relative advantage (competitiveness), compatibility (consistency), trialability (experimentation), observability (visibility), and complexity (difficulty). The research into security, privacy, and reliability involved current issues, consequences of the issues, and strategies to minimize the challenges.

IoT Defined

Many people may have heard about IoT but may not understand its meaning. IoT refers to an open and partially standardized technology infrastructure that enables

interaction between devices over the Internet using unique addressing schemes (Ahsan et al., 2016). IoT devices include radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, refrigerators, and many other heterogeneous devices that communicate wirelessly (Gonnot et al., 2015). The devices are often in a larger computer network and are connected to backend servers (Boos, Guenter, Grote, & Kinder, 2013). If the device has an IP address and transfers data over a network, almost anything is possible.

IoT may be used with multiple technologies and frameworks. IoT is a technology infrastructure that enables multiple technologies to interact with each other to exchange data (Yang et al., 2013). IoT devices include any object that can connect to the Internet, including smartphones, toys, fitness devices, heavy machinery, home appliances, and many others (Greene, 2015). Yang et al. (2013) described IoT as a paradigm that connects objects or things to the Internet by wireless or wired technologies to achieve the desired goals. Characteristics within IoT include ubiquitous communication, pervasive computing, and ambient intelligence (Borgia, 2014; Konstantinidis, Bamparopoulos, Billis, & Bamidis, 2014). IoT is a combination of ubiquitous computing, pervasive computing, the Internet, sensing technologies, communication technologies, and embedded devices (Borgia, 2014). The IoT device ecosystem can divide into sensor hardware platforms, sensor operating systems, software processing and development environments, and sensor data integration platforms (Swan, 2012). Organizations may consider adopting IoT because the framework may offer the flexibility they need to successfully implement innovative technology.

IoT has standards that may be favorable for some organizations and unfavorable to others. Vendors have introduced several proprietary platforms for IoT, leading to a lack of standardized software platforms for IoT devices and making it difficult for devices to communicate with each other (Yun, Ahn, Choi, & Kim, 2016). Yun et al. (2016) referred to a use case for IoT where an alarm clock, a toaster, and a coffee maker all communicate with each other to prepare breakfast during the wake-up time. The scenario assumes there is a common platform for the devices to communicate with each other. Before a wider user adoption, an open standard is necessary to ensure the interoperability of devices between various technology vendors (Andersson & Mattsson, 2015; Bąk, Czarnecki, & Deniziak, 2015). Therefore, IoT adoption may be difficult for organizations that have not implemented the standards required by IoT.

IoT includes several standards that may be used by organizations. Organizations have been using conventional standards such as RFID, barcodes, or quick response codes for identification purposes, although these technologies are intended for tracking purposes rather than real-time data requests (Jara, Parra, & Skarmeta, 2014). IoT may compliment these conventional standards with the addition of new standards. Bąk et al. (2015) referred to the ability for IoT to use GPS positions to track and provide a complete movement profile of a certain person. Hence, IoT is able to enhance conventional tracking methods by incorporating the use of sensors.

Distance may be a determining factor for the technology that is used by organizations when considering communication between IoT devices. IoT devices are connected to the Internet using technology standards such as RFID, WiFi, Bluetooth,

NFC, ZigBee, Z-Wave, and 6LoWPAN (Gonnot et al., 2015). Organizations may choose to limit device connectivity within the organization. However, organizations may gain the most value from IoT by making it available on the Internet for ubiquitous computing.

IoT connectivity between devices is similar to an Internet connection with computers. Connectivity between IoT devices is managed by a central node, which requires registration upon connection of each device (Gonnot et al., 2015). Yun et al. (2016) proposed the use of object identifiers (OIDs) for devices to identify themselves on the Internet, like a MAC address for a computer. OIDs are managed in a hierarchical manner where the central node is the parent of the tree (Yun et al., 2016). OIDs are series of numbers separated by a dot and are composed of the resource ID (location of the device on the parent tree), manufacturer number, model number, serial number, and expanded number (Yun et al., 2016). IoT devices may use IPv6 as the communication protocol to communicate with other devices (Konstantinidis et al., 2014). Thus, connectivity between devices is not very different from how computers operate today.

The capabilities of IoT depend on the devices and the intended use of the technology. IoT devices can sense, monitor, automate, and control objects (Bąk et al., 2015). IoT has a presence in many applications across multiple industries including security, tracking and tracing, payment, health, remote control and maintenance, and metering (Andersson & Mattsson, 2015). Bąk et al. (2015) provided an example of a car navigation system connecting to an Internet system that controls and monitors the traffic in a city as a method to avoid congestion. These same assets make smartphones valuable for IoT users because one device can manage multiple demands in an effective manner.

Similarly, the healthcare industry uses smartphones to monitor the health or progression of chronic diseases in patients due to the capabilities of IoT (Konstantinidis et al., 2014). Hence, organizations can look for effectiveness when considering the value of IoT adoption.

Some IoT consumers may be intrigued with the technology while others may have doubts about its growth and acceptance. IoT will grow to estimated hundreds of billions of connected devices by the year 2020 (Jara, Varakliotis, Skarmeta, & Kirstein, 2014). IoT devices enable people to enrich their lives due to the technology's diverse functionality. Several industries use IoT where use cases include tracking products, monitoring smart homes, and remote monitoring of patients (Andersson & Mattsson, 2015). Specific examples of IoT use include remote monitoring of a patient's heart rate after a recent heart transplant, a farm animal with a biochip transponder for identification purposes, and an automobile that has built-in sensors to alert the driver when the tire pressure is low (Shin, 2014). IoT has proven to be a positive impact in society and presents more opportunities for social change across industries, especially in medicine.

Organizational Benefits of IoT Adoption

Several industries have implemented IoT because of the organizational benefits it provides including organizational efficiency and employee productivity. The combination of high volume data and IoT has created opportunities for organizations to create systems to share knowledge internally and make informed business decisions (Cao, Guo, Liu, & Gu, 2015). The organization can then analyze the data to make better decisions and strategic business moves. The United Parcel Service is an example of a company using

IoT sensors on its delivery vehicles to monitor speed, mileage, stops and health of the vehicles (Bi & Cochran, 2014). The United Parcel Service can analyze the data captured to improve operational efficiency by the sensors to reduce fuel consumption.

IoT offers many benefits to the environmental and agricultural industries. IoT plays a significant role in the prediction of the water supply from snowmelt to meet the human, environmental, agricultural, and industrial demands for water (Fang et al., 2015). The data may be used as a proactive way to issue earlier flood warnings to the public. IoT has also been applied to tracking of food products. Tracking food products can ensure food safety and operational efficiency for the organization (Da Xu, He, & Li, 2014). Boulos and Al-Shorbaji (2014) depicted Barcelona's smart city solution where IoT sensors are disbursed throughout the city to provide real-time information about traffic flow, weather conditions, and pollution. Such data may be used to streamline city operations, reduce costs, and improve the environment (Boulos & Al-Shorbaji, 2014). These benefits enable cities and organizations to automate tasks that would otherwise require manual labor.

IoT is also evident in the healthcare industry because of the use of medical devices that are attached to instruments. Many medical devices, sensors, and diagnostic and imaging devices are synonymous with IoT (Islam, Kwak, Kabir, Hossain, & Kwak, 2015). The demand for medical devices has led to the need for innovative technology such as IoT to meet patients' demands for healthcare (Sametinger, Rozenblit, Lysecky, & Ott, 2015). Medical sensors and wearable sensors have been linked to IoT because they enable healthcare professionals to access patient data remotely and in real-time (Li, Xu,

& Zhao, 2015). The technology may be used to improve the quality of life for many patients with a potential to save lives using remote surgery (Islam et al., 2015). The ability to perform operations across the globe is a significant change in society as patients will no longer need to travel across cities, states, or countries to get the care they need.

Organizations may consider using IoT to improve efficiency and productivity. Doctors have the need to reduce administration work and the need to filter calls for emergencies so that they can shift their focus and time on patients in need of critical care (Lu, Liu, & Guan, 2013). Many hospitals have adopted IoT to manage critical patient information in a more effective way resulting in less administrative tasks (Hwang, Kim, & Rho, 2015). IoT is used to monitor changes in patients' vital signs and provide feedback to healthcare personnel in an automated fashion so they can maintain optimal health for all patients while reducing the burden of entering patient information into the healthcare system manually (Su et al., 2013). IoT can address challenges in healthcare that would normally require people to physically attend to them. Advances in technology have enabled healthcare organizations to find value in IoT because IoT helps with automation and reduces the need for a hands-on approach.

IoT Security Issues

As technology continues to advance, the number of security vulnerabilities may continue to increase. IoT can present security vulnerabilities on the network because of the use of wireless devices reachable by adversaries (Islam et al., 2015). Wireless security issues in IoT include denial of service (DoS) attacks, forgery/middle attacks, and heterogenious network attacks (Jing, Vasilakos, Wan, Lu, & Qiu, 2014). These security

issues are not very different than the vulnerabilities in existing, less-advanced systems compared to IoT. However, IoT introduces the challenges at a larger scale because of IoT's capability of transmitting large amounts of data upon request or in an automated fashion.

Physical IoT security can include damages invoked by humans such as theft of devices, employee error, and terrorist attacks. Physical security poses a significant risk such as bad data or malfunctioning devices that may be caused by an environmental threat, employee error, or a physical attack. IoT devices spend most of the time unattended, leading to physical attacks (Atzori, Iera, & Morabito, 2010). In a survey about IoT security, Borgohain, Kumar, and Sanyal (2015) raised security vulnerabilities such as clear text login information and clear text data processing, which can result in theft of sensitive information.

The various IoT security issues are categorized into three major categories in this study to offer suggested solutions and strategies researched and implemented in other industries. The categories include communication, authentication, and access control (Roman et al., 2013). The communication category involves communication between IoT devices and the network and is arguably the most difficult of the three categories to contain (Aldosari, Snasel, & Abraham, 2016). Depending on the IoT device and the protocol it uses for communication, different security vulnerabilities may be present (Jing et al., 2014). The next category is authentication, where users access a system by identifying themselves using a user name and password (Weber, 2015). Users would only be authenticated if the system credentails are consistent with the credentials in the

directory service. Finally, access control manages users to ensure they have the appropriate authority to carry out their responsibilities (Roman et al., 2013). Access controls limit user access to systems and prevent breaches (Jing et al., 2014). Limiting user access may be the first step to address IoT security risks.

The need for a security strategy. The decision for organizations to adopt in IoT depends highly on exploring a security strategy to ensure sensitive data remains secure. Farash, Turkanovic, Kumari, and Holbl (2015) proposed the need to address several security threats including DoS, password change, user impersonation, smart card, man-in-the-middle, and several other attacks. Borgohain et al. (2015) highlighted the need for sound security measures, which include intrusion detection systems, cryptography, and stenography to counter security flaws because of the transmission of sensitive information between devices on the network. These security measures will help to address many of the existing vulnerabilities today.

In comparison to computers, IoT devices may pose greater security risks because of the number of devices transmitting data on the network. Therefore, suitable countermeasures to malicious attacks are important to prevent a data breach (Sametinger et al., 2015). A data breach is an incident involving unauthorized access to sensitive data resulting in a potential compromise of confidentiality, integrity, and availability of the affected data (Sen & Borle, 2015). Data breaches have been a popular security topic for most organizations lately because of the difficulty in containing threats. Data breach incidents are on the rise, leading to severe financial and legal implicaions for organizations affected by the incidents (Sen & Borle, 2015). Holtfreter and Harrington

(2015) referenced the data breach numbers across industries in the United States to explain the significance of the security issues. There were 2,280 reported data breaches and over 512 million compromised records between the years 2005 and 2010 (Holtfreter & Harrington, 2015). The data may explain the need for additional measures to supplement technology and ensure sensitive data remain secure.

IoT security policy. Irrespective of the technology used, organization IT leaders may limit security vulnerabilities by ensuring members of their organization understand its importance. Organizations often have a security policy, which is one way of elucidating the importance of security and the practices of the organization based on responsibility. Gadzama, Katuka, Gambo, Abali, and Usman (2014) referred to a security policy and its intent to stimulate a safe and secure environment and to ensure there is training available for employees' awareness in an effort to reduce security risks. People and technology both play a significant role in reducing security risks. Technical measures are insignificant if people provide login credentials to unauthorized people (Sametinger et al., 2015). Humans present security vulnerabilities such as end-users with limited knowledge of social engineering, poor password selection, and disgruntled employees (Jacobsson, Boldt, & Carlsson, 2015). The misuse of the credentials may not have been the intention. However, awareness of such threats enables employees to prevent such incidents.

Enforcing security at an organization begins with leadership support. Osho and Onoja (2015) presented different case studies to illustrate the importance of leadership support and education about cyber security and monitoring. Leadership support is

essential in ensuring that the organization lowers security risks because they have the authority to approve such initiatives. Sen and Borle (2015) pointed out that investing in IT security does not guarantee organizations will reduce the risk of security breaches. Gaynor, Bass, and Duepner (2015) argued that more attention must be paid towards non-technical human-related issues such as information security awareness and training. Organization IT leaders considering IoT adoption must consider a security policy to ensure a successful adoption as the policy would enforce the strategies throughout the organization.

IoT security in healthcare. IoT may eventually have a significant presence in the healthcare industry due to IoT's capability to provide patients advanced care such as real-time monitoring. However, those benefits also include security challenges. Hayhurst (2014) referred to the breaches during the year 2013 where 7.1 million patient health records were breached, which was an increase of 138% over 2012. Therefore, the impact of security issues in healthcare is signficant. A security issue can easily lead to a safety issue for patients and ultimately cause them harm as a result of erroneous information (Sametinger et al., 2015). Attackers with malicious intent can also steal devices and cause harm to patients either by identity theft or by modifying information (Atzori et al., 2010). Therefore, security standards are pivotal to protect healthcare organizations using IoT, especially as it relates to life or death situations.

The healthcare industry has potential to benefit the most from IoT, but appropriate measures must be implemented to protect patient information. Gaynor et al. (2015) posited standards in healthcare are used to safeguard patients' information against

security threats. One of those standards includes the health insurance portability and accountability act (HIPAA), which is intended to protect the integrity of patient data and ensure the data remains confidential (Sametinger et al., 2015). However, additional measures are necessary as those standards may not be enough to address the different types of threats. Gaynor et al. (2015) argued HIPAA is too vague and does not specify how sensitive information should be protected. Hayhurst (2014) referred to the need for organizational policies and procedures to address security vulnerabilities. A security policy can have specfic standards such as data encryption, access controls, authentication and other controls to limit security threats from inside and outside the organization (Hayhurst, 2014). Therefore, healthcare organizations that consider IoT adoption should include a security strategy prior to implementation to ensure a successful adoption.

IoT Privacy Issues

Privacy is another factor organizations consider when deciding to adopt IoT. Weber (2015) described privacy as the concealment of personal information complemented with the treatment of the data. The advent of sensor-rich devices such as IoT has made privacy difficult to control because of the volume and speed of the information shared at organizations (Weinberg, Milne, Andonova, & Hajjat, 2015). Privacy challenges exist because of malware, theft, and lack of awareness and training in keeping information confidential (Roman et al., 2013). Private information about a person can be collected without the person being aware (Atzori et al., 2010). Organization leaders are hesitant in adopting IoT because they lack the knowledge

necessary to address such vulnerabilities. Before searching for a solution, it is important to first gain a better understanding of the vulnerabilities.

IoT privacy may have multiple consequences due to the availability of sensitive data on devices and networks. Cyber criminals primarily use malware to gain access to unauthorized data, leading to information alteration or destruction (Sbora, 2014). Methods of malware include viruses, worms, trojan horses and spyware (Osho & Onoja, 2015). Advances in technology has led to additional and more complex techniques of cyber criminal activity including hacking, social engineering, identity theft and forgery (Osho & Onoja, 2015). IoT is a primary example of advanced technology where adversaries may obtain access to unauthorized data. Furthermore, unattended IoT devices are vulnerable as they may be physically stolen or manipulated such that the data is altered (Atzori et al., 2010). Each vulnerability is a potential threat to privacy and without proper awareness at an organization level there is risk of exacerbating the vulnerabilities and may ultimately lead to a privacy breach.

Organization training about IoT privacy may help reduce human error and promote awareness throughout the company. Most users are not aware of the proper security methods to protect sensitive information (Heffetz & Ligett, 2014). Wikina (2015) stated that 85% of security breaches occur off-network. Mishandling of data by employees poses vulnerabilities for organizations and can potentially lead to breaches. In 2013, 83% of the patient health record breaches resulted from theft of unencrypted laptops (Hayhurst, 2014). Organizations are unable to quantify the return on investment on employee training as a method to prevent a privacy breach (Caldwell, 2016).

Therefore, organization leaders will find it difficult to invest in employee training without sufficient data to prove training will help reduce IoT privacy risks.

Despite the privacy concerns, organizations have a need to share data prodigiously, which is the reason for investing in advanced technology such as IoT (Roman et al., 2013). In the car manufacturing industry, organizations would like to share information to facilitate production of cars (Reddy, 2014). Brody and Pureswaran (2015) suggested that the farming industry will gain value from IoT in ways that is nonexistent currently as IoT will enable collaboration between farmers, biotechnology companies, farm equipment manufacturers and capital providers to make farmers more productive. Real-time information allows decision makers to make informed decisions and speed up operations (Zhang et al., 2015). Protecting privacy is often counter-productive for some organizations since the data generated by IoT is intended to improve processes and reduce operational costs (Lee & Lee, 2015). The advantages of real-time information may lead organization leaders to reconsider privacy as a top priority depending on the information being shared. Therefore, organization leaders may develop a stategy to balance the organization's needs with IoT privacy solutions when considering IoT adoption.

The need for a privacy strategy. As with security, organization leaders must address privacy challenges with a strategy to reduce the complexity of IoT. Low complexity enables organizations to make the integration between systems easier and propel a successful adoption (MacLennan & Belle, 2014). Therefore, complexity requires a balance between the needs and open privacy challenges for organizations to consider

adopting of IoT. New technology carries opportunities that have an organizational, social and cultural impact which is the reason for the difficulty in creating a single rule or law to address all the privacy issues (Weber, 2015). An IoT strategy is necessary to address many of the privacy challenges within the infrastructure to meet the organization's standard confidentiality requirements.

Organization IT leaders must consider embedded processes within the organization infrastructure to accommodate for IoT's privacy vulnerabilities. Atzori et al. (2010) explained that control of the diffusion of information is impossible to manage using existing techniques. A privacy strategy to address data in transit and data at rest must be established to ensure appropriate control of sensitive data while ensuring confidentiality. Gubbi, Buyya, Marusic, and Palaniswami (2013) suggested the use of encryption to ensure the sensitive data from IoT remains confidential from attackers outside of the organization. Prevention of attackers from inside the organization may be addressed using authorization techniques to prevent unauthorized users from accessing IoT data (Jing et al., 2014). Furthermore, physical security techniques such as tamper-resistant packaging and secure routing of networks is necessary to ensure confidentiality for unattended IoT devices and from real-time data access (Islam et al., 2015). To ensure such strategies are realized by employees, the inclusion of the techniques may be included in a privacy policy.

IoT privacy policy. As with security issues, organizations are concerned about IoT privacy issues. One way to address the privacy issues is to have a policy in which employees follow the guidelines. The first step may be to include the IoT privacy

guidelines in training to ensure employees understand the importance of sensitive data and the ramifications if the guidelines are not obeyed. Organizations need to train employees on basic privacy procedures to recognize deceptive techniques used by fraudsters and identity thieves, such as social engineering (Wikina, 2015). Organizations must put more focus on training individuals on IoT to improve awareness of potential vulnerabilities (Gaynor et al., 2015). Therefore, organization leaders may deem it necessary to include annual IoT privacy training for all employees as a reminder of the importance of keeping data confidential. Access controls and authorization exist to manage confidentiality (Miorandi et al., 2012). Such controls are intended to prevent unauthorized access by internal employees, external vendors and partners outside of the organization to ensure trust exists between parties to effectively manage day to day operations.

A data breach may damage an IoT organization's image because it would lead consumers to think that their personal information leaked. Data privacy preservation is an important aspect of achieving trust in IoT (Yan, Zhang, & Vasilakos, 2014). IoT has immense potential, but there is a risk of privacy loss due to the integration between systems (Borgohain et al., 2015). IoT privacy is a concern for personally identifiable information (PII) and organizations' proprietary information (Miorandi et al., 2012). The loss of privacy can be an advantage for competitors if they knew the organization is struggling in a particular market. Open access to confidential information may expose an organization's financial data (Borgohain et al., 2015). Jacobsson et al. (2015) referred to the issue of personal information leaking by describing smart homes and the sensitive

devices that contain private information such a surveillance camera or personal wearable devices. The same issues exist in healthcare where patients are using IoT devices to monitor their glucose levels or blood pressure levels, so the privacy challenges exist across industries.

Organizations may consider including privacy solutions as part of a security policy because both security and privacy challenges may be addressed by using similar techniques. Organizations that adopt IoT devices must ensure their teams are aware of both security and privacy issues so that the devices are designed to limit vulnerabilities for IoT consumers (Jacobsson et al., 2015). On the other hand, some organizations may not have as much of a concern regarding privacy challenges because of their industry. Organizations in the social media industry may approach privacy differently than a healthcare organization (Xu & Bélanger, 2013). What may be a privacy concern in healthcare may be a very different problem in some other industries such as social media. For that reason it is imperitive for organizations that are considerig IoT adoption to balance the privacy challenges and possible solutions to the challenges with the benefits IoT presents prior to making the decision to adopt it. In the end, it is up to the organization to decide whether they believe the value of IoT devices is worth the risk.

IoT privacy in healthcare. Many healthcare organizations would like to see improvement of IoT privacy issues before considering IoT adoption. Lee and Lee (2015) argued that challenges with IoT in healthcare include a user's location, health conditions, and purchase preferences because the service providers feel the protection of privacy is counter-productive since the goal of IoT is to improve the quality of life while decreasing

the service provider's operating costs. As a result, service providers defer to IoT users preferences to determine whether users want to use a device that enhances their lives, albeit with the privacy challenges, or live without the use of IoT devices and the concerns surrounding IoT privacy. For example, medical patients may risk their privacy by opting into a remote monitoring system located in their home to prevent adverse health events from escalating to emergency room visits (Lee & Lee, 2015). In critical cases where a patient's life is affected, privacy may be overlooked to save the patient's life. However, if the organization has an opportunity to keep patient data confidential, they are obligated to do so.

In most cases, healthcare organizations are required to protect IoT data due to regulations. Regulations such as HIPAA affect data collection and the privacy of the data (Weber, 2015). Rosenbaum (2014) indicated HIPAA regulations require healthcare organizations to de-identify or anonymize patient data that is shared publicly. HIPAA is one method healthcare organizations must factor into a privacy policy. Healthcare organizations that fail to follow regulations will be fined and the incident may lead to a bad reputation (Johnson, 2014). As organizations look to adopt IoT, they must first consider such regulations in their IoT privacy policy to ensure rules and regulations are not overlooked when IoT is adopted. The regulations exist to protect patient privacy, but also serve as a reminder for healthcare organizations to address privacy issues when new services are offered.

IoT Reliability Issues

Organizations may argue that reliability in communication between devices is the most important factor for IoT adoption. Organizations use reliability to measure the availability of a system (Lopez, 2013). Reliability is considered a combination of two qualities: accuracy and precision (Cafiero, Melgar-Quiñonez, Ballard, & Kepple, 2014). Accuracy refers to the limit of systematic errors, while precision addresses the limit of accidental errors (Cafiero et al., 2014). The goal for reliability of critical systems is 99.99% availability (Drtil, 2013). However, IoT devices operate on several layers that dependent on each other, which makes it difficult to keep systems highly available. Reliability in IoT is based on the device, the software applications used to attach to other systems and the ability to connect to the Internet or other devices (Borges Neto, Silva, Martins Assunção, Mini, & Loureiro, 2015). Issues regarding the reliability of IoT are affected by the device hardware, software, network, power of devices, and range of the devices (Lopez, 2013). IoT reliability issues may vary depending on the type of connectivity such as RFID, WiFi, ZigBee and others (Islam et al., 2015). Organizations considering IoT adoption must realize there is always a chance for a reliability issue at any given time (Atzori et al., 2010). Therefore, they must be realistic and account for potential reliability issues.

Reliability of systems is important for most IoT consumers because they want to the technology to work when they need to use it. There are multiple factors in systems reliability. Availability is one of the most important factors. Availability refers to the percentage of time a given system is available for use in the way designers built the

system (Lopez, 2013). Organizations would like to have 100% availability in IoT systems, but that is not realistic mainly because of the maintenance required in those systems (Lopez, 2013). Organizations offer availability of services ranging from 90% to 99.9% (Drtil, 2013). Some organizations may offer 99.999% availability, which means the system or service will be unavailable for only five minutes during the entire year. However, not many organizations can guarantee that much uptime. Other than maintenance, several other factors or incidents can affect availability including hardware failure, power outage, computer virus, SPAM, WAN failure, LAN failure and software failure (Drtil, 2013). Thus, organizations must have a contingency plan to address such incidents.

Performance is another reliability factor organizations believe to be one of the most important aspects of real-time devices. Roman et al. (2013) explained that IoT architecture must assure a certain level of availability and performance to be considered a solution for consumers. The communication network is one important factor to consider when looking to improve IoT performance. There is a possibility for the network to be congested due to the volume of data (Atzori et al., 2010). The addition of IoT devices can cause network congestion and may lead to latency issues (Gubbi et al., 2013). Therefore, organizations may organize a strategy to ensure IoT network performance is acceptable and reliability issues are addressed.

The need for a reliability strategy. Reliability may be an afterthought for organizations considering a new innovation such as IoT. Typically, IoT device manufacturers do not focus primarily on reliability (Peppet, 2014). However, reliability is

necessary for most organizations to benefit from IoT (Jing et al., 2014). Thus, a strategy is necessary for organizations to address reliability, particularly high availability and performance (Roman et al., 2013). High availability is one way to address availability issues for systems that require significant availability (Franke, Johnson, & König, 2014). IoT is no exception because many consumers would expect IoT to be a fault tolerant system. One way to achieve high availability is to eliminate single point failures and add redundancy to the system so that if there was a hardware failure, the backup hardware would take requests (Lopez, 2013). The drawback for IoT is the use of single hardware user devices. There are often situations where the consumer uses a single IoT device to transmit data, hence creating a single point of failure (Roman et al., 2013). However, IoT devices communicate with the middleware servers which can be configured for high availability (Kanso, Toeroe, & Khendek, 2014). The middleware servers contain the data captured by the IoT devices and will retain the information in the event the device is damaged (Franke et al., 2014). Therefore, high availability is a method organizations may consider utilizing when constructing a strategy.

Network performance is another important issue to address in a reliability strategy. Reducing complexity on the network is important because it will improve processing efficiency and ensure higher availability (Patil, Mihovska, & Prasad, 2014). Meanwhile, reducing complexity also will also help to prevent data loss because of the downtime it poses for IoT device consumers (Patil et al. 2014). Organizations may prevent performance issues on the network by scaling IoT devices and the network as a method to prevent congestion (Atzori et al., 2010). Limiting devices on each network

segment will reduce the complexity of the network and limit potential latency issues (Gubbi et al., 2013). In addition, software design is another method organizations may use to improve reliability on the network (Wan, Zou, Zhou, Lu, & Li, 2014). Chatterjee and Shukla (2016) described the importance of testing and uncovering the faults to improve the quality and reliability of the software. Although network performance may be a non-functional requirement, it is still an important part of the IoT ecosystem as it will help to reduce reliabilty risks (Jacobsson et al., 2015). Thus, a remediation plan is necessary to recover from network performance issues.

IoT reliability policy. Organizations IT leaders may consider creating a reliability policy before adopting IoT at their organization. Reliability is an important part of an organization's trust in a product because it is a direct reflection of the quality of the product (Corredor, Metola, Bernardos, Tarrío, & Casar, 2014). Availability and performance are two metrics organizations may use to measure reliability. Organization IT leaders would like to see a resilient IoT architecture to ensure a certain level of availability and performance (Roman et al., 2013). Organization IT leaders may determine a minimum level of reliability required based on the applications supported. For instance, the retail industry uses IoT primarily to predict consumer behavior and trends while the healthcare industry uses IoT for real-time monitoring of patients (Reddy, 2014). Between the two industries, leaders from a healthcare organization may have a higher reliability expectation than an organization in the retail industry due to the circumstances and urgency of keeping IoT systems available with acceptable performance for continuous patient monitoring. Guaranteeing a minimum level of

reliability is very difficult (Corredor et al., 2014). Organization IT leaders may consider creating an IoT reliability policy with minimal levels of availability and performance measures to illustrate worst case scenarios. The measures will help organization IT leaders determine whether they will accept such minimal performance for IoT applications.

Software reliability may be improved by developing efficient test cases (Chatterjee & Shukla, 2016). The goal of test cases is to find faults in the system, especially for organizations that use IoT in critical situations requiring high availability and low latency. Some test cases may be used to uncover faults while others may be used to add a sufficient load to validate the scalability and latency of the IoT infrastructure (Kyriazis & Varvarigou, 2013). Valid test cases would ensure production use cases are reproduced in a non-production environment (Cleveland & Ellis, 2014). Test cases may help organizations be proactive by addressing IoT issues before they are reported in production. Moreover, additional test cases may enhance test coverage and offer greater confidence in IoT reliability (Chatterjee & Shukla, 2016). Therefore, organization IT leaders may consider improving the chances of high availability and reduce latency to ensure a positive experience by including testing in the reliability policy.

IoT reliability in healthcare. Organizations in the healthcare industry may be hesitant to adopt IoT as early adopters due to reliability concerns. For critical systems, such as those in healthcare, IoT devices require a higher level of reliability (Islam et al., 2015). The healthcare industry currently does not have high reliability in many IoT systems because of the variation of adverse events where those systems may fail, hence

making the issues difficult to reproduce (Chassin & Loeb, 2013). Unreliable IoT devices might lead to mistakes or loss of data (Yuanfang et al., 2016). In healthcare, those faults may lead to unrecoverable circumstances such as patient deaths (Wan et al., 2014). Healthcare organization IT leaders may create an IoT strategy to ensure the system is highly available when doctors and patients need it most (Li, Sun, Bi, Su, & Wang, 2014). Chassin and Loeb (2013) suggested healthcare organizations may attain high reliability by collectively working together to report small problems or unsafe conditions before they are a substantial risk. High reliability may be achieved with the use of organization policy, processes, and procedures (Patil et al., 2014). The healthcare industry can make substantial progress toward high reliability using the strategies outlined in this study.

The characteristics of the DOI theory was used as a framework in this study to explore security, privacy, and reliability stragies for IoT adoption. Organizations may consider a balanced solution between security, privacy, and reliability issues with the least amount of complexity to gain a relative advantage over their competitors (Knebel, Leimeister, & Krcmar, 2006). Organizations interested in IoT must observe their usage of existing technology and combine it with IoT to ensure there is compatibility between systems (Islam et al., 2015). Understanding consumer needs and applying the DOI characteristics to security, privacy, and reliability strategies used by organization IT leaders to adopt IoT devices may enable the organization an opportunity to be successful in the adoption. Research is necessary to address areas of security, privacy, and reliability until there is a single standard in which all organizations can utilize (Greene, 2015). An organization willing to consider adoption of IoT devices may leverage testing as a major

part of their strategy to ensure IoT adoption is successful (Girtelschmid, Steinbauer, Kumar, Fensel, & Kotsis, 2014). However, additional strategies may be required to assemble a solution for IoT adoption.

The DOI theory supported this research by exploring strategies using the characteristics exhibited by organizations that adopted innovative technology. The five characteristics from the DOI theory (Rogers, 1962) were used to explore security, privacy, and reliability strategies for IoT adoption. The strategies identified from this study may equip healthcare organization IT leaders with knowledge and insight to adopt IoT.

Diffusion of Innovations: Five Characteristics

Diffusion of Innovations Theory

Rogers (1962) defined the DOI theory as the process by which adopters communicate the innovation over time with members of society. The innovation may be a new event, process, technology or object that is planned to be utilized by the adopters (De Massis & Kotlar, 2014). Rogers (1962) employed five characteristics in the DOI theory that contribute to an innovation's rate of adoption. The characteristics and their definitions include: (a) relative advantage (the perception that the innovation is more beneficial than the current practice); (b) complexity (the innovation's ease of use); (c) compatibility (the degree to which the innovation aligns with the existing cultural values and norms of those who adopt it); (d) trialability (the possibility of experimenting with the innovation for a limited time); and (e) observability (the degree to which the results of the innovation is visible by others) (Rogers, 1962).

The motivation for IoT adoption may vary from one organization to another. MacLennan and Belle (2014) explained that organizations often have technological and external requirements that are decisive factors when considering IoT adoption. Technology requirements refer to the technology and information systems available to the organization (MacLennan & Belle, 2014). External requirements refer the environment to which the organization operates including market conditions, regulatory influence, industry pressure and competitiveness with other vendors (Li, Zhao, & Yu, 2015). During this study, I used the five characteristics of the DOI theory to align the technological and external factors with organization goals to address the knowledge gap in developing IoT security, privacy, and reliability strategies. Thus, the knowledge from this research will equip organization IT leaders with information to consider for IoT adoption.

While conducting this study, I utilized the the five characteristics of the DOI theory, which consists of compatibility, relative advantage, trialability, observability, and complexity (Rogers, 1962). The five characteristics were instrumental to this study because they were used to explore the security, privacy, and reliability strategies to adopt IoT. During this study, I examined each DOI characteristic with security, privacy, and reliability to present a perspective for organization IT leaders to ruminate when considering IoT adoption. The exploration also built knowledge for organization IT leaders to evaluate aspects of IoT adoption they may not have considered. The results of the review will instill confidence in organization leaders to make an educated decision regarding IoT adoption based on examples and use cases presented from prior research.

Compatibility

The DOI theory defines compatibility as a measure of consistency between existing values, past experiences, and requirements (Rogers, 1962). Existing values describe the norms, strategies, goals or best practices of the potential organization that is considering adopting the innovation (McMullen et al., 2015). An example of existing values may include a skill the organization employees embody, which would be sustained with the adoption of the innovation (Sung & Choi, 2014). Past experiences refers to the accumulation of the potential adopter's past experiences with innovations (Rogers, 1962). If the past experiences are positive, the organization considering the adoption would be optimistic. However, if the past experiences were negative, the organization would be apprehensive about the adoption. Finally, requirements refer to the needs of the organization that is considering the adoption of the new technology (Gluhak et al., 2011). Thus, organization IT leaders must consider compatibility as an important characteristic for IoT adoption.

Compatibility is a significant DOI characteristic when adopting IoT devices because it affects the functional requirements and is instrumental in security, privacy, and reliability strategies to enable the adoption of IoT devices. Yung-Ming (2015) described compatibility as the extent to which the innovation is perceived to be consistent with the adopters' beliefs, values, and needs. Compatibility plays a significant role for consumers because the goal for any adoption is to limit the interface changes, so end users do not have to worry about training.

Compatibility between systems and applications remain a critical aspect of adopting IoT devices. MacLennan and Belle (2014) conducted a study and confirmed the positive relationship between compatibility for users and project success in organizational adoption of service-oriented architecture. IoT backward compatibility and flexibility is required during adoption to ensure a seamless transition from the previous technology (Islam et al., 2015). IoT would introduce the integration of multiple heterogeneous networks requiring new security, privacy, and reliability standards (Jing et al., 2014). Therefore, the consistency in the existing and new communication channels are imperative to ensure successful adoption (Miorandi et al., 2012). As professionals introduce new security, privacy, and reliability standards for IoT, compatibility will become increasingly important.

Compatibility and IoT security. The compatibility component of DOI is used to apply existing values, past experiences and requirements during the adoption of an innovation (Rogers, 1962). Olsson, Skovdahl, and Engström (2014) studied DOI to explain participants' experiences using passive positioning alarm (PPA), illustrating that there is a greater possibility that the innovation would be adopted if it was compatible with existing values. In the same manner, compatibility and IoT security are important to organization IT leaders because they must consider how to best position IoT into their organization's infrastructure.

Consumers must secure IoT in three layers including the physical perception layer, transportation layer, and application layer (Jing et al., 2014). As a result, each layer may require different security mechanisms to ensure the data and communication remain

secure. Compatibility and IoT security are also important for organization IT employees because the technology must correspond to their skills. Safari, Safari, and Hasanzadeh (2015) referred to a study where the skills of IT resources were an influential factor in the adoption of software as a service (SaaS). Organizations often consider the employees' technical knowledge and skills prior to adopting a new technology (Lai, Lin, & Tseng, 2014). Compatibility of IoT security skills are imperative for employees, especially since security is a top concern for most organizations.

Compatibility and IoT privacy. Compatibility is a characteristic in the DOI theory that is used to gauge potential adopters' beliefs and preferences based on existing values (Rogers, 1962). Al-Jabri and Sohail (2012) conducted a study about mobile banking adoption in Saudi Arabia and found that compatibility was the most significant determinant to predict mobile banking adoption by using customer preferences. The researchers concluded that users valued the innovation, but were concerned about the privacy issues and cyber attack vulnerabilities the innovation presented (Al-Jabri & Sohail, 2012). User privacy and personal information should be preserved based on the policy and agreement of users for organizations to remain compliant (Yan et al., 2014). The compatibility between IoT and privacy standards must be aligned at each layer of the architecture including the device, application, network and database for organizations to adopt the innovation (Boos et al., 2013). However, regulated IoT privacy standards have not been defined for IoT devices (Maras, 2015). Weber (2015) conducted an IoT privacy study and revealed that new safeguards for privacy must be created due to the growth in

information technology. Compatibility between systems and applications remain a critical aspect of adopting IoT devices.

Compatibility and IoT reliability. Compatibility is a DOI characteristic that may be used to compare past experiences and values with the adoption of a new innovation (Rogers, 1962). Gu, Schniederjans, and Cao (2015) completed a study about customer relationship management adoption in supply chain organizations and used the compatibility characteristic to illustrate that system availability is a critical aspect of software diffusion. The researchers' study findings are similar to IoT reliability because organizations must ensure reliability standards are compliant for systems to be available (Sanchez et al., 2014). Griggs (2014) used the IEEE 802.11a/b/g/n standards as an example to illustrate the dependency devices such as smartphones, laptops, IP cameras, sensors and others have on such standards to maintain high availability. However, if the systems are incompatible with the standards, the reliability of those systems may become unpredictable (Islam et al., 2015). Li et al. (2014) referred to a study about healthcare professionals and their reliance on IoT-based Emergency Response Systems (ERS) since their decision is based on the information generated by ERS. The impact of IoT reliability standards is essential in systems such as an ERS and would require compatibility to be an emphasis for organizations considering IoT adoption.

Relative Advantage

Relative advantage is another characteristic in the DOI theory. Relative advantage underlines an innovation's benefits such that it supersedes the existing technology (Rogers, 1962). Rogers (1962) explained that the innovation's relative advantage may be

measured in economic terms, but other factors that may be advantageous to the organization will lead to a more rapid rate of adoption. Organizations must consistently provide value to their customers to stay ahead of the competition. McMullen et al. (2015) referred to relative advantage as an effective concept that provides value for an organization such as process improvement or cost effectiveness. For example, banks must reduce the risks perceived by customers by offering guarantees to protect them from security and privacy vulnerabilities (Al-Jabri & Sohail, 2012). As a result of reducing the risks, the incentives of mobile banking would improve the rate of adoption since the innovation would provide a relative advantage for users. When IT leaders consider adoption, they often do not want to put the business at risk by making a drastic change to the IT solution. However, competing organizations will look to find a relative advantage through innovation.

Relative advantage is a significant DOI characteristic for organization IT leaders considering the adoption of IoT. Olsson et al. (2014) described relative advantage as an added benefit or improvement upon the existing technology by adopting an innovation. Organizations considering IoT adoption look to IoT as a new way to solve problems that pre-existing technologies may not have addressed (Ahsan et al., 2016). For example, IoT's advantages include sensing how one drives a car, monitors their home appliances, controls the energy in their homes, and manages heartbeat and glucose levels (Peppet, 2014). IoT adoption in hospitals is another example of innovative technology superseding benefits of existing technology (Lai, Lin, & Tseng, 2014). According to Lai et al. (2014), RFID enables hospitals to collect data automatically and help to track assets and people.

Therefore, relative advantage is a factor that may be used to promote innovative technology, especially for organizations considering IoT adoption.

Rogers (1962) indicated that relative advantage is often the most significant DOI characteristic influencing adoption. Al-Jabri and Sohail (2012) applied DOI's relative advantage characteristic in the context of mobile banking as it provided benefits such as immediacy, convenience and affordability to customers. In a study about factors that influence telecare adoption, Sugarhood et al. (2014) used relative advantage to describe advantages of telecare, which included improved quality of life for patients, cost and efficiency savings for health providers, and peace of mind for the user and their family. However, Rogers (1962) also noted that the perceived attributes of the innovation determine the relative advantages and disadvantages of the innovation to the potential adopter. Al-Jabri and Sohail (2012) shared issues from the mobile banking study, including security and privacy risks. Likewise, Sugarhood et al. (2014) described reliability issues and risks in the telecare study since the devices used GPS technology and depended on a satellite signal. Similar risks surface in many innovations, especially IoT.

Although IoT offers relative advantage to organizations across multiple industries, organization IT leaders have doubts about IoT adoption because of IoT security, privacy, and reliability vulnerabilities. Yun et al. (2016) conducted an IoT study about programming smart spaces based on IoT systems and concluded IoT security is a big concern for building smart spaces because there is opportunity for malicious hackers to record sensitive data. In an IoT study about collaborative sensing intelligence framework,

Yuanfang et al. (2016) posited that privacy issues exist in the IoT framework and adversaries may gain access to sensitive data without a sufficient authorization model. Gonnot et al. (2015) conducted a study about home automation using IoT and noted IoT reliability issues such as a resource-intensive protocol that is unreliable for home automation. The experiences from these studies may assist organization IT leaders develop strategies that are necessary to address or reduce IoT security, privacy, and reliability challenges such that relative advantage benefits may be realized with limited concerns or disadvantages.

Relative advantage and IoT security. The relative advantage component of DOI is used for economic profitability, social value, or to gain a competitive advantage by using an innovation (Rogers, 1962). Kohles, Bligh, and Carsten (2013) used the DOI's relative advantage characteristic to describe an innovative perspective where employees were asked to develop the organization's vision. Employees were encouraged to contribute to the organization's vision to gain a relative advantage over communication and decisions that would typically rely on formal leaders (Kohles et al., 2013). Solutions to IoT security present an opportunity for organizations to have a relative advantage over their competitors (Borgia, 2014). Lee and Lee (2015) concluded that the IoT innovation cycle has insufficient security standards. Li, Xu, and Zhao (2015) conducted a quantitative study about IoT where survey participants indicated that security is often the most demanding requirement for potential IoT adopters and that a solution for IoT security would add considerable value for organizations considering IoT adoption. Jacobsson et al. (2015) highlighted the importance of a properly formulated security

policy by addressing security at the system, network and application layers. An organization's security policy creates a safe and secure working environment while ensuring stability, confidence, and competitiveness over other organizations (Gadzama et al., 2014).

Relative advantage and IoT privacy. Relative advantage is a DOI characteristic applied by organizations to improve operational efficiency by using an innovation (Rogers, 1962). Cobban, Edgington and Clovis (2008) conducted a study to improve processes at dental hygiene practices by aligning roles and responsibilities to grant dental hygienists a relative advantage as it enabled the practice to operate more effeciently. IoT is an innovation that may offer improved productivity for potential adopters, however limited solutions in IoT privacy prevent organizations from its adoption (Atzori et al., 2010). An IoT privacy policy is necessary to protect sensitive data to ensure organizations see the value in IoT adoption (Yan et al., 2014). A recent study by Basanta, Huang, and Lee (2016) about healthcare services for elderly citizens indicated the benefits of IoT and its effectiveness in providing value to elderly patients, but emphasized that the lack of privacy standards in IoT is still a concern since sensitive data about patients are available on the Internet. Addressing privacy is an important regulatory initiative and the best solution is to invest in systems that support the organization's processes, practices, and technical design (Mulligan & Bamberger, 2013).

Relative advantage and IoT reliability. Relative advantage is a DOI characteristic that may be used to describe the rate of adoption based on an innovation's economic value (Rogers, 1962). Chen (2013) conducted a study where the adoption of

mobile banking services provided users with relative advantage due to the reliable access to banking information and the convenience of using a banking application. The adoption also reduced the time and location constraints for users and provided a return on investment for the bank due to improved service performance and service efficiency (Chen, 2013). Likewise, potential IoT adopters may benefit from a return on investment by using a cloud service provider to help keep systems highly available (Bąk et al., 2015). High availability is an important concept for IoT, especially for critical systems such as those in healthcare that rely on timely information (Gubbi et al., 2013). A study conducted by Bąk et al. (2015) described the importance of IoT reliability in a client-server architecture where embedded systems act as smart clients and the Internet application as a server of the system. The study revealed that organizations often use IoT applications as real-time systems with wireless capabilities and require high availability for organizations to realize the benefits of the innovation (Bąk et al., 2015). Therefore, IoT reliability standards are important for organizations considering IoT adoption as standards will ensure availability, sufficient performance, and will enable the organization to gain a relative advantage.

Trialability

Trialability is another characteristic in the DOI theory. Trialability refers to the extent to which the innovation can be experimented on a limited basis to test its qualities prior to adoption (Rogers, 1962). Trials are evident in the software industry as consumers may install the software called trialware for a limited time to learn about the functionality and may eventually purchase it if they determine it is useful (Li & Cheng, 2014).

Likewise, trials exist in the healthcare industry where drugs are administered for patients to experiment and determine if it will heal the patient's health problem (National Cancer Institute, 2016). Trialability is important because it helps potential adopters preview the innovation prior to adoption. Windsor et al. (2013) applied DOI's trialability characteristic in a study about smoking cessation to determine the benefits of the treatment in the program. Windsor et al. (2013) concluded experimentation helped to determine the innovative treatment had clear advantages over other interventions. In another study, Hayes, Eljiz, Dadich, Fitzgerald, and Sloan (2015) used DOI's trialability characteristic to experiment with computer simulations to improve patient-flow at a hospital. Hayes et al. (2015) found that computer simulation enabled the staff to visualize process changes and accelerated the adoption of the process changes.

Trialability may play a significant role in adopting a new technology such as IoT. IoT may result in changes to an organization's infrastructure, especially if the current systems are incompatible with IoT (Boos et al., 2013). Organizations may be reluctant to adopt innovative technology such as IoT because they cannot afford to disrupt the business or because of strict governance standards (Islam et al., 2015). Organizations that have the option to experiment with the technology before they adopt it may see the benefits and risks in advance. Studies have shown that trialability reduces uncertainty about an innovation's adoption (Wang, 2014). In a study about cloud computing adoption by SMEs, adopters claimed that trialability affected their decision positively because it enabled them to experiment with the technology in advance and reduce risks prior to adoption (Alshamaila et al., 2013). Reducing risk is an important asset for most

organizations (Boos et al., 2013), so trialability may become increasingly important for organization IT leaders considering IoT adoption.

The leap to IoT presents many challenges due to many dependencies such as security, privacy, reliability, and other dependencies that are specific to each industry. For that reason, trialability presents an opportunity for organizations to experiment and test the technology to ensure their business can benefit from the technology prior to adoption (Dash, Bhusan, & Samal, 2014). The ability to experiment with IoT security, reliability, and privacy issues may reduce the risk of organization IT leaders when considering IoT adoption. A DOI study about the adoption rate of e-journal publishing by Sanni et al. (2013) described the importance of trialability as it may prevent risks due to previous exposure to the innovation. The authors explained that trialability was a significant factor in the study because publishers with experience submitting papers to e-journals were more likely to adopt e-journals than publishers without experience. Therefore, the correlation between prior experience and likelihood for future adoption is positive (Sanni et al., 2013). The study by Hayes et al. (2015) coincided with the idea that potential adopters would feel more comfortable knowing they have experimented with the innovation, hence preventing the hospital staff from making mistakes. Organizations may consider experimenting with IoT security, privacy, and reliability prior adoption to learn and plan for the features and risks that come with the innovation (Reddy, 2014). Planning for the features and risks would enable organizations to see how the technology benefits their organization in a manner that adheres to their specific processes (Fang et al., 2015). Organizations considering IoT adoption may value the innovation, however,

the value will be appreciated after the adoption when IoT is integrated with systems in the organization's infrastructure (Atzori et al., 2010).

Trialability and IoT security. Trialability is a DOI characteristic that refers to the capacity to experiment with the innovation for a limited time prior to adoption (Rogers, 1962). In an empirical study on free trials, Lee and Tan (2013) explained the importance of trialability for software consumers as freeware and trialware enabled consumers to preview innovative software to ensure it meets their requirements prior to their purchase. IoT security has a range of challenges and would require experimentation at different layers of infrastructure security including the application layer, a network layer and a physical perception layer to provide a solution (Aldosari et al., 2016). Evaluating IoT security will enable organizations to be proactive by limiting security vulnerabilities during examination of features and limitations (Kim et al, 2015). Xia, Yang, Wang, and Vinel (2012) synthesized literature and found that trialability of IoT security was a frequent requirement for organizations since they were unable to evaluate IoT solutions within their infrastructure prior to adoption. Organizations are reluctant to build an IoT infrastructure because of the associated costs and the potential of presenting vulnerabilities to exisiting systems (Kim et al, 2015). Consequently, organization IT leaders must consider other possibilities where trialability is an option for IoT security to position the organization for IoT adoption.

Trialability and IoT privacy. Trialability refers to the increase in the rate of an innovation's adoption by evaluating it prior to its implementation (McMullen et al., 2015). Chung and Holdsworth (2012) utilized the DOI theory in a quantitative study by

surveying 530 participants from Kazakhstan, Morocco, and Singapore and indicated that the Y Generation participants were concerned about privacy violations with mobile commerce and suggested that mobile service providers should consider trials and permission-based mobile marketing to instill trust in mobile commerce. Similarly, evaluating new privacy mechanisms for IoT may directly influence the rate of adoption since traditional methods are impractical (Swan, 2012). Trialability would enable organizations to evaluate IoT and prevent privacy challenges such as counterfeiting (Zhang, Zou, & Liu, 2011). A quantitative study was conducted by Alkhater, Wills, and Walters (2015) about factors affecting an organization's decision to adopt IoT revealed that privacy and trialability were influential factors for adoption as cloud computing would enable organizations to experiment with IoT privacy since the cloud service provider would manage the infrastructure. As studies suggest, trialability and IoT privacy play an important role as experimentation and evaluation of IoT privacy may increase the rate of IoT adoption at organizations.

Trialability and IoT reliability. Trialability is a DOI characteristic that denotes the likelihood for an innovation's potential adoption after it is evaluated (Chen, 2013). A qualitative case study conducted by Jwaifell and Gasaymeh (2013) concluded that trialability was instrumental in the English language teachers' adoption of interactive whiteboards in the Modern Systems School in Jordan because teachers attended workshops where interactive whiteboards were presented to enable teachers to learn and experiment with the tool while ensure consistency, stability and accuracy of the tool. In the same manner, Gluhak et al. (2011) suggested that trialability of IoT devices is

necessary as it allows for an understanding of reliability limitations such as a lack of availability. Trialability for IoT is important because testing of sensor devices would enable companies to address the challenge of having a single point of failure (Girtelschmid et al., 2014). Knebel et al. (2006) conducted a study about the strategic importance of IoT and the need for decision makers to gain perspective on the innovation by suggesting a pilot project for companies as the pilots would aid professionals to experience the reliability limitations of IoT, including lack of availability, stability, and performance. Pilots have proven to be useful as it enables companies to test the feasibility, use, and value of IoT to ensure it is a reliable innovation for the business before commiting to its adoption (Andersson & Mattsson, 2015). Pilots may also provide organizations an opportunity to test IoT reliability within their infrastructure to ensure it meets or exceeds their minimum reliability requirements.

Observability

The next characteristic in the DOI theory is observability. Rogers (1962) explained that observability is the process of making the innovation visible by discussing it or observing its results with stakeholders. Observability is a key factor in the adoption of innovation because the innovation's perception is positively related to the rate of adoption (Rogers, 1962). Observability enables an opportunity to promote the innovation to stakeholders that may decide to adopt it. Al-Jabri and Sohail (2012) applied observability in the mobile banking study to illustrate seeing the effect of mobile banking transactions immediately and conveying the benefits to others. The exposure to the transactions enabled mobile banking customers to learn about its benefits, ultimately

facilitating the adoption (Al-Jabri & Sohail, 2012). In a study about computer simulation, Hayes et al. (2015) explained that observability was a key factor to staff acceptance because the simulations provided visual representations of the innovative practices which were discussed between staff members to ensure a shared understanding. The visualizations also enabled the staff to predict the outcome of the process changes, leading to cost savings and safety at the hospital (Hayes et al., 2015).

Observability is relevant to IoT adoption because organizations must observe the IoT to ensure the organization benefits from it. The key to observability in any organization is to ensure they observe a successful or working trial and that the trial has met its objective (McMullen et al., 2015). Kohles et al. (2013) utlized the observability characteristic in the study about leader-follower communications to illustrate how an organization's vision is perceived. Followers observed managers or other leaders as they guided their work based on the organization vision (Kohles et al., 2013). The observations gave followers confidence that they can apply the same vision in their work (Kohles et al., 2013). As a result, the organization was able to benefit from the innovation. Sanchez et al. (2014) conducted a study about the deployment and experimentation architecture of an IoT experimentation facility and revealed IoT is difficult to experiment at organizations for the purpose of observation due to the hardware and software resources required. However, organizations considering IoT adoption may benefit from observing other organizations that have adopted IoT to see how IoT provides value for them.

Observability of IoT security, privacy, and reliability may be valuable for organization IT leaders considering IoT adoption. Observation helps to ensure the innovations provide benefits for organizations (Ju et al., 2016). Observability is the degree to which the results of the use of the innovation are visible to stakeholders, particularly the organization leadership group (Windsor et al., 2013). It is essential for organization IT leaders to observe successful results in IoT so that they can feel confident that they addressed security, privacy, and reliabiilty factors as a result of the adoption. However, IoT security, privacy, and reliability may not be observable. Despite technological advances, observing IoT is difficult because there are limitations with emulating realistic conditions (Sanchez et al., 2014). Consequently, observability may not be a major factor when organizations consider IoT adoption. Many other studies have found that observability did not influence adoption. Kapoor, Dwivedi, and Williams (2014) reviewed 226 relative innovation articles based on the five characteristics of the DOI theory and found that relative advantage, compatibility, and complexity influenced adoption while observability did not influence adoption in the literature that was reviewed. Therefore, observability may be difficult to use as a factor to inflence IoT adoption.

Observability and IoT security. Observability is a DOI characteristic that makes the innovation results visible to stakeholders (Rogers, 1962). Alam, Khafibi, Ahmad, and Ismail (2007) conducted a survey during a quantitative study about the factors influencing the adoption of Internet-based e-commerce in electronic manufacturing companies in Malysia and revealed that observability of security challenges had a

significant influence on the adoption because the companies were able to learn and communicate methods necessary to manage the security challenges prior to the adoption. Likewise, Knebel et al. (2006) suggested IoT pilot projects for the purpose of observing security functionality as the pilot program would enable organizations to make the innovation visible to stakeholders to ensure it met their requirements. Research and experimentation are necessary to observe and ensure the organization meets all security requirements for IoT (Silva & Maló, 2014). A study about the evaluation of an IoT security system at the European Technology Platform on Smart Systems Integration (EPoSS) revealed that observability helped developers expose IoT security challenges at the physical perception layer, transport layer, and application layer during the pilot projects as they were able to address those vulnerabilities prior to adoption (Zhang, Zou, & Liu, 2011). Organizations IT leaders must observe the IoT market and consider cybersecurity protection for business processes and information assets prior to adoption to prevent a potential impact to their organization (Bughin, Chui, & Manyika, 2015).

Observability and IoT privacy. Rogers (1962) explained that observability is a DOI characteristic used to demonstrate an innovation and reduce uncertainty. Olatokun and Igbinedion (2009) conducted a quantitative study about the adoption of Automatic Teller Machines (ATMs) in Nigeria where 428 participants were surveyed and found that observability was instrumental in the respondents' request for banks to remedy ATM privacy vulnerabilities to improve uncertainty in the adoption of ATM services. Similarly, organizations may pilot IoT and apply observability to generate feedback from stakeholders and find solutions to IoT privacy threats before adoption (Maras, 2015). The

feedback may help organizations create a strategy to preserve IoT privacy, prevent attacks, and gain the stakeholders' confidence to enable IoT adoption (Farooq, Waseem, Khairi, & Mazhar, 2015). Notra, Siddiqi, Gharakheili, Sivaraman, and Boreli (2014) conducted an experimental study about IoT privacy risks with emerging household appliances and demonstrated privacy vulnerabilities and found that survey respondents were unclear about the privacy implications of IoT devices. The researchers concluded that without observability, IoT users were unaware of the IoT privacy vulnerabilities and that proper tools must be developed particularly at the network level to prevent attacks to popular IoT devices such as Nest and WeMo.

Observability and IoT reliability. Observability refers to the results of an innovation such that it stimulates discussions (Rogers, 1962). In a case study about integrating mobile devices into the nursing curricula, Doyle, Garrett, and Currie (2014) applied the observability characteristic as a framework in a study to guide the implementation of moble devices and found that observation and demonstration of mobile devices using simulations and pilots contributed to its adoption. In the same way, IoT has been marketed to enable communication and connection of all objects, leading potential IoT adopters to observe the market and determine whether it is a reliable way of communication at their organization (Chang, Dong, & Sun, 2014). This is relevant for organizations as reliability must is an important requirement to ensure smooth and uninterupted operation (Sanchez et al., 2014). In a study about smart, autonomous and reliable IoT, Kyriazis and Varvarigou (2013) found that organizations must create strategies to manage IoT volatility by observing reliability patterns in IoT environments

to improve the quality and availability of data. A reliability strategy is important as it would enable efficient and highly reliable IoT systems for businesses that expect high availability all the time (Franke et al., 2014).

Complexity

The final DOI characteristic is complexity. Complexity highlights the innovation's usability and comprehension (Rogers, 1962). Complexity may be a major factor for potential adopters because the innovation may require a high learning curve. The complexity of e-journals was a significant factor in the adoption because publishers who were familiar with e-journals were more likely to adopt it than those who had yet to use e-journal platforms (Sanni et al., 2013). Familiarity may explain Rogers' (1962) position about complexity being negatively related to the innovation's rate of adoption. A quantitative study conducted about mobile banking services to explore perceptions of innovation benefits and risks revealed that users are reluctant to use mobile banking services if they require more mental effort than traditional banking services (Chen, 2013). Therefore, organizations must consider complexity as an important characteristic prior to adopting the innovation.

IoT uses usability, learnability, utilization of the technology and device to measure complexity (Penjor & Zander, 2016). Rogers (1962) posited complexity is the degree to which an organization's members posses a high level of knowledge and experise. The complexity of IoT may require a higher learning curve for end users and IT resources, making the innovation counterintuitive. For example, a study conducted by Boos et al. (2013) referred to the complexity of using IoT to control accountability at

organizations. The researchers revealed that controlling IoT capabilities is not trivial due to the automation aspect of IoT. Adopting innovative technology is difficult, but when the complexity of the technology is high, it makes the adoption even more difficult (Safari et al., 2015). As studies suggest, if an innovation is difficult to use, the likelihood of adoption is low. Therefore, organizations must consider reducing IoT complexity prior to implementation.

IoT security, privacy, and reliability vulnerabilities make complexity an essential DOI characteristic in this study. IoT presents several challenges for organization executives, including technological interoperability and heightened cyber security risks (Bughin et al., 2015). Organization IT leaders often want to adopt a technology that can easily integrate with their existing systems and applications (Suhasini & Suganthalakshmi, 2015). Otherwise, the complexity of a technology such as IoT may make it difficult to integrate, maintain or upgrade for organization members. During a study about IoT experimentation over a smart city testbed, Sanchez et al. (2014) revealed that IoT infrastructure is complex and risky in an organizational setting due to the security and reliability vulnerabilities. Therefore, organization executives must develop strategies to reduce complexity while reducing the risks presented by IoT (Sanchez et al., 2014).

Complexity and IoT security. Complexity is a DOI characteristic that refers to the understanding and use of innovation for potential adopters (Rogers, 1962). During a study about organization issues in the adoption of health information technology innovations, Creswell and Sheikh (2013) found compatibility to be a major obstacle in

the adoption of innovations as system complexity often led to issues with usability and required extra time to perform funcions due to the intense learning on the part of the user. In the same manner, IoT security is complex because various security requirements for data exchange between devices makes it a challenge to design a single solution (Aldosari et al., 2016). Borgia (2014) suggested there is significant complexity to IoT security as organizations must prevent compromise of credentials, network attacks, and vulnerabilities to communications to guarantee security. Andersson and Mattsson (2015) conducted a study about service innovations enabled by IoT and established that IoT technology covers many applications areas such as security, tracking, payment, metering, health remote control and maintenance and others, which makes IoT security difficult to address as a standard solution due to the complexity. Therefore, individual organizations must have a strategy to addresses the security vulnerabilities for their corresponding organization (Zhang & Yu, 2013).

Complexity and IoT privacy. An innovation that is perceived as complex or difficult to use is unlikely to be adopted (Rogers, 1962). Nan, Zmud, and Yetgin (2014) conducted a study to construct an integrated model for a virtual lab using prior literature and the DOI theory and revealed that innovation processes make well controlled lab experiments and field surveys complex as they produce unexpected and confounded results. Likewise, protection of IoT privacy preferences are complex since they may vary from one person to another (Zhou & Piramuthu, 2015). The complexity of a privacy solution may limit IoT adoption as it may present options that may be too difficult to use or understand (Yang et al., 2013). Zhou and Piramuthu (2015) conducted a study about a

customized privacy model for IoT and suggested that privacy protection is often enforced in uniform regardless of the disparate requirements of each individual. IoT privacy is too complex to include as part of a uniform solution and would require a privacy protection regulation mechanism to maximize overal social privacy requests and increase the rate of adoption (Zhou & Piramuthu, 2015).

Complexity and IoT reliability. Rogers (1962) explained that the complexity of an innovation is negatively related to its rate of adoption. Complexity is a DOI characteristic that was applied by Aslani and Naaranoja (2015) during a qualitative study about the use of innovations at healthcare centers in Finland, where the researchers revealed that innovations have failed in the healthcare sector due to the complexity of the innovation process. The complexity of IoT systems increase exponentially when compared to typical software systems because there are more components to manage such as the device, the wireless connection, performance of the device, and the network that connects the devices (Zhu, Lu, Han, & Shi, 2016). The reliability concerns of the IoT components have prevented organizations from adopting IoT because of potential risks it may present at any given time (Li, Zhao, & Yu, 2015). Marinissen et al. (2016) conducted a study about IoT testing challenges where reliability was identified as a complex component in developing effective test strategies in the enterprise because of limitations such as low-power wireless sensor nodes, leaving devices active for a short time frame. The complexity of the reliability risks presented by IoT may be too difficult for potential adopters to accept, thus preventing IoT adoption (Gross, 2016).

Analysis of Related Theories

The theory of reasoned actions (TRA) has been used in research to explain user attitude, subjective norm, and behavioral intention, which influence technology acceptance and utilization (Mishra et al., 2014). I focused on strategies to adopt IoT using DOI in this study. DOI is similar to TRA because both theories utilized three constructs, including user attitude, subjective norm and beliefs. The five characteristics of the DOI theory align well with those constructs, particularly compatibility (subjective norm), trialability (behavioral intention), and observability (user attitude). TRA varies from DOI because DOI does not address whether an innovation is actually accepted or used by a potential adopter (Sarabdeen & Ishak, 2015). Respectively, DOI theory offers additional characteristics such as relative advantage and complexity, which are instrumental to describe the organizational value and the potential difficulties of addressing security, privacy, and reliability strategies for IoT adoption.

The technology acceptance model (TAM) is an extension of TRA and includes technology acceptance based on a users' perceived usefulness (PU) and perceived ease-of-use (PEOU) (Yung-Ming, 2015). TAM is similar to DOI because both models attempt to understand adoption and user acceptance. TAM varies from DOI because TAM focuses on the individual user with the concept of PU. Also, TAM does not include the five DOI characteristics necessary to influence organization IT leaders to adopt new technology and improve the innovation's rate of adoption. As a result, DOI was better suited for this study as it addressed the security, privacy, and reliability factors using the

five characteristics as the framework to determine the consequences of IoT adoption and the benefits versus the costs of the innovation.

The technology, organization, and environment (TOE) framework addresses technology adoption by using a process that is based on technology context, organizational context, and environmental context (MacLennan & Belle, 2014). Similarities between TOE and DOI include technology acceptance as the technology context of TOE is often linked to the five characteristics of DOI. The difference between TOE and DOI includes TOE's emphasis on environmental context which accounts for competitive pressure, industry, market scope and supplier computing support (Alshamaila, Papagiannidis, & Li, 2013). The objective of this study was to explore strategies organization IT leaders use for security, privacy, and reliability to enable the adoption of IoT devices. Also, I used the IT industry as an example to diffuse the strategies for IoT adoption in other industries. Therefore, DOI was the most suitable framework to address each objective.

Limitations of Diffusion of Innovations Theory

The DOI theory offers a good framework for a proposed intervention (McMullen et al., 2015). However, there are several limitations that organization IT leaders must consider about the theory. First, the adoption of the DOI theory does not analyze a particular firm's technological capabilities, which can affect the users' perception of the new technology (Kim & Pae, 2014). Since the theory uses user perceptions, the perceptions may ultimately affect the adoption or rejection of the innovative technology. Moreover, the DOI theory does not include a strategy for a particular industry such as

healthcare (Cobban et al., 2008), thus, leaves it to organization IT leaders to address factors such as security, privacy, and reliability when adopting innovative technology. This is important because strategies may vary from one organization to another. Also, organizations must consider other industry factors such as compliance and regulatory standards because the DOI theory does not consider compliance and regulatory standards across all industries (MacLennan & Belle, 2014). Therefore, organizations in the manufacturing industry may diffuse IoT while organizations in the healthcare industry may struggle to adopt IoT due to such standards.

Usage of Diffusion of Innovations Theory in Research

Researchers have applied the DOI theory by Rogers (1962) in a variety of industries and contexts. Some researchers have utilized the adopter categories in their research to illustrate the timing of organizations that show interest in adopting an innovation. The adopter categories include innovators, early adopters, early majority, late majority, and laggards (Rogers, 1962). Penjor and Zander (2016) used the five adopter categories of DOI during a case study to describe the perceptions of a virtual learning environment for educational institutions. Chun, Sautter, Patterson, and McGhan (2016) used the five adopter categories of the DOI theory to describe the age of study participants and explore the reason for adopting a pharmacy-based influenza vaccine in the United States between 1993 and 2013. The authors concluded by explaining that relative advantage and compatibility were more relevant to younger adults, while different interventions were warranted for older adults (Chun et al., 2016).

Arulchelvan (2014) used the adopter categories in a study to analyze the usage and reach of new media technologies such as websites, blogs mobile phones and SMS in the parliament elections in 2009. The DOI theory was used in the study to understand the rate of adoption of the new technologies. Arulchelvan concluded that every major political party tried to use all the available new media tools and revealed India is in the stage of early majority adopters. Arulchelvan discovered mobile phone was the fastest and most effective way to reach voters. The studies are relevant to IoT adoption because each study included factors such as time and process improvements that influenced the adoption of the corresponding innovation.

The use of diffusion innovation theory research in such a broad and diverse collection of industries and organizations supports the use of adoption categories where timing is essential. The timing of the adoption may be categorized by the into the five adopter categories identified by Rogers (1962). However, the adopter categories may not always explain the initial reason for the lack of adoption. As a result, researchers may choose to use the DOI's five characteristics to qualify the innovation prior to the categorization.

Researchers have benefited from the five characteristics of DOI including compatibility, relative advantage, trialability, observability, and complexity (Rogers, 1962). The characteristics offer insight into the factors that influence the adoption of innovation. Safari et al. (2015) explored the five characteristics in their research to illustrate the influence of technology, organization, and the environment when considering adoption of Software as a Service (SaaS). Safari et al. concluded describing

the five characteristics as factors influencing and explaining the reason for the adoption of SaaS. The study illustrated the use of the characteristics but did not include the adopter categories because the categories would not clearly describe the reasons for adoption.

Dash et al. (2014) found the five characteristics were good predictors for attitude towards adoption of mobile banking. Dash et al. concluded compatibility and trialability were the two main factors that influenced customer adoption of mobile banking in India. The results from the study may help with IoT adoption as it offers insight into the user's motivation to adopt the innovation. Also, the factors also offered insight to the reasons for the adoption rather than the length of time it took to adopt the innovation successfully. Therefore, the characteristics described will help organizations interested in adopting new technology such as IoT.

Finally, Sugarhood et al. (2014) applied the five characteristics in their research about the use of telecare technologies to identify and explore factors that influence adoption. The study resulted in a better understanding of the impact of adopting new technology such as telecare due to the complexity and coordination required between people and organizations (Sugarhood et al., 2014). The benefits of the innovation, compatibility with personal values and lifestyle, ease of use, experimentation of the innovation, and the visibility of the benefits depicted the five characteristics of the diffusion of innovation (Sugarhood et al., 2014). The study was about the adoption of IoT and the diffusion of innovation theory because it described the complexity of an innovation and the difficulty of adoption due to the stakeholders involved in the process.

The researchers also addressed each of the five characteristics, leading to a thorough observation and decision to adopt the innovation.

The DOI theory is a framework used in research to describe the rate of adopting an innovation. Also, the five characteristics of the theory may be used to explore the reasons for an adoption. Researchers have found the level of complexity to be inversely proportional to the level of adoption (Sugarhood et al., 2014). Research has shown a greater relative advantage in the innovation contributes to the adoption (Cobban et al., 2008). Finally, greater compatibility, trialability, and observability result in a higher adoption rate (Rogers, 1962). Research has shown the five characteristics are important to explore IoT adoption, particularly when considering the security, privacy, and reliability strategies.

Transition and Summary

This section included a background and review of the literature regarding security, privacy, and reliability strategies to adopt IoT at a healthcare organization. IoT is a new and innovative technology and offers many benefits to providers and consumers across industries. Before considering adopting IoT, organization IT leaders must first develop security, privacy, and reliability strategies to ensure they reduce the risks to consumers. IoT poses risks, vulnerabilities, and benefits to organizations. Hence, organization IT leaders must be able to provide a balanced strategy to ensure there is value for consumers.

The DOI theory offers five characteristics that align those challenges and benefits to IoT. Benefits include compatibility between IoT and the existing technology. Relative

advantage is another benefit for the organization. Trialability is the next diffusion of innovation characteristic to ensure the technology meets organizational standards. Next, organizations may use observability to examine the technology and the benefits to the organization. Finally, low complexity may be used to ensure little maintenance in support for the technology while ensuring there is a continuous advancement to improve the technology and lower risks. IoT has great potential. As objects and systems exchange information on networks, consumer expectations may change with the technology. Organization IT leaders must acknowledge the changes introduced by the innovative technology and understand the organizational and customer demand to ensure there is a reason to adopt the technology.

Section 2 includes an outline of the intent, research design, population sample, and analytical methods used for the study of IoT adoption. Section 3 includes an overview of the study and a presentation of findings from the analysis of collected data. Section 3 also includes the discussion of applications of the research to professional practice and the presentation of recommendations, reflections, and conclusions resulting from the conduct of the study.

Section 2: The Project

In this section, I expand on Section 1 by including details about the research method, design, and processes involved in this study. I define the role of the researcher, criteria for participant selection, population sampling, and ethical research. Also, in Section 2, I explain the data collection, organization, and analysis processes used in this study. Finally, the section includes consideration of reliability and validity issues in the context of the research study.

Purpose Statement

The purpose of this qualitative exploratory case study was to explore strategies that organization IT leaders use for security, privacy, and reliability to enable the adoption of IoT devices. The population consisted of organization IT leaders including the CIO, CISO, enterprise architect, data center manager, and IT director from an IT organization in Stamford, Connecticut who has implemented IoT strategies. The IT leadership team participated in semistructured interviews to explore the security, privacy, and reliability strategies used at the organization to enable the adoption of IoT. The implications for positive social change include the potential for improvement to IT practices as the IoT devices have sensors that make routine decisions and perform common tasks based on human tendencies. There is also the potential to contribute to new knowledge and insights that may lead to discovery, such as the prevention of CTE. If athletes wore sensors to detect the impact of objects to their head, athletic officials may be able to implement preventative measures based on the number of concussions for an athlete as a solution to prevent CTE.

Role of the Researcher

I was the primary instrument in the data collection process. Humans act as a research instrument to convey the uniqueness of the qualitative researcher's role throughout the data collection and analysis process (Guba & Lincoln, 1985). A researcher conducting a case study has the responsibility to design the study, develop astute interview questions, confirm participant responses to ensure understanding between the researcher and participant, and eliminate personal bias from the study (Cronin, 2014). My role in this qualitative single case study was to design the study, develop interview questions, collect the data, organize the data, and analyze the data. The role of the researcher also included exploring multiple perspectives during the data collection process while limiting bias (Kavoura & Bitsani, 2014). As the primary instrument, I mitigated my bias by presenting the results of the study from the participants' perspective.

I had 13 years of professional experience in the software industry without any IoT experience prior to this study. Researchers with experience in the topic of the study will add value but must avoid influencing the evidence due to bias (Mecca et al., 2015). My lack of experience in IoT and limited experience in security, privacy, and reliability enabled me to limit bias on the topic for this study. My interest in the NFL was the main reason I chose to conduct research on this topic as IoT may have the potential to improve the safety of football players. I had initial conversations with an organization member to determine if the organization qualified for my study. I did not have a previous professional relationship with the member of the potential organization prior to this

study. After institutional review board (IRB) approval, I asked the member to participate in my study. A researcher-participant relationship helps researchers gather rich data due to the trust between parties (Collins & Cooper, 2014). I had multiple conversations with the member of the organization and continued to stay in touch to build rapport and ensure there was trust between the participant and myself.

I performed research and data collection for this study ethically. The Belmont Report summarized the distinction between research and practice, the three basic ethical principles, and the application of these principles (U.S. Department of Health & Human Services, 1979). Participants and the organization remained confidential in the study, and I focused on the evidence rather than the participants. The Belmont Report protocol offers support to respect human subjects, beneficence, and justice (Hammer, 2016). To ensure ethical conduct, I followed the Belmont Report protocol. This process included stating all relevant information in an informed consent form to appraise the participant. It was vital to perform this action prior to research to maintain the ethical boundaries within the Belmont Report Protocol (Largent, Grady, Miller & Wertheimer, 2013). I completed the National Institutes of Health Office of Extramural Research training course (certification number: 1763549) to protect human research participants and included the certificate in Appendix A.

Researchers may create bias due to their personal experiences, personal values, and perspectives during data analysis (Kavoura & Bitsani, 2014). Research findings must reflect the participants' experiences and perspectives of the inquiry and not the researcher's biases, motivations, or perspectives (Guba & Lincoln, 1985). Bias may

threaten the credibility of a study because it may lead to manipulation or distortion of data (Guba & Lincoln, 1985). I mitigated personal bias by being aware of my own experiences, values, and perspectives in this research study. I used open-ended interview questions to record the participants' experiences. I did not express my own experiences or perceptions of the study topic to avoid influencing the interview participants and avoid bias in the data collected.

I used an interview protocol as a guide when conducting interviews. The interview protocol aids the researcher with a prepared list of questions so the researcher can focus more on responses for each participant instead of memorizing questions (Rivard, Fisher, Robertson, & Mueller, 2014). The interview protocol contained a set of interview questions for each participant, which allowed me to listen to each participant responses attentively. Gioia, Corley, and Hamilton (2013) suggested the use of an interview protocol during interviews as it focuses on the research question and prevents lead-the-witness type questions. Rivard et al. (2014) provided a process for interviews that includes five steps: building rapport, avoiding leading questions, avoiding interrupting the witness, allowing for long pauses, and asking follow-up questions to fill in gaps. I used the same interview protocol for all participants to ensure consistency between interviews and focused on the participants' experiences as that helped to reduce personal bias. Participants had an opportunity to respond to each interview question and offered additional insights and perspectives on the security, privacy, and reliability strategies to adopt IoT. Therefore, interviews were the instrument of choice for this study to explore each participant's perspective about strategies to enable the adoption of IoT.

The interview protocol is outlined in Appendix B and includes the interview questions for this case study.

Participants

The eligibility criterion was an important factor when considering participants for this study. Selecting participants was one of the most important aspects of research because data collection served as evidence to ensure the research was credible (Elo et al. 2014). In qualitative research, experiences with the phenomenon serve as the basis for the selection of study participants (Moustakas, 1994). Meanwhile, an adequate sample is required in research to ensure credibility (Marshall, Cardon, Poddar, & Fontenot, 2013). The study included interviews with an IT organization's leadership team with decision responsibility to create or offer input on strategies to adopt IoT at an organization in Stamford, Connecticut. Organization IT leaders included positions such as a CIO, executive vice president, vice president, director, senior application developer, and senior project manager (Alimo-Metcalfe, 2010). The participants' job title had to indicate that they were an organization IT leader within their organization. Thus, the participants were leaders of an IT organization with direct experience using security, privacy, and reliability strategies to adopt IoT.

The main contact for the organization offered to act as a mediator and helped me gain access to potential research participants after Walden University IRB approval (approval number 06-21-17-0241112). Mediators are employees or managers of the organization who help to gain access to eligible research participants (Peticca-Harris, deGama, & Elias, 2016). After reviewing the eligibility criteria of the study, the mediator

identified a number of potential participants. Mediators can also assist researchers by locating documents that are important to the research study (Boblin, Ireland, Kirkpatrick, & Robertson, 2013). The mediator also helped me gain access to company documents.

As a first step to develop a working relationship with participants, I asked the mediator to forward my email invitation (see Appendix C) and consent form to eligible participants. A mediator may use their relationships with colleagues within an organization to facilitate contact between a researcher and the potential participants (Kristensen & Ravn, 2015). A mediator can increase trust between the researcher and the participants because of their relationship with colleagues at the participating organization (Fischer-Lokou, Guéguen, Lamy, Martin, & Bullock, 2014). After I received email responses from participants indicating that they were willing to participate voluntarily in the study, I followed up with an email to arrange a time to schedule each interview and offered to meet prior to the interviews if participants had questions. If participants did not sign the consent form prior to the interviews, I reminded them with an email and the consent form that informed them about my study's background, procedures, voluntary nature of the study, benefits, risks and privacy of the study.

I asked all research participants to sign the consent form to ensure the study adhered to the IRB requirements. Researchers must comply with academic institutional requirements while planning and organizing their study, including obtaining approval from ethics boards (Peticca-Harris et al., 2016). I used the consent form to help participants recognize that their privacy was protected in this study. Researchers may build trust and establish a working relationship by keeping participant information

confidential (Hoyland, Hollund, & Olsen, 2015). The quality of the consent process depends on the researcher's ability to explain and discuss the research study (Kamuya, Marsh, Kombe, Geissler, & Molyneux, 2013). After participants signed and emailed the consent forms, I began scheduling interviews.

Each participant had an opportunity to ask questions by email or by phone prior to interviews to ensure they were comfortable with the interview process. Haahr, Norlyk, and Hall (2014) stressed that the researcher and participant interaction during the interview process influences trust and confidentiality. When I scheduled interviews with participants, I summarized the interview process to ensure they were comfortable with the process. Researchers can help participants prepare for interviews by summarizing the interview protocol to ensure participants know what to expect during the interview (Doody & Noonan, 2013). I explained the interview process by referencing the interview protocol in Appendix B. I reminded participants that participation in the study was voluntary and that the participant and organization names would remain confidential in the study.

I developed a working relationship with the participants by creating an environment where each participant was comfortable to enable in-depth and exhaustive interviews. A comfortable environment enabled participants to provide in-depth responses to research questions, which was otherwise unlikely if they were concerned about their privacy and confidentiality (Drake, 2013; Yin, 2014). This strategy helped participants feel relaxed and enabled them to offer transparent feedback to the interview

questions such that the feedback added depth and breadth to the study as it addressed the primary research question.

Research Method and Design

Prior to selecting a research method for this study, I conducted a review of research methods that were suitable for this study. A review of the current research methods includes three methodologies: qualitative, quantitative, and mixed methods (McCusker & Gunaydin, 2015). All three methods were viable for research, but qualitative methods offered a deeper understanding of the issue studied than quantitative methods (Palinkas, 2014). Ultimately, I selected a qualitative method and exploratory single case study design to answer the research question. Qualitative research is pertinent for exploratory studies and stimulates further research on a larger scale (Cronin, 2014). Case studies allow for a holistic understanding of a phenomenon within real-life contexts from the perspective of those who experienced the phenomenon (Stake, 1995). A qualitative exploratory case study was appropriate for this research because it allowed for a deep understanding of the organization IT leaders' perspective when exploring security, privacy, and reliability strategies to enable the adoption of IoT devices.

Method

In this study, I explored experiences and personal viewpoints using qualitative research to answer the primary research question. Researchers may use qualitative research to provide insight into each participants' experience (Grossoehme, 2014). I used qualitative research to explore each participant's experiences in this study. Qualitative research allows for vibrant discussions enriched with personal experiences and

perspectives (Moustakas, 1994). I chose qualitative research because it allowed for open discussions between the participants and myself. For instance, I asked open-ended questions to allow participants to share their personal experiences and perspectives while providing in-depth responses about IoT adoption strategies. Qualitative research allows researchers to use interview questions that provide the participants an opportunity to offer in-depth responses (Frels & Onwuegbuzie, 2013). If a participant response required additional information or clarification, I asked additional probing questions. Qualitative researchers use inductive reasoning to examine the context, interpretation, and meaning of participants' experiences (Yilmaz, 2013). In this study, I used inductive reasoning to explore participants' experiences about the security, privacy, and reliability strategies used to adopt IoT devices.

I considered using a quantitative research method for this study. Quantitative research is intended to generalize and predict data through deductive reasoning and fails to provide insight into the participants' personal experiences (Yilmaz, 2013). This research study provided insight into participants' experiences about security, privacy, and reliability strategies to adopt IoT devices. In contrast, quantitative research addresses phenomena by use of numerical data through mathematical methods or statistics (McCusker & Gunaydin, 2015). Numerical data would not provide insight about the participant's experiences about IoT adoption. Hence, I did not use numerical data to explain the phenomenon. In quantitative studies, researchers test preconceived hypotheses (Frels & Onwuegbuzie, 2013). The focus of my study was not testing hypotheses, so a quantitative study was not appropriate. Thus, quantitative research was

not selected for this study because I did not seek to test a hypothesis or apply numerical measurements to substantiate data.

I considered using mixed methods research for this research study. Mixed methods research uses a combination of qualitative and quantitative methods and shares benefits of each research method (Palinkas, 2014). The mixed methods approach is appropriate for research requiring deep analysis of qualitative data and multivariate analysis of quantitative data (McCusker & Gunaydin, 2015). A mixed methods approach may be used when neither a quantitative nor a qualitative approach is sufficient by itself to comprehend the research topic (Petersen, Piper, Liedeman, & Legg, 2015). Since quantification of data was not required to answer the research question of this study, neither quantitative nor mixed methods research was necessary for this study. The focus of this study was solely on participants' experiences. As a result, qualitative research was the best-suited research method for this study as it offered a deep understanding of security, privacy, and reliability strategies used by organization IT leaders to adopt IoT devices.

Research Design

An exploratory single case study design was selected for this qualitative research study. Qualitative design types include narrative research, phenomenology, ethnography, and case study (Palinkas, 2014). I chose an exploratory single case study design to acquire a thorough understanding of the security, privacy, and reliability strategies organization IT leaders use to adopt IoT devices. Boblin et al. (2013) noted that case studies allow researchers to understand a phenomenon holistically from the participants'

viewpoint. Interviewing each participant about his or her experiences regarding security, privacy, and reliability strategies allowed me to gain a holistic understanding of the phenomenon. Moreover, this single case study required depth in exploring the strategies of the individual organization.

This case study included how, what, and why questions during interviews and during the review of company documents to gain a deeper understanding of the phenomenon. Case study research may be used to answer how and why questions regarding phenomena (Cronin, 2014; Yin, 2014). The analysis of company documents complemented the interviews and expanded on my understanding of the strategies used by the organization to adopt IoT devices. Cronin (2014) referred to the focus of individual case study research since the researcher can investigate everything, including individuals, groups, activities, or a specific phenomenon. Case studies are typically about complex events and behavior occurring within real-life context (Yin, 2014). I chose a case study design to conduct a thorough inquiry into the complex phenomenon regarding the security, privacy, and reliability strategies used to adopt IoT devices. This case study explored strategies used by IT leaders at a single organization to adopt IoT by using interviews and company documents to gain a thorough perspective on the experiences of the participants.

Phenomenology is a research design that I considered for my study. A phenomenology study contains lived experiences and events from the phenomenon (Moustakas, 1994). Grossoehme (2014) indicated that phenomenology research focuses on participant experiences and their meanings. Although participant experiences were

essential for my study, using a phenomenology research design did not allow me to collect company documents to offer insight from an organization's perspective. Marshall and Rossman (2016) stated that phenomenological design permits data collection from the conduct of interviews but does not allow for the gathering of information from publicly available documents. The phenomenological design allows researchers to apply how individuals experience daily life and how their world becomes significant to the researchers (Wells, 2013). The focus of my study was to explore the strategies organization IT leaders used to adopt IoT and was not based on how individuals experienced daily life. Thus, a phenomenology study did not address the specific details about one organization's strategy and the impact security, privacy, and reliability had on the adoption of IoT. Therefore, a phenomenology study was not a good fit for this study.

Ethnographic research was also considered for this research study. Ethnography offers an insider's perspective of group's conceptual world (Grossoehme, 2014). Ethnographic researchers immerse themselves into the lives of participants and make choices on the data collected about the relationships of the study (Cunliffe & Karunanayake, 2013). I used interviews and company documents during data collection and did not require observation of participants' daily lives. An ethnographic study is the method of choice when the goal is to understand a culture (Keutel, Michalik, & Richter, 2014). I explored strategies to adopt IoT from the perspective of research participants and did not seek to understand a culture. Therefore, an ethnographic study was outside of the scope of this study.

Finally, I considered using a narrative study for my research. A narrative study entails gathering artifacts and life experiences for storytelling the ways humans experience the world (Wolgemuth, 2014). I focused on strategies used to adopt IoT at an IT organization and did not focus on how humans experience the world. Narrative researchers use a story relating to an individual's experience and may address oppressed societies (Berry, 2016). Although stories about an individual's experience may have contributed to this study, it was not required to explore strategies used by organization IT leaders to adopt IoT. Narrative research design allowed a researcher to approach and understand meaning in relation to humans and their lives with the concept of narrative emerging in a variety of ways within different contexts and situations (Gockel, 2013). I focused on an organization's strategy and did not involve the life experiences of an individual since an individual's life experiences would not yield the appropriate data to answer my research questions. Thus, a narrative study was not applicable to this study.

I included data from multiple sources to achieve data saturation during this study. Data triangulation of multiple data sources and the depth of data collected from multiple data sources is a means to achieve data saturation (Fusch & Ness, 2015). Data saturation includes adding new participants in the study until new information is no longer present (Svensson & Doumas, 2013). Face-to-face interviews using the same set of questions will facilitate data saturation (Fusch & Ness, 2015). The research design for this study was a single case study where participants from one organization contributed to the study using face-to-face interviews. Interviews were conducted until no new information is present. In addition to interviews, I collected data from company documents relating to security,

privacy, and reliability strategies, policies, and processes. I tracked the data I collected from these multiple sources to facilitate triangulation and to determine when I had achieved data saturation. The lack of any new emerging data or concepts will lead to data saturation (Houghton, Casey, Shaw, & Murphy, 2013). I collected data until no new information was generated indicating I achieved data saturation.

Population and Sampling

The population of my study consisted of organization IT leaders at a single organization in Stamford, Connecticut. Organization IT leaders included positions such as CIO, CTO, CISO, directors, and senior managers (Alimo-Metcalfe, 2010). I specifically targeted an organization that adopted IoT during this study. The population characteristics in a qualitative study relate to participants' subjective experience with the phenomenon (Berger, 2015). The population of my study all had experience using security, privacy, and reliability strategies to enable IoT adoption, which was the phenomenon of my study. The first step in the data collection process was to define the study population by using inclusion and exclusion criteria (Robinson, 2014). The study population only included organization IT leaders who had knowledge or perceptions of security, privacy, and reliability strategies to adopt IoT at their organization.

An eligibility criterion was necessary to focus on a specific population for this study. It is essential to ask questions about the participant selection criteria to ensure sound sampling and data saturation can be reached (Elo et al., 2014). An appropriate sample is composed of participants who best represent or have knowledge of the research topic (Kish & Verma, 1986). Thus, it is necessary to have an eligibility criterion to ensure

participant homogeneity (Guest et al., 2006). The eligibility criteria for participants in the study included (a) being over the age of 18 years, (b) being currently employed by the participating IT firm, (c) occupying an organization IT leadership position, and (d) willing to share their experiences about IoT, (e) having knowledge or perceptions of security, privacy, and reliability strategies to adopt IoT at their organization.

I used a census sampling strategy for this study to collect data from the population that met the eligibility criteria. The primary objective of a census is to collect detailed data from the population such that the data presents a complete picture of the study phenomenon (Kish & Verma, 1986). The population of this study consisted of IT leaders at a single organization in Stamford. I estimated that there were approximately 10 IT leaders in the organization. Census sampling is appropriate for studies requiring participants with particular knowledge and experience about a research topic (Kish & Verma, 1986). Participants for this study included a small population of organization IT leaders at a single organization. Census sampling is appropriate for a study when interviewing a smaller and limited total population is feasible (Charman et al., 2015). A census involves selecting all participants in the study population (Omondi, Ombui, & Mungatu, 2013). I used a census sampling strategy to interview all individuals in my study population. The population for my study was small and finite so a census sampling strategy was the best option to provide a complete and detailed understanding of the phenomenon.

The sample size for this study consisted of all participants who met the eligibility criteria. A suitable sample size directly relates to a study's data saturation (Marshall et

al., 2013). A study about the degree of data saturation involving in-depth interviews concluded researchers could potentially reach data saturation with six to twelve interviews (Guest, Bunce, & Johnson, 2006). The census sample for this single case study consisted of 10 organization IT leaders in Stamford, Connecticut. Census sampling enables researchers to use small sample sizes because of the participants' depth of knowledge about the research topic (Kish & Verma, 1986). Interviewing participants with direct knowledge and experience of the phenomenon may reduce the sample size necessary for data saturation (Malterud, Siersma, & Guassora, 2016). Therefore, the interviews included all of the estimated population of 10 organization IT leaders in the study that met the eligibility criteria requiring knowledge and experience using security, privacy, and reliability strategies for IoT adoption in an IT organization. I interviewed all participants in the study population until no new information was present.

An interview setting that is convenient for participants will promote a comfortable interaction between researcher and participant and encourage participants to provide detailed responses to questions (Doody & Noonan, 2013). Seitz (2016) suggested a quiet room without noise and distraction to ensure participants remain focused. The participants' work environment may be distracting and may negatively affect the data collection or the audio recording, so finding an ideal time and space to conduct interviews is important (Deakin & Wakefield, 2013). Based on the participants' preference, I conducted face-to-face interviews in a conference room at a nearby facility or at the workplace of the participants. To prevent distractions during the interviews, I

reserved a conference room where there was no background noise. Once the interviews began, I closed the door and closed all blinds, if they existed.

I used the data I collected from multiple sources to facilitate triangulation and achieved data saturation. Researchers may reach data saturation by using triangulation of multiple data sources while enhancing the reliability and validity of the study (Fusch & Ness, 2015). I interviewed participants until no new information was present. Researchers will achieve data saturation when participants respond with no new information or if new participants replicate the data (Marshall et al., 2013). In addition to interviews, I collected data from company documents and artifacts relating to security, privacy, and reliability strategies, policies, and processes. Company documents included an enterprise architecture plan, security plan, disaster recovery plan, business continuity plan, privacy/confidentiality breach management plan, standard operating procedures, policy documents, procurement documents, project post mortems and historical notes that supplemented interview participants' feedback. Data saturation is realized when information emerges so repeatedly that the researcher can expect it (Frels & Onwuegbuzie, 2013). The lack of any new emerging data or themes will lead to data saturation (Houghton et al., 2013). I continued to collect data from interviews and company documents until there were no new themes generated, indicating I reached data saturation.

Ethical Research

To protect participants, Walden University IRB requires researchers to seek permission before commencing research. Informed consents are necessary and important

in research to ensure participant privacy (Elsrud, Lalander, & Staaf, 2016). I obtained approval from the IRB (approval number 06-21-17-0241112) prior to data collection at the participating IT organization. All participants in my study acknowledged their willingness to participate in my study by confirming their consent in accordance with the IRB guidelines. The consent form provided information on the intent of the study, benefits, risks, confidentiality and right to withdraw. Also, Walden IRB requires researchers to complete a human research protections training course prior to data collection. I received a certification of completion for the "Protecting Human Research Participants" training course issued by the National Institutes of Health (NIH) with certification number 1763549 to ensure the privacy of all participants (see Appendix A).

The consent form provided information on the intent of the study, benefits, risks, confidentiality, and right to withdraw. Informed consents may include the scope of the research, description of the information to be obtained, expected benefits and risks, voluntary nature of the test, possibility of refusal, future use of the data, and the confidentiality of the outcomes (Ayuso, Millán, Mancheño, & Dal-Ré, 2013). Participants replied to my email with the words "I consent" prior to their participation in the study to ensure they acknowledged my responsibility of protecting their privacy. Participants had the option to withdraw from the research process anytime, including after signing the consent form. Participants were able to withdraw from the study verbally or in writing. If a participant were to withdraw from the study, I would have immediately destroyed any data collected from that participant. I used census sampling to interview everyone in my study population so replacing participants who withdrew was not

applicable since I interviewed everyone in the population. Participants who receive incentives in a study may fabricate their interview responses to gain the incentive (Robinson, 2014). There were no incentives to participate in the study to avoid coercion by the researcher and to avoid fabrication of data by participants. The absence of incentives allowed participants to withdraw from the study at their discretion anytime without penalty.

I masked the research participant and organization names to safeguard confidentiality and privacy by using unique and fictional names. Masking of research data identifiable to the organization or participants ensured the data remained confidential (Heffetz & Ligett, 2014). The actual participant names corresponded to participant code names from this study and was stored in an encrypted spreadsheet that was only accessible to me. I assigned numbers to participants such as Participant 1 and Participant 2 to guarantee confidentiality and privacy. The researcher should maintain participant privacy and confidentiality throughout the study by concealing the identity of participants and protecting the data collected (Grossoehme, 2014). All private and confidential information such as interview recordings and company documents containing the organization's name will be stored on a password-protected flash drive for 5 years after CAO approval to protect the participants' confidentiality. The flash drive and any physical data collected during data collection will remain in a locked storage cabinet. After 5 years, I will destroy all physical and electronic copies of the research data, including the consent forms, interview recordings, and transcribed data. I conducted all interviews in a private and confidential manner without disclosing any identifying

information such as names, e-mails or phone numbers to anyone outside of the study participants at the organization. Prior to data collection, all potential participants received an invitation (see Appendix C) to participate in the study and an informed consent form detailing the privacy and confidentiality information to protect study participants.

Data Collection

Instruments

I was the primary instrument during data collection for this qualitative research study. Researchers are considered the primary data collection instrument because they gather data through interviews and interactions in qualitative research (Houghton et al., 2013; Yilmaz, 2013). During the semistructured interviews, I asked open-ended questions to explore participant experiences and addressed the primary research question. Researchers explore participant experiences to identify and interpret common themes (Moustakas, 1994). A qualitative study requires researchers to focus on data collection, data organization, and data analysis (Collins & Cooper, 2014). As the primary collection instrument in this study, I collected, organized, and analyzed qualitative data to answer the primary research question.

During this study, I used semistructured interviews as the primary data collection method and a review of company documents as a secondary collection method. Primary data in qualitative case studies include original data collected from interviews (Thomas, 2015). Secondary data includes data previously collected for a different purpose such as a different research study (Riegel & Dickson, 2016). I supplemented interviews by using member checking to ensure accuracy and validity. I used company documents to verify

my findings from the interviews. Even though secondary data collection methods play an explicit role in case study research, Yin (2014) suggested that researchers use documents as inferences, or a secondary data collection method, to verify findings from the primary data source. Using more than one data source to understand a phenomenon will result in triangulation (Denzin, 1978). I used company documents as the secondary data collection method to verify my findings from the primary data collection method and to demonstrate triangulation in this study.

During this study, I included face-to-face semistructured interviews as part of the data collection process to gain insight into perspectives of organization IT leaders who used strategies to implement IoT adoption. Researchers can develop a rapport with participants during face-to-face interviews (Irvine et al., 2013; Seitz, 2016). During semistructured interviews, participants who experienced the phenomenon reflect on their experiences (Gioia, 2013). I asked follow-up questions when necessary during the interviews to get clarification on participants' responses. Semistructured interviews are the most effective means of gathering information for qualitative research because of the flexibility in designing and refining the interview protocols and in conducting the interviews (Irvine, Drew, & Sainsbury, 2013). I maintained flexibility during interviews by listening to participants as they answered questions. I refined the interview protocol as needed to ensure the interview questions were clear.

The audio of each interview was recorded for reference. Grossoehme (2014) suggested the use of two audio recorders with fresh batteries during interviews to ensure there is no data loss if one of the audio recorders fail. Audio recordings may be used to

ensure accuracy of the data collected during interviews (Fairbrother et al., 2014). I used two audio recorders to record the audio of the interviews to ensure the accuracy of information with the permission of each participant. Researchers can use the slow and normal play back speeds to accurately transcribe interviews (Patel, Shah, & Shallcross, 2015). I listened to the audio recordings more than once to ensure I accurately transcribed the interview data.

The interview protocol (see Appendix B) for this study consisted of pre-interview activities, interview questions, and post-interview activities. When preparing semistructured interviews, researchers create a set of fixed questions to enable participants to share feedback about their experiences (Morse, 2015). Interview protocols are instructions interviewers follow to ensure consistency between interviews, which increases the reliability of the study (Patel et al., 2015). The quality of the study depends on the quality of the research questions (Grossoehme, 2014). My pre-interview activities consisted of an introduction, verification of each participant's informed consent, and a reminder for participants about recording audio and participant confidentiality. An interview protocol is a guide for the researcher to complete the interview process in a consistent format and objective (De Ceunynck, Kusumastuti, Hannes, Janssens, & Wets, 2013). The interviews started by turning on the audio recording device, stating the participant's identifying code, stating the date and time, asking the interview questions, asking the participant to share any other relevant information and stopping the audio recording. My post-interview protocol explained the concept of member checking,

scheduling a follow-up interview, thanking participants and providing my contact information to participants.

Member checking confirmed my interpretation of each participant's interview. Member checking is a process where the researcher shares the interpretation of each interview result with corresponding participants to improve the accuracy, credibility, and validity (Leech & Onwuegbuzie, 2007; Lub, 2015; O'Sullivan & Conway, 2016; Guba & Lincoln, 1985). I enhanced the accuracy, credibility, validity, and reliability of the interview data by using member checking to confirm my understanding of each participant's responses until no new information was present. Researchers may use member checking to establish dependability by allowing the participants to verify the accuracy of the researchers' account of their experiences (Guba & Lincoln, 1985). Morse (2015) added that member checking is one strategy researchers use to increase the reliability of the study by confirming the interpretation of the data collected from participants who experienced the phenomenon. I began member checking after the initial interview by scheduling follow-up face-to-face interviews with each participant. I interpreted the interviews from the audio recordings.

During member checking interviews, I asked each participant to confirm my interpretations and understanding from their interview to ensure it accurately reflects their experiences, meanings, and perspectives. Researchers may utilize member checking as an instrument to allow participants to expand on the information provided during the initial interviews (Palinkas, 2014). If any information was unclear to me, I asked each participant follow-up questions to seek clarification of the data. Member checking

eliminates the possibility of the researcher misconstruing the qualitative data and taking the interviewees' responses out of context (Lub 2015; Birt, Scott, Cavers, Campbell, & Walter, 2016). Researchers may use member checking as a continual process to analyze, interpret themes from the data and present the interpretations to participants for confirmation (Birt et al., 2016). I continued the member checking process by scheduling interviews until all participants confirmed my interpretations and no new information was present.

I was the primary instrument for collecting and reviewing all company documents shared by the participating organization. Researchers conducting case studies strive to represent the multiple realities described by study participants and interpret data collected from document reviews and interviews to construct descriptions of phenomena (Stake, 1995; Bansal & Corley, 2011). Document reviews is one of the most common techniques for data collection in qualitative research (Palinkas, 2014). Document reviews may include company documents such as reports, project documentation, historical records, and archived documents (Boblin et al., 2013). Company documents used in this study included post mortems, meeting minutes, presentations, email communication, policies, standard procedures, security plans, architecture plans and other means of information useful to the study.

A review of company documents was used to supplement interviews and explain security, privacy, and reliability strategies that led to the adoption of IoT devices. These documents can be used to inform researchers with background information about the firms participating in the study, the type of product innovation they undertake, and the

approaches they use to administer product innovation activities (De Massis & Kotlar, 2014). Internal company documents provide contextual information about events that cannot be observed (Stake, 1995). Documents complement interviews as they can be used to validate information and add context to other data sources (Boblin et al., 2013). After completing interviews, I analyzed the company documents to supplement the interview data and highlight decisions, perspectives, and meanings to exemplify the thinking behind the organization's security, privacy, and reliability strategies to adopt IoT devices.

I used methodological triangulation in this study to collect data from more than one data source. Four types of triangulation identified by Denzin (1978) and Patton (1999) include (a) methodological triangulation, (b) investigator triangulation, (c) theory triangulation, and (d) data source triangulation. I used methodological triangulation to analyze the data in my study. Methodological triangulation refers to using more than one data source in qualitative research to understand a phenomenon (Denzin, 1978). Methodological triangulation is the use of two or more sets of data and is used to establish validity (Morse, 2015; Gebauer, Paiola, & Saccani, 2013). Methodological triangulation involves crosschecking complimentary data collection methods to increase the consistency and credibility of a study (Denzin, 1978). I used semistructured interviews and company documents for triangulation as two data collection methods enabled me to crosscheck the data. Methodological triangulation of interviews and use of internal documents strengthened the evidence while increasing reliability and validity of the research (Cronin, 2014; Gebauer et al., 2013). Therefore, I used methodological

triangulation to analyze the data from interviews and company documents to achieve accuracy, reliability, and validity in the data.

Data Collection Technique

Data collection began by conducting face-to-face semistructured interviews consisting of eight questions using the interview protocol in Appendix B. The interview protocol served as a guide during the interviews. The interviews were conducted in a setting that was comfortable for participants. Building rapport helps participants relax and creates an open environment where participants can share information with little hesitation (Berger, 2015). The interview protocol included an introduction to describe the study and included rapport building to make the participants comfortable before asking interview questions for the study (Rivard et al., 2014). I began the interview protocol by introducing myself to each participant and thanked them for participating. I reminded participants about the contents of the signed consent emails and gave them an opportunity to ask questions or share their concerns.

Next, I explained the interview process to each participant and explained that the interviews would be audio recorded, transcribed, and interpreted by me. I reminded participants that the recording was part of the data collection and would remain confidential. I turned on the audio recording devices and announced the date and identifying code name of the participant. I asked the participant the first question in my interview protocol and allowed them to finish their response before moving on to the next question. If a participant response required additional information or clarification, I asked probing questions. Researchers must preserve flexibility by adjusting the interview

protocol based on participant responses to gain the most out of interview responses (Gioia et al., 2013). I refined the interview protocol as necessary to ensure the interview questions were clear and enabled participants to address the primary research question. I continued through the interview questions until all questions are answered.

After the interview questions and responses were complete, I asked participants if they wanted to share additional information about the topics covered during the interview. I asked participants if they were aware of any company documentation that may be relevant to the topics discussed. I explained the concept of member checking and scheduled a follow-up interview to review my interpretations with each participant. I completed the interview by turning off the audio devices and thanked the participant for contributing to the study.

After each interview was complete, I transcribed the audio recordings of each interview into separate Microsoft Word documents. I removed any identifiable information from the transcription and used code names for each participant to ensure confidentiality. An audio recording of an interview enables researchers to listen to an interview multiple times to increase their understanding during transcription (Gale, Heath, Cameron, Rashid & Redwood, 2013). The audio recording of interviews allows researchers to listen and interpret the interviews based on their understanding (Morse, 2015). I interpreted the transcriptions based on my understanding of the literature and the feedback presented by participants during interviews. While interpreting the transcriptions, I searched for themes between the literature and interview feedback. Transcribing audio allows researchers to analyze the data and search for themes (Irvine et

al., 2013). I continued this process with each transcription in preparation for member checking interviews.

After each individual interview was complete, I scheduled a follow-up interview with each participant for member checking. Member checking enhances the credibility of the data collected in the study (Houghton et al., 2013). In preparation for the member checking interview, I analyzed the data collected from the preliminary interview, interpreted the data, and searched for themes. Researchers use member checking to explore the credibility of data and share the results with participants to check for accuracy (Birt et al., 2016). During each member-checking interview, I asked the participant to confirm my interpretations and understanding from their interview to ensure it accurately reflected their experiences, meanings, and perspectives. Participants' experiences and the researcher's interpretation of the interview may be confirmed during member checking (Birt et al., 2016). If any information was unclear to me, I asked participants follow-up questions to seek clarification of the data. I asked each participant if he/she had any new data to share with me. If I received new information from the participant, I scheduled an additional follow-up interview and repeated the member checking process. A researcher continues member checking until the participants confirm all interpretations, the participants provide no new information and additional clarification is no longer required (Caretta, 2016). I repeated the member checking process by scheduling interviews until all participants confirmed all my interpretations and no new information was present.

Company documents that contained the organization's policies and procures were used to corroborate information from other data sources. Qualitative researchers use

information found in documents to support information from other data sources such as interviews (Gebauer et al., 2013). Company documents supplemented the data from the interviews and helped to provide a more thorough understanding of the data. A review of current policy documentation strengthened the findings and led to a greater understanding of a study (Yilmaz, 2013). Internal company documents provide contextual information about events that cannot be observed (Stake, 1995). I emailed the primary contact of the organization to help identify and provide access to company documents pertaining to security, privacy, and reliability strategies for IoT adoption. I emailed the participants who identified the documents during interviews to determine the source and purpose of the documents.

Data Organization Techniques

Data organization was a critical component for analyzing and interpreting my study's data. Gioia et al. (2013) explicated that efficient organization of data allows researchers to analyze the data more effectively, leading to an effective delivery of the findings in the study. Efficient organization of data reduces mistakes and facilitates analysis for effective communication of the study's findings (Gorgolewski & Poldrack, 2016). Data organization techniques in research include data storage, security, preservation, retrieval, and ethical considerations (Pinfield, Cox, & Smith, 2014). I used a password protected Microsoft Excel spreadsheet to organize all artifacts including consent forms, emails, transcripts, and date of interviews. I used Microsoft Word to write consent forms, document the interview process and transcribe individual interviews in separate documents. I used separate folders in my encrypted flash drive to organize

participant information, interview data, audio recordings, member checking data, and organization artifacts. I also used sub-folders to categorize the data and artifacts.

All organization and participant names were masked in this study to ensure confidentiality. Masking may be used to keep organization and participant names confidential (Heffetz & Ligett, 2014). Grossoehme (2014) encouraged the practice of data confidentiality to ensure individuals in the study are not identified by others outside of the study. I mapped the masked code names with the real participant names in a password-protected Microsoft Excel spreadsheet for my reference only. I assigned each participant a masked code name ranging from Participant 1 to Participant 10 to maintain their confidentiality and track their data. I only included the masked code names in the study to avoid links between the data and the participants or the organization. Drake (2013) suggested the removal of links between the participant and the data to prevent re-identification. Also, I stored all private and confidential data such as signed consent forms, interview recordings, and company documents containing the organization's name on a password-protected flash drive stored in a locked storage cabinet. After 5 years of CAO approval, I will destroy all physical and electronic copies of the research data, including the consent forms, interview recordings, and transcribed data.

Data Analysis Technique

Data analysis began by searching the data I collected continually until I had a meaningful answer to my research question on security, privacy, and reliability strategies organization IT leaders use to adopt IoT devices. Data analysis is one of the most important steps in a research study (Leech & Onwuegbuzie, 2007). Researchers may use

inductive reasoning by searching for patterns in the data to understand actors' perspectives (Guba & Lincoln, 1985). I analyzed interviews, company documents and artifacts relating to security, privacy, and reliability strategies, policies, and processes. I categorized the data into themes and developed an understanding on strategies organization IT leaders used to adopt IoT. Constant comparison analysis is also known as coding, where the researcher categorizes the data into smaller and meaningful chunks (Leech & Onwuegbuzie, 2007). I also sought to understand and interpreted the meaning of all the participants' perspectives. Qualitative researchers may follow a process where they can interpret or gain an understanding of data through inductive reasoning (Yilmaz, 2013). Thus, I used methodological triangulation to find a meaningful answer to my research question.

The purpose of my data analysis was to uncover themes from multiple data sources that answered the central research question. Using more than one type of analysis can improve the rigor and trustworthiness of the findings (Leech & Onwuegbuzie, 2007). I used methodological triangulation by supplementing interview data with company documents to gain a thorough understanding of the security, privacy and reliability strategies used to adopt IoT. Researchers use methodological triangulation to develop a thorough understanding of the phenomenon, as it will improve the accuracy, reliability, and validity of the research study (Denzin, 1978). Researchers use methodological triangulation to ensure that data is rich in depth by using different levels and perspectives of the same phenomenon (Fusch & Ness, 2015). Methodological triangulation was fitting

for my study because it enabled me to search for the same themes across multiple data sources.

I used coding in this study to look for explanations, patterns, relationships and underlying meanings of the data. Coding refers to the constant comparison of data (Miles & Huberman, 1994). Coding allows the researcher to categorize the data from multiple sources into smaller and meaningful chunks (Leech & Onwuegbuzie, 2007). Coding allows qualitative data to be shown efficiently and demonstrates the presence of constructs and their relationships (Bansal & Corley, 2011). During the data analysis process, I performed the following activities in sequence:

1. Familiarized myself with all the data collected from the interviews and company documents to produce themes.
2. Listened to interview recordings, read interview transcripts and reviewed all company documents.
3. Generated a list of codes that represented the data and my research question.
4. Continued to add to the list of codes as new codes emerged from the data.
5. Used codes to search and distinguish themes, patterns, and relationships in the data.
6. Categorized the codes, established major themes, and ensured they aligned with my primary research question.
7. Repeated the steps above until no new themes and codes were found and the primary research question had a meaningful explanation.

Researchers use NVivo Qualitative Data Analysis Software (QDAS) during data collection, data analysis and data representation (Woods, Paulus, Atkins, & Macklin, 2015). NVivo can be helpful for researchers as a data management tool while offering a comprehensive audit trail as it can capture decisions made by the researcher during the research process (Houghton et al., 2013). I used NVivo to manage my data and kept an audit of my decisions during data collection and data analysis. NVivo can facilitate the search patterns for words, codes or themes (Leech & Onwuegbuzie, 2007). I utilized the search features in NVivo to facilitate my findings during data analysis.

Data analysis began by importing the data I collected into NVivo to manage and organize the data, analyze the data, and find insights within all of the collected data. During data analysis, data was organized such that concepts or categories were created to indicate the trustworthiness of the study (Elo et al., 2014). NVivo increased the accuracy of the themes or codes generated from the data because it searched all of the imported data to produce the resulting themes or codes (Woods et al., 2015). NVivo software was used for coding, mind-mapping, and to identify themes and categorized the data into meaningful units to gain a better understanding of the data. The word count feature of NVivo was used as an additional type of analysis to find the frequency of words used by participants during interviews and in company documents. Word count allows for searching for patterns in the data, which may result in themes (Miles & Huberman, 1994). The use of NVivo supplemented my findings by generating word trees, word clouds, mind maps, and graphs to provide a visual representation of the data and summarized my findings.

I found major themes by searching for patterns and recurring themes that correlated with security, privacy, and reliability strategies and the five characteristics of the DOI theory. Categorizing the data will help researchers correlate the major themes in the literature and the conceptual framework and answer the primary research question (Boblin et al., 2013). Major themes made themselves present after a thorough analysis of the data (Frels & Onwuegbuzie, 2013). I included data from the literature review when it was relevant to my research question, conceptual framework or data I collected during data collection. Including data from the literature will enhance the search to find major themes (Bansal & Corley, 2011). I searched for newly published studies that were relevant to my research question, conceptual framework or data I collected. I included new studies I found during my data analysis. I repeatedly sorted, arranged, assembled and analyzed the data until major themes and trends emerged that were consistent with my research question.

Reliability and Validity

During this study, I included reliability and validity strategies to produce a quality research study. Establishing data reliability and validity is essential in qualitative analysis (Houghton et al., 2013). Qualitative researchers must address reliability and validity when designing, analyzing, and judging the quality of a study (Patton, 1999). Qualitative researchers conceptualize the concepts of reliability and validity in research as trustworthiness, rigor, and quality (Yilmaz, 2013). This section includes a description of the strategies I executed to ensure I addressed validity and reliability in this study.

I included the use of an interview protocol and member checking during this study to ensure reliability. Reliability in qualitative research refers to the consistency and repeatability across researchers and studies (Lancaster, Kolakowsky-Hayner, Kovacich, & Greer-Williams, 2015). Reliability is the result of a process that produces a dependable, consistent, and replicable outcome (Houghton et al., 2013). I used the interview protocol as a guide to ensure consistency in the process during interviews. Meanwhile, I used member checking to ensure consistency in my interpretation of each participant interview. Researchers may use a variety of strategies to ensure reliability in qualitative research (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). However, it can be difficult to replicate a qualitative study due to the subjective nature of the researcher and participants. One way a researcher can demonstrate reliability is to document research procedures during the process (Grossoehme, 2014). Therefore, I used an interview protocol, member checking to demonstrate reliability and ensured the findings were consistent, and dependable based on the data collection processes.

This qualitative research study seeks to be accurate, reliable, valid, and trustworthy. Validity relates to the accuracy of the research data (Yilmaz, 2013). Guba and Lincoln (1985) developed criteria to ensure rigor in qualitative research and used the term trustworthiness to describe credibility, transferability, dependability, and confirmability. These criteria are equivalent to the quantitative criteria of internal validity, external validity, reliability, and objectivity respectively (Morse, 2015). The four criteria for trustworthiness are relevant for qualitative research studies to be authentic,

reliable and transparent (Cronin, 2014). I used strategies to address each individual criterion in the following subsections.

Dependability

I used an interview protocol, member checking, and methodological triangulation to ensure dependability during this study. Guba and Lincoln (1985) explained that dependability is an alternative criterion for judging the reliability and trustworthiness of qualitative research. Dependability refers to the integrity and stability of collected data and findings (Marshall & Rossman, 2016). I included member checking to ensure completeness and accuracy in the interpretation of the interview data. Researchers may have a variety of strategies to ensure data dependability, such as member checking and triangulation (Carter et al., 2014). I used the interview protocol (see Appendix B) to establish consistency between participants during the semistructured interviews. Qualitative researchers can also document processes and procedures to establish dependability in the research (Marshall & Rossman, 2016). Triangulation decreases the deficiencies of a single source, as the interpretation of multiple sources will instill more confidence in the findings (Cronin, 2014). Therefore, I used methodological triangulation to confirm my findings and improved the dependability of this study.

I included an audit trail to increase dependability throughout the study. Dependability in a study includes the use of an audit trail (Houghton et al., 2013). An audit trail includes an outline of decisions made by researchers and provides a rationale for the judgments (Guba & Lincoln, 1985). I explained all the processes and phases of the research elaborating on every aspect of the study. I described in detail the purpose of the

study, the design of the study and the participants. Maintaining an audit trail of records, notes and documents on all aspects of the research procedure enhances the dependability of a study (Frels & Onwuegbuzie, 2013; Marshall & Rossman, 2016). I provided an audit trail by detailing the collection of data, analysis of the data, the development of the themes and interpretation of the results. NVivo can provide a comprehensive audit trail to represent decisions made by researchers during the research process (Houghton et al., 2013). I used NVivo as a qualitative data analysis software tool to ensure an audit trail was documented and organized.

Credibility

This single case study sought to achieve credibility by including organization IT leaders as participants in the study. Credibility refers to the accurate identification of participants to ensure truthfulness in the data (Elo et al., 2014). For this case study, organization IT leaders participated in interviews to field questions about strategies they used to adopt IoT devices for their organization. I used member checking to confirm my interpretation of each interview. Member checking is the most important technique for establishing credibility by allowing the participants to verify the accuracy and credibility of the researchers' account of their experiences (Lincoln & Guba, 1985). Birt et al. (2016) explained that reporting member checking outcomes makes the research credible, not the procedure to complete it. The participants shared their first-hand experiences of the phenomena during data collection. To achieve credibility in the study, the evidence of the phenomena came from participants who were involved in the decision to adopt IoT devices at their organization.

Transferability

During this study, I included rich descriptions of the context and procedures to ensure transferability of the research. Transferability refers to the researcher's responsibility to describe the research adequately for readers to make an informed decision about the transfer of the findings to another context (Guba & Lincoln, 1985). Stake (1995) suggested using a thick description to describe the research such as accounts of the context, research methods used and examples of raw data. Since this was a single case study, findings were based on an individual IT organization and may not be suitable to other contexts. Unlike external validity, transferability does not involve broad claims (O'Sullivan & Conway, 2016). However, findings can be theoretically transferable to other contexts if researchers provide rich data with a detailed description of the case study (Lub, 2015). Therefore, I provided thick descriptions for future readers to determine whether they can apply this research in the future.

Confirmability

During this study, I presented objective findings to ensure confirmability. Confirmability refers to the objectivity of the data's accuracy, relevance or meaning (Elo et al., 2014). I used methodological triangulation by reviewing company documents to confirm findings from interviews. As with dependability, researchers can use triangulation and an audit trail to address confirmability (Morse, 2015; Houghton et al., 2013). Likewise, the interview protocol, recording of interviews and member checking contributed to confirmability. Researchers achieve confirmability once they establish credibility, transferability and dependability (Frels & Onwuegbuzie, 2013). Furthermore,

the use of NVivo software confirmed findings and themes because of constant comparison analysis (Leech & Onwuegbuzie, 2007). NVivo helped to identify the reoccurring themes in the data and was an indication that data saturation was achieved.

I used data from semistructured interviews and company documents to achieve data saturation. The lack of any new emerging data or concepts will lead to data saturation (Houghton et al., 2013). I used in-depth semistructured interviews with IT leaders at a single IT organization. I interviewed participants until no new information was present. A researcher achieves data saturation when interviews with research participants do not yield new themes (Higginbottom, Rivers, & Story, 2014). I used company documents to confirm findings from the interviews. Data saturation is realized when information emerges so repeatedly that the researcher can expect it (Frels & Onwuegbuzie, 2013). Repetition of data and failure to identify new themes led to evidence of saturation.

Transition and Summary

Section 2 included the intent, research design, population sample, and analytical methods used for this study about IoT adoption. Conducting a qualitative case study enabled exploration of security, privacy, and reliability strategies to adopt IoT devices at an IT organization in the state of Connecticut. I gathered data from the review of company documents and conducted semistructured interviews to build understanding and knowledge of leadership strategies to support IoT adoption. Section 3 includes an overview of the completion of the study and a presentation of findings from the analysis of collected data. Section 3 also includes the application of the research to professional

practice and the presentation of recommendations, implications for social change, reflections, and conclusions resulting from the conduct of the study.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative exploratory case study was to explore strategies that organization IT leaders use for security, privacy, and reliability to enable the adoption of IoT devices. I collected data from a leadership team in the Stamford, Connecticut area in the United States, interviewing and performing member-checking sessions with eight organization IT leaders and collecting 15 company documents. The IT leaders I interviewed were executives or were a part of a management group with direct reports and had decision responsibility regarding security, privacy, and reliability strategies for IoT adoption. In this study, I used the DOI theory as the conceptual framework to explore strategies used by an organization to address the security, privacy, and reliability concerns of IoT and close the knowledge gap in the literature.

Data collection included semistructured interviews with each participant and the collection of company documents pertaining to security, privacy, and reliability. I used semistructured interviews to gain details, which allowed for clarification from each participant. Company documents from the organization provided methodological triangulation of the data. The collection of company documents included marketing collateral, PowerPoint presentations, policy documents, procurement documents, and videos of interviews with the leadership team discussing IoT and security, privacy, and reliability. Interview responses and company documents were loaded into NVivo software, which helped categorize themes from the participants' responses.

Presentation of the Findings

The main research question that guided this study was as follows: What are security, privacy, and reliability strategies used by organization IT leaders to adopt IoT devices?

This section encompasses a dialogue of the five main themes I identified through the study. I used methodological triangulation to analyze the data from semistructured interviews with follow-up member checking interviews, an audit trail, and company documents and procedures related to IoT security, privacy, and reliability strategies. The presentation of the findings from the data collection includes the case organization's security, privacy, and reliability strategies and how the DOI theory influenced those strategies. Four major themes emerged during my analysis: securing IoT devices is critical for IoT adoption, separating private and confidential data from analytical data, focusing on customer satisfaction goes beyond reliability, and using IoT to retrofit products. These themes illustrate potential strategies related to securing sensitive data, segmenting confidential data for privacy, and ensuring the reliability of the services delivered to clients by using IoT.

Theme 1: Securing IoT Devices is Critical for IoT Adoption

The security of IoT devices was the first theme to emerge from data collection. IoT has earned a bad reputation amongst organizations because of the number of security vulnerabilities it presents. The participating organization acknowledged and addressed IoT security requirements to comply with regulations prior to implementing their revamped products. Study findings showed that security was an essential part of the case

organization, irrespective of the technology. Multiple participants indicated that security is part of the philosophy and is an essential factor when gaining a customer's trust. An IoT security strategy was also essential when collaborating with partners or clients because it gave them credibility to conduct business. Participant 5 indicated there are many similarities in the security strategies between IoT and existing technologies. The security strategy included limiting access to the devices, securing the network, limiting access to the customer network where the devices were located, and using encryption.

All eight participants at the case organization indicated that security was a critical factor for IoT adoption, and 13 of 15 company documents supported the theme (see Table 1). All participants indicated the need for having a security strategy so that their clients can focus on productivity and efficiency gains without having to worry about managing access controls or preventing adversaries from accessing their devices. All participants pointed out that there are regulations around security and that this was the highest priority requirement when considering strategies for IoT adoption. Seven of eight participants also referenced the decisions around the security strategy and suggested that IoT had a negative public image resulting from incidents that led to security breaches at other organizations. The case organization avoided using the phrase Internet of Things when marketing their product and discussing security strategies with clients. Two of eight participants indicated that when presenting the IoT products to clients, they addressed their products as solutions rather than IoT devices.

Table 1

Frequency of First Major Theme

	Participant		Document	
Major theme	Count	References	Count	References
Securing IoT devices is critical for IoT adoption	8	77	13	98

The security strategy described by the case organization aligns with several studies found in the literature where IoT users expressed security as the biggest concern. According to a survey about ongoing European projects on IoT security, major security challenges included the need for access controls, policy enforcement, trust, mobile security, secure middleware, and authentication with authentication and access controls receiving the most responses (Balte, Kashid, & Patil, 2015). Ravindran, Yomas, and Jubin Sebastian (2015) indicated that IoT includes machine-to-machine, machine-to-man, man-to-machine, or machine-to-mobile communication and that security vulnerabilities exist at the application layer, the transport layer, and the sensing layer. The feedback from Participants 1, 2, 4, and 5 indicated that they secured their IoT solution at every endpoint when connecting to the cloud, including the three layers cited. In addition to the securing the layers above, existing security measures such as firewalls, antivirus, and intrusion detection systems were implemented.

As the conceptual framework of this study, the five characteristics of the DOI theory explain the case organization's IoT security strategy. Ramavhona and Mokwena (2016) suggested that the five characteristics of the DOI theory and the external factors awareness and security were critical in the factors that influenced the adoption of Internet banking in South African rural areas. The findings revealed that the intention to adopt Internet banking services could be predicted by awareness, compatibility, trialability, and

security (Ramavhona & Mokwena, 2016). The case organization's approach followed the DOI theory as a guideline to adopt and implement security strategies for innovative technologies such as IoT. They illustrated compatibility by using existing security standards to secure IoT. Although additional infrastructure for the cloud was added, IoT used many of the existing security procedures and technologies. Choi and Kwak (2016) suggested additional security measures are necessary for IoT devices because it introduces sensors. Choi and Kwak also noted that organizations must address vulnerabilities at each layer. Participants 1, 2, and 5 indicated that they addressed the complexity of securing IoT in multiple layers by using existing security procedures and technologies.

The case organization focused on delivering a solution that provided value for their customers and included security as an integral part of that solution. A trial period would provide customers with an opportunity to test the solution to ensure it meets their security requirements. Trials allow organizations the necessary time to test all the possible use cases for the candidate product (Nair, 2017). This aligned with Participant 2's feedback where the case organization experimented with the IoT devices internally before releasing it to their clients. Participant 1 agreed that trialability was an important part of securing IoT devices because the solution was tested end to end to limit vulnerabilities to the devices, internal network, customer network, and the cloud. The strategy was to conduct tests internally including penetration testing before launching a pilot for a few customers for a short duration to ensure stability before releasing the solution for the entire customer base. Participant 6 added that this proved to be valuable

for the organization and their customers because it enabled continuous development and small releases to limit defects while providing the core security functionality requested by their customers.

The case organization began their security procedures ensuring that their existing access controls would be compatible with the IoT devices. Compatibility was significant for the case organization because they wanted to use their existing security infrastructure to limit users from accessing the IoT devices. There were only a limited number of users who would use the product, thus limiting the chance of a breach if an unauthorized user accessed the device or if the device was stolen. Authorization, authentication, and access controls limit user access and limit accidental harm to IoT devices (Iqbal, Suryani, Saleem, & Suryani, 2016). In a study about IoT security solutions, the compatibility between the IoT devices and the security infrastructure was a vital part of IoT adoption (Li, Tryfonas, & Li, 2016). In a similar study, Pasha, Shah, and Pasha (2016) supported the need for access controls as it limited access to the data or resources in an IoT system by using existing infrastructure to authorize and authenticate users. Participant 3 reinforced the point that access controls enabled the case organization to leverage their existing directory servers to authorize users. Participant 4 indicated that they limited user access on the devices to prevent users from accidental threats or from insider threats. Compatibility of access controls for IoT devices was also important for customers because they did not want their network to connect with other external networks including with the case organization's network to limit exposure to sensitive data such as credit card data, medical statements, and financial statements.

Encryption is another method that is compatible with most existing infrastructure to keep IoT data secure. The case organization used hardware security modules on the IoT devices and software to encrypt all data. Encryption allows IoT devices to keep data secure while it is in transit to prevent potential DoS attacks (Kang, Park, Kwon, & Jung, 2015). Participant 2 posited that their devices are designed to transmit messages over an open network thanks to their existing encryption processes and procedures. Participant 3 advised that the process of encryption is compatible with any platform, including IoT and mobile. The devices connect to the cloud/data center over a Transport Layer Security (TLS) connection. Participant 8 added that they are unable to access the device on the customer's network, so the customer's network is used to send the analytical data to the cloud when the device is online. This reduces concerns from customers because the client networks are isolated from the case organization's network and does not require changes to the client organizations to conduct business. Jing et al. (2014) recommended against cloud computing if the organization has sensitive data, such as medical and financial data. The case organization decided against that recommendation, although the data sent to the cloud were not sensitive. Furthermore, Participant 1 suggested that the organization's strategy was to secure the data at the customer site before it reached the cloud. Moving to the cloud has become a trend for many organizations because of the cost benefits in comparison to the cost of a data center. In addition, the data can remain secure with appropriate processes. In an international survey about influential IT management trends, 70% of respondents indicated that they would outsource their infrastructure to a cloud service provider (Luftman et al., 2015). Participant 4 suggested

that organizations are concerned about security in the cloud but can overcome their fear by using their existing encryption schemes in cloud. Participant 5 added that if a move to the cloud is not on an organization's roadmap in the future, they might not survive due to the costs of maintaining an infrastructure. Thus, organizations must plan accordingly to ensure they do not fall far behind.

In addition, compatibility plays a role with the Internet connectivity and the network where the IoT device is connected. IoT devices that interact over the cloud should be equipped with capabilities including security keys, cryptographic algorithms, and hidden IDs for them to remain secure (Puliafito, Celesti, Villari, & Fazio, 2015). The feedback from Participant 6 was consistent with the study's strategy because the case organization used their existing hardware-based security procedures and created a unique certificate that was stored on each hardware-secured device to manage the Internet connectivity from the device. Participant 1 added that the certificate on the IoT device along with a public key from the server is located on the hardware module and allows for mutual authentication between the device and the server. Pasha et al. (2016) supported this mutual authentication process and suggested the use of TLS with a certificate validation mechanism for authentication and secure key distribution. As a supplemental security strategy, Participant 1 suggested rotating the device certificate over time or blacklisting the devices if the device falls into the wrong hands or if someone tampers with the device.

Complexity is another DOI characteristic that affects security because more than one solution may be required to reduce security vulnerabilities. However, not all

solutions have to be technical. Bullée et al. (2015) suggested that the development of a security culture could be a countermeasure against security vulnerabilities. Vuuren (2016) suggested security awareness and education to change the mindset and behavior of employees since information security technology controls are often not enough. Most participants indicated that security is part of their organizational principles because it is complex and requires a greater team to ensure data remains secure. Participant 5 indicated that many security strategies are determined during an Architectural Review Board where employee participation is encouraged as a method to build awareness in the organization to limit vulnerabilities such as insider threats and vulnerabilities. Also, understanding the threats, implications, and possible solutions to the threats would only help employees speak confidently with customers about the security of the devices. Participant 5 pointed out that there are security reviews that ensure that products meet the product requirements for security. Participant 7 added that there are numerous internal security requirements that require implementation prior to making the solutions available to customers. An example of internal security requirements includes the monitoring of IoT devices to detect suspicious activity (Jin-Xin, Chin-Ling, Chun-Long, & Kun-hao, 2017). Participant 1 supported the complexity of security and added that they also conduct penetration testing on the IoT device and the network to ensure the device remains secure. Thus, the complexity of IoT required the case organization to have more than one solution to ensure the data remains secure.

The DOI characteristics of observability and relative advantage are two characteristics in the DOI theory that did not play a significant role in the security

strategy even though the characteristics were a significant part of IoT adoption overall. IoT security lacks a standard that causes friction for organizations because the risks involved are higher than the return on investment (Lee & Lee, 2015). The growing IoT security concerns prevent potential adopters from integrating IoT as a solution (Li et al., 2015). Since IoT security was not a feature to present to leadership, observability did not play a role in security. Relative advantage was also not relevant for security because of the lack of standards and risks involved to secure IoT devices.

Organization IT leaders should consider a framework such as the DOI theory as a guide to build a security strategy. Organization IT leaders should emphasize the need for a security strategy and build a culture where security is a priority. The culture should establish formal review processes that includes cross-functional teams where security strategies may be deliberated. These review processes should clearly establish the goals and objectives for the meetings and an implementation strategy to ensure the product is secure for their customers. The security strategy should include a trial period for customers to use the product and ensure that it meets their security requirements.

Theme 2: Separating Private and Confidential Data From Analytical Data

The separation of private data from analytical data on IoT devices was the second theme to emerge from data collection. Keeping private data confidential is important for organizations to gain their customers' trust. The case organization understood the importance of privacy and tried to address privacy issues during the requirements discussions. Participant 5 indicated that an organization's existence relies on keeping PII confidential for several reasons, including regulatory requirements and client

requirements. People have debated privacy issues for centuries so it is essential for organization leaders to address it when introducing a new technology such as IoT (Zhou & Piramuthu, 2015). However, keeping data confidential is challenging because IoT's objective is to make data available for organizations to make better decisions. Participants 1, 3, 4, 5, and 7 suggested that a privacy strategy is important for any technology, especially for IoT because of the volume of data it transmits. Thus, they were required to have a privacy strategy to address industry regulatory requirements and their client requirements.

All eight participants at the case organization indicated that privacy was a critical factor for IoT adoption. Nine of 15 company documents supported the theme (see Table 2). All participants indicated the need for a privacy strategy to ensure confidentiality and to meet regulatory requirements. Participants 1 and 5 explained that privacy is all about securing your communication with the IoT device and not allowing other users to look at it. Participants 2 and 3 explained that the case organization is highly regulated and that they must adhere to the best practices for privacy. Participants 4 and 5 explained that data is encrypted while it is in transit to ensure it remains private. Five of eight participants pointed out that the same encryption processes would exist regardless of the technology because the goal was to encrypt all data in transit and all data at rest. Six of eight participants also explained that the case organization did not collect PII. However, all data were treated the same regardless of whether the data was sensitive.

Table 2

Frequency of Second Major Theme

	Participant		Document	
Major Theme	Count	References	Count	References
Separating private and confidential data from analytical data	8	61	9	67

An effective privacy policy helps to gain the trust of business partners and clients. Multiple studies found in the literature supports the privacy strategy described by the case organization where IoT users expressed privacy as an important part of conducting business. In a study about the resistance of IoT adoption, professional football players and coaches described the lack of privacy IoT would bring to the league because a controlled predictive model would judge each player on their performance instead of allowing each player to learn from their failures on the field (Trequattrini, Shams, Lardo, & Lombardi, 2016). Similarly, third party applications may intercept the location of IoT devices since devices often share their location with other devices (Hahn, 2017). IoT users may not know they are sharing that data or they may share it unwillingly which lead to privacy issues. The case organization had the same concerns about privacy. Participant 4 described the importance of encryption when the data is in transit. Participant 1 added that there are no inbound connections coming into the network where the IoT devices exist as that policy would reduce any privacy issues from the outside network. The case organization's clients acknowledged that the case organization had intentions on keeping all data private. These privacy strategies led to a trustworthy relationship between the case organization and their clients.

The five characteristics of the DOI theory helps to explain the case organization's privacy strategy in detail. A study about IoT adoption at a healthcare company revealed

that the five characteristics of the DOI theory was a key factor in building a privacy strategy to keep patient data confidential while using IoT (Carr, 2015). The case organization faced a similar dilemma of exposing rich, analytical data and keeping private customer data confidential at an early stage when they deliberated on IoT requirements. Compatibility and complexity are two DOI characteristics that played important roles in the privacy strategy. The case organization determined that the best strategy to keep private data confidential was to segment the customer data from the analytical data. Segmenting the private data enabled customers to use IoT without having to modify their existing privacy strategy since they would manage the sensitive data prior to the data reaching an IoT device. Participant 1 explained there is no reason to collect PII because the case organization's focus is on customer efficiency and productivity. Participant 4 suggested PII poses a risk that is unnecessary for what the case organization is trying to accomplish. Participant 5 added that segmenting the PII and the analytical data was the best way to eliminate the privacy risks while still being able to capture analytical data that lead to customer efficiency gains.

Meanwhile, the privacy strategy was low in complexity for the case organization because the only data they used was from the products, which did not contain sensitive user data. The concept of segmenting the data was very important because it addressed the privacy concerns customers had when using IoT. Takai-Igarashi et al. (2017) supported this strategy in their study about genome-based personalized healthcare where they separated the genome data from the sensitive health data. Likewise, a study about end-of-life care included the use of two separate databases to separate the PII data from

the analytical data (Maetens et al., 2016). Meanwhile, several studies in the literature revealed that alternative methods such as de-identifying or anonymizing the data was not effective. Rubinstein (2016) explained that private data may be de-identified, but anonymization was not always a contentious concept because the de-identified data may link to sensitive data. In fact, regulatory standards require organizations to follow a standard operating procedure to ensure sensitive data remains private (Wang, Tsai, Kao, & Hong, 2014). The case organization believes that their method is the safest and least complex way of protecting customer data and it meets the regulatory requirements. Participant 3 explained that the privacy strategy was not complex, addressed the regulatory requirements, and helped to avoid the collection of sensitive data altogether. Participant 7 indicated that the best way to protect private data is to not collect it.

Trialability was another DOI characteristic that played an important role when validating the case organization's privacy strategy. Trialability enables organizations to overcome the fear of privacy by experimenting and allowing customers to provide constructive feedback for improvement (Waite & Harrison, 2015). Similarly, the case organization piloted the IoT devices with a few customers to validate the privacy strategy. They found that the IoT device only transmitted product data, which contained information about how the case organization's clients used their products. Participant 5 explained that key indicators from the data included that manner in which users used the product, the frequency in which they used it and the challenges they had with it, leading to opportunities to optimize the product. The analytical data aided the case organization to up-sell their products while optimizing the client experience without the need for

sensitive customer data. The analytical data provided facts and saved them from guessing about the best methods to enable an improved client experience to allow for a better client experience. This strategy was optimal in preventing a data breach on IoT devices because sensitive data did not exist on the IoT devices. As an additional privacy strategy, the organization used TLS encryption to secure all data in transit and data at rest in case there was any possibility of clients inadvertently sharing sensitive data on the devices. Participant 8 added that their policy is to treat all customer data as sensitive, even if it does not contain private data.

As with the security strategy, observability and relative advantage are two characteristics in the DOI theory that did not play a significant role in the privacy strategy. Technologies have proposed several privacy protection strategies, but most of them are independent and aim at protecting specific privacy attributes (Lu, Qu, Li, & Pan, 2015). Although the trialability of the IoT device demonstrated the benefits of the privacy strategy, the strategy itself was not a feature to help customers get past their internal privacy risks. In fact, IoT has the potential to increase privacy vulnerabilities because it is an additional system to transmit data. Tran (2017) suggested that IoT creates new privacy issues that can lead to consumer harm not covered under traditional privacy statutes. Likewise, relative advantage was not relevant for privacy because the privacy strategy did not enable the case organization to deliver a solution for IoT privacy. Instead, the case organization delivered a privacy strategy to limit vulnerabilities specifically for IoT. Therefore, the responsibility to address privacy vulnerabilities for the internal data would fall on customers.

The DOI theory proved to be a helpful guide to build a privacy strategy. Although the case organization did not use PII or confidential information, they took additional measures to protect their customers from exposing private data before it reaches the IoT device. To reduce privacy vulnerabilities, organizations should separate the sensitive data from the analytical data. In addition, organization leaders should use encryption to keep data confidential in case customers share private data. The privacy strategy should be low in complexity and meet regulatory requirements. Organization IT leaders should experiment with the privacy strategy internally, then pilot the privacy strategy with a few customers to validate the protection of all private data as it will help to gain their customer's trust and reduce any privacy fears when considering IoT adoption.

Theme 3: Focusing on Customer Satisfaction Goes Beyond Reliability

The third theme that emerged from data collection was reliability. IoT reliability has been another concern for many organization IT leaders because their expectations include high availability and high accuracy. The case organization explained that accuracy was more important to their business than high availability because the intent for the analytical data was to improve each customer's efficiency and productivity. According to a study about fiber optic sensing and IoT, the authors concluded that the accuracy and reliability of IoT was essential when connecting a variety of networks (Zeng & Gao, 2014). In a separate study, Bhatia and Sood (2016) explained that IoT provided a higher quality of care for patients in the intensive care unit (ICU) because of the accuracy of the alert data, which resulted in efficiencies that were otherwise difficult to manage manually. Likewise, the case organization used a reliability strategy to ensure

they addressed their customer's IoT requirements. Participant 3 indicated that there are similarities in their IoT reliability strategy when compared to other technologies at the case organization.

All eight participants at the case organization agreed that reliability was an important factor for IoT adoption (see Table 3). Four of eight participants added that high availability was not as important when compared to accuracy because the focus was primarily on customer satisfaction. Five of 13 company documents supported the theme where customer requirements and satisfaction drove the reliability strategy. All eight participants indicated that a reliability strategy was necessary to explain that the focus for reliability was the delivery of accurate information to customers. However, the case organization had to pitch the IoT reliability strategy delicately to their customers because IoT was the recent culprit for numerous breaches and significant downtime at organizations. The case organization did not present their solution as the "Internet of Things" because they acknowledged that there was a negative perception of IoT and they did not require customers to connect their IoT products on WiFi every day. However, they did include a requirement to connect the IoT device to their WiFi once a month to ensure they received the analytical data.

Table 3

Frequency of Third Major Theme

	Participant		Document	
Major theme	Count	References	Count	References
Focusing on customer satisfaction goes beyond reliability	8	48	5	43

Participants advised that their IoT business model did not make high availability a priority because most customers do not require a high uptime for the IoT devices. Participant 6 explained that their business model was different from other business models such as smart cities where IoT high availability is more important. Participant 4 suggested that their customers' reliability requirements may change in the future, but the case organization's customers currently do not have high availability at the top of their priority list. Contrary to the participant feedback, results from multiple studies in the literature revealed that IoT high availability is important to organizations. A study about multipath load balanced routing for IoT explained that network reliability is critical when transmitting data in an environment where organizations use IoT in multiple domains (Tseng, 2016). During a study about IoT in smart city services, Lanza et al. (2015) described the significance of reliability because the services are required to be highly available to ensure public safety and to inform citizens of bad weather conditions, collision warnings, and up to date traffic information in a timely manner. The case organization's IoT reliability strategy was slightly different. Although the case organization supported high availability for their products, they positioned their reliability strategy to include accurate analytical data from the IoT devices every 30 days. This strategy goes against many study findings in the literature because ubiquitous computing implies that devices are always available. A vital characteristic of IoT includes ubiquitous communication, where devices can communicate anytime and anywhere (Konstantinidis et al., 2014; Borgia, 2014). Participant 6 indicated that many customers used the IoT device only on an as-needed basis. Participant 7 added that

excluding the requirement to keep the IoT devices on and connected at all times helped to reduce the friction for customers. Participant 8 added that their focus was on the customer requirements rather than the requirements of the technology.

Relative advantage, complexity, trialability, and observability are characteristics from the DOI theory that supported the case organization's reliability strategy. The case organization's attention to their customers' requirements enabled them to gain a relative advantage over their competitors by providing a reliable IoT product. Likewise, multiple studies in the literature used IoT to provide benefits to gain a relative advantage. A study about a wireless network relay emphasized the relative advantage of having ubiquitous IoT access where the reliability facilitates the quality of the network and increases the chance of IoT adoption (Du, Lu, Sun, Zhang, & Sun, 2017). An e-health study about improving the connection and communication between multiple systems revealed that IoT provides a relative advantage because it enables the ability to access data from anywhere at any time, which was not possible with the existing infrastructure (Suciu, 2015). The case organization had similar challenges to improve the reliability between systems, process the analytical data, and provide feedback to customers to help them become more productive. The relative advantage for the case organization included an opportunity to upsell their products and increase their return on investment. Meanwhile, their customers would be more productive, more efficient, and would lower their operational costs. Participant 3 and Participant 8 indicated that they reduced the complexity of not being able to communicate across networks since the IoT devices were located within each customer network. Participant 2 and Participant 7 explained that the

reliability of the devices were equally important when they were offline because when the devices eventually connected, all the analytical data would be transmitted to the cloud.

The case organization lowered the complexity of their IoT reliability strategy because of the difficulty in keeping their product highly available and accurate at all times. Instead, they sought feedback from customers to gain an understanding about the reliability features that matter most to their business. A good IoT reliability strategy is often less complex and is easier to maintain because there are not as many pieces to manage when compared to a more complex strategy (Chatterjee & Shukla, 2016). During a study about transmission reliability evaluation for wireless sensor networks, Zhu et al. (2016) explained that reliability is complex because it is multidimensional and includes connectivity, performance, and accuracy. The case organization acknowledged that reliability could be very complex, so they focused on customer feedback and made the reliability strategy easy to understand for their customers. Participant 3 indicated that customers would only be required to plug in their IoT devices only once a month so that they can remove the requirement of high availability for customers who did not want to keep their devices online at all times. Participant 4 elucidated that their customer IoT requirements included lower operational costs, connecting multiple systems while remaining on the same network, and improving productivity and efficiency. The case organization met all the requirements with the proposed IoT reliability strategy and the strategy enabled a positive experience for customers.

Similar to the security and privacy strategies, trialability played an important role in the reliability strategy. Studies have shown that trialability is an important asset for an adoption because it enables both the vendor and the customer to see the solution in action. In a study about gateway performance for IoT devices, researchers discovered that trialability was necessary to validate the consistency of the results for high reliability IoT devices (Min, Xiao, Sheng, Quanyong, & Xuwei, 2014). Similarly, an IoT study about device-oriented automatic semantic annotation revealed that researchers were able to confirm the accuracy of the devices through experimentation (Liu, Li, & Deng, 2017). Data accuracy was an essential reliability requirement for the case organization. Participants 4 and 5 implied that although a high uptime was not necessary, the accuracy of the data was important based on feedback provided by customers during the pilot. On the contrary, Participants 1 and 2 indicated that a high uptime was necessary because some customers connected to the IoT device frequently to transmit the analytical data to the cloud. The lack of analytical data would prevent the case organization from providing services to make their customers more efficient and more productive. Therefore, trialability was helpful for the case organization because it substantiated the need for high availability and high accuracy based on feedback from customers.

The DOI characteristics observability and trialability both correlated to the case organization's reliability strategy because of their approach to drive reliability requirements based on customer feedback. Multiple studies have shown observability and trialability interconnected when a solution is ready to be distributed for consumption. Wang, Duan, and Shi (2015) experimented with IoT devices and adjusted their reliability

strategy based on their observation of the device learning capabilities in their study. Similarly, a study about test cases for Ecommerce systems demonstrated the researchers' ability to optimize the accuracy of Ecommerce systems based on observations from previous test cases and from experimentation (Alzubi, 2015). Participants 2 and 5 explained that observations from their customer base was exceptional because the direct feedback resulted in adjustments to the reliability strategy. Participants 4 and 8 explained that their executives observed customer feedback from previous events and added input to their IoT reliability strategy to ensure that it met the customer requirements. Participant 5 added that several prospective customers spoke with the case organization's existing customers and observed the benefits that IoT reliability had on the existing customers. The prospective customers later decided they would like to join the customer base.

Compatibility was not a factor in the case organization's reliability strategy because IoT was a new technology and they did not have any previous experience to drive their strategy. Instead, the case organization leaned on feedback from their customers to accelerate their reliability strategy. In addition, participants did not comment on compatibility relative to their reliability strategy. However, all eight participants explained that compatibility was a factor in IoT adoption as a whole.

Organization IT leaders should consider the DOI theory when formalizing a reliability strategy. Organization IT leaders should stress the need for a less complex reliability strategy and demonstrate their desire for customer satisfaction. They should also request direct feedback from customers because it will ensure they gain a relative advantage while providing value for their customers. Organization IT leaders should

observe customer feedback during a pilot because that will allow customers to see the solution and allow the organization IT leaders to adjust their reliability strategy.

Theme 4: Using IoT to Retrofit Products

The final theme to emerge was the case organization's strategy to use IoT devices to retrofit existing products. The case organization's IT leaders were hesitant to adopt IoT because they were afraid that customers had a negative perception of IoT and the need for a new IoT infrastructure. A new infrastructure was risky because it had potential to cause compatibility issues with the case organization's existing products, which would lead to a significant investment to correct the issues. In addition, customer satisfaction would suffer due to the technical challenges with compatibility. Thus, the case organization's strategy was to deploy IoT without forcing their customers to upgrade their product or move to a new infrastructure. Participants 1 and 5 explained that they looked for ways to retrofit their products with IoT rather than introduce it as a main feature. Participants 6 and 8 elucidated that many customers used their existing security policies when sending data to the IoT device, making it seamless to use the new services.

Six of eight participants provided feedback about the requirement for the case organization to adopt IoT and retrofit existing products. Four of 18 company documents supported the theme (see Table 4). Participants 3, 5, and 8 explained that the case organization's approach was to avoid introducing a complex product that customers would disapprove. Participants 6 and 7 suggested that they responded to customer feedback to provide the requested services that did not require customers to make a significant investment. All six participants described the importance of not mentioning

"The Internet of Things" as a product to their customers because they understood that customers would not accept IoT due to the negative perceptions. Instead, the case organization pitched the solution as a retrofitted solution that offers services to enable customers to be efficient and productive.

Table 4

Frequency of Fourth Major Theme

	Participant		Document	
Major theme	Count	References	Count	References
Using IoT to retrofit products	6	22	4	18

The case organization looked for ways to modernize their legacy product for reporting and analytics purposes, but it was missing an important feature – Internet connectivity. IoT was a good option to connect multiple legacy devices and to enable Internet connectivity on those devices. However, IoT presented security, privacy, and reliability concerns that would cause customers friction when considering adoption. The case organization reviewed all the concerns and developed an infrastructure to ensure there are no privacy, security and reliability issues. However, there were also concerns about potential infrastructure changes that were required to enable IoT adoption. These concerns also align with several studies in the literature where a new infrastructure was evident. At the conclusion of their study, Li, Tryfonas, and Li (2016) revealed that IoT requires a new security infrastructure based on the new technical standards. A separate study about IoT and business process redesign in seaports coincided with the required infrastructure changes and added that the investment costs to switch to the new infrastructure was high (Ferretti & Schiavone, 2016). Participants did not agree on the

notion that they had to change their infrastructure to adopt IoT. Participants 1 and 5 said that with proper planning and a good design, a change in infrastructure was not necessary. Participants 3 and 7 added that IoT use cases vary and some use cases require new infrastructure, but that was not the case with their organization. Thus, the case organization promoted the solution in ways that demonstrated value to their customers and included the point that a new infrastructure was not required to implement the solution.

All five characteristics of the DOI theory were applicable to retrofitting the case organization's product. The DOI characteristic compatibility was the main consideration for the case organization when retrofitting the legacy product. IoT had to be compatible with the existing product to ensure customers gained more value from it. Research has shown that compatibility is an important consideration for upgrades and enhancements. A study about building evacuation services and IoT determined that many parts must be compatible between software-hardware and traditional-new deployed systems in order to overcome security challenges (Gokceli, Zhmurov, Gunes, & Ors, 2017). Another study about analog to digital converters revealed that IoT must be compatible with the consumers' existing values (Zurita, Freire, Tedjini, & Moshkalev, 2016). The feedback from Participant 3 aligns with the studies because the case organization avoided changing the main functionality of their product and limited security, privacy, and reliability vulnerabilities. Participant 8 added that the case organization extended the services of the legacy product to provide improved services and allow customers to use the products effectively. After confirming that the extension of the services was compatible with the

legacy product and new vulnerabilities were not present, the case organization deployed their product to customers with the added benefit of analytical data.

Relative advantage was relevant because the case organization wanted to sell a solution that provided current value and future value using existing products. Retrofitting the product was also an advantage for their customers because modernizing a frequently used product provided value to their business. Multiple studies revealed in their findings that organizations adopted IoT to modernize their business processes. Mishra, Chang, and Chung-Chih (2015) explained that IoT enabled organizations to use enhanced connectivity to automate and regulate numerous BI-applications. Another study about IoT challenges, applications, and trends revealed that farmers make use of IoT to modernize activities related to agriculture, weather forecasting, yielding, and water regulation (Kaur and Kaur, 2017). Participant 5 explained that IoT was a good opportunity to upsell services that the case organization offered without having to make a significant investment. Participant 8 described the benefits that IoT generated for both the case organization and their customers including upselling, productivity gains, and lowering overall costs for both the case organization. Participant 7 added that the analytical data provided accurate maintenance data, which helped to reduce costs for customers because they were able to use the product in a more effective manner. Thus, relative advantage played an important role during the modernization of the case organization's product.

Complexity was another DOI characteristic that played a role in this study due to the support of IoT in the cloud. The case organization had to manage a cloud

infrastructure to retrofit their product with the IoT solution and gain access to the analytical data. This aligns with an IoT study about a healthcare organization that found the process of designing an IoT cloud infrastructure for a legacy application to be complex due to a lack of standardization (Ullah et al., 2017). A similar study about IoT wearable medical devices added that there is great difficulty in balancing the security, privacy, and reliability requirements of an infrastructure while upgrading a product (Lomotey, Pry, & Sriramoju, 2017). The feedback from participants complimented the literature regarding the additional security and privacy measures and the need to upgrade applications in the cloud, particularly around automated reporting and several other back office systems. Participant 8 explained that the cloud added security, privacy, and reliability risks, but it was the optimal solution to address the needs of customers when retrofitting their product. Participant 1 explained that securing the applications in the cloud added a level of complexity that did not exist previously. Participant 5 added that they tried to use existing methods such as encryption in the cloud to ensure the data remained secure while delivering services to their customers. The case organization was able to adopt IoT and enhance their product because of their leadership team's message to simplify the adoption.

Observability was the next DOI characteristic used by the case organization to adopt IoT. The IT leadership team observed the need to provide a more productive and efficient method for customers to use their product. The case organization's customers eventually requested a more efficient and effective way to use their product based on how they actively used it. Multiple studies in the literature have shown that IoT is effective for

productivity and efficiency gains. Ferretti and Schiavone (2016) discovered that IoT adoption's efficiency and productivity gains were worth the high investment costs because the gains outweighed the costs. Yu, Nguyen, and Chen (2016) conducted a study in China with a sample size of 207 high-technology organizations and found that the use of IoT to modernize their products led to efficiency gains, reduced production costs, and reduced material consumption. These studies are similar to the case organization when they automated processes to improve customer productivity and efficiency before their customers requested it. In addition to the productivity and efficiency improvements, the solution enabled the case organization to upsell their products to their customers. Participant 7 explained that the visibility to the analytical data allowed the case organization to send their customers product accessories automatically when they were low in stock. Participant 5 added that this product with IoT has generated the most sales than any other product in the history of the organization because of the visibility into the analytic data, which has resulted in a great return on investment. Therefore, observability was a significant asset in the case organization's IoT adoption as it provided value for both the case organization and their customers.

Trialability is another DOI characteristic that factored in the IoT adoption process. The case organization asked existing customers to participate in a pilot to test and provide feedback about the retrofitted IoT solution before they sold it. The pilot helped the case organization because the feedback from existing customers helped them address regression issues from the existing product. The trialability strategy aligns with other

studies that showed organizations using pilots to test and validate new and innovative technology such as IoT.

A study about an organization that provided public logistics services discovered that piloting enabled them to address issues before deploying the final IoT solution for the public (Qiu, Luo, Xu, Zhong, & Huang, 2015). A construction project in Hong Kong used a pilot to demonstrate advanced decision-making by using IoT to provide a basis for real-time visibility and traceability of the prefabrication-based construction process (Zhong et al., 2017). The pilot facilitated by the case organization yielded valuable feedback from customers because customers immediately saw the productivity gains, which was a significant improvement from the original product. Participant 5 suggested the pilot program was very successful and generated visibility for the IoT solution, which helped when selling the product. Participant 1 added that the pilot allowed customers to see and test the IoT solution, which made them more comfortable before they purchased it. Thus, trialability played an important role for both the case organization and for their customers. The visibility from the pilot raised awareness about the benefits of the IoT solution and helped the case organization sell it.

The DOI theory proved to be a helpful guide to retrofit the legacy product using IoT as a solution. Each of the five DOI characteristics played an important role in the adoption of IoT and presented a relative advantage for both the case organization and their customers. Organization IT leaders considering IoT adoption should observe their customers base to determine if IoT can add more value to their businesses. Organization IT leaders should consider and account for IoT compatibility issues for product upgrades

and enhancements. Organization IT leaders should also reduce the complexity of IoT by first using best practices and pre-existing methods before creating new processes that would require more effort for them and their customers to implement IoT. Finally, organization IT leaders should consider using a pilot during IoT adoption because the customer feedback would improve the quality of the solution and a pilot would help to ensure the organization addresses the primary requirements for the requested solution.

Applications to Professional Practice

The specific IT problem that formed the basis of this research was the perceived lack of security, privacy, and reliability strategies used by organization IT leaders to enable the adoption of IoT devices. Participants in this study provided strategies that organization IT leaders may use to adopt IoT devices. There were different thoughts on security and privacy best practices, indicating that the myriad best practices in the industry applied to different types of projects in a variety of ways. The majority of participants stated that they relied on industry best practices as a guideline. After evaluating the collected data, I identified four primary themes: security, privacy, reliability, and retrofiting the product. Organization IT leaders may use these results as a guide to develop security, privacy, and reliability strategies.

Leaders who are actively seeking to implement IoT at their organization require current information on security, privacy, and reliability prior to adoption because of rapid changes in technology. The knowledge gained from such information will enable organization leaders to ensure appropriate processes and strategies are in place prior to IoT adoption. In addition, the information will allow organization leaders to plan for

solutions in case of new security, privacy, and reliability vulnerabilities. Thus, IoT knowledge was necessary across the organization to ensure a successful adoption. This study's findings were significant to professional business practices in several ways. The best way to describe the findings was to use the DOI characteristics as a vehicle.

Trialability was an important concept for the participating organization in this study due to the lack of knowledge and the vulnerabilities present with IoT. The organization's ability to conduct pilots and experiment with the solution before making it available for public consumption instilled more confidence in the leadership team about the final product. Although risks were known and identified during the experimentation, the organization had to prepare for future vulnerabilities. In fact, the organization had to prepare to field frequently asked questions from consumers relating to security, privacy, legal, and servicability amongst others. Data from this study provides information on the knowledge acquired by organization leaders when formulating strategies to adopt IoT devices and prevent vulnerabilities. Due to the emergence of IoT solutions across industries, best practices from use cases and studies that were made public enabled for a better understanding of IoT adoption. Trialability enhanced the organization's understanding of IoT adoption and made it relative to the solution offered to its consumers.

Compatibility and complexity both played an important role in IoT adoption for the participating organization. IoT had to fit the organization's products and services model, so there was a requirement to port the existing products to use IoT and deliver improved products and services. Meanwhile, the complexity of IoT required further

preparation because IoT is an open framework where data had the potential of being exposed. Therefore, knowledge about the nuances of IoT was required, particularly around security, privacy, and reliability. In fact, the participating organization maintained security certifications to remain credible and ensure trust when advising clients. Additional processes were required to safeguard the data such as limited access to data within the organization to prevent attacks. As a contingency plan the participating organization had to consider legal issues due to the nature adversarial access to data. Even with the precautions illustrated, it was important to consider the increasing rate of data loss.

The next characteristic that was apparent for the participating organization was relative advantage. The organization naturally considered ways to improve productivity, efficiency, and provide value for their customers in order to build strategic relationships. IoT adoption expedited that process due to the ability to derive operational insights from the IoT data. The participating organization utilized IoT to learn about what the organization does well and enabled the business to make better decisions. Thus, the total cost of ownership (TCO) was advantageous considering the value IoT brought to the organization. The most important aspect of productivity and efficiency gains was the value it provided to clients, which ultimately led to stronger relationships.

The final DOI characteristic that had an impact on the participating organization was observability. Contrary to the limted reference for observability in the case studies identified in the literature review, observability was an important element for the organization to decide on IoT adoption. Observability was important, especially since

there was a lack of knowledge about using IoT. IoT was discussed because the organization's challenges and business goals were present and IoT was a solution that had the potential to address those challenges while using technology as a platform to meet the business goals. The concept of using technology as a tool to address organizational challenges is an important takeway from this study. Many organizations often use a new technology to gain an advantage over their competitors when selling products. In the case of the participating organization, the goal was to address challenges within the organization to provide value for clients. Therefore, the visibility of IoT within the organization demonstrated the need for adoption.

The research findings in this study revealed the participating organization's strategies when considering IoT adoption. The study also includes advantages of using the DOI theory as guidance to determine strategies when considering IoT adoption. The knowledge gained about IoT may come different sources, including from previous studies or use cases. However, organizations must consider experimenting with IoT for a trial period to ensure they account for the risks and vulnerabilities it presents. In addition, experimentation with IoT may uncover some complex issues such as compatibility with existing products that may pose a challenge for organizations. Therefore, it is important for organizations to asses other factors beyond relative advantage when considering IoT adoption.

Implications for Social Change

Organizations must understand the risks and rewards of IoT before adoption. Understanding the risks and rewards of IoT requires knowledge. The findings from this

research add to the existing body of knowledge by providing information on the security, privacy, and reliability strategies used to adopt IoT. The implication for social change include the ability for IT organizations to develop tools for detection, prevention, and monitoring of issues. Organizations may benefit from the strategies outlined in this study to improve productivity, efficiency, and provide a better experience for clients. This study's findings and recommendations may serve as a basis for positive social change. Study data supported the conclusion that organizations may achieve IoT adoption by having security, privacy, and reliability strategies to address or limit the vulnerabilities that come with the technology. This research may raise awareness in support of developing and implementing strategies to adopt IoT.

This study may be of value to society as its findings may better position organization leaders for success when considering IoT adoption. Data analysis indicated there is a relationship with the DOI characteristics and IoT adoption as organization leaders who look to implement an innovation must be familiar with each characteristic as a framework to the innovation's acceptance. The DOI characteristics were important as it relates to IoT adoption because it highlighted the areas of concern, particularly around security, privacy, and reliability. Thus, this research addressed characteristics for each area of concern to mitigate the risks prior to adoption.

This study will also indirectly benefit IoT consumers because it illustrated vulnerabilities that organizations must address. Key concerns for most IoT consumers include security and privacy. Reliability was also an important consideration for IoT, especially for organizations such as those in the healthcare industry. IoT has the potential

to play a bigger role in the healthcare industry because it would enable a more convenient option to receive medical care. In some cases, IoT may prove to be a life-saving technology, so reliability would be essential to ensure timely responses of real-time data in critical situations. Another example of IoT making a difference is in smart cities where there is a smaller footprint of pollution. The efficiency of energy combined with the ability to control traffic in an efficient manner will undoubtedly reduce pollution in our cities.

Recommendations for Action

I explored strategies that organization IT leaders use for security, privacy, and reliability to enable the adoption of IoT devices. Study findings showed that security, privacy, and reliability strategies are important for IoT adoption while retrofitting an existing product and porting it with IoT provides value for customers. Organization IT leaders should build a culture where security is a priority for IoT. The organization should create a formal review process with cross-functional teams where they discuss security, privacy, and reliability strategies. The outcome of the review processes should lead to clearly established goals and objectives with an implementation strategy.

Organization IT leaders should separate all IoT sensitive data from the analytical data to protect user privacy. In addition, organization IT leaders should use encryption to keep all IoT data private in case customers share confidential data. The IoT privacy strategy should be low in complexity and meet regulatory requirements. When possible, organization IT leaders should avoid using PII or confidential information to protect IoT users from exposing confidential information. Organizations IT leaders should have a

privacy strategy that addresses confidential data on the network. Limiting access to the network where the IoT device is located will reduce the number of vulnerabilities.

Organization IT leaders should reduce the complexity of a reliability strategy. The leadership team should seek feedback from their customers to ensure they meet their requirements rather than addressing general reliability requirements. Organization IT leaders should plan to include high availability and high accuracy in their reliability strategy. The feedback from customers will determine whether high availability and high accuracy are both required.

Organization IT leaders should include a trial period to allow customers to experiment with the IoT solution and ensure that it meets their security, privacy, and reliability requirements. The trial period will likely instill confidence in customers because they would install the product in their infrastructure and may choose to retrofit an existing product with IoT. Organization IT leaders should consider using their existing best practices for security, privacy, and reliability since there are a lack of standards for IoT. Organization IT leaders should collaborate with their customers to deliver an IoT solution where they agree on security, privacy, and reliability strategies to reduce vulnerabilities. Collaboration will maximize the value for all parties involved.

In general, this study might be beneficial to key community stakeholders and organization IT leaders. I will disseminate a high-level summary of the results of this study to the community stakeholders and research participants via email. Wherever possible, I intend to share the research results using effective and appropriate platforms

such as my place of employment, lectures, conferences, trade journals, and training seminars.

Recommendations for Further Study

I have several recommendations for further research, some deriving from the limitations noted in this research and others arising from the findings of this study. The limitations of this research included the potential influence of bias and preconceived notions on the results due to the subjective nature of qualitative research. The first recommendation is to continue this research with additional qualitative studies at other case organizations to compare with the results of this study. The researchers who conduct additional qualitative studies will provide a greater sample of participants, reduce bias, and generalize the results since the consolidated data would be a result of more than one organization's perceptions and experiences. Also, the inclusion of industries such as manufacturing, transportation and medical would add more insight about how other organizations have addressed security, privacy, and reliability strategies for IoT adoption. The researchers would provide insights about the differences between industries and the role that regulations may play for each particular industry. Researchers conducting such a study may also present an opportunity for standardization and potentially provide a starting point for organization IT leaders to develop strategies for IoT adoption.

Since I only focused on the organization IT leaders' perceptions for my research, I recommend performing the same research and include participants who are software engineers, enterprise architects, and business users to allow for more feedback from users and IT resources. The IoT users and IT resources developing and integrating IoT

solutions would add field knowledge that may contribute to the information organization IT leaders need to develop strategies for IoT adoption. Also, the feedback from the participants will result in a diverse set of perceptions based on their roles and responsibilities that may bring awareness to organizations about specific roadblocks that prevent organizations from adopting IoT. The feedback may also present solutions to those roadblocks, which may contribute to a strategy to assist with IoT adoption.

The acceptance of IoT was a concern for the case organization and especially their customers. Multiple participants commented on this point because of recent breaches that contributed to IoT devices. A few unexpected participant comments included the case organization's intent to present their IoT solution to customers without using the phrase IoT because of the negative perceptions about IoT. This point warrants further research because breaches have increased exponentially in recent years, but not all of it has contributed to IoT. I recommend further research to explore the common pitfalls for general breaches, common pitfalls for IoT breaches, and how IoT may prevent breaches in the future. The result of the study may contribute to a change in security, privacy, and reliability strategies or it may possibly result in organization IT leaders' acceptance of the risk of a breach if the value for IoT adoption is more profitable.

Reflections

My experience with the doctoral study was a small sample of the vicissitudes of life. I never intended to obtain a doctorate, but I found the urge to push myself to reach a goal that many have not achieved. I quickly realized that this process would be much more difficult than I had anticipated. However, I was very determined and driven to

complete what I had started. During the process, I learned how to conduct research, how to analyze data, and how to write the results in a way that may be noteworthy to others. I enjoyed learning about topics that may contribute to my career.

As a professional who has worked as a software engineer, a manager, and an architect involved with delivering software solutions, I have always been interested in solving problems for clients. I have no experience using or developing applications for IoT, but I had exposure to the concepts of DOI and human-computer interactions throughout my career. In this research, I was as attentive as possible in my analysis to remain objective in the results, though it is possible that I unknowingly and unintentionally biased this research through the framing of interview questions and analysis of the collected data. During the study, I learned that presenting an innovative idea to executives will gain more visibility when it addresses an existing problem at that organization and does not require a significant investment to move the idea forward.

Summary and Study Conclusions

Organization IT leaders consider adopting IoT because it provides a relative advantage for their organization. Upon their decision to adopt it, organization leaders communicate the need for IoT to the rest of the organization and share the potential benefits the organization may gain from the adoption. However, IoT adoption is both subjective and complex. Security, privacy, and reliability remain the biggest concerns for many organizations and this study proved that to be true based on the data collected at the case organization. Although security and privacy may remain prominent issues that prevent organizations from adopting IoT, piloting IoT may positively change the

perception of organization IT leaders. IoT requires experimentation to ensure that it meets customer requirements and is compatible with their existing systems. Organizations that are on the fence about IoT adoption may be swayed when they see IoT used within their organization. Organization IT leaders are not concerned about whether IoT can offer benefits to the organization because their interest in IoT proves that fact. They are apprehensive about the vulnerabilities it may present the organization. These vulnerabilities must be planned and strategized to ensure that the organization's gains exceeds the vulnerabilities for IoT.

References

Ahsan, M., Talib, M. R., Sarwar, M. U., Khan, M. I., & Sarwar, M. B. (2016). Ensuring interoperability among heterogeneous devices through IoT middleware. *International Journal of Computer Science and Information Security, 14*(4), 251-255. Retrieved from https://sites.google.com/site/ijcsis

Alam, B., Doja, M. N., Alam, M., & Malhotra, S. (2013). Security issues analysis for cloud computing. *International Journal of Computer Science and Information Security, 11*(9), 117-125. Retrieved from https://sites.google.com/site/ijcsis

Alam, S. S., Khafibi, A., Ahmad, M. I. S., & Ismail, H. B. (2007). Factors affecting e-commerce adoption in the electronic manufacturing companies in Malaysia. *International Journal of Commerce & Management, 17*(1/2), 125-139. doi:10.1108/10569210710776503

Alimo-Metcalfe, B. (2010). An investigation of female and male constructs of leadership and empowerment. *Gender in Management, 10*(2), 640-648. doi:10.1108/17542411011092309

Aldosari, H. M., Snasel, V., & Abraham, A. (2016). A novel security layer for Internet of things. *Journal of Information Assurance & Security, 11*(2), 58-66. Retrieved from http://www.mirlabs.org/jias

Ali, I., Sabir, S., & Ullah, Z. (2016). Internet of things security, device authentication and access control: A review. *International Journal of Computer Science and Information Security, 14*(8), 456-466. Retrieved from https://sites.google.com/site/ijcsis

Al-Jabri, I. M., & Sohail, M. S. (2012). Mobile banking adoption: Application of diffusion of innovation theory. *Journal of Electronic Commerce Research, 13*(4), 379-391. Retrieved from http://www.jecr.org

Al-Jamal, M., & Abu-Shanab, E. (2015). Privacy policy of e-government websites: An itemized checklist proposed and tested. *Management Research and Practice, 7*(3), 80-95. Retrieved from http://mrp.ase.ro

Alkhater, N., Wills, G., & Walters, R. (2015, August). *Factors affecting an organisation's decision to adopt cloud services in Saudi Arabia (pp. 553-557)*. Paper presented at the 2015 3rd International Conference on Future Internet of Things and Cloud (FiCloud), Rome, Italy. doi:10.1109/FiCloud.2015.16

Alshamaila, Y., Papagiannidis, S., & Li, F. (2013). Cloud computing adoption by SMEs in the north east of England: A multi-perspective framework. *Journal of Enterprise Information Management, 26*(3), 250-275. doi:10.1108/17410391311325225

Alzubi, K. (2015). Generating test cases for E-commerce systems. *International Journal of Computer Science Issues, 12*(2), 327-333. Retrieved from http://www.ijcsi.org

Andersson, P., & Mattsson, L. (2015). Service innovations enabled by the Internet of things. *Industrial Marketing and Purchasing Journal, 9*(1), 85-106. doi:10.1108/IMP-01-2015-0002

Arulchelvan, S. (2014). New media communication strategies for election campaigns: Experiences of indian political parties. *Online Journal of Communication and Media Technologies, 4*(3), 124-142. Retrieved from http://www.ojcmt.net

Aslani, A., & Naaranoja, M. (2015). A systematic-qualitative research for diffusion of innovation in the primary healthcare centers. *Journal of Modelling in Management, 10*(1), 105-117. doi:10.1108/JM2-04-2013-0016

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of things: A survey. *Computer Networks, 54*(15), 2787-2805. doi:10.1016/j.comnet.2010.05.010

Ayuso, C., Millán, J. M., Mancheño, M., & Dal-Ré, R. (2013). Informed consent for whole-genome sequencing studies in the clinical setting. Proposed recommendations on essential content and process. *European Journal Of Human Genetics, 21*(10), 1054-1059. doi:10.1038/ejhg.2012.297

Bailey, M. W. (2016). Seduction by technology: Why consumers opt out of privacy by buying into the Internet of things. *Texas Law Review, 94*(5), 1023-1054. Retrieved from http://www.texaslrev.com

Bąk, S., Czarnecki, R., & Deniziak, S. (2015). Synthesis of real-time cloud applications for Internet of Things. *Turkish Journal of Electrical Engineering & Computer Sciences, 23*(3), 913-929. doi:10.3906/elk-1302-178

Balte, A., Kashid, A., & Patil, B. (2015). Security issues in Internet of things (IoT): A survey. *International Journal of Advanced Research in Computer Science and Software Engineering, 5*(4), 450-455. Retrieved from http://www.ijarcsse.com

Bansal, P., & Corley, K. (2011). The coming of age for qualitative research: Embracing the diversity of qualitative methods. *Academy of Management Journal, 54*(2), 233-237. doi:10.5465/AMJ.2011.60262792

Basanta, H., Huang, Y. P., & Lee, T. T. (2016, April). *Intuitive IoT-based H2U healthcare system for elderly people* (pp. 1-6). Paper presented at the IEEE 13th International Conference on Networking, Sensing, and Control (ICNSC), Mexico City, Mexico. doi:10.1109/ICNSC.2016.7479018

Berger, R. (2015). Now I see it, now I don't: Researcher's position and reflexivity in qualitative research. *Qualitative Research, 15*(2), 219-234. doi:10.1177/1468794112468475

Berry, L. E. (2016). The research relationship in narrative enquiry. *Nurse Researcher, 24*(1), 10-14. doi:10.7748/nr.2016.e1430

Bhatia, M., & Sood, S. K. (2016). Temporal informative analysis in smart-ICU monitoring: M-HealthCare perspective. *Journal of Medical Systems, 40*(8), 1-15. doi:10.1007/s10916-016-0547-9

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*(13), 1-10. doi:10.1177/1049732316654870

Boblin, S. L., Ireland, S., Kirkpatrick, H., & Robertson, K. (2013). Using Stake's qualitative case study approach to explore implementation of evidence-based practice. *Qualitative Health Research, 23*(9), 1267-1275. doi:10.1177/1049732313502128

Boos, D., Guenter, H., Grote, G., & Kinder, K. (2013). Controllable accountabilities: The Internet of Things and its challenges for organisations. *Behaviour & Information Technology, 32*(5), 449-467. doi:10.1080/0144929X.2012.674157

Borges Neto, J. B., Silva, T. H., Martins Assunção, R., Mini, R. F., & Loureiro, A. F. (2015). Sensing in the Collaborative Internet of Things. *Sensor, 15*(3), 6607-6632. doi:10.3390/s150306607

Borgia, E. (2014, December 1). The Internet of things vision: Key features, applications and open issues. *Computer Communications, 54*(1), 1-31. doi:10.1016/j.comcom.2014.09.008.

Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of Internet of things. *International Journal of Advanced Networking & Applications, 6*(4), 2372-2378. Retrieved from http://www.ijana.in

Boulos, M. N. K., & Al-Shorbaji, N. (2014). On the Internet of things, smart cities and the WHO healthy cities. *International Journal of Health Geographics, 13*(1), 10. doi:10.1186/1476-072X-13-10

Breslow, J. M. (2014, September 30). *76 of 79 Deceased NFL Players Found to Have Brain Disease – Concussion Watch*. Retrieved from http://www.pbs.org/wgbh/pages/frontline/sports/concussion-watch/76-of-79-deceased-nfl-players-found-to-have-brain-disease

Brody, P., & Pureswaran, V. (2015). The next digital gold rush: How the Internet of things will create liquid, transparent markets. *Strategy & Leadership, 43*(1), 36-41. doi:10.1108/sl-11-2014-0094

Bughin, J., Chui, M., & Manyika, J. (2015). An executive's guide to the Internet of Things. *McKinsey Quarterly, 2015*(1), 1-9. Retrieved from http://www.mckinsey.com/insights/mckinsey_quarterly

Cafiero, C., Melgar-Quiñonez, H. R., Ballard, T. J., & Kepple, A. W. (2014). Validity and reliability of food security measures. *Annals of New York Academy Of Sciences, 1331*(1), 230-248. doi:10.1111/nyas.12594

Caldwell, T. (2016). Making security awareness training work. *Computer Fraud & Security, 2016*(6), 8-14. doi:10.1016/S1361-3723(15)30046-4

Cao, X., Guo, X., Liu, H., & Gu, J. (2015). The role of social media in supporting knowledge integration: A social capital analysis. *Information Systems Frontiers, 17*(2), 351-362. doi:10.1007/s10796-013-9473-2

Caretta, M. A. (2016). Member checking: A feminist participatory analysis of the use of preliminary results pamphlets in cross-cultural, cross-language research. *Qualitative Research, 16*(3), 305-318. doi:10.1177/1468794115606495

Carr, A. (2015). An examination of the adoption of RFID technology in healthcare organizations. *Organization Development Journal, 33*(4), 81-102. Retrieved from http://www.isodc.org

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014, September). The use of triangulation in qualitative research. Oncology Nursing Forum, 41(5), 545–547. doi:10.1188/14.ONF.545-547

Chang, Y., Dong, X., & Sun, W. (2014). Influence Of Characteristics Of The Internet Of Things On Consumer Purchase Intention. S*ocial Behavior and Personality, 42*(2), 321-330. doi:10.2224/sbp.2014.42.2.321

Charman, A. J., Petersen, L. M., Piper, L. E., Liedeman, R., & Legg, T. (2015). Small area census approach to measure the township informal economy in South Africa.

Journal of Mixed Methods Research, 11(1), 36-58. doi:10.1177/1558689815572024

Chassin, M. R. and Loeb, J. M. (2013). High-Reliability Health Care: Getting There from Here. *Milbank Quarterly, 91*(3), 459-490. doi:10.1111/1468-0009.12023

Chatterjee, S., & Shukla, A. (2016). Effect of Test Coverage and Change Point on Software Reliability Growth Based on Time Variable Fault Detection Probability. *Journal Of Software (1796217X), 11*(1), 110-117. doi:10.17706/jsw.11.1.110-117

Chen, C. (2013). Perceived risk, usage frequency of mobile banking services. *Managing Service Quality, 23*(5), 410-436. doi:10.1108/MSQ-10-2012-0137

Choi, S., & Kwak, J. (2016). Enhanced SDIoT security framework models. *International Journal of Distributed Sensor Networks, 12*(5), 1-12. doi:10.1155/2016/4807804

Chun, G. J., Sautter, J. M., Patterson, B. J., & McGhan, W. F. (2016). Diffusion of pharmacy-based influenza vaccination over time in the united states. *American Journal of Public Health, 106*(6), 1099-1100. doi:10.2105/AJPH.2016.303142

Chung, K., & Holdsworth, D. K. (2012). Culture and behavioural intent to adopt mobile commerce among the Y Generation: Comparative analyses between Kazakhstan, Morocco and Singapore. *Young Consumers, 13*(3), 224. doi:10.1108/17473611211261629

Cleveland, S., & Ellis, T. J. (2014). Orchestrating end-user perspectives in the software release process: An integrated release management framework. *Advances in Human - Computer Interaction, 2014*. doi:10.1155/2014/805307

Cobban, S., Edgington, E., & Clovis, J. (2008). Moving research knowledge into dental hygiene practice. *Journal Of Dental Hygiene, 82*(2), 1-10. Retrieved from http://www.adha.org/jdh

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods, 13*(1), 88–103. Retrieved from http://ejournals.library.ualberta.ca/index.php/IJQM/index

Corredor, I., Metola, E., Bernardos, A. M., Tarrío, P., & Casar, J. R. (2014). A lightweight web of things open platform to facilitate context data management and personalized healthcare services creation. *International journal of environmental research and public health, 11*(5), 4676-4713. doi:10.3390/ijerph110504676

Cresswell, K., & Sheikh, A. (2013). Organizational issues in the implementation and adoption of health information technology innovations: An interpretative review. *International journal of medical informatics, 82*(5), 73-86. doi:10.1016/j.ijmedinf.2012.10.007

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher, 21*(5), 19-27. doi:10.7748/nr.21.5.19.e1240

Cunliffe, A. L., & Karunanayake, G. (2013). Working within hyphen-spaces in ethnographic research implications for research identities and practice. *Organizational Research Methods, 16*(3), 364-392. doi:10.1177/1094428113489353

Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics, 10*(4), 2233-2243. doi:10.1109/TII.2014.2300753

Dash, M., Bhusan, P. B., & Samal, S. (2014). Determinants of Customers' Adoption of Mobile Banking: An Empirical Study by Integrating Diffusion of Innovation with Attitude. *Journal Of Internet Banking & Commerce, 19*(3), 1-21. Retrieved from http://www.arraydev.com/commerce/jibc

Deakin, H., & Wakefield, K. (2013). Skype interviewing: Reflections of two PhD researchers. *Qualitative Research, 14*(5), 603-616. doi:10.1177/1468794113488126

De Ceunynck, T., Kusumastuti, D., Hannes, E., Janssens, D., & Wets, G. (2013). Mapping leisure shopping trip decision making: Validation of the CNET interview protocol. *Quality & Quantity, 47*(4), 1831-1849. doi:10.1007/s11135-011-9629-4

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy, 5*(1), 15-29. doi:10.1016/j.jfbs.2014.01.007

Denzin, N.K. (1978). *Sociological methods: A sourcebook.* New York, NY: McGraw-Hill.

Doody, O., & Noonan, M. (2013). Preparing and conducting interviews to collect data. *Nurse Researcher, 20*(5), 28-32. doi:10.7748/nr2013.05.20.5.28.e327

Doyle, G., Garrett, B., & Currie, L. (2014). Integrating mobile devices into nursing curricula: Opportunities for implementation using Rogers' Diffusion of Innovation model. *Nurse Education Today, 34*(5), 775-782. doi:10.1016/j.nedt.2013.10.021

Drake, G. (2013). The ethical and methodological challenges of social work research with participants who fear retribution: To 'do no harm'. *Qualitative Social Work, 13*(2), 304-319. doi:10.1177/1473325012473499

Drtil, J. (2013). Impact of information security incidents - theory and reality. *Journal Of Systems Integration (1804-2724), 4*(1), 44-52. Retrieved from http://www.si-journal.org/index.php/JSI

Du, Q., Lu, N., Sun, L., Zhang, X., & Sun, B. (2017). Robust relay in narrow-band communications for ubiquitous IoT access. *Journal of Sensors, 2017*(1), 1-11. doi:10.1155/2017/9270907

Dutton, W.,H. (2014). Putting things to work: Social and policy challenges for the Internet of things. *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 16*(3), 1-21. doi:10.1108/info-09-2013-0047

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis. *SAGE Open, 4*(1). doi:10.1177/2158244014522633

Elsrud, T., Lalander, P., & Staaf, A. (2016). Internet racism, journalism and the principle of public access: Ethical challenges for qualitative research into 'media attractive'court cases. *Ethnic and Racial Studies, 39*(11), 1943-1961. doi:10.1080/01419870.2016.1155719

Fairbrother, P., Ure, J., Hanley, J., McCloughan, L., Denvir, M., Sheikh, A., & McKinstry, B. (2014). Telemonitoring for chronic heart failure: The views of patients and healthcare professionals - a qualitative study. *Journal Of Clinical Nursing, 23*(1/2), 132-144. doi:10.1111/jocn.12137

Fang, S., Xu, L., Zhu, Y., Liu, Y., Liu, Z., Pei, H., & ... Zhang, H. (2015). An integrated information system for snowmelt flood early-warning based on Internet of things. *Information Systems Frontiers, 17*(2), 321-335. doi:10.1007/s10796-013-9466-1

Farash, M. S., Turkanovic, M., Kumari, S., & Holbl, M. (2015, June 10). An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks, 36*(1), 152-176. doi:10.1016/j.adhoc.2015.05.014

Farooq, M. U., Waseem, M., Khairi, A., & Mazhar, S. (2015, February). A Critical Analysis on the Security Concerns of Internet of Things (IoT). *International Journal of Computer Applications, 111*(7), 1-6. doi:10.5120/19547-1280

Ferretti, M., & Schiavone, F. (2016). Internet of things and business processes redesign in seaports: The case of hamburg. *Business Process Management Journal, 22*(2), 271-284. doi:10.1108/BPMJ-05-2015-0079

Fischer-Lokou, J., Guéguen, N., Lamy, L., Martin, A., & Bullock, A. (2014). Imitation in mediation: Effects of the duration of mimicry on reaching agreement. *Social Behavior and Personality: An international journal, 42*(2), 189-195. doi:10.2224/sbp.2014.42.2.189

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling & Development, 91*(2), 184-194. doi:10.1002/j.1556-6676.2013.00085.x

Franke, U., Johnson, P., & Konig, J. (2014). An architecture framework for enterprise IT service availability analysis. *Software and Systems Modeling, 13*(4), 1417-1445. doi:10.1007/s10270-012-0307-3

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from http://www.nova.edu/ssss/QR

Gadzama, W. A., Katuka, J. I., Gambo, Y., Abali, A. M., & Usman, M. J. (2014). Evaluation of Employees Awareness and Usage of Information Security Policy in Organizations of Developing Countries: A Study of Federal Inland Revenue Service, Nigeria. *Journal of Theoretical & Applied Information Technology, 67*(2), 443-460. Retrieved from http://www.jatit.org

Gale, N. K., Heath, G., Cameron, E., Rashid, S. & Redwood, S. (2013). Using the framework method for the analysis of qualitative data in multi-disciplinary health research. *BMC Medical Research Methodology, 13*(1), 117. doi:10.1186/1471-2288-13-117

Gaynor, M., Bass, C., & Duepner, B. (2015). A tale of two standards: Strengthening HIPAA security regulations using the PCI-DSS. *Health Systems, 4*(2), 111-123. doi:10.1057/hs.2014.17

Gebauer, H., Paiola, M., & Saccani, N. (2013). Characterizing service networks for moving from products to solutions. *Industrial Marketing Management, 42*(1), 31-46. doi:10.1016/j.indmarman.2012.11.002

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research notes on the Gioia methodology. *Organizational Research Methods, 16*(1), 15-31. doi:10.1177/1094428112452151

Girtelschmid, S., Steinbauer, M., Kumar, V., Fensel, A., & Kotsis, G. (2014). On the application of big data in future large-scale intelligent smart city installations. *International Journal of Pervasive Computing and Communications, 10*(2), 168-182. doi:10.1108/ijpcc-03-2014-0022

Gluhak, A., Krco, S., Nati, M., Pfisterer, D., Mitton, N., & Razafindralambo, T. (2011). A survey on facilities for experimental Internet of things research. *IEEE Communications Magazine, 49*(11), 58-67. doi:10.1109/MCOM.2011.6069710

Gockel, A. (2013). Telling the ultimate tale: The merits of narrative research in the psychology of religion. *Qualitative Research in Psychology, 10*(2), 189-203. doi:10.1080/14780887.2011.616622

Gokceli, S., Zhmurov, N., Gunes, K. K., & Ors, B. (2017). IoT in action: Design and implementation of a building evacuation service. *Journal of Computer Networks and Communications, 2017*(1), 1-13. doi:10.1155/2017/8595404

Gonnot, T., Yi, W., Monsef, E., & Saniie, J. (2015). Home Automation Device Protocol (HADP): A Protocol Standard for Unified Device Interactions. *Advances in Internet of Things, 5*(4), 27-38. doi:10.4236/ait.2015.54005

Gorgolewski, K. J., & Poldrack, R. A. (2016). A practical guide for improving transparency and reproducibility in neuroimaging research. *PLoS Biology, 14*(7) doi:10.1371/journal.pbio.1002506

Greene, J. (2015). TIM Lecture Series-The Internet of Everything: Fridgebots, Smart Sneakers, and Connected Cars. *Technology Innovation Management Review, 5*(5), 47-49. Retrieved from http://www.timreview.ca

Griggs, S. (2014). SAFE & SECURE. *Industrial Safety and Hygiene News, 48*(8), 46. Retrieved from http://www.ishn.com

Gross, G. (2016, April 11). *Consumers want more value from home IoT products.* Retrieved from http://www.cio.com/article/3054221/internet-of-things/consumers-want-more-value-from-home-iot-products.html

Grossoehme, D. H. (2014). Overview of qualitative research. *Journal of health care chaplaincy, 20*(3), 109-122. doi:10.1080/08854726.2014.925660

Gu, V. C., Schniederjans, M. J., & Cao, Q. (2015). Diffusion of innovation: Customer relationship management adoption in supply chain organizations. *International Journal of Quality Innovation, 1*(1), 1-17. doi:10.1186/s40887-015-0006-6

Guba, E., & Lincoln, Y. (1985). *Naturalistic inquiry.* Newbury Park, CA: Sage.

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. doi:10.1016/j.future.2013.01.010

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods, 18*(1), 59-82. doi:10.1177/1525822X05279903

Haahr, A., Norlyk, A., & Hall, E. O. (2014). Ethical challenges embedded in qualitative research interviews with close relatives. *Nursing Ethics, 21*(1), 6-15. doi:10.1177/0969733013486370

Hahn, J. (2017). Security and privacy for location services and the Internet of things. *Library Technology Reports, 53*(1), 23-28. Retrieved from https://journals.ala.org/ltr

Hammer, M. J. (2016). Informed consent in the changing landscape of research. *Oncology Nursing Forum, 43*(5), 558-560. doi:10.1188/16.ONF.558-560

Hatleback, E., & Spring, J. M. (2014). Exploring a mechanistic approach to experimentation in computing. *Philosophy & Technology, 27*(3), 441-459. doi:10.1007/s13347-014-0164-9

Hayes, K. J., Eljiz, K., Dadich, A., Fitzgerald, J., & Sloan, T. (2015). Trialability, observability and risk reduction accelerating individual innovation adoption decisions. *Journal of Health Organization and Management, 29*(2), 271-294. doi:10.1108/JHOM-08-2013-0171

Hayhurst, C. (2014). Is your patient data secure? *Biomedical Instrumentation & Technology, 48*(3), 166-173. doi:10.2345/0899-8205-48.3.166

Heffetz, O., & Ligett, K. (2014). Privacy and data-based research. *The Journal of Economic Perspectives, 28*(2), 75-98. doi:10.1257/jep.28.2.75

Higginbottom, G., Rivers, K., & Story, R. (2014). Health and social care needs of Somali refugees with visual impairment (VIP) living in the United Kingdom: A focused ethnography with Somali people with VIP, their caregivers, service providers, and members of the Horn of Africa Blind Society. *Journal of Transcultural Nursing, 25*(2), 192-201. doi:10.1177/1043659613515715

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the united states. *Journal of Financial Crime, 22*(2), 242. doi:10.1108/JFC-09-2013-0055

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher, 20*(4), 12-17. doi:10.7748/nr2013.03.20.4.12.e326

Hoyland, S., Hollund, J. G. & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education, 49*(2), 224 – 232. doi:10.1111/medu.12622

Hwang, Y. M., Kim, M. G., & Rho, J. J. (2015). Understanding Internet of Things (IoT) diffusion Focusing on value configuration of RFID and sensors in business cases (2008–2012). *Information Development, 32*(4), 969-985. doi:10.1177/0266666915578201

Iqbal, A., Suryani, M. A., Saleem, R., & Suryani, M. A. (2016). Internet Of Things (Iot): On-Going Security Challenges And Risks. *International Journal of Computer Science and Information Security, 14*(11), 671-682. Retrieved from https://sites.google.com/site/ijcsis

Irvine, A., Drew, P., & Sainsbury, R. (2013). 'Am I not answering your questions properly?'Clarification, adequacy and responsiveness in semistructured telephone and face-to-face interviews. *Qualitative Research, 13*(1), 87-106. doi:10.1177/1468794112439086

Islam, S. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of things for health care: A comprehensive survey. *IEEE Access, 3*(1), 678-708. doi:10.1109/ACCESS.2015.2437951

Jacobsson, A., Boldt, M., & Carlsson, B. (2015, September 14). A risk analysis of a smart home automation system. *Future Generation Computer Systems, 56*(1), 719-733. doi:10.1016/j.future.2015.09.003

Jara, A. J., Fernandez, D., Lopez, P., Zamora, M. A., & Skarmeta, A. F. (2014). Lightweight MIPv6 with IPSec support. *Mobile Information Systems, 10*(1), 37-77. doi:10.3233/MIS-130171

Jara, A. J., Lopez, P., Fernandez, D., Castillo, J. F., Zamora, M. A., & Skarmeta, A. F. (2014). Mobile digcovery: Discovering and interacting with the world through the Internet of things. *Personal and Ubiquitous Computing, 18*(2), 323-338. doi:10.1007/s00779-013-0648-0

Jara, A. J., Parra, M. C., & Skarmeta, A. F. (2014). Participative marketing: Extending social media marketing through the identification and interaction capabilities from the Internet of things. *Personal and Ubiquitous Computing, 18*(4), 997-1011. doi:10.1007/s00779-013-0714-7

Jara, A. J., Varakliotis, S., Skarmeta, A. F., & Kirstein, P. (2014). Extending the Internet of Things to the Future Internet through IPv6 support. *Mobile Information Systems, 10*(1), 3-17. doi:10.3233/MIS-130169

Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of things: Perspectives and challenges. *Wireless Networks, 20*(8), 2481-2501. doi:10.1007/s11276-014-0761-7

Jin-Xin, H., Chin-Ling, C., Chun-Long, F., & Kun-hao, W. (2017). An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing. *Journal of Sensors, 2017*(1), 1-11. doi:10.1155/2017/3734764

Johnson, B. (2014). Comply with regulations or risk paying hefty fines: Ten tips for choosing call recording to help ensure compliance. *The Journal of Medical Practice Management, 29*(5), 290-293. Retrieved from https://greenbranch.com

Jwaifell, M., & Gasaymeh, A. M. (2013). Using the diffusion of innovation theory to explain the degree of english teachers' adoption of interactive whiteboards in the modern systems school in Jordan: A case study. *Contemporary Educational Technology, 4*(2), 138-149. Retrieved from http://www.cedtech.net

Ju, J., Kim, M. S., & Ahn, J. H. (2016). Prototyping Business Models for IoT Service. *Procedia Computer Science, 91*(1), 882-890. doi:10.1016/j.procs.2016.07.106

Kamuya, D., Marsh, V. M., Kombe, F., Geissler, P. W., & Molyneux, C. S. (2013). Engaging communities to strengthen research ethics in low-income settings: Experiences and lessons from setting up a network of community representatives

in a busy research site. *Developing World Bioethics, 8*(4), 1-18. doi:10.1525/jer.2013.8.4.1

Kang, N., Park, J., Kwon, H., & Jung, S. (2015). ESSE: Efficient secure session establishment for Internet-integrated wireless sensor networks. *International Journal of Distributed Sensor Networks, 11*(8), 1-11. doi:10.1155/2015/393754

Kanso, A., Toeroe, M., & Khendek, F. (2014). Comparing redundancy models for high availability middleware. *Computing, 96*(10), 975-993. doi:10.1007/s00607-013-0361-x

Kapoor, K. K., Dwivedi, Y. K., & Williams, M. D. (2014). Rogers' innovation adoption attributes: A systematic review and synthesis of existing research. *Information Systems Management, 31*(1), 74-91. doi:10.1080/10580530.2014.854103

Kaur, J., & Kaur, K. (2017). Internet of things: A review on technologies, architecture, challenges, applications, future trends. *International Journal of Computer Network and Information Security, 9*(4), 57-70. doi:10.5815/ijcnis.2017.04.07

Kavoura, A. & Bitsani, E. (2014). Methodological considerations for qualitative communication research. *Procedia - Social and Behavioral Sciences, 147*(1), 544-549. doi:10.1016/j.sbspro.2014.07.156

Keutel, M., Michalik, B., & Richter, J. (2014). Towards mindful case study research in IS: A critical analysis of the past ten years. *European Journal of Information Systems, 23*(3), 256-272. doi:10.1057/ejis.2013.26

Khansa, L., & Zobel, C. W. (2014). ASSESSING INNOVATIONS IN CLOUD SECURITY. *The Journal of Computer Information Systems, 54*(3), 45-56. doi:10.1080/08874417.2014.11645703

Kim, H., Lim, J., & Lee, K. (2015). A Study of K-ISMS Fault Analysis for Constructing Secure Internet of Things Service. *International Journal Of Distributed Sensor Networks, 2015*(1), 1-12. doi:10.1155/2015/474329

Kim, N., & Pae, J.,H. (2014). Does intra-firm diffusion of innovation lead to inter-firm relationship benefits? the cases of innovation providers and adopters. *The Journal of Business & Industrial Marketing, 29*(6), 514-524. doi:10.1108/JBIM-03-2012-0053

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education: Examining assumptions and limitations of research. *British Journal of Educational Technology, 44*(4), 536–543. doi:10.1111/bjet.12049

Kish, L. & Verma, V. (1986). Complete censuses and samples. *Journal of Official Statistics, 2*(4), 381–395. Retrieved from http://www.degruyter.com/view/j/jos

Knebel, U., Leimeister, J. M., & Krcmar, H. (2006). Strategic importance of RFID-The perspective of IT decision makers in Italy. *Journal of Information Technology Management (JITM), 17*(4), 1-12. Retrieved from http://www.aom-iaom.org/jitm.html

Ko, W., Chiou, S., Lu, E., & Chang, H. K. (2014). Modifying the ECC-based grouping-proof RFID system to increase inpatient medication safety. *Journal Of Medical Systems, 38*(9), 66. doi:10.1007/s10916-014-0066-5

Kohles, J. C., Bligh, M. C., & Carsten, M. K. (2013). The vision integration process: Applying Rogers' diffusion of innovations theory to leader–follower communications. *Leadership, 9*(4), 466-485. doi:10.1177/1742715012459784

Kok-Seng Wong, & Kim, M. H. (2014). Towards self-awareness privacy protection for Internet of things data collection. *Journal of Applied Mathematics, 2014*. doi:10.1155/2014/827959

Konstantinidis, E. I., Bamparopoulos, G. G., Billis, A. S., & Bamidis, P. D. (2014). Internet of things for an age-friendly healthcare. *Studies in health technology and informatics, 210*(2014), 587-591. doi:10.3233/978-1-61499-512-8-587

Kristensen, G. K., & Ravn, M. N. (2015). The voices heard and the voices silenced: Recruitment processes in qualitative interview studies. *Qualitative Research, 15*(6), 722-737. doi:10.1177/1468794114567496

Kroener, I., & Wright, D. (2014). A Strategy for Operationalizing Privacy by Design. *Information Society, 30*(5), 355-365. doi:10.1080/01972243.2014.944730

Kyriazis, D., & Varvarigou, T. (2013). Smart, Autonomous and Reliable Internet of Things. *Procedia Computer Science, 21*(1), 442-448. doi:10.1016/j.procs.2013.09.059

Lai, H., Lin, I., & Tseng, L. (2014). High-level managers' considerations for RFID adoption in hospitals: An empirical study in taiwan. *Journal of Medical Systems, 38*(2), 1-3. doi:10.1007/s10916-013-0003-z

Lancaster, G., Kolakowsky-Hayner, S., Kovacich, J., & Greer-Williams, N. (2015). Interdisciplinary communication and collaboration among physicians, nurses, and unlicensed assistive personnel. *Journal of Nursing Scholarship, 47*(3), 275-284. doi:10.1111/jnu.12130

Lanza, J., Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., & Gutierrez, V. (2015). Large-scale mobile sensing enabled Internet-of-things testbed for smart city services. *International Journal of Distributed Sensor Networks, 11*(8), 1-15. doi:10.1155/2015/785061

Largent, E., Grady, C., Miller, F. G. & Wertheimer, A. (2013). Misconceptions about coercion and undue influence: Reflections on the views of IRB members. *Bioethics, 27*(9), 500–507. doi:10.1111/j.1467-8519.2012.01972.x

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons, 58*(4), 431-440. doi:10.1016/j.bushor.2015.03.008

Lee, Y.-J., & Tan, Y. (2013). Effects of Different Types of Free Trials and Ratings in Sampling of Consumer Software: An Empirical Study. *Journal of Management Information Systems, 30*(3), 213-246. doi:10.2753/MIS0742-1222300308

Leech, N. L., & Onwuegbuzie, A. J. (2007). An array of qualitative data analysis tools: A call for data analysis triangulation. *School Psychology Quarterly, 22*(4), 557-584. doi:10.1037/1045-3830.22.4.557

Li, M., Zhao, D., & Yu, Y. (2015). TOE drivers for cloud transformation: Direct or trust-mediated? *Asia Pacific Journal of Marketing and Logistics, 27*(2), 226-248. doi:10.1108/apjml-03-2014-0040

Li, N., Sun, M., Bi, Z., Su, Z., & Wang, C. (2014). A new methodology to support group decision-making for IoT-based emergency response systems. *Information Systems Frontiers, 16*(5), 953-977. doi:10.1007/s10796-013-9407-z

Li, S., Tryfonas, T., & Li, H. (2016). The Internet of things: A security point of view. *Internet Research, 26*(2), 337-359. doi:10.1108/IntR-07-2014-0173

Li, S., Xu, L. D., & Zhao, S. (2015). The Internet of things: A survey. *Information Systems Frontiers, 17*(2), 243-259. doi:10.1007/s10796-014-9492-7

Li, Z., & Cheng, Y. (2014). From free to fee: Exploring the antecedents of consumer intention to switch to paid online content. *Journal of Electronic Commerce Research, 15*(4), 281-299. Retrieved from http://www.jecr.org

Liu, F., Li, P., & Deng, D. (2017). Device-oriented automatic semantic annotation in IoT. *Journal of Sensors, 2017*(1), 1-14. doi:10.1155/2017/9589064

Lomotey, R. K., Pry, J., & Sriramoju, S. (2017). Wearable IoT data stream traceability in a distributed health information system. *Pervasive and Mobile Computing, 40*(1), 692-707. doi:10.1016/j.pmcj.2017.06.020

Lopez, G. (2013). REAL-TIME OPERATIONAL AVAILABILITY FOR IT-INTENSIVE SYSTEMS. *Journal Of Applied Global Research, 6*(17), 62-83.

Lu, X., Liu W., & Guan, Y. (2013). iPhone Independent Real Time Localization System Research and Its Healthcare Application. *Advances in Internet of Things, 3*(4), 53-65. doi:10.4236/ait.2013.34008

Lu, X., Qu, Z., Li, Q., & Pan, H. (2015). Privacy information security classification for Internet of things based on Internet data. *International Journal of Distributed Sensor Networks, 11*(8), 1-8. doi:10.1155/2015/932941

Lub, V. (2015). Validity in Qualitative Evaluation Linking Purposes, Paradigms, and Perspectives. *International Journal of Qualitative Methods, 14*(5), doi:10.1177/1609406915621406

Lucas, S. R. (2014). Beyond the existence proof: Ontological conditions, epistemological implications, and in-depth interview research. *Quality & Quantity, 48*(1), 387–408. doi:10.1037/a0038087

Luftman, J., Derksen, B., Dwivedi, R., Santana, M., Zadeh, H. S., & Rigoni, E. (2015). Influential IT management trends: An international study. *Journal of Information Technology, 30*(3), 293-305. doi:10.1057/jit.2015.18

MacLennan, E., & Belle, J. (2014). Factors affecting the organizational adoption of service-oriented architecture (SOA). *Information Systems & E-Business Management, 12*(1), 71-100. doi:10.1007/s10257-012-0212-x

Maetens, A., Schreye, R. D., Faes, K., Houttekier, D., Deliens, L., Gielen, B., . . . Cohen, J. (2016). Using linked administrative and disease-specific databases to study end-

of-life care on a population level. *BMC Palliative Care, 15*(1), 1-10. doi:10.1186/s12904-016-0159-7

Malterud, K., Siersma, V. D. & Guassora, A. D. (2016). Sample size in qualitative interview studies: Guided by information power. *Qualitative health research, 26*(13), 1753-1760. doi:10.1177/1049732315617444

Maras, M. (2015). Internet of things: Security and privacy implications. International *Data Privacy Law, 5*(2), 99-104. doi:10.1093/idpl/ipv004

Marinissen, E. J., Zorian, Y., Konijnenburg, M., Chih-Tsun, H., Ping-Hsuan, H., Cockburn, P., & ... Reyes, C. (2016). IoT: Source of test challenges. *IEEE European Test Symposium, 2016*(1), 1-10. doi:10.1109/ETS.2016.7519331

Maroon, J. C., Winkelman, R., Bost, J., Amos, A., Mathyssek, C., & Miele, V. (2015). Chronic Traumatic Encephalopathy in Contact Sports: A Systematic Review of All Reported Pathological Cases. *Plos ONE, 10*(2), 1-16. doi:10.1371/journal.pone.0117338

Marshall, B., Cardon, P., Poddar, A., & Fontenot, R. (2013). Does sample size matter in qualitative research? A review of qualitative interviews in IS research. *The Journal of Computer Information Systems, 54*(1), 11-22. doi:10.1080/08874417.2013.11645667

Marshall, C., & Rossman, G. (2016). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage.

McCusker, K., & Gunaydin, S. (2015, October). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion, 30*(7), 537-542. doi:10.1177/0267659114559116

McMullen, H., Griffiths, C., Leber, W., & Greenhalgh, T. (2015). Explaining high and low performers in complex intervention trials: A new model based on diffusion of innovations theory. *Trials, 16*(1), 1-16. doi:10.1186/s13063-015-0755-5

Mecca, J., Gibson, C., Giorgini, V., Medeiros, K., Mumford, M., & Connelly, S. (2015). Researcher Perspectives on Conflicts of Interest: A Qualitative Analysis of Views from Academia. *Science & Engineering Ethics, 21*(4), 843-855. doi:10.1007/s11948-014-9580-6

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). Thousand Oaks, CA: Sage.

Min, D., Xiao, Z., Sheng, B., Quanyong, H., & Xuwei, P. (2014). Design and implementation of heterogeneous IOT gateway based on dynamic priority scheduling algorithm. *Transactions of the Institute of Measurement and Control, 36*(7), 924-931. doi:10.1177/0142331214527600

Miorandi, D., Sicari, S., Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications, and research challenges. *Ad Hoc Networks, 10*(7), 1497-1516. doi:10.1016/j.adhoc.2012.02.016

Mishra, D., Akman, I., & Mishra, A. (2014). Theory of reasoned action application for green information technology acceptance. *Computers in human behavior, 36*(1), 29-40. doi:10.1016/j.chb.2014.03.030

Mishra, N., Chang, H., & Chung-Chih, L. (2015). An IoT knowledge reengineering framework for semantic knowledge analytics for BI-services. *Mathematical Problems in Engineering, 2015*(1), 1-12. doi:10.1155/2015/759428

Moreno, M. A., Goniu, N., Moreno, P. S., & Diekema, D. (2013). Ethics of social media research: Common concerns and practical considerations. *Cyberpsychology, Behavior, and Social Networking, 16*(9), 708-713. doi:10.1089/cyber.2012.0334

Morse, J. M. (2015). Critical analysis of strategies for determining rigor in qualitative inquiry. *Qualitative health research, 25*(9), 1212-1222. doi:10.1177/1049732315588501

Moustakas, C. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications Inc.

Mulligan, D. K., & Bamberger, K. A. (2013). What Regulators Can Do to Advance Privacy Through Design. *Communications Of The ACM, 56*(11), 20-22. doi:10.1145/2527185

Nair, H. (2017). Prioritizing scenarios for test in an enterprise cloud application: An industrial case study. *Software Quality Professional, 19*(3), 13-24. Retrieved from http://www.asq.org/pub/sqp

Nan, N., Zmud, R., & Yetgin, E. (2014). A complex adaptive systems perspective of innovation diffusion: An integrated theory and validated virtual laboratory. *Computational and Mathematical Organization Theory, 20*(1), 52-88. doi:10.1007/s10588-013-9159-9

National Cancer Institute. (2016, June 27). *What Are Clinical Trials?* Retrieved from https://www.cancer.gov/about-cancer/treatment/clinical-trials/what-are-trials

Notra, S., Siddiqi, M., Gharakheili, H. H., Sivaraman, V., & Boreli, R. (2014, October). *An experimental study of security and privacy risks with emerging household appliances (pp. 79-84).* Paper presented at the 2014 IEEE Conference on Communications and Network Security (CNS), San Francisco, CA. doi:10.1109/CNS.2014.6997469

Olatokun, W. M., & Igbinedion, L. J. (2009). The Adoption of Automatic Teller Machines in Nigeria: An Application of the Theory of Diffusion of Innovation. *Issues In Informing Science & Information Technology, 6*(1), 373-393. Retrieved from http://iisit.org

Olsson, A., Skovdahl, K., & Engström, M. (2016). Using diffusion of innovation theory to describe perceptions of a passive positioning alarm among persons with mild dementia: A repeated interview study. *BMC geriatrics, 16*(1), 1-6. doi:10.1186/s12877-016-0183-8

Omondi, M. P., Ombui, K., & Mungatu, J. (2013). Factors affecting effective strategy implementation for attainment of Millennium Development Goal 5 by international reproductive health non-governmental organizations in Kenya. *The TQM Journal, 25*(5), 507-519. doi:10.1108/09596110110403712

Oriwoh, E., al-Khateeb, H., & Conrad, M. (2016, May 27). *Responsibility and Non-repudiation in resource-constrained Internet of Things scenarios.* Paper presented

at the 2015 International Conference on Computing and Technology Innovation (CTI 2015), Bedfordshire, United Kingdom. doi:10.13140/RG.2.1.4030.3124

Osho, O., & Onoja, A. D. (2015). National Cyber Security Policy and Strategy of Nigeria: A Qualitative Analysis. *International Journal of Cyber Criminology, 9*(1), 120-143. doi:10.5281/zenodo.22390

O'Sullivan, D., & Conway, P. F. (2016). Underwhelmed and playing it safe: Newly qualified primary teachers' mentoring and probationary-related experiences during induction. *Irish Educational Studies, 35*(4)*,* 1-18. doi:10.1080/03323315.2016.1227720

Palinkas, L. A. (2014). Qualitative and Mixed Methods in Mental Health Services and Implementation Research. *Journal Of Clinical Child & Adolescent Psychology, 43*(6), 851-861. doi:10.1080/15374416.2014.910791

Patel, M. R., Shah, K. S., & Shallcross, M. L. (2015). A qualitative study of physician perspectives of cost-related communication and patients' financial burden with managing chronic disease. *BMC Health Services Research, 15*(1), 1-7. doi:10.1186/s12913-015-1189-1

Pasha, M., Shah, S. M. W., & Pasha, U. (2016). Security framework for IoT systems. *International Journal of Computer Science and Information Security, 14*(11), 99-104. Retrieved from https://sites.google.com/site/ijcsis

Patil, S., Mihovska, A., & Prasad, R. (2014). An IoT Virtualization Framework for Fast and Lossless Communication. *Wireless Personal Communications, 76*(3), 449-462. doi:10.1007/s11277-014-1717-z

Patton, M.Q. (1999). Enhancing the quality and credibility of qualitative analysis. *Health Sciences Research, 34*(5), 1189–1208. Retrieved from https://www.ncbi.nlm.nih.gov

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: Sage.

Penjor, S., & Zander, P. (2016). Predicting Virtual Learning Environment Adoption: A Case Study. *Turkish Online Journal Of Educational Technology, 15*(1), 69-81. Retrieved from http://www.tojet.net

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. *Texas Law Review, 93*(1), 85-178. Retrieved from http://www.texaslrev.com

Peticca-Harris, A., deGama, N. & Elias, S. R. S. T. A. (2016). A dynamic process model for finding informants and gaining access in qualitative research. *Organizational Research Methods, 19*(3), 376–401. doi:10.1177/1094428116629218

Pinfield, S., Cox, A. M., & Smith, J. (2014). Research data management and libraries: Relationships, activities, drivers and influences. *Plos ONE, 9*(12), 1-28. doi:10.1371/journal.pone.0114734

Puliafito, A., Celesti, A., Villari, M., & Fazio, M. (2015). Towards the integration between IoT and cloud computing: An approach for the secure self-configuration of embedded devices. *International Journal of Distributed Sensor Networks, 11*(12), 1-9. doi:10.1155/2015/286860

Qiu, X., Luo, H., Xu, G., Zhong, R., & Huang, G. Q. (2015). Physical assets and service sharing for IoT-enabled Supply Hub in Industrial Park (SHIP). *International Journal of Production Economics, 159*(1), 4-15. doi:10.1016/j.ijpe.2014.09.001

Ramavhona, T. C., & Mokwena, S. (2016). Factors influencing Internet banking adoption in south african rural areas. *South African Journal of Information Management, 18*(2), 1-8. doi:10.4102/sajim.v18i2.642

Ravindran, R., Yomas, J., & Jubin Sebastian, E. (2015). IoT: A Review on Security Issues and Measures. *International Journal of Engineering Science and Technology, 5*(6), 348-351. Retrieved from http://www.estij.org

Reddy, A. S. (2014). Reaping the benefits of the Internet of Things. *Cognizant Reports*. Retrieved from https://www.cognizant.com

Rehman, A. U., Rehman, S. U., Khan, I. U., Moiz, M., & Hasan, S. (2016). Security and privacy issues in IoT. *International Journal of Communication Networks and Information Security, 8*(3), 147-157. Retrieved from http://www.ijcnis.org

Rennie, D. L. (2012). Qualitative research as methodical hermeneutics. *Psychological Methods, 17*(3), 385–398. doi:10.1037/a0029250

Riegel, B., & Dickson, V. V. (2016). A qualitative secondary data analysis of intentional and unintentional medication nonadherence in adults with chronic heart failure. *Heart & Lung, 45*(6), 468-474. doi:10.1016/j.hrtlng.2016.08.003

Rivard, J. R., Fisher, R. P., Robertson, B., & Mueller, D. H. (2014). Testing the Cognitive Interview with Professional Interviewers: Enhancing Recall of Specific Details of

Recurring Events. *Applied Cognitive Psychology, 28*(6), 917-925. doi:10.1002/acp.3026

Robinson, O. C. (2014). Sampling in Interview-Based Qualitative Research: A Theoretical and Practical Guide. *Qualitative Research In Psychology, 11*(1), 25-41. doi:10.1080/14780887.2013.801543

Rogers, E. M. (1962). *Diffusion of innovations:* 1st ed. New York: Free Press.

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), 2266-2279. doi:10.1016/j.comnet.2012.12.018

Rosenbaum, B. P. (2014). Radio frequency identification (RFID) in health care: Privacy and security concerns limiting adoption. *Journal of Medical Systems, 38*(3), 1-19. doi:10.1007/s10916-014-0019-z

Rubinstein, I. S., & Hartzog, W. (2016). ANONYMIZATION AND RISK. *Washington Law Review, 91*(2), 703-760. Retrieved from https://www.law.uw.edu/wlr

Sarabdeen, J., & Ishak, M. M. M. (2015). Impediment of privacy in the use of clouds by educational institutions. *Journal of Advances in Information Technology, 6*(3), 167-172. doi:10.12720/jait.6.3.167-172

Sáenz-Royo, C., Gracia-Lázaro, C., & Moreno, Y. (2015). The Role of the Organization Structure in the Diffusion of Innovations. *Plos ONE, 10*(5), 1-13. doi:10.1371/journal.pone.0126076

Safari, F., Safari, N., & Hasanzadeh, A. (2015). The adoption of software-as-a-service (SaaS): Ranking the determinants. *Journal of Enterprise Information Management, 28*(3), 400-422. doi:10.1108/jeim-02-2014-0017

Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security Challenges for Medical Devices. *Communications Of The ACM, 58*(4), 74-82. doi:10.1145/2667218

Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., ... & Pfisterer, D. (2014). SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks, 61*(1), 217-238. doi:10.1016/j.bjp.2013.12.020

Sanni, S. A., Ngah, Z. A., Karim, N. A., Abdullah, N., & Waheed, M. (2013). Using the Diffusion of Innovation Concept to Explain the Factors That Contribute to the Adoption Rate of E-journal Publishing. *Serials Review*, 39250-257. doi:10.1016/j.serrev.2013.10.001

Sbora, C. (2014). Indicators for determining collaborative security level in organizational environments. *Informatica Economica, 18*(4), 131-143. doi:10.12948/issn14531305/18.4.2014.12

Seawright, J., & Gerring, J. (2008). Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly, 61*(2), 294-308. doi:10.4135/9781473915480.n31

Seitz, S. (2016). Pixilated partnerships, overcoming obstacles in qualitative interviews via Skype: A research note. *Qualitative Research, 16*(2), 229-235. doi:10.1177/1468794115577011

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal Of Management Information Systems, 32*(2), 314-341. doi:10.1080/07421222.2015.1063315

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), 519-531. doi:10.1016/j.tele.2014.02.003

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*(1), 146-164. doi:10.1016/j.comnet.2014.11.008

Silva, E. and Maló, P. (2014). IoT Testbed Business Model. *Advances in Internet of Things, 4*(4), 37-45. doi:10.4236/ait.2014.44006.

Stake, R. (1995). *The art of case study research*. Thousand Oaks, CA: Sage.

Su, H., Wang, Z., & An, S. (2013). MAEB: Routing Protocol for IoT Healthcare. *Advances in Internet of Things, 3*(2A), 8-15. doi:10.4236/ait.2013.32A002

Suciu, G., Suciu, V., Martian, A., Craciunescu, R., Vulpe, A., Marcu, I., . . . Fratu, O. (2015). Big data, Internet of things and cloud convergence - an architecture for secure E-health applications. *Journal of Medical Systems, 39*(11), 1-8. doi:10.1007/s10916-015-0327-y

Sugarhood, P., Wherton, J., Procter, R., Hinder, S., & Greenhalgh, T. (2014). Technology as system innovation: A key informant interview study of the application of the diffusion of innovation model to telecare. *Disability & Rehabilitation: Assistive Technology, 9*(1), 79-87. doi:10.3109/17483107.2013.823573

Suhasini, R., & Suganthalakshmi, T. (2015). Corporate E-learning. *Asia Pacific Journal of Management & Entrepreneurship Research, 4*(1), 176-198. Retrieved from http://apjmer.org

Sung, S. Y., & Choi, J. N. (2014). THE ROLES OF INDIVIDUAL DIFFERENCES AND INNOVATION PROPERTIES IN MULTIPLE FORMS OF INNOVATION IMPLEMENTATION. *Social Behavior and Personality, 42*(7), 1201-1219. doi:10.2224/sbp.2014.42.7.1201

Svensson, L. & Doumas, K. (2013). Contextual and analytic qualities of research methods exemplified in research on teaching. *Qualitative Inquiry, 19*(6), 441-450. doi:10.1177/1077800413482097

Swan, M. (2012). Sensor Mania! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0. *Journal of Sensor and Actuator Networks, 1*(3), 217–253. doi:10.3390/jsan1030217

Takai-Igarashi, T., Kinoshita, K., Nagasaki, M., Ogishima, S., Nakamura, N., Nagase, S., . . . Yaegashi, N. (2017). Security controls in an integrated biobank to protect privacy in data sharing: Rationale and study design. *BMC Medical Informatics and Decision Making, 17*(1), 1-12. doi:10.1186/s12911-017-0494-5

Thomas, J. A. (2015). Using unstructured diaries for primary data collection. *Nurse researcher, 22*(5), 25-29. doi:10.7748/nr.22.5.25.e1322

Tran, A. H. (2017). The Internet of things and potential remedies in privacy tort law. *Columbia Journal of Law and Social Problems, 50*(2), 263-298. Retrieved from http://www.columbia.edu/cu/jlsp/

Trequattrini, R., Shams, R., Lardo, A., & Lombardi, R. (2016). Risk of an epidemic impact when adopting the Internet of things. *Business Process Management Journal, 22*(2), 403-419. doi:10.1108/BPMJ-05-2015-0075

TRUSTe. (2016). *TRUSTe/NCSA Consumer Privacy Index - US, 2016 [Infographic]*. Retrieved from https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us

Tseng, C. H. (2016). Multipath load balancing routing for Internet of things. *Journal of Sensors, 2016*(1), 1-8. doi:10.1155/2016/4250746

Tyagi, S., Darwish, A., & Khan, M. (2014). Managing Computing Infrastructure for IoT Data. *Advances in Internet of Things, 4*(3), 29-35. doi:10.4236/ait.2014.43005.

Ullah, F., Habib, M. A., Farhan, M., Khalid, S., Durrani, M. Y., & Jabbar, S. (2017). Semantic interoperability for big-data in heterogeneous IoT infrastructure for healthcare. *Sustainable Cities and Society, 34*(1), 90-96. doi:10.1016/j.scs.2017.06.010

U.S. Department of Health & Human Services. (1979). *The Belmont Report*. Retrieved from http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html

Veena, D.K., Devaraj, D., Rajasree, P.M., & Oberoi, A. (2014, November 27). *A compact sensor system for concussion mitigation in helmets - A concept prototype (pp. 363-366).* Paper presented at the 2014 International Conference on Contemporary Computing and Informatics (IC3I), Mysore, India. doi:10.1109/IC3I.2014.7019704

Vogl, S. (2013). Telephone versus face-to-face interviews mode effect on semistructured interviews with children. *Sociological Methodology, 43*(1), 133-177. doi:10.1177/0081175012465967

Vuuren, I. E. V. (2016). IT security trust model - securing the human perimeter. *International Journal of Social Science and Humanity, 6*(11), 852-858. doi:10.18178/ijssh.2016.V6.761

Waite, K., & Harrison, T. (2015). Online banking adoption: We should know better 20 years on. *Journal of Financial Services Marketing, 20*(4), 258-272. doi:10.1057/fsm.2015.19

Wan, J., Zou, C., Zhou, K., Lu, R., & Li, D. (2014). IoT sensing framework with inter-cloud computing capability in vehicular networking. *Electronic Commerce Research, 14*(3), 389-416. doi:10.1007/s10660-014-9147-2

Wang, E. S. T. (2014). Perceived control and gender difference on the relationship between trialability and intent to play new online games. *Computers in Human Behavior, 30*(1), 315-320. doi:10.1016/j.chb.2013.09.016

Wang, J., Duan, S., & Shi, Y. (2015). Multi-objects scalable coordinated learning in Internet of things. *Personal and Ubiquitous Computing, 19*(7), 1133-1144. doi:10.1007/s00779-015-0888-2

Wang, S., Tsai, Y., Kao, H., & Hong, T. (2014). On anonymizing transactions with sensitive items. *Applied Intelligence, 41*(4), 1043-1058. doi:10.1007/s10489-014-0554-9

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627. doi:10.1016/j.clsr.2015.07.002

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), 615-624. doi:10.1016/j.bushor.2015.06.005

Wells, A. (2013). The importance of design thinking for technological literacy: A phenomenological perspective. *International Journal of Technology & Design Education, 23*(3), 623-636. doi:10.1007/s10798-012-9207-7

Whitmore, A., Agarwal, A., & Da Xu, L. (2015). The Internet of Things - A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274. doi:10.1007/s10796-014-9489-2

Wikina, S. B., PhD. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management, 2014*(1)*,* 1-6. Retrieved from http://perspectives.ahima.org

Wilson, F., & Post, J. E. (2013). Business models for people, planet (& profits): Exploring the phenomena of social business, a market-based approach to social value creation. *Small Business Economics, 40*(3), 715-737. doi:10.1007/s11187-011-9401-0

Windsor, R., Cleary, S., Ramiah, K., Clark, J., Abroms, L., & Davis, A. (2013). The Smoking Cessation and Reduction in Pregnancy Treatment (SCRIPT) Adoption Scale: Evaluating the Diffusion of a Tobacco Treatment Innovation to a Statewide

Prenatal Care Program and Providers. *Journal of Health Communication, 18*(10), 1201-1220. doi:10.1080/10810730.2013.778358

Wolgemuth, J. R. (2014). Analyzing for critical resistance in narrative research. *Qualitative Research, 14*(5), 586–602. doi:10.1177/1468794113501685

Woods, M., Paulus, T., Atkins, D. P., & Macklin, R. (2015). Advancing qualitative research using qualitative data analysis software (QDAS)? Reviewing potential versus practice in published studies using ATLAS. ti and NVivo, 1994–2013. *Social Science Computer Review, 34*(5), 597-617. doi:10.1177/0894439315596311

Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems, 25*(9), 1101-1102. doi:10.1002/dac.2417

Xu, H., & Bélanger, F. (2013). Information Systems Journal Special Issue on: Reframing Privacy in a Networked World. *Information Systems Journal, 23*(4), 371-375. doi:10.1111/isj.12026

Yan, Z., Zhang, P., & Vasilakos, A. (2014). A survey on trust management for Internet of Things. *Journal of Network and Computer Applications, 42*(1), 120-134. doi:10.1016/j.jnca.2014.01.014

Yang, L., Yang, S. H., & Plotnick, L. (2013). How the Internet of things technology enhances emergency response operations. *Technological Forecasting & Social Change, 80*(9), 1854-1867. doi:10.1016/j.techfore.2012.07.011

Yilmaz, K. (2013). Comparison of Quantitative and Qualitative Research Traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2), 311-325. doi:10.1111/ejed.12014

Yin, R. K. (2014). *Case study research: Designs and methods* (5th ed.). Thousand Oaks: Sage.

Yu, X., Nguyen, B., & Chen, Y. (2016). Internet of things capability and alliance. *Internet Research, 26*(2), 402-434. doi:10.1108/IntR-10-2014-0265

Yuanfang, C., Gyu Myoung, L., Lei, S., & Crespi, N. (2016). Industrial Internet of Things-Based Collaborative Sensing Intelligence: Framework and Research Challenges. *Sensors (14248220), 16*(2), 1-19. doi:10.3390/s16020215

Yun, J., Ahn, I.-Y., Choi, S.-C., & Kim, J. (2016). TTEO (Things Talk to Each Other): Programming Smart Spaces Based on IoT Systems. *Sensors, 16*(4), 1-21. doi:10.3390/s16040467

Yung-Ming, C. (2015). Towards an understanding of the factors affecting m-learning acceptance: Roles of technological characteristics and compatibility. *Asia Pacific Management Review, 20*(3), 109-119. doi:10.1016/j.apmrv.2014.12.011

Zeng, W., & Gao, H. (2014). Optic fiber sensing IOT technology and application research. *Sensors & Transducers, 180*(10), 16-21. Retrieved from http://www.sensorsportal.com

Zhang, B., Zou, Z., & Liu, M. (2011). *Evaluation on security system of Internet of things based on fuzzy-AHP method (pp. 1–5)*. Paper presented at the IEEE international

conference on E -Business and E-Government (ICEE), Shanghai, China. doi:10.1109/ICEBEG.2011.5881939

Zhang, Y. C., & Yu, J. (2013). A study on the fire IoT development strategy. *Procedia Engineering, 52*(1), 314-319. doi:10.1016/j.proeng.2013.02.146

Zhong, R. Y., Peng, Y., Xue, F., Fang, J., Zou, W., Luo, H., ... & Huang, G. Q. (2017). Prefabricated construction enabled by the Internet-of-Things. *Automation in Construction, 76*(1), 59-70. doi:10.1016/j.autcon.2017.01.006

Zhou, W., & Piramuthu, S. (2015). Information relevance model of customized privacy for IoT. *Journal of Business Ethics, 131*(1), 19-30. doi:10.1007/s10551-014-2248-y

Zhu, X., Lu, Y., Han, J., & Shi, L. (2016). Transmission reliability evaluation for wireless sensor networks. *International Journal of Distributed Sensor Networks, 12*(2), 1-10. doi:10.1155/2016/1346079

Zurita, M., Freire, R. C. S., Tedjini, S., & Moshkalev, S. A. (2016). A review of implementing ADC in RFID sensor. *Journal of Sensors, 2016*(1), 1-14. doi:10.1155/2016/8952947

Appendix A: Human Subject Research Certificate of Completion

Certificate of Completion

The National Institutes of Health (NIH) Office of Extramural Research certifies that **Daud Kamin** successfully completed the NIH Web-based training course "Protecting Human Research Participants".

Date of completion: 05/14/2015

Certification Number: 1763549

Appendix B: Interview Protocol

Interview Title: Exploring Security, Privacy, and Reliability Strategies to Enable the Adoption of IoT

A. I will introduce myself to the participant and thank them for participating.
B. I will verify receipt of the consent form and answer any questions and concerns of the study participant.
C. I will collect the signed consent from the study participant.
D. I will remind the study participant that the interview will be recorded and the interview will remain strictly confidential.
E. I will turn on the recording device, announce the study participant identifying code, and announce the date and time of the interview.
F. I will start the interview with the first question and continue through to the last question.
    1. What is your current position and your responsibilities?
    2. How long have you been in your current position?
    3. How many years of experience do you have in working with IoT?
    4. What security, privacy, and reliability strategies have you used to adopt IoT devices?
    5. How did you determine to use security, privacy, and reliability strategies to adopt IoT devices?

6. What methods worked best in the security, privacy, and reliability strategies to adopt IoT devices?
7. What strategies did you use to ensure IoT compatibility issues were addressed?
8. What strategies does IoT provide to gain a relative advantage over existing technologies?
9. How did you test or pilot IoT to ensure meeting organizational objectives?
10. How did the visibility of IoT enable its adoption at your organization?
11. How did your strategies address the complexity of IoT adoption?

G. End interview questions and ask if there is any other information they would like to share.

H. Inform the participant about the concept of member checking, which will be used to verify the accuracy of the initial interview.

I. Thank the participant for partaking in the study. Confirm the participant has contact information for any follow-up questions and concerns.

Appendix C: Participant Invitation

Dear [participant]:

My name is Daud Kamin and I am a Doctor of Information Technology (DIT) student at Walden University. I am conducting a doctoral study to examine how organization IT leaders strategize the adoption of Internet of Things (IoT). My study is intended to explore the following question: What are security, privacy, and reliability strategies used by organization IT leaders to adopt IoT devices?

All organization and participant names will remain confidential in the study. I have included a consent form for your review and signature, prior to your participation in this study. The informed consent form provides background information on the study and outlines your rights during the interview process.

Based on your experiences with IoT devices, I would like to interview you in order to gather information about your perceptions and beliefs about strategies to adopt IoT devices at [organization name]. The interview will take approximately 30-45 minutes of your time and scheduled at your convenience within the next 2 weeks, following completion of the Walden University IRB process. I will conduct this in-person interview at a location that is most convenient for you. I am also inviting you to share with me any company or public documents such as e-mails, administrative documents, reports, and/or memoranda that you feel may provide additional information about the strategies used to adopt IoT. However, please note the provision of any documents on your part is voluntary. If you do not wish to provide documents, I am still asking that you participate in the study as an interviewee.

Please contact me if you have any questions or would like additional information. My contact information is in my signature below. I kindly request an informal response to this letter indicating your agreement via email as your response will ensure I have gathered a sufficient sample of interview participants prior to the beginning of the data collection process. Following IRB approval, I will kindly contact you to schedule the interview. I thank you in advance for your consideration and your support of my study.

Sincerely,
Daud Kamin
<email and phone redacted>