2020

Exploring the Relationship Between IoT Security and Standardization

James Jenness Clapp
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

James J. Clapp

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. Gary Griffith, Committee Chairperson, Information Technology Faculty
Dr. Jodine Burchell, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

Chief Academic Officer and Provost
Sue Subocz, Ph.D.

Walden University
2020

Abstract

Exploring the Relationship Between IoT Security and Standardization

by

James J. Clapp

MSIT, Walden University, 2018

MIS, University of Phoenix, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Abstract

The adoption of the Internet of Things (IoT) technology across society presents new and unique challenges for security experts in maintaining uninterrupted services across the technology spectrum. A botnet implemented over 490,000 IoT connected devices to cripple the Internet services for major companies in one recent IoT attack. Grounded in Roger's diffusion of innovations theory, the purpose of this qualitative exploratory multiple-case study was to explore implementation strategies used by some local campus IT managers in educational institutions in the United States to secure the IoT environment. The participants were 10 IT local campus IT managers within educational institutions across the Southeast portion of the United States who have implemented strategies to secure IoT devices. The data were collected by interviewing 10 IT managers and collecting documentation available to the public from 4 institutions. Four themes emerged after analysis using data triangulation: restricting IoT access to the network, network isolation to secure IoT devices from the network, adoption by leadership to secure IoT inside the network, and strong shared partnership with peer organizations through observation. The research will benefit IT professionals and organizations through enhanced security and the community providing a more enhanced learning experience for all involved locally through IoT adoption. A secure IoT environment may contribute to positive social change by increasing IoT adoption to better serve societal needs.

Exploring the Relationship Between IoT Security and Standardization

by

James J. Clapp

MSIT, Walden University, 2018

MIS, University of Phoenix, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2020

Dedication

I dedicate this doctoral dissertation to my beautiful wife and daughter (Janine and Jenna). It has been with the sacrifice of not having me in their life to the fullest for the last four years, and for this, I say thank you. I have missed many events that my daughter was in because a paper was due; thanks for your sacrifice, Jenna. I want to thank my wife for the encouragement by not allowing me to give up. I am so proud of all that you both have accomplished and hope this accomplishment makes you proud. Remember, anything is possible with enough support.

Acknowledgments

There are so many people I want to thank for encouraging me and helping me along this journey. Thanks to those who believed in me along the journey and for those individuals who were standing in the crossroads of my education, I say thank you. I personally want to thank my Chair, Dr. Griffith, for always being there for me when honestly, I was frustrated beyond belief. He was kind and could redirect me to reach the final goal. I also want to thank my committee members Dr. Burchell for providing feedback that was detailed and concise and was greatly appreciated. I also want to thank Dr. Case for helping me through the transition of committee members; honesty, thank you for believing in me when others did not. A special thanks to my teammates who I have developed a lifelong friendship with, and for being here, I owe you both Steve Knese and Vivian Lyon; without your encouragement, I could not have done this, I owe you both. And a very special thanks to my students who encouraged me through this process.

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 5

Interview/Survey Questions 5

Conceptual Framework 6

Definition of Terms 7

Assumptions, Limitations, and Delimitations 8

Assumptions 8

Limitations 8

Delimitations 8

Significance of the Study 9

Contribution to Information Technology Practice 9

Implications for Social Change 9

A Review of the Professional and Academic Literature 10

Diffusion of Innovations Theory 11

Diffusion of Innovations Compatibility 14

Compatibility Security Policies 15

Compatibility Security Practices 16
Compatibility IoT device Design 17
Complexity 20
Diffusion of Innovation Application 22
Observability 22
Observability Security Policies 22
Observability Security Practices 23
Observability IoT device Design 23
Trialability 24
Trialability Security Policies 24
Trialability Security Practices 25
Trialability IoT device Design. 26
Analysis of Supporting Theories 26
Analysis of Contrasting Theories 28
Internet of Things 29
State of IoT Security 36
IoT Device State of Security 40
The Importance of IoT Security Strategies 41
IoT Security Policies and Standards within Educational Institutions 44
IoT Applications within Educational Environments 46
Relationship of Study to Previous Research 48
Transition and Summary 51

Section 2: The Project 53
Purpose Statement 53
Role of the Researcher 53
Participants 56
Research Method and Design 57
Method 57
Research Design 60
Population and Sampling 62
Ethical Research 66
Data Collection 68
Instruments 68
Data Collection Technique 73
Data Organization Techniques 77
Data Analysis Technique 78
Reliability and Validity 81
Dependability 82
Credibility 84
Transferability 84
Confirmability 85
Transition and Summary 86
Section 3: Application to Professional Practice and Implications for Change 87
Overview of Study 87

Presentation of the Findings....88
Applications to Professional Practice....112
Implications for Social Change....116
Recommendations for Action....117
Recommendations for Further Study....119
Reflections....120
Summary and Study Conclusions....121
References....123
Appendix A: NIH Certificate of Compliance....155
Appendix B: Interview Protocol....156
Interview/Survey Questions....156
Appendix C: Consent Form....158

List of Tables

Table 1 Matrix of Literature Comparison 10

Table 2 Minor and Major Themes Network Access Restriction 90

Table 3 Minor and Major Themes for Network Isolation 97

Table 4 Minor and Major Themes Adoption by Leadership 103

Table 5 Minor and Major Themes Strong Shared Partnership 108

Section 1: Foundation of the Study

Background of the Problem

The importance of Internet of Things (IoT) connected devices becomes more apparent as the quality of life for many people improves with the application of IoT devices. This fast-paced technology provides many benefits, such as allowing the aging population to remain independent longer through sensors that are IoT connected (Cahill et al., 2019). The projected growth of IoT connected devices highlights the need to ensure the devices remain secure. Some predictions indicate that IoT connected devices will possibly exceed 19 billion by 2019 (Castillo & Thierer, 2015).

The trend towards the adoption of IoT devices within manufacturing, healthcare, education, and home environments is applying a focus on IoT security. There is a need across domains for a standardized set of security practices that secure IoT connected devices (Tryfonas & Li, 2016). Securing the IoT requires that policies be implemented within a framework that encompasses all the domains such as manufacturing healthcare and education, and the home environment. The need for security is due to the method of design and manufacture and the configuration process of IoT connected devices, and the absence of an incentive for companies to design security into the product (Chatfield & Reddick, 2019). The incentive to secure IoT connected devices is missing if manufacturers do not design security into the device; there is no accountability. The absence of security is evident in many current attacks against IoT (Davar, 2017). The Mirai botnet crippled the Internet in 2016 for a short period. For the adoption of IoT

devices to be accepted, security issues need to be addressed, and standards need to be adopted.

Problem Statement

The National Security Agency (NSA) identified IoT devices as a critical point of vulnerability within a network of interconnected devices (Richards et al., 2016). A demonstration of the effect of having compromised IoT devices online occurred in 2016, in which over 493,000 IoT devices were part of a botnet that impacted the entire East Coast (Chacko & Hayajneh, 2018). The general information technology (IT) problem is a lack of security policies and practices in IoT device design, potentially affecting Internet devices' global security. The specific IT problem is that some local campus IT managers in educational institutions across the Southeast portion of the United States lack security implementation strategies for securing IoT environments.

Purpose Statement

The purpose of this qualitative exploratory multiple-case study was to explore implementation strategies used by some local campus IT managers in educational institutions in the United States to secure the IoT environment. This study's targeted population consisted of local campus IT managers within educational institutions across the Southeast portion of the United States that have implemented strategies to secure IoT devices. Positive social change may be realized by improving the quality of education and services provided to the communities due to improving the security of IoT devices within educational institutions.

Nature of the Study

The most appropriate method for this study was a qualitative methodology. This method was implemented to explore the strategies used to mitigate security issues that prevent IoT devices' adoption in educational institutions. Cronin (2014) identified that a qualitative method allows the researcher to focus on the strategies, themes, practices, and patterns surrounding a given topic or scenario. Such methodology was appropriate for this study because qualitative studies allow for the in-depth exploration of a phenomenon and the understanding of strategies to mitigate security issues on specific educational institutions. A qualitative method allows for focusing the real-life experiences of those implementing the strategies within their operational environment (Palinkas, 2014).

This methodology also provided a means for determining IT managers' strategies of confidentiality integrity and availability through deployment practices to secure IoT devices within institutions. A quantitative methodology is primarily used to test hypotheses based on numerical information from identifiable variables that can easily be measured (Scrutton & Beames, 2015). Because my aim was to understand the strategies used to secure an IoT environment and not test a hypothesis based on dependent and independent variables, a quantitative method was not chosen. Mixed methods combines qualitative and quantitative methods to answer research questions (Johnson & Onwuegbuzie, 2004; Venkatesh, Brown, & Sullivan, 2016). Because I did not test a hypothesis, and I did not use a quantitative method, mixed-method was not chosen for this study.

The design chosen for this research study was a multiple-case research design. This design allows for the emergence of themes to guide the research while permitting an in-depth investigation (Killingback, Tsofliou, & Clark, 2017). This multicase study design allowed the researchers to focus on exact IoT security strategies specific to multiple educational institutions. Multiple case study results provide a stronger foundation by comparing evidence and triangulating data from more than one case study. Multiple-case studies allow for an understanding of the dissimilarities and parallels among all cases (Baxter & Jack, 2008), which was useful for studying IoT device adoption. Implementing a single-case study does not provide sufficient depth for many studies (Eisenhardt & Graebner, 2007).

What was needed was to compare results across multiple environments; this surpasses the limits of using past models. Through a multicase study, provided evidence is likely to be more reliable. The outcome of the research is directly related to the type of method implemented by the researcher. It is critical in the initial planning stages to ensure the design fits the research and contributes to answering the research question.

The ethnographic research design concerns the study of people, a culture, and the interaction between them (Williamson, 2006). Ethnography is inappropriate for this study because I wanted to research strategies for securing IoT environments. Phenomenology focuses on humans' lived experiences and the rich description of the experience (Matua & Van der Wal, 2015); thus, it was not appropriate for the study because this study did not focus on individuals' lived experiences. This study was about applying and developing

strategies and not about the meaning of lived experiences, so phenomenology was not an appropriate choice for a research design.

Research Question

What strategies do local campus IT managers in the Southeastern portion of the United States use to implement secure IoT devices within educational institutions?

Interview/Survey Questions

1. What IoT strategies have you used within your institution to implement IoT technology?
2. What method did you use within your institution to adopt policies that allowed for implementing IoT strategies?
3. What method did you use within your institution to adopt practices that allowed for implementing IoT strategies?
4. What strategies did you use within your institution to ensure that IoT policies and practices are effective?
5. What methods provided the best results when implementing practices and policies within the institution?
6. How has the adoption of IoT within other institutions impacted the adoption within your institution?
7. How did your organization address the issues associated with the complexity of IoT devices?

8. What security implementation strategies do you feel work best overall regarding policies and practices?

Conceptual Framework

The diffusion of innovations (DOI) theory is the basis for this study's conceptual framework as defined by Rogers (1962). DOI stems from five attributes of innovation, including relative advantage, compatibility, complexity, trialability, and observability. Relative advantage of IoT can effect social change through global implementation. There are instances in which the DOI theory is used to study the adoption of technologies (Kolasińska-Morawska, Sułkowski, & Morawski, 2019). One such study, conducted by Vafaei-Zadeh, Ramayah, Wong, and Hanifah (2017), implemented the theory of DOI in research modeling. Vafaei-Zadeh et al.'s primary focus was the adoption of Internet security software and was evaluated against perceived use of Internet security software in relationship to security software and factors affecting the decision to adopt such technology. The software adoption study by Vafaei-Zadeh et al. indicated that compatibility is key to adoption, as are observability and trialability. However, the research also indicated that product image did not appear to impact adoption. The results indicated that the participant's adoption was based on advantages and value; however, surprisingly, the same respondents were not concerned with ease of use or image, thus concluding these elements were not contributing factors in adoption (Vafaei-Zadeh et al., 2017).

The DOI theory is used to implement various types of emerging technology (Kolasińska-Morawska et al., 2019). Various examples of emerging technology

implementation are found in educational institutions in which IT managers have deployed various IoT technologies to help improve learning outcomes for students within various institutions. The use of IoT devices in education contributes to learning experience quality (Tew, Tang, & Lee, 2017; Zhu, Yu, & Riezebos, 2016). I implemented Rogers's (2010) theory of DOI to understand the methods used to secure educational institutions' IoT environment. The study benefited by mapping compatibility, relative advantage, and adaption to securing IoT devices within the campus environment to understand the barriers and opportunities to the adoption of secure IoT devices within the institution and its advantages and disadvantages. Smart IoT devices' implementation provides innovative technologies that enable students to learn better and faculty to deliver interactive, hands-on instruction (Department of Education, 2013). Students might improve their knowledge as a result of secure IoT devices. The DOI theory's application to strategies implemented by local campus IT managers within educational institutions in the Southeastern United States to secure the IoT environment might help improve effectiveness and efficiency of student and faculty daily learning engagement.

Definition of Terms

IoT. A basic interaction between objects and people enables the communication between people and the environment (Atzori, Iera, & Morabito, 2017).

IoT security. Composed of various interconnected devices and objects that comprise humans, services, and machine to machine. These devices can share data between devices and the individuals the devices serve (Atzori et al., 2017).

Assumptions, Limitations, and Delimitations

Assumptions

Research assumptions can provide unintended consequences if not tested. As the assumptions are primarily focused on the researcher's perception, the assumption must be tested to ensure independent verification (Zhang, Lin, & Qi, 2018). The first assumption made in this research study is that the participants understood the research question and answered the questions to the best of their understanding. The next assumption was that the participants possessed a background in IT and understood the basics required to secure a network.

Limitations

Research studies have limitations and are defined as an uncontrollable threat affecting the validity of the study (Ellis & Levy, 2009). One of the studies' limitations is reflected in IT administrators' use on each campus as participants. The understanding of securing the institution might not be as applicable to other organizations. The current study was also limited to 10 research participants, and as such, this could cause issues in the application to a larger population.

Delimitations

The study delimitation being confined to what the research is limiting in scope or what you, as the researcher not going to do (Ellis & Levy, 2009). This research's boundaries are defined as the research participants chosen from educational institutions responsible or have some understanding of network security. Another delimitation is the use of 10 research participants across two organizations. The final delimitation is using a

multi-case research study and the absence of larger institutional data from major educational institutions with contrasting infrastructures.

Significance of the Study

Contribution to Information Technology Practice

This study's significance is in yielding results that may help IT managers of educational institutions understand how to secure IoT environments and possibly allow them to provide a more enhanced learning experience. The emergence of IoT technology on a global scale and the absence of security standardization could affect modern technology's adoption within society (Li, Xu, & Zhao, 2015). The study's benefits may enable IoT adoption within the classroom, providing a better learning experience for the student through security standardization.

Implications for Social Change

Securing IoT devices might improve society globally by contributing to safer student data and instituting a more secure learning environment. Securing IoT devices within an educational institution might ensure safer student data and provide societal benefits by ensuring students' data remains safe. Positive social change may be realized by improving the quality of education and services provided to the communities due to improving IoT devices' security within educational institutions and the communities. The securing of IoT devices might increase students and faculty's learning outcomes, productivity, and efficiency and provide a more secure environment without fear of privacy loss.

A Review of the Professional and Academic Literature

The research question of what strategies IT leaders use to implement a secure IoT environment within their educational institution is the core of this research project. To understand the strategies being implemented will help to contribute to the growth of IoT acceptance within the educational institution. The CIA triad and the theory of DOI were tools that provided as a foundation a means to guide this study.

The Literature review includes content obtained from IEEE Xplore, Proquest, Google Scholar, ACM, EBSCO, FTC, NSA. There are 225 articles and journals included in this research, of which there are 116 citations in the literature review. Of the articles and journals in the literature review, 87% are peer-reviewed, and 72% published within the last 5 years of the research.

Table 1

Matrix of Literature Comparison

Reference Data	Total Number
Total References	225
Total Peer-References References	197
Total Nonpeer Reviewed References	28
Seminal Sources	1
Conference Papers	5
Total published within 5-year period from publication	132
Total published outside of 5-year period from publication	86
Total percentage of peer-reviewed source material	87.92
Total percentage of material published within a 5-year period	72.32%
Total percentage published within 5-year period and peer-reviewed	71.82%

The primary focus of the literature review was to establish that a void in research existed. Evidence that IoT security standards could impact the adoption of IoT technology within various organizations and institutions. The theory of the DOI and the

CIA triad was used as a touchstone for this study to help understand IoT security and device adoption.

Diffusion of Innovations Theory

Rogers's (2003) DOI theory defined communication as a process in which participants create and share information within a societal setting to achieve a mutual understanding (Rogers, 2003). Diffusion is a social process, and that acceptance is usually an atypical outcome of this social process. The results are usually based on the initial terms of acceptance that help determine the innovations' changes through acceptance (Dearing & Cox, 2018). Rogers further defined the DOI theory as the process in which individuals who accept an innovation communicate through various channels over a period to participants of a societal setting. Technology innovation can spread through network clusters with people responding to promoting a rapid diffusion of technology (Kreindler & Young, 2014). Rogers noted that diffusion is a unique method of conveying new ideas through communication. These new ideas indicate an uncertainty anchored on the newness of the idea in the message. The diffusion and acceptance of new ideas may determine the success of a security adoption within an institution based on previous experiences of its users and adopters.

The theory of DOI originated to help understand and explain how products disperse or diffuse over a given period. For individuals to adopt the idea or accept the product or idea first, the individual or a societal group needs to recognize the innovation as new as well as providing benefit and then permitting diffusion (Lien & Jiang, 2017). The purpose of adopting technology might have various origins between different

institutions due to the potential challenges and perceived roadblocks to adoption (Haddud, DeSouza, Khare, & Lee, 2017). Factors that can influence the success of IT include innovation, acceptance, and communication channels as the general characteristics of the innovation and the adopters and social system that the technology is being adopted within (Rogers, Quinlan, & Singhal, 2004).

The acceptance of new technology, such as IoT, might be impacted by various external and internal factors. Some factors are based on the user's acceptance of how well the technology is accepted (Venkatesh, Morris, Davis, & Davis, 2003). Various factors impact the adoption of technology within an institutional environment, thus perceived from an individual's perception of technology and usefulness. Schiller (2003) highlighted that teachers' attitudes towards technology could impact an individual's willingness to adopt technology in the classroom. Furthermore, perception can influence technology adoption (Blackwell, Lauricella, & Wartella, 2014; Buabeng-Andoh, 2018; Schiller, 2003). Various issues can impact the adoption of technology within an institution either positively or negatively. Determining these factors and the influencers of these factors can help understand the possible impact of new technology on students and technology administrators' educational institutions.

I implemented the theory of DOI based on five characteristics used as a touchstone to explain why new ideas or technology spread (Rogers, 2003). The five elements of the DOI theory are compatibility, relative advantage, trialability, observability, and complexity (Rogers, 1962). As highlighted by Rogers (2003), the five characteristics helped to understand the adoption of IoT technology and securing the

technology within the educational institution, and the need to ensure compatibility of the devices to encourage adoption.

The current study will help local educational security administrators understand the benefits of IoT of secure IoT devices and contribute to the students learning outcomes from adopting a more secure IoT device platform. The IoT device adoption can provide for a more in-depth learning experience for the student as well as Smart campus infrastructure enabling the tracking of students to also contribute to enhanced learning outcomes; however, with all of the advancements come risks such as privacy and security (Kassab, DeFranco, & Voas, 2018). The current research study may help to facilitate understanding of the adoption of IoT devices within the campus environment and understand what factors influence the adoption of security for the institution and the students.

I implemented the theory of DOI to help understand potential roadblocks to new technology within an organization. The theory of DOI was used to focus on compatibility, relative advantage, trialability, observability, and complexity (Rogers, 1962). The DOI theory provided a lens to understand why a lack of security policies and practices in IoT device design exists. Hopefully, the results will enable IT and managers to evaluate a more comprehensive plan when developing an IoT design within the educational institution. The synthesis was obtained from an analysis of the DOI theory provided. As a result of contributing to IT managers within educational institutions to help institute strategies to implement a more secure IoT environment within the educational setting.

Diffusion of Innovations Compatibility

Rogers (2003) defined compatibility as a level of which innovation is perceived as being aligned with current values and or the experience and in alignment with the group of potential adopters. Rogers further defined that the innovation can be defined as being compatible or incompatible with the existing standards of normal or previously introduced concepts. Compatibility can be defined as evaluating the harmony between new technology and elements of the individual relationship to the environment that the technology implementation will occur (Karahanna, Agarwal, & Angst, 2006). Various factors might impact the adoption of technology, such as technology compatibility within the institution. Examples of personal experience with technology could impact adoption. Rogers stated that past experiences from the interaction with the interpersonal networks appear to be a key indicator in the process of diffusion.

Understanding the theory of DOI and how compatibility will impact adoption by the target population will help understand the needs within the organization. Determining the compatibility of new technology and how the innovation can meet the user's current needs and the level of alignment that the proposed technology fits with the current values of the adopters and the adopter's belief system within the organization (Rogers, 2003). Understanding the reasons for the delay in IoT adoption related to factors such as failure to understand the added value that IoT technology brings to the organization. (Hwang, Kim, & Rho, 2016). Various factors can impact the acceptance of new technology within an organization. Understanding the perception of previous technology and the individual

needs of the adopters and the perception of the technology concerning the organization's current needs will help understand organization adoption.

Users' previous experience will come into play based on the previous user experience interaction with the technology for users to feel comfortable with technology adoption. Questions may be asked, such as was the graphical user interface easy to use, or was the device easy to update? Previous experience with technology can impact how a potential adopter views the new technology; thus, the experience can retard or accelerate adoption (Tsai, Chang, Chen, & Yung-Sheng, 2017). However, previous experience, good or bad, is the tool that is used as a benchmark to make these decisions as innovation based on experiences that individuals are familiar with (Rogers, 2003). Technology compatibility is a determinate factor when adopting new technology, and the compatibility will affect the adopter's choice based on the technologies' past experiences.

Compatibility Security Policies

The compatibility element of the DOI theory applies to how the technology or innovation aligns with current or existing ideas of the individuals who will use the technology (Rogers, 2003). Ideas that are more compatible with previous experience or appear to align with the current adopters' situation would possibly be received more favorably (Zhang, Wen, Li, Fu, & Cui, 2010). Security policy adoption within an institution will be contingent upon alignment with the organizational needs and the current mission statement. Other concerns requiring address are found in developing a security policy that would be the constant nature of the change of IoT devices represent

to the organization and, as such, would require a policy that is compatible with current policies and allows for changes that IoT represents to the organization.

The securement of IoT devices within an institution could benefit from a security model that would ensure potential IoT adoption is compatible with present policies and technology. A three-layer architecture would provide a mechanism to ensure the compatibility of the institutions' goals. A cross-layering security method through all of the facets that IoT devices interact with would provide a mechanism for securing the IoT (Atzori et al., (2017). A clearly stated security policy would include IoT security as a touchstone to measure the technology and ensure compatibility.

Compatibility Security Practices

The theory of DOI uses the idea of compatibility as a touchstone to determine if the induvial who would be adopting the technology perceives the innovation as adding value based on previous experience (Rogers, 2003). The security would be accepted if not considered as compromising the privacy of the individual. Applying best-case security practices will ensure that the institution provides a secure environment and ensures compatibility with existing practices for the users. A systematic approach to security practices will ensure continued privacy practices (Porambage et al., 2016). Another element to consider in security practices is device compatibility in which the user can configure the device based on previous experience. The manufacturer should provide backward compatibility by allowing user interaction protocols to remain compatible (Fawaz & Shin, 2019). Proactive security practices allow for backward

compatibly of IoT devices to allow the user to quickly and easily configure the device based on previous knowledge.

Compatibility IoT Device Design

The theory of DOI and compatibility looks at previous experiences in adoption (Rogers, 2003). The changing nature of IoT lends to the issues between device design compatibility. Examples of device compatibility issues can be found within the implementation of high-frequency technology; however, the research case provided highlights the compatibility of IoT technology adoption issues within the supply chain management process (Tu, 2018). Previous experience of the manufactures and engineers seems to play a key role in current product design issues.

Relative advantage. Relative advantage is another key element of the DOI theory. The relative advantage concept is based on the benefit that the innovation or idea is viewed as better than the technology or idea it replaces (Rogers, 2003). Rogers (1962) indicated that relative advantage might be determined in the form of economic, convenience, satisfaction however indicated by Rogers is that the technology or new ideas must be perceived as having value; thus, the greater the added value, the more readily the adoption rate would occur.

The relative advantage identifies how a strong society perceives IoT technology's advantages and what technology is replacing (Rogers, 2010). The importance of understanding the reasons for IoT device acceptance by consumers is indicated by Lowe and Alpert (2015). They stated that perception is only new if the customer perceives it as new. Compatibility of IoT device security is the extent of IoT technology that is being

replaced compares with existing technology, as highlighted by Rogers (2010). The perception of compatibility can be related to the degree of perceived usefulness of the replaced IoT devices. Complexity is measured by the level of how hard the technology is to use or how difficult to implement (Rogers, 2010) and is evaluated through usability. Trialability refers to permitting technology evaluation on a trial basis before its permanent adoption (Rogers, 2010). Observability is defined by how readily the results are visible to others that would enable adopting this new technology (Rogers, 2010). The conceptual framework that DOI provides fits this study because of the security issues related to IoT adoption. IoT device complexity and compatibility contribute to the absence of IoT device adoption, which has contributed to an absence of standardization.

For a business to maintain a competitive edge, the organization must consider adopting new technology and the factors that impact the adoption. Furthermore, IT in the business environment was considered a luxury; however, this is no longer the case (Lee & Runge, 2001). Factors that influence technology adoption within an organization can be linked to the individuals within the organization who are the early adopters and linked to the leaders' personality within the organization and the technical leadership (Lee & Runge, 2001). The relationship between compatibility and relative advantage is similarly linked together as relative advantage is framed as an incremental benefit through technology implementation or use (Karahanna & Straub, 1999). The impact that the manager or technology champion within an organization can have on the successful adoption of technology within an organization can either contribute to successful

adoption; however, if the relationship between compatibility and relative advantage is not considered, it can also impact adoption within the organization.

Relative advantage security policies. Proper security policy development and implementation within an organization requires key stakeholder buy-in and recognizing the importance of adherence before a security event. Rogers (2003) indicated that early adopters might be ahead of others when adopting a new technology even if the perceived relative advantage was not yet visible. Rogers further indicated that most adopters do not adopt until their peers establish that the innovation was successful. Security policies are written with various factors that must be accounted for, such as the human element considered to be the weakest link in the chain (Guo, Yuan, Archer, & Connelly, 2011). Security policy adoption by individuals within an organization is critical to remaining secure; furthermore, policy adoption by management and employees before an event occurs. Password expiration policies are another area where all key stakeholders might not support the organization's perceived value; all key stakeholders must see a relative advantage to the organization and help support security policy adoption.

Relative advantage security practices. The advantages of security adoption within an organization encompass many factors that involve the human element. Rogers (2003) described relative advantage is one of the strongest predictors of the adoption rate of innovation, as indicated by scholars of diffusion. The human element and the impact of technology adoption can be categorized into different groups such as desirable verse undesirable and functional as well as nonfunctional thus, the consequences have a direct effect within the environment in which the innovation diffusion occurred be it negative or

positive (Reid & Niekerk, 2014). Security adoption within the organization can be perceived negatively or positively depending upon the adopters' previous experiences.

Relative advantage IoT device design. Security can also be perceived through a financial perspective or impact on the institution. Relative advantage can be measured in terms of economic gain or benefit (Rogers, 2003). The cost of ensuring that a device is secure when designed is impacted by the quick turn-around time that is allotted for device design and deployment (O'Neill, 2016). Relative advantage and anticipated cost of product deployment and design can impact the DOI as the perceived cost can affect the innovation's security.

Complexity

Device ease of use can, in many instances, be associated with adoption as well as a technology investment. Rogers (2003) indicated that complexity is directly related to how easy it is to use or implement; thus, the more complicated it is, the slower the technology or device's adoption. Devices that are complicated to set up or implement, such as wireless router user interfaces, could impact adoption. The configuration to work properly out of the box or the user interface is easy to navigate are issues that could impact the device's sales.

Complexity security policies. Security policies of an organization can be the frontline of protection, and if breached, can have long-lasting consequences; thus, many factors can influence policy adoption within the institution. Rogers (2003) indicated that complexity parallels innovation as not being perceived as simple to understand. Security policies that are hard for adopters to understand can impact the acceptance within the

organization. It is suggested that the policy be developed with the focus being a user-centric based policy (Mollah, Azad, & Vasilakos, 2017). Security policies that are complex present a challenge for adopters to understand could foreshadow security issues for the institution.

Complexity of Security Practices. Organizational security practices are the product of adherence to a security policy; thus, it could hamper adoption or implementation if the practice requirements are too complex. Examples of this are found in password selection. Complex password policies are found to negatively impact the user and the organization's perception by placing unreasonable demands on the user for increased password complexity, thereby impacting security and how the public sees the organization (Curtis, Carre, & Jones, 2018). Other issues that could also impact the organization's security are the requirement of complex passwords due to the requirement many users reuse passwords, which impacts security and productivity (Farrell, 2008). Security policies need to align with the user's abilities to ensure policy practice adherence, thus ensuring the policies meet both the user and the organization's needs.

Complexity IoT device Design. When implemented by the end-user, IoT device design products must be configured and administered with minimal interaction. Furthermore, simplicity must be part of the product design consideration factors and low overhead (Choi, 2018). Complexity issues must be considered when designing an IoT product. IoT devices by design come with a unique set of issues that further device complexity could impact adoption if added to the list of issues already being addressed. It is essential to understand that inherent limitations are already associated with IoT devices

(Dinculeană & Cheng, 2019). There is a need for the device designer to ensure an experience that is user-centric and considers the relationship between the user and the device, thus allowing the designer to focus on other issues impacting device design.

Diffusion of Innovation Application

Observability

The final element of the DOI framework is Observability. Rogers (2003) identifies the concept of observability as the degree to which the outcome is either communicated or visible to individuals. The adoption of 3d print technology within various organizations could be affected by how well the 3d printing technology can be observed and perceived as adding value (Marak, Tiwari, & Tiwari, 2019). Observability is a critical element in product adoption as the observability can take on many forms either by product observation or by data observation. Rogers also indicated that observability is directly related to adoption and how fast the innovation is accepted. Thus, observability can lead to innovation adoption if the technology observed provides enough information to help the potential adopter feel comfortable with the technology.

Observability Security Policies

Organizational security policies, when implemented properly, contribute to the insurability of an organization. One such case study viewed from an insurance company looks at the security policies and implementations to determine if the company is providing self-protection to receive cybersecurity insurance (Oğüt, Raghunathan, & Menon, 2011). The study focused on determining if the organization was self-protecting by using observability as a tool, and the results would impact the client's insurability.

Network connectivity must remain secure between devices, and this trust can be obtained through device monitoring. Rogers (2003) indicated that the device's physical display or appearance contributes to the system's elements. Thus, different perspectives of observation of security policies affecting the security policy development refer to the trust of other entities or beliefs; the trust focuses on the previously observed behavior or actions of other entities (Boukerch, Xu, & EL-Khatib, 2007). Wireless security can be obtained through a system of observed trust not by humans as much as by the technology, thus taking the observer's perspective and assigning the observer's role to the technology through gained trust.

Observability Security Practices

Security compliance within an organization can be affected by many different factors. One case study indicated that some of the key elements of a security policy are based on observed influence from other organizational policies, impacting how security practices are implemented within a different organization (Daud, Rasiah, George, Asirvatham, & Thangiah, 2018). Furthermore, there is a need to take a holistic approach while not excluding nonorganizational data and including it as part of the complete solution when implementing security practices.

Observability IoT device Design

IoT security design involves methods to promote secure coding through promoted observation of techniques. Rogers (2003) defined observability as visible results to others of an innovation. In many cases, visible results can encourage others to implement the same techniques being utilized to encourage the use of new technology. Examples of

implementing new technology within institutions are linked to collaborations and observed methods of overcoming perceived security issues and obstacles to eLearning (Tanye, 2016). Observability promotes learning adoption and can increase the overall perceived security by eLearning students allowing them to participate in online learning.

Trialability

Trialability is associated with being a characteristic of the theory of DOI. The characteristic helps to provide insight into understanding innovation adoption based on a partial trial basis (Rogers, 2003). Examples of trialability can be found in the software industry. A software product can be provided to an end-user on a time-limited basis, allowing the user to evaluate the software before purchase (Cheng & Tang, 2010). Free software trials have permitted the end-user to try various software types before purchase; however, the software is limited in functionality in many cases. One such example is a case study on cloud computing adoption that evaluated three separate cases in which trialability is an essential factor in cloud service adoption due to piloting the services before implementation (L. Morgan & Conboy, 2013). Trialability allows for assessing a product before commitment, such as cloud computing or application software, thus benefiting the adopter and the service provider, can be realized before adoption.

Trialability Security Policies

Trialability is a key element when evaluating new security policies or equipment, especially when the technology is new, like IoT. Security policies within the institution play a critical role in securing organizational needs (Herath & Rao, 2009). Some situations indicate that starting with a pilot project can help a company determine if the

need is there without entirely investing in IoT technology (Lee, B., and Lee, J., 2015). Furthermore, new IoT security policies may require a pilot for a limited period to determine if the implementation is working within the institution.

IoT applications and trialability provide a touchstone for evaluating working solutions in real-world scenarios. Examples of real-world can be found in a pilot project using IoT to manage food safety is based in China as a project that is designed to ensure that the food is fresh and the supply chain is more transparent to the user; the project includes the implementation of security protocols (Liu et al., 2016). Using a pilot program can be a good example of technology's trialability within a real-world environment, thus providing the adopter's valuable information that otherwise might not be available.

Trialability Security Practices

Security practices encompass physical and personnel assets; however, the primary element of security practices involves people. However, the personnel must implement and practice the security policies implemented, and thus, it becomes vital to ensure that the policies harmonize with the people (Deibert & Rohozinski, 2010). When the institution allows for a security policy to be implemented on a trial basis it allows the institution an opportunity to determine if the policy fits the institutional needs. Furthermore, as noted by Rogers (2003), trialability provides the user an opportunity to remove the uncertainty, thus allowing the advantage of doing by learning. Test pilot programs allow organizations to try before complete implementation, thus ensuring the

needs of the institution and the people adopting the technology and the technology are a good fit.

Trialability IoT device Design.

Providing an environment to test and design an IoT device while ensuring security before complete deployment could ensure a more secure device. Many companies promote free samples to encourage product adoption (Gene, Nguyen, & Kanji, 2006). Manufactures of digital content offer free samples to encourage product adoption and increase the organizations' sales that implemented this as a technique (Chen, Duan, & Zhou, 2017). Companies that provide free products on a trial basis or in limited quantity can contribute to IoT device security design and product improvement of a companies' devices or content.

Open-source software is another area in which trialability can contribute to a more secure IoT device design. The advantage of open-source software is that it has contributed to software adoption for an application due to the software's open nature and the cost associated with the software (Morgan, Lorraine & Finnegan, 2007). Trialability using open source software may improve the device design due to the benefits of open source development software, allowing for crowdsourced security development and testing.

Analysis of Supporting Theories

Contrasting parallel and opposing theories help to provide a foundation for establishing a foundation for research. The theory of Technology Acceptance Model (TAM) highlights that compatibility, complexity, and observability impact individuals'

attitudes or perception, thereby affecting the adoption of the technology (Min, So, & Jeong, 2019). The similarities between the technology acceptance model and the DOI are very similar as both appear to help understand the influences in adopting the technology. Furthermore, to understand the factors that influence IoT security's adoption within the educational institution, innovation diffusion allows for. In contrast, TAM allows for the focus to evaluate the individual's acceptance of new technology (Min et al., 2019). In contrast, the DOI theory allows for the focus on various elements that impact the technology's adoption. If the focus of the study were to understand the reason for adopting IoT security within an educational institution, the TAM theory would be applicable; however, the purpose of this study was to understand the IoT security adoption within the institution and thus is not appropriate for my research study.

The next parallel theory to be evaluated will be the theory of the organizational technology environment. The theory of (TOE) was developed by (Tornatzky, Fleischer, & Chakrabarti, 1990) as a tool for The Theory of (TOE) is used for understanding why firms adopt technology such as motivation factors (Cao, Ajjan, Hong, & Le, 2018). The theory of (TOE) parallels nicely with the DOI theory in that both theories explore why organizations adopt technology and factors that influence the adoption of this technology. Many research studies have used the (TOE) theory as a touchstone for evaluating technology adoption (Cruz-Jesus, Pinheiro, & Oliveira, 2019). Both the theory of DOI and (TOE) look at external technologies for adoption into the organization and technology that originates within the organization as the source. I did not select (TOE) as a theory due to some of the elements in the theoretical framework did not align well with

my research even though a large percentage of the (TOE) framework aligned some elements did not such as top management readiness and competitive pressure thus for this reason. Another viable option is the inclusion of the DOI framework as well as the (TOE) frame in the study together. However, this would provide an overlap between theories, and as such, I did not include the (TOE) framework in this study.

Analysis of Contrasting Theories

Unified Theory of Acceptance and Use of Technology model. The Unified theory of acceptance and use of technology (UTAUT) model was developed by Venkatesh et al. (2003) and is the next theory to be considered. The implementation of UTAUT in research provides a framework to help understand technology adaption, much like the DOI theory. This comparison is accomplished using four key touchstones: performance expectancy, effort expectancy, social influence, and facilitating conditions (Rempel & Mellinger, 2015). The use of (UTAUT) originally was for management to understand employees' use of technology (Rempel & Mellinger, 2015). I did not intend to evaluate these four factors that affect the adoption of technology in my research. My research intends to explore the methods that are successful in adopting security within the institution and thus was not appropriate for my research study.

The next framework to be evaluated is the theory of reasoned action (TRA). This theory provides a touchstone to help understand behavior. (Goldenberg & Laschinger, 1991). The purpose of this study was not focused on the understanding of an individual's behavior. The primary use of (TRA) is to understand how individuals will react to specific circumstances in an environment and how individuals will react to specific

behaviors (Taufique, Siwar, Chamhuri, & Sarah, 2016). The theory of reasoned action (TRA) explicitly applies the focus of an individual's reactions and, as such, is not the focus of my research and is not being included as a possible framework.

Internet of Things

The term (IoT) is a concept that is new to society and can improve many people's quality of life. The acronym IoT being credited to Kevin Ashton, a founder of Auto_ID Center, an organization associated with the Massachusetts Institute of Technology. While the definition of IoT varies greatly, one common element is the interconnection of devices to a global network that shares data specific to the environment with other devices to improve a process (Gubbi, Buyya, Marusic, & Palaniswami, 2013). This interconnection of devices includes the technologies related to IoT (Berte, 2018). By encompassing connected devices and technologies that comprise the IoT, the definition of IoT also allows for remote management of devices, data acquisition of control devices, and their endpoints. IoT is complex; while there is no one definition, the definition must include devices, technology, and their interconnection.

IoT's current emerging technology is relatively new to society and may touch many daily living facets, such as the teaching and learning methods and processes (Bajracharya, Blackford, & Chelladurai, 2018). IoT technologies obtain information about the devices' current environment contributing to continual process improvement (Funk, Lin-Lin, Shao-Wen, & Yen-Kuang, 2018). Three elements common to the architecture of IoT devices are hardware, middleware, and presentation (Gubbi et al.,

2013). These three elements contribute to the operation and design of the IoT environment.

Due to society's ever-expanding energy demands, the requirement to manage these resources securely is required. The IoT-connected power grids paradigm provides effective solutions; however, this solution comes with a new set of security challenges (Kimani, Oduol, & Langat, 2019). The implementation of a managed power grid increases the attack surface that must be defended against.

Security attack surfaces are increasing due to the nature of connected IoT devices and the networks these devices reside on. Issues related to the decentralized nature of IoT connected devices presents a new set of issues that hamper the ability to defend against random attack (Meyer, Haase, Eckert, & Klauer, 2017). The IoT objects generate a tremendous amount of traffic and, as such, are relatively vulnerable to various types of network as well as physical attacks.

Social IoT connected devices is another arena that must be protected from attack as these devices communicate with each other to provide services in terms of common outcomes for society. New methods of network virtualization can manage bandwidth and provide functionality in regards to socially connected IoT devices as well as provide security to the network and, by extension, provide privacy (Sun, Huang, Sangaiah, Zhu, & Du, 2019). The holistic method for managing not only bandwidth usage of IoT connected devices in a virtual environment but also ensuring privacy and security will possibly provide a more secure IoT connected device.

The use of a touchstone or benchmark to measure the various elements of IoT security is required in this research study. The implementation of confidentiality, integrity, and availability (CIA triad), as defined by (Petac & Duma, 2018), was used within the literature review to determine inclusion in this research study. Confidentiality applies to IoT in the sense that the data is only available to intended parties; integrity ensures the accuracy of the data, and availability ensures that data is available when required (Petac & Duma, 2018). The use of the CIA triad helped ensure that data included in the literature review includes these requirements.

The CIA triad provides a means to determine an organization's security posture and help improve the state of security within the organization. The CIA triad evaluates the information to determine the threat level of data exposure, and will the information be available when the data is requested? (Albuquerque, Villalba, Orozco, Buiati, & Tai-Hoon, 2014). The last element of the CIA triad is the integrity of the data pertaining to maintaining the data's integrity. Integrity is key to having trust in the packets' source with a degree of assurance that the content is not altered (Sherman et al., 2018). Data manipulation through modifying the results could impact an individuals' safety within the IoT environment. Some research has indicated that the home environmental control systems have been attacked and many other connected devices within the network (Cruz et al., 2019). Various reasons for the proliferation of non-secure IoT devices, as indicated by Cruz et al. (2019), appear to stem from manufactures creating devices quickly to fill the needs of the consumer with little focus on security. Connected IoT devices with the

home network could potentially compromise your personal information or, at a minimum, cause service disruption.

IoT consists of various types of connectivity protocols to operate properly. These connectivity protocols include, for example, the use of Wi-Fi, cellular, and Bluetooth technologies for standard device communication (Berte, 2018). Standard communication is an active form of device interaction through various communication protocols. Other types of communication devices associated with IoT include Zigbee Z-Wave and Near Field Communications (NFC), as well as Radio Frequency Identification tags (RFID). The device can be passive or active depending upon the design and application needs (Garcia, Ruiz, & Gomez-Nieto, 2016). NFC and RFID tags provide different services to the devices to which they are connected. For example, they may track inventory or enable a user to pay for a vendor item from a machine.

Other types of IoT connected devices include smart light bulbs, smart thermostats, smart televisions, intelligent cameras, and industrial control systems (ICS) responsible for controlling motors inside of manufacturing facilities (Berte, 2018). It is important to note that these devices, by controlling lighting or temperature, are using a limited amount of computing power to accomplish a task the device is specifically designed to achieve (Khan & Herrmann, 2019; Qi & Liu, 2018). Thus, understanding the various IoT device applications and limitations will possibly help to define the mechanisms that encompass the IoT.

IoT connected devices use various means to obtain information from within the environment the devices are connected. Sensors are an integral part of the data

acquisition and control element that defines the IoT as it is through the acquisition of data obtained from sensor modules enable IoT connected devices to contribute to the decision process and provide information about the environment in which connected (Roy, Misra, & Raghuwanshi, 2019). The decision process includes information transmitted to a connected cloud or another endpoint device. The sharing of information is usually shared through various protocols and sensors, making the IoT smart (García, Ruiz, & Gómez-Nieto, 2016). Thus, communication occurs using NFC and BLE as well as Cellular, which enables smart devices to interconnect.

Environmental sensors enable the obtaining of real-world data from within an environment. The proliferation of IoT connected devices is linked to the availability of affordable environmental sensors that are used for data acquisition within IoT connected devices (Gary, 2017). Various sensors such as strain, motion, temperature as well as accelerometers are a part of the devices that make up the input devices for the IoT sensing environment (Umek, Zhang, Tomažič, & Kos, 2017). Medical and industrial sensors provide for monitoring either in a healthcare facility or within an industrial environment.

Environmental sensors can serve a diverse group of needs enabling people to live a better quality of life. The various types of sensors can monitor sports activities to improve an athlete's performance (Umek et al., 2017). Other implementations of IoT devices are in healthcare monitoring, allowing the aging among us to remain independent and allow for better quality and extended life (Fattah, Sung, Ahn, Ryu, & Yun, 2017). Biological sensors from the human body can be monitored from a central point, allowing

for real-time analysis of the patient's physical and physiological status ensuring continued care (Fattah et al., 2017). Various types of environmental monitoring devices designed for a specific purpose, such as those used in the medical field, provide patient monitoring for various purposes.

The last element to be included with IoT devices is the software that encompasses the automation and data analytics and the Operating system and firmware. The various types of firmware enable the device to functionally accomplish a specific task, such as reporting data and firmware updates to and from the cloud (Lin & Bergmann, 2016). Furthermore, the IoT device will require connectivity to the network and as such requires the IoT device to work within a software-defined network and provide seamless communication while operating in a small footprint and remaining energy efficient which while providing communication to other devices enabling interactive connectivity with the smart home environment (Zikria, Yu, Afzal, Rehmani, & Hahm, 2018). Implementing these technologies and software combined with network connectivity contributes to the IoT environment and defines IoT.

To better understand IoT security issues, it would be appropriate to look at purpose-built applications associated with IoT devices. Some IoT device designs have limited computing power, thus implement firmware that could be problematic for securing the device and the associated network (Gresham, 2017; Tewari & Gupta, 2018). The IoT device can be updated through an associated network and provide the extension of connectivity to many types of devices such as industrial controls, traffic light monitoring, and networked vehicles through onboard systems (Sheng, Mahapatra, Zhu, &

Leung, 2015). Defining many of the IoT device types and sensor interaction provides a clearer understanding of the IoT as well as and the methods used for communication and data acquisition.

Design standardization issues between the various device manufacturers and the implementation of multiple protocols contribute to the current state of IoT security. Interoperability between devices allows for communication between various vendors using various device communication protocols (Gary, 2017). Differing organizations define the standardization between IoT devices. Each organization identifies security and interoperability; thus, a common thread that appears to remain constant is the standardization of communication protocols (Aftab et al., 2019). A common thread between all key stakeholders appears to indicate that security standards are critical to IoT security. Security issues are observed within Internet-connected children's toys such as baby monitors and smart devices that possibly can expose the privacy and security of individuals on the network (FBI, 2017). Security issues arising from an absence of standardization of security appear to impact the privacy of children's' toys and home video systems as a small representation of security issues that represent attack vectors for malicious actors.

The proliferation of IoT connected devices presents a new set of challenges, such as standardization and interoperability between different manufacturers' devices. Such efforts as a united alliance bring together key stakeholders in the IoT field to help create platforms that allow for IoT usage across varying domains (Araujo, Mitra, Saguna, & Åhlund, 2019). Interoperability between various key stakeholders in terms of the

platform will provide a more secure environment as the need for expanding bandwidth and security increases as IoT device usage increases.

The implementation of IoT device design provides various advantages such as input and output device monitoring for varied environments. Some examples of IoT design applications are used to maximize agriculture crop harvesting and use of limited land through IoT management of hydroponic farming (Belhekar, Thakare, Budhe, Shinde, & Waghmode, 2018). IoT secure device deployment's significance can be observed in monitoring the carbon footprint to ensure nation-state compliance for the Paris Climate treaty (Ravindranath, Chaturvedi, & Kumar, 2017). To mention only a few of the advantages of IoT technology such as crop harvesting and land management, and carbon footprint monitoring, contribute to the advantages of IoT.

State of IoT Security

IoT security needs to provide a foundation that can be trusted and allow expansion. One of the most common IoT attacks that many individuals are familiar with occurred in 2016. The attack involved DYN corporation, a DNS resolver for news organizations and companies such as Twitter and The New York Times. The attack impacted customers who were denied the ability to complete transactions due to a denial of service perpetrated by many home IoT connected devices worldwide, resulting in one of the most substantial denials of service outages to date (Almeida, Doneda, & Abreu, 2017). The culprit in this attack was, in many instances, a home-based video camera with default username and passwords that were hardcoded into the device being used within the botnet that attacked the DYN server (Davar, 2017). Small footprint technology such

as IoT may potentially deny a significant e-commerce provider through a botnet-controlled attack.

The proliferation of IoT connected devices within a global setting impacts users' security without the individual's knowledge. Society is changing the methods used to communicate with each other and has possible negative side effects, such as the loss of privacy and personal data (Hernández-Ramos et al., 2018). Due to the ever-demanding needs that technology places on society in terms of the loss of privacy, there becomes apparent that a need to control privacy and the requirement for new and emerging security mechanisms that can fill the security void is needed.

Securing IoT devices in the deployment process presents a unique set of challenges within various environments. Some of the challenges of securing IoT devices is due to the linking protocols that Bluetooth devices use to connect to send and receive data (Zeadally, Siddiqui, & Baig, 2019). Another of the security issues with Bluetooth communications is once a device is pared, a request is not sent again for pairing; thus, there is a trust relationship that can be exploited between Bluetooth devices (Zeadally et al., 2019). Various protocols such as wi-fi and Bluetooth present another unique set of security challenges due to the trust relationship that these devices present to the network.

Wireless security issues for IoT connected devices represent only a fraction of the overall security-related events. The heterogeneous nature of IoT connected devices includes many different device manufacturers and various types of operating systems and protocols that share a common need for security; furthermore, updating firmware may involve taking critical systems off-line (Gresham, 2017). Some of the issues facing IoT

design are found in the small form factor of the device itself. With limited computing power, the devices can accomplish basic input-output tasks; however, the device lacks the computing power to prevent a malicious attack (Ali & Awad, 2018). Other areas of improvement, however, still need to be addressed.

Standardization is currently an issue between various device manufacturers due to the key stakeholders having different needs for a purpose-built device that must operate inside of another network. Presently, the standards are currently specific to the manufacturer's needs and the standard implemented for bi-directional communication, contingent upon the geographical location for permitted frequencies use(Bandyopadhyay & Sen, 2011). Standardization could help secure the IoT environment by ensuring that all devices manufactured are compatible.

IoT security standardization also involves the update process for IoT connected devices. When IoT devices are deployed, if the device cannot be updated online or by the end-user, the device is either out of date or becomes less secure (Bhattarai & Wang, 2018). Issues with programming and code development present a unique set of security issues for IoT development. Examples of this are found in C code development for IoT devices in using a small footprint that C code offers. There are drawbacks to using the C programming language because developers may not necessarily focus on security due to the device's open-source nature. This open-source nature creates new issues when in the development process, as the creation of function calls can compromise the device and may not be adequately addressed before deployment (Bhattarai & Wang, 2018). Standards between engineers and coders, as well as device manufacturers, could help to

secure the IoT environment. Regulation of IoT devices could prevent device deployment issues as currently, there are no standards, rules, or regulations. Due to IoT's size and complexity and the objects' heterogeneous nature, it is increasingly difficult to manage (Ünver, 2018). The need for communication and standardization is an essential element in securing the IoT environment. The absence of standardization is apparent in the medical device sector of IoT connected devices. One such device manufacturer had over twelve thousand connected devices open to attack on the Internet (Chacko & Hayajneh, 2018). The absence of standards across the IoT industry can potentially impact many IoT devices' safety and security.

The IoT is a conglomeration of embedded devices employing various operating systems and embedded firmware. Various factors, such as time firmware over the operating system being implemented (Padilla, Baccelli, Eichinger, & Schleiser, 2016). For the IoT device to remain secure, there must be current updates deployed to the IoT device to ensure that security flaws are addressed (Ojo, Giordano, Procissi, & Seitanidis, 2018). Other related issues specific to IoT security are found within the lack of design to push out new firmware updates. The device is purpose-built with minimal resources to keep the cost down and provide a purpose-built device with low footprint power requirements (Ojo et al., 2018). Device design could include firmware updates; however, time to market is still a significant concern for manufacturers.

More advanced IoT connected devices such as Single Board Computers (SBC) may present a unique set of challenges due to software and board design requirements. Some aspects are due to the inherent technical capabilities of the device design. Some of

the capabilities presented by (SBC) devices are in software updates and flexibility of running an operating system that can access updates and help minimize back door access through the development process (Rivas & Kliarsky, 2017). Various standards of device design and a plethora of Operating systems and firmware versions from different vendors may contribute to the security issues of IoT devices. Many issues related to IoT security can be traced to security issues in the design process. Implementing a multi-tiered approach to security through two-way trust relationships can strengthen the security weaknesses in connected networks with (SBC) devices (Malina, Hajny, Fujdiak, & Hosek, 2016). Design diversity will contribute to data privacy across the network and minimize security-related issues.

IoT Device State of Security

New technologies such as 3d printing and attendance tracking systems and interactive whiteboards can add value to the educational setting. While embedded design engineers continue to make inroads into security, the defense of many embedded devices is still not secure due to the various types of attacks against embedded systems (Fournaris, Fraile, & Koufopavlou, 2017; Papp, Ma, & Buttyan, 2015). IoT devices are considered embedded systems that can be used to attack other systems in the network due to security vulnerabilities associated with these devices (Hameed, Khan, & Hameed, 2019). A side-channel attack against an IoT device would allow the attacker to obtain proprietary information related to an organization's intellectual property with potential financial impact (Ding et al., 2019). Routers are not the only devices that could be

impacted by poor security; other potential threats exist in student tracking systems and pose potential threats to those individuals monitored by the devices.

The Importance of IoT Security Strategies

IoT device adoption within an institution could be contingent upon the device not compromising its security or those the institution serves. Thus, it is essential to understand the various methodologies used to secure the institution through device securement. The first step in securement is in the device's design phase, while drivers such as economic and a lack of understanding of the security risks associated with the design are contributing factors to poor security (Gloria, 2016). The need to understand and overcome these inherent issues in the early stages of design, development, and deployment can be associated with understanding device development's driving factors.

IoT security design in the early stages of development can shape the device's overall security and the network the device is connected to. The United States trade commission commenced legal action against Trendnet, an IoT manufacturing company, as the (FTC) contends that the company implemented practices that violated the law and could impact the customer using the device (Maras, 2015). Building security into devices before the device is manufactured, and not after, is something that companies need to consider before the design process is undertaken (FTC Staff, 2015). The very nature of the IoT lends to the issues of security with a machine to direct machine interaction, eliminating the need for human interaction while at the same time the amount of devices connected is increasing daily (O'Neill M, 2016). State legislation may contribute to securing IoT connected devices by requiring security standards for connected devices.

Device security issues appear to be more critical in a machine to machine interaction due to the absence of direct user interaction related to the management of the IoT device.

Security Updates provide another means of protection for IoT connected devices. Security updates for connected devices are essential as many manufacturers use the firmware that is static or unable to be updated as well as different protocols that can impact the security within the network even if the devices connected are secured the IoT non-secure devices are a threat vector (Lin & Bergmann, 2016). To remain secure, there is a need to ensure that the firmware update process remains uninterrupted. It is essential to secure the data transmission to ensure that the update is not tampered with; thus, preventing tampering of the firmware will help minimize asset loss or even threat to health monitoring systems (Lin & Bergmann, 2016).

IoT firmware updates present a unique set of challenges for the expansion and growth of IoT. One reason that IoT firmware updates are an increasing threat vector is the update cycle for the IoT devices is slow because the devices were not intended to be updated automatically or are considered a one-time use only device (Pering, Farrington, & Dahm, 2018). IoT firmware update delays can impact the network's security and privacy and the individuals' privacy in which the device is connected.

Another aspect of IoT security is the associated hardware the device is functioning on. Understanding the relationship between the protection of the hardware and its impacts on the device's design might be necessary to understand the relationship between hardware and software security. Basic memory and processing of data are the building blocks of an IoT device; thus, the purpose of the IoT device is to affect the

purpose of the device (Ojo et al., 2018). The more complex the IoT monitoring device's complex requirements, the more advanced the device's capabilities must be for the purpose-built device (Ojo et al., 2018). Furthermore, the more advanced features the application calls for, the more expense incurred in the development and manufacturing of the device; thereby, minimum device design requirements are related to the driving factors of development and security (Ojo et al., 2018).

IoT security practices that provide additional layers of protection for firmware updates help prevent unauthorized access to devices and personal identity exploitation by manipulating the firmware (Lin & Bergmann, 2016). Aside from device cloning and the loss of intellectual property, device security is also a real threat when the firmware is exposed, allowing a hacker to reverse engineer the firmware and find various attack vectors to permit an intrusion either into the device only or provide a pivot from the device into the network (Khera, 2017). Legacy equipment that is either not patched or not capable of being patched due to the firmware or Operating system no longer being supported by the manufacturer can lead to severe consequences for companies and individuals who rely on these technologies (Khera, 2017). Furthermore, firmware and Operating systems security are contingent upon updateable security patches for continued protection.

IoT security patches for operating systems, as well as firmware updates, are another area of concern. Issues arise in the update process in which the file is corrupt and presents an attack vector to the organization through a malicious payload. In contrast, the Firmware or the Operating system is updated (Broström, Zhu, Robucci, & Younis, 2018).

Akin to the trusted platform module (TPM) in which the changes made to the device would be monitored and reported. Furthermore, due to device limitations, this platform would possibly not work with IoT devices due to the device processing power restrictions, thus a need for alternative methods to monitor and report any changes to the base configuration of an IoT device within the network (Broström et al., 2018).

Various IoT security solutions are being postulated that attempt to solve the problem of IoT device patch updates. One such solution for IoT updates is through the decentralization of IoT patches. Each IoT node as an update mechanism within the larger network through a blockchain network (Leiba et al., 2019). The idea of using IoT nodes to help provide IoT firmware updates using only a small amount of memory is to decentralize the update process and increase the speed at which the updates are provided. Other issues in patching IoT connected devices are related to the device's mobility and the continually changing environment. Solutions for IoT sensor devices within environments that are in constant flux require continual updates through over the air transmission of firmware, as this method presents another unique set of issues in terms of degraded signal and lost updates (Lee, 2018). Security updates for mobile devices and sensors present challenges and an expense on behalf of the device manufactures, impacting the update process and potentially the data's confidentially and integrity due to over the air update failure or availability issues.

IoT Security Policies and Standards within Educational Institutions

Planning for the protection of critical resources can help prevent network breaches from escalating when security events occur. Security policy development and

planning should include an element that covers the IoT aspect of security and clearly defines policies that outline the decision process from purchasing and procurement to the installation of the IoT devices as well as continued updates of the operating system or firmware. Furthermore, developing a multilayered security policy would possibly minimize the threat exposure to the institution.

Defining a firm security policy with clearly stated objectives and outcomes can contribute to an institution's overall security stance and possibly instill trust in a member of the organization. Some of the requirements for a firm security policy include background screenings to ensure a secure environment (Federal Communications Commission, 2017). The establishing basic tenets can provide a clearer view of the climate and situational awareness through each process, such as procurement by establishing that the IoT equipment provider is on an approved vendor list (Federal Communications Commission, 2017). The use of an approved vendor list ensures that the device acquisition meets specified regulatory standards for procurement and implementation.

Other standards included in security policy for IoT devices consists of the deployment and use of encryption protocols and agreed upon types of encryption. The institutional security environment encompasses diverse device types by numerous manufacturers influenced by different driving factors that impact IoT devices' security, such as encryption standards and require a holistic approach to IoT security (Gloria, 2016). An endpoint to endpoint encryption protocols and standards provides a more

secure IoT environment (Hernández-Ramos et al., 2018). Security threats appear to be reduced when encryption is implemented in various forms.

Some security issues needing addressing when selecting an IoT device is to ensure that the firmware is updateable and that the keypairs and passwords are not hardcoded into the firmware (Wang et al., 2018). Other suggestions include ensuring the device can receive firmware updates, providing continued support and security to the device's environment (Zandberg, Schleiser, Acosta, Tschofenig, & Baccelli, 2019). Security policy development could benefit by including a patch management requirement from the vendor and an agreement with the vendor to mitigate patch management issues if the device is unable to be patched or updated (Gloria, 2016).

IoT Applications Within Educational Environments

IoT within the educational environment can include many different devices for various purposes. Such devices as smart boards and interactive highlighters for enhancing students' learning experience can be found within the IoT classroom (Mershad & Wakim, 2018)**.** Another advantage of IoT devices is the enabling students to complete lab experiments without having to be physically present and receive the same learning benefit as those seated in the classroom through IoT enhanced devices (Mershad & Wakim, 2018). The potential benefit to rural learning communities can be obtained in educational remote lab training that otherwise might not be possible (Gary, 2017).

Remote laboratories may provide many different benefits to the educational experience. One such IoT device implemented by Transylvania University in Romania uses the National Instruments board termed the Electronic Laboratory Virtual

Instrumentation Suit board (Elvis) (Ursutiu, Samoila, & Bergmans, 2013). The use of (Elvis) interactive environment allows the student to connect a virtual lab board, thus providing the student with real-world experience (Ursutiu et al., 2013). Technology, such as the Elvis board, brings advances to the educational learning environment. The Elvis board technology allows for this learning platform's adaption into learning management systems such as Moodle (Ursutiu et al., 2013). While implementing the Elvis interactive development board enables students to connect to the university server, this also provides students access to resources from home that they might otherwise not be able to use (Ursutiu et al., 2013). Benefits to the learner in an online or seat application gained from the ELVIS board include completing the lab from home without losing lab resources such as a traditional environment.

Areas that IoT can also provide benefit to is the educational environment through the use of monitoring physical teaching of sports games and sports teaching by providing various sensor data and feedback in training classrooms would allow for the teacher to modify the process to help benefit the learner (Dang & Li, 2014). The implementation of IoT provides new feedback tools to help enhance the athlete's performance and learning experience. Other examples of real-time health monitoring can be found in the phone and wearable technology such as watches with enabled sensors that provide biomedical data allowing for patient supervision (Wan et al., 2018).

Physical security is another area that IoT monitoring can provide benefits. One such area of added value is found in IoT attendance monitoring of students provides improved attendance tracking of students, possibly contributing to better attendance

accountability (Irawan, Adriantantri, & Farid, 2018). Attendance tracking systems that can provide a record of daily attendance notification to parents of absent students can help keep the parents apprised of the students' progress as attendance is usually mapped to student progress (Irawan et al., 2018). Another area of physical security is found in the IoT control mechanism used to provide building access.

Physical security access and monitoring can be considered as a key foundation for most security policies. Critical infrastructure controlled by programmable logic controllers is also susceptible to cyber-attack (Gresham, 2017). Medical device control and manufacturing and power grid control are another area of connected device security that must be protected (Gresham, 2017). Security solutions for medical devices and power grid control impact our daily living and are critical to survival. The need for IoT security solutions is present in the clearly defined IoT security breaches.

IoT security benefits from existing models that provide a benchmark to help determine if the proposed IoT technology will fit the institutions' current security scheme and align with the institutional vision. One such model implements a cross layering that includes privacy and security within the model, thus providing a security approach. The network layer is evaluated to ensure the network remains secure and provides compatibility with current security (Atzori et al., 2017). Security models that address as many threat vectors as possible can provide solutions to current threats.

Relationship of Study to Previous Research

Researchers have implemented the DOI theory in research for many years. The DOI theory provides for the study of varying cultures and how technology impacts

communication and helps understand elements affecting diffusion within an environment (Tang-Mui & Teng, 2017). The theory of DOI provides a means to understand the motivations of varying peoples and cultures.

One such study in which the researchers implemented the DOI theory was conducted in London, England, in November of 2017 and focused on digital technology in the retail industry (Pantano & Vannucci, 2019). The researchers appear to implement the DOI theory as a tool to understand the market demand for retail marketing while implementing the five characteristics of the DOI theory and implementing elements that aligned with a retail research project. The findings in the London area indicated that adopters were willing to sacrifice privacy for convenience in terms of the shopping experience (Pantano & Vannucci, 2019). The researchers gained a better understanding of motivation factors that affected the willingness to adopt new technology based on acceptance (Pantano & Vannucci, 2019). The study mainly focused on the perceived acceptance to help align with the retailer environment (Pantano & Vannucci, 2019). This review provided the researcher and understanding of how technology and innovation adaptors or early adopters are willing to accept a product; however, in this study, the trend appeared to be even if the product did not fully protect the individual's privacy (Pantano & Vannucci, 2019). Implementing the theory of DOI allowed the researcher to observe five separate store locations to help understand motivation factors in adopting technology by individuals.

The next study using the DOI framework evaluated mobile banking adoption by individual stakeholders and was conducted using a blogging technique in which the

researchers established a blog for three months; thus, the samples were not geographically centralized through the use of social media such as Facebook and LinkedIn (Mullan, Bradley, & Loane, 2017). The researchers indicated that 81 percent of the respondents were male from Asia, and 40 percent from North America. The study implements Delphi with blogging to help analyze the data to help research complex data generated by the DOI theory (Mullan et al., 2017). The study's results allowed for an understanding of how to differentiate one institution from another regarding user acceptance through enhanced security as a motivating factor (Mullan et al., 2017). Thus, understanding the motivating factors impacting the adoption of new technology such as mobile banking, the use of the DOI theory provided evidence for mobile banking providers of the value of multichannel banking.

The final study that implemented the DOI theory occurred in Taiwan and evaluated 134 data sets to determine a retail store chain's willingness to adopt RFID technology within an environment (Tsai, Lee, & Wu, 2010). Some of the DOI elements included relative advantage, complexity as a means to determine wiliness to adopt RFID technology. Simultaneously, the study results indicated that relative advantage and complexity impacted the rate of adoption and if the organization was fully prepared for the adoption of technology (Tsai et al., 2010). The study further indicated that slow user adoption due to an absence of standardization as causation, furthermore it appeared maintenance and existing IT system integration related to complexity also impacted the adoption of RFID technology (Tsai et al., 2010).

Transition and Summary

The literature review section attempted to provide insight into IoT issues regarding a lack of security policies and IoT device design practices. The literature review provided some connection between IoT security across all domains and a parallel between educational institutions' security. Furthermore, the literature review highlights standardization issues and IoT security roadblocks to adoption by IT administrators. The risks to students and society are highlighted as well as standardization. Thus, for successful implementation of IoT security, the IT administrator needs to reduce the institution's overall security threat vectors and provide a comprehensive security plan for securing the institution.

The literature review focused on using the Theory of DOI and the touchstone used to evaluate the research throughout this project. The DOI theory has five basic tenants determining if technology will be accepted and the factors that affect this acceptance. The first characteristic is compatibility; thus, a need to ensure security technology is compatible with current security policies and technology and people. The second is relative advantage, and this touchstone compares the question of how will this new IoT device provide advantages in learning? The next characteristic is Trialability; this touchstone will help introduce security policies on a limited basis to determine acceptance. Observability is the next touchstone used to determine if the security methods implemented to protect the IoT devices are effective. The last touchstone is complexity, and it is used to evaluate the IoT device interaction between individuals and technology. Thus, using the five characteristics of the DOI theory provides as a

touchstone to help understand and clarify the research and act as a tool to help determine how to apply the research in the of securing of IoT devices within an institution and contributing to a more secure institutional environment.

Section two of the proposal highlights the role of the researcher and the intended participants. Section two also highlights the research methods and the intended design, and the method used to collect the data. Section three of the proposal highlights the results from section two of the research project and how the research provides possible results for securing IoT devices within an educational institution from the study's findings.

Section 2: The Project

In Section 2, I define the researcher's role and the process used for selecting the participants. Section 2 defines the selection of a qualitative multicase research method. Section two also describes the use of purposive sampling for this research study. Section 2 will cover the protection extended to the research participant's credibility, dependability, confirmability, and transferability. I implemented strong approaches to rigor to ensure that the study has credibility.

Purpose Statement

The purpose of this qualitative exploratory multiple-case study was to explore implementation strategies used by some local campus IT managers in educational institutions in the United States to secure the IoT environment. The study is focused on local campus IT managers within educational institutions across the Southeast portion of the United States that have implemented strategies to secure IoT devices. Positive social change may be realized by improving the quality of education and services provided to the communities due to improving IoT devices' security within educational institutions. Contribution to new knowledge is possible by identifying elements that can secure IoT environments through standardization and mitigation techniques.

Role of the Researcher

Researchers in a qualitative case study are the primary instrument in the data collection process. I was the primary instrument in the collection of data for this research study. My role as the collection instrument was to collect the data, sort the data, and then organize the data into groups resulting in themes. As the primary instrument, it is the goal

to present the data while attempting to minimize personal bias by being a good listener and remaining adaptive (Yin, 2014). My role in this multiple case study was to develop interview questions that align with the overarching question. I also conducted in-depth interviews with the participants while attempting to minimize personal bias.

I have 30 years of experience in electronics and IT with some experience in PLCs and embedded applications specific to IoT devices. I also have 12 years of computer security instruction and currently hold a Certified Ethical Hacker Certification. My current background helps provide a foundation for research; however, IoT technology is such a new field of study that minimizing bias would be possible. I currently have no experience with IoT and security within an educational institution. Ensuring rigor in my research is critical to the validity and acceptance of the results. My case study's approach to the rigor attempted to adhere to is credibility, dependability, confirmability, and transferability (Houghton, Casey, Shaw, & Murphy, 2013). I also implement strong approaches to rigor to ensure that the study has credibility. I currently have no relationship with the participants of this study or to the specific topic of research. I have some exposure to the organization as a faculty member; however, I have no connection to the sister campuses and no influence over potential participants.

The Belmont Report helps to define the three moral and ethical principles that must be adhered to by the researcher, such as (a) respect for persons, (b) beneficence, and (c) justice (Sims, 2010). I conducted my research with the participant being fully aware of the interview process and reviewing the participant's informed consent form before the interview. I have also completed the appropriate training and received a certificate

indicating that the training was completed successfully. I also provided an executive summary of the coded findings to the IT administrators at each institution that participated in the research.

Personal bias is inherent to the researcher due to life experiences; mitigating personal bias helped ensure credibility. To reduce personal bias, a researcher should ensure that the questions asked are standardized to minimize bias in the research and minimize observed bias (Malone, Nicholl, & Tracey, 2014). As the primary instrument of this research, my goal was to ensure the questions were not leading and did not reflect my personal bias or conflicts of interest. An interview protocol helped minimize bias. This allowed me to remain neutral and only act as a facilitator. One method used to accomplish this is using the interview questions as a checklist to ensure that all questions are asked of each participant in the same manner and ensure questions are not leading the participant or fail to investigate an answer in-depth (Qu & Dumay, 2011). Remembering to pause or lean in during the interview is essential; this will allow the participant to respond and show sensitivity (Moser & Korstjens, 2018).

I encouraged the participant to speak freely during a face-to-face interview, and I refrained from steering the participants' thoughts. Data interpretation occurred based on the results and transcribing from an audio-recorded interview in a verbatim method. All audio should be recorded verbatim to reflect the actual interview (Sutton & Austin, 2015). Coding was implemented to identify themes and any possible differences that the research may reveal (Cunningham, Menter, & Young, 2017). The use of coding provided a means to determine patterns of themes and contribute to the research findings.

Participants

The selection of participants for this study included IT administrators from local educational institutions across the United States' Southeast region. The criteria for selecting these participants was determined by researching educational institutions in the Southeastern section of the U.S that implement IoT devices within the institution. I contacted them by e-mail or by telephone, as well as social media. The primary criteria for selection were based on the participants' role in administering the local campus's IT campus that the study is focusing on. Organization selection was based on educational institutions that have IoT implemented on-premise.

The selection of participants is a critical milestone in the research process, thus ensuring that participants have experience in the topic of research is critical to the participant selection (Cypress, 2017). For my study, I used social media and e-mail. I searched the Internet for educational institutions that implement IoT technology and use some of the sister campuses for the university institution that I currently work as an instructor. The study's credibility is crucial to the research's acceptance, and I did utmost to ensure that the truthful depiction of the research participants is represented to the best of my ability and that of the research.

The strategy for establishing a working relationship was based on contacting the vice president of the organizations responsible for the IT department's oversight and requesting a list of the most experienced IT administrators at each institution that they serve. The vice president acted as a mediator between me and the potential participants. The use of a mediator helped connect me and the participants as each came from different

perspectives. Using a mediator helped introduce the researcher to the participants (Shaw, 2018). This selection process was based on a minimum of degree and a minimum of 2 years of experience in an IT administrator's role. I reviewed the websites to determine the administration's information to help determine each institution's contacts.

I obtained contacts through the Chief Information Officers or Chief Operations Officer for participants and both organizations' permission. My study included 10 participants, nine members from one university system that has 20 different campuses throughout the southeastern United States, and the other from a local community college also in the same region.

Research Method and Design

Method

Researchers conducting research studies may implement one of these three different methods of research. These methods include (a) qualitative analysis, (b) quantitative analysis, and (c) mixed methods research. Researchers who need to understand the subject's lived experiences, including perspective and meaning from the participant's perspective, will implement qualitative research to answer these questions (Hammarberg, Kirkman, & de Lacey, 2016). I implemented a qualitative study for this research as I researched the participants' lived experiences to help understand IoT Security Strategies used within an educational institution. Cronin (2014) indicated that a qualitative research study allows the researcher to focus on specific strategies or patterns directly related to a specific topic. The use of qualitative analysis contributed to the study's rigor through pattern matching and allowing for the development of themes based

on the research findings. The implementation of qualitative analysis for this particular research study is appropriate as it allowed the studies to focus on being directed to those living the real-world experience (Palinkas, 2014).

The need to understand lived experience phenomena in a multi-case study was the basis for selecting a qualitative research method. Using a qualitative multicase study allows for an understanding of how different case studies contribute to understanding different audiences (Creswell, Hanson, Clark, & Morales, 2007). Implementing a multicase study helped to contribute to a richer and more rigorous research study. The value of studying the IT administrator within an educational institution provided for a real-life experience interview that provided valuable insight into the process of security IoT within an institution and provided research benefits contributing to a more secure environment.

A quantitative research method uses experiments and surveys to test a hypothesis. The quantitative study's goal was primarily to determine or test a hypothesis with measurable variables (Scrutton & Beames, 2015). Quantitative research is premised on core elementary assumptions that the researcher is removed from the research and the absence of human interaction (Macur, 2013). This study's goal was not to test a hypothesis or work with variables; a quantitative research method did not meet this study's needs. Understanding how the participant's experiences can benefit the research is critical to understanding the phenomenon being researched. Qualitative researchers seek to understand from the participants perspective their own lived experiences (Yin, 2014). As the goal was to understand an IT professional's lived experience and provide deep

insight and understanding of lived phenomena, it was appropriate to implement a qualitative methodology.

Mixed methods research combines qualitative and qualitative research methods into a single study result (Johnson & Onwuegbuzie, 2004; Venkatesh et al., 2016). One of the issues with mixed methods that would exclude it from consideration in this research study is that when there is a divergence between the two research methods, the researcher's responsibility is to follow the discrepancy (Doyle, Brady, & Byrne, 2016). Doyle et al. (2016) also indicated that the discrepancy could be associated with combing research methods when, in actuality, the study did not fit the qualifications for a mixed-methods approach. Implementing a mixed methods research study must be taken with caution and ensure that the research objectives can be met with a mixed methodology. However, assessing the research to ensure that it meets these qualifications is paramount before implementing a research method.

The proposed touchstone for mixed methods research includes (a) triangulation, (b) complementarity, (c) development, (d) initiation, and (e) expansion (Greene, Caracelli, & Graham, 1989). It is important to note that the research study did not need to quantify numbers to answer the overarching research question, and as such, a mixed methods research method was not chosen for this study. The focus of this research study was to focus primarily on the lived experiences of the participant and thus contribute to more understanding of IoT device security within educational institutions. Furthermore, this research study aimed to understand strategies used to secure an IoT environment and was not designed to test a hypothesis based on dependent and independent variables, so a

mixed method was not appropriate. For this reason, I have chosen a qualitative case study.

Research Design

Research studies, such as a multicase studies, implement various techniques to collect data to answer the overarching research question. I have chosen an exploratory multi-case study for this qualitative research study.

A multicase study will allow for the emergence of themes to come to light and then be used as a tool to guide the research and provide a means to ensure depth of research (Killingback et al., 2017). A multicase provides an understanding of the similarities between case studies (Baxter & Jack, 2008). The primary purpose of not implementing a single case study is the absence of depth that a single case study provides (Eisenhardt & Graebner, 2007). Implementing a multicase study provided evidence that is more reliable due to the nature of multicase research directly through the assessment of multiple sources of information from different case studies.

Various types of research methods were considered for this research study, such as an ethnography and phenomenology. The study of ethnographic research is focused on cultures and the interaction between people within the culture. (Williamson, 2006). While focusing on individuals' behaviors, ethnographic research did not provide usable results for this research study as this study was not focusing on cultural interactions. As the researcher, I did not become involved in each organization's culture to live the experience. Understanding people's cultures would require the use of an ethnographic study. I implemented a multicase qualitative research study to provide results based on

interview feedback and a theme using semistructured interviews. I also obtained documents from either the organization's website or internal documents that help reflect the IT administrator's perspective on IoT security and how best the IT administrator secure IoT devices within the network.

Another method is phenomenology, as it focuses on the individual's lived experience and a detailed explanation of the individual's experience (Matua & Van der Wal, 2015). Understanding lived experience is essential to the research process and would contribute to my research study. However, this method's limitations include only obtaining inferences from the individuals' lived experiences (Rossman & Marshall, 2016). Observing only the lived experience excluded this method from being used as the objective was to look at the overall picture of the organization and the IT administrator role in regard to the implementation of IoT security. It is important to note that this research would benefit from elements of phenomenological research approach; however, applying all of the elements would not have been practical due to the main characteristics of phenomenology based on analyzing the participant's qualities and interpretations of the participant (Padilla-Díaz, 2015).

I implemented a multicase research design for this study. A multicase study provided a means for the exploration of a process of events. To confirm data saturation was achieved, I used the interview process to obtain meaningful information and included documents from the institutions' website and internal documentation. Internal documentation and various data sources help explore the phenomenon being researched (Baxter & Jack, 2008). In qualitative studies, data saturation is reached when there are no

new categories or themes (Fusch, Fusch, & Ness, 2018). Ensuring that data triangulation is applied to the interviews and the institution's documents helps to ensure the studies repeatability and provides credibility (Fusch et al., 2018). Data I used internal and external institutional documents and a semistructured interview process and data triangulation to ensure that the research has reached saturation. Data saturation becomes apparent at the end of the research when all the various data types are triangulated, and no more new content comes to light from the triangulation (Fusch et al., 2018). The case study's implementation allowed for capturing the IT administrators' experience within the educational institution and helped develop a recommended strategy to secure the intuitional IoT environment. The use of the case study allows for exploring individuals or organizations (Yin, 2014). The use of a case study provided this research study valuable information helping to answer the overarching research question.

Population and Sampling

This study's target population consisted of local campus IT managers in educational institutions across the Southeast portion of the United States. The local campus IT administrators selected were those exposed to the constantly changing demands of IoT security with the educational institution. System administrators are called upon to perform various duties within the network system, from IT administration to security oversight (Burgess, 2003). Targeting individuals who met specific criteria through a particular sampling method helped increase the study results' richness.

The population for this research study had experienced in the administration of IT services within the educational institution. For this study, I implemented purposive

sampling to help identify IT administrators that meet specific criteria to answer the research question. Purposive sampling allows for selecting a sample based on a population (Suri, 2011). Using purposeful sampling maximized minimal resources and quickly identified individuals who have experience with the research phenomenon. Selecting individuals who have experience with the phenomenon requires flexibility in obtaining participants that meet specific criteria. Purposive sampling, as applied to research, is a standard method for obtaining research participants (Yin, 2014). I implemented purposive sampling for this research study. Purposive sampling, in this case, study, was used for determining a participant's qualifications only. The purposive sampling portion denotes the inclusion of a case that provided added meaning to the research (Yin, 2014). The importance of using purposive sampling allows for as a means for deliberately selecting participants with rich experience of IT administration skills and using purpose sampling provided a means to target those qualified individuals.

Targeting individuals ensures data saturation. It was necessary to secure enough participants to meet predefined research requirements. Research participants can be chosen for a research study based on predefined criteria while also attempting to minimize bias (Moser & Korstjens, 2018). One such study implemented specific criteria for qualifying a research participant and defined the target audience to ensure the study could reach saturation and remain feasible in terms of time and resources (Guest, Bunce, & Johnson, 2006). Ensuring that data saturation has occurred is critical to the success of the study. Choosing a study population based on a set criterion helped ensure data saturation within a targeted population. Data saturation is the goal of all qualitative

inquiry research studies and is the standard that the study is measured by (Guest et al., 2006). Ensuring data saturation has occurred provided to the study credibility and allows the study to be duplicated by other researchers. The participants for this research study were also required to meet specific criteria to ensure their success. One criterion for participant selection (a) must be over 21 years of age; (b) was an IT administrator within an educational institution; (c) participant must know about IT security within a network related to confidentiality, integrity, availability; and (d) participant must be willing to share their experiences.

The importance of ensuring that the interview setting is free of distraction is crucial to a successful study. The interview setting should be quiet and free of distractions (Elwood & Martin, 2000). This study's intended interview setting occurred in a small virtual conference room due to COVID 19 restrictions. In each location, the door was closed to allow for focus and to ensure a clear recording and minimal distractions to the participants.

The appropriate sample size for qualitative research studies varies. The small sample size can vary from five to as many as 50 participants; research indicated that some studies reached saturation with only 10 participants (Guest et al., 2006). A smaller sample size can allow the researcher to focus on the research and the participants and possibly provide a more detailed finding. Code saturation is possible with 9 participants in the study, according to (Hennink, Kaiser, & Marconi, 2017). For this qualitative multicase study, I used 10 participants to ensure that code saturation is possible. One such study indicated that data saturation could be obtained with a population of between six to

12 participants (Guest et al., 2006). I also ensured that once IRB approval was obtained, I communicated with the appropriate individuals at each institution and ensured that they understood the protocols and that all personally identifiable information will be removed, identifying the institution and participant. I also ensured that the participants before the research interview process were provided with a consent confirmation document and a signed document. I reviewed the interview process with the participant and asked if there are any questions or concerns that they might have?

Complete data saturation is the only true method of ensuring that the study size is adequate for the projected population requirement. Saturation of data is the primary standard of qualitative research (Guest et al., 2006). Ensuring data saturation is achieved can be accomplished with the implementation of data triangulation. Researchers indicate that when the emergence of no new codes or themes emerge and the study, it can be reproduced; then, data saturation has occurred (Guest et al., 2006). Study replication is also essential. For the researcher to have enough information to provide for the study being repeated contributes to the studies' credibility; thus, once no new codes emerge, then saturation is achieved. Ensuring that the research study yielded the complete depth of information is considered an indicator that data saturation has occurred (O'Reilly & Parker, 2013). Understanding the criteria for complete depth and breadth of information discovery contributes to complete data saturation and would require no further interviews.

Data saturation was achieved after all of the interviews had been coded. The documents obtained have been analyzed concerning the participant's organization and has

contributed to answering the overarching research question, then I stopped collecting data. The foundation of a qualitative research study is founded on trust; thus, the use of member checking ensured rigor and that the meaning of the research participants meaning was conveyed properly that the participants that the results of the interview process reflected the participant's views (Birt, Scott, Cavers, Campbell, & Walter, 2016). I provided the participants with an adequate amount of time to review the transcripts and provide feedback, thus ensuring that they were involved in interpreting the data. Furthermore, including the study participant as part of the member checking is critical to ensuring accuracy (Birt et al., 2016). Also, addressing discrepancies or interpretations that do not align with the actual participant's feelings or perspectives, they were modified to reflect those of the participant.

Ethical Research

The protection of research participants is critical to data collection, and as such, the identity of the stakeholder's human rights must be protected. Various methods of ensuring participant protection should be implemented, such as informed consent, which includes continued consent before starting the interview (Byrne, 2001). Informed consent was obtained before the interview was conducted and provided the participant with the opportunity to decline being interviewed at any point during the process. The informed consent form was in a PDF format that the participant would sign virtually when they agreed to participate in the study. The informed consent form can be found in the appendix Appendix C.

Ensuring the participants who volunteer are volunteering for the right reason, such as wanting to see a more secure IoT environment — ensuring that the motivation of the participant is not coerced and anything that is received should be secondary and not the reason for participation (Erlen, Sauder, & Mellors, 1999). Providing a token of appreciation, such as a gift card for coffee, would be acceptable, and I did not advise the participant of this before starting the interview. Thus, making sure that no incentive is offered before the research collaboration was started ensured that if the participant does not feel comfortable in any way, they could not be part of the research without any negative consequences.

The Walden University IRB process requires preapproval before a researcher can start the process of research. Thus, ensuring that all requirements are meet and that the participants identify, and human rights were protected. To ensure that the research study is ethically based, it is essential to implement morally sound practices. One such method for ensuring ethical standards is through informed consent and the ability to withdraw from the study and complete confidentiality (Ngozwana, 2018). Reminding the participant that withdrawing from the study at any time is their right if they are so inclined as they were not obligated to participate. Walden University requires that researchers obtain the IRB approval confirmation number before the research starts and ensures that the researcher has completed proper training in protecting fundamental human rights, ensuring the participants' dignity. To be compliant with the IRB process, I completed the National Institutes of Health Training (NIH) and received a completion certificate. Certificate Number 2488136 completed in September of 2017.

Trust is essential when conducting research. The need to protect the research participants is required; thus, I implemented a coding system for the research participants and the participants' institutions. Ensuring that the names are anonymized with pseudonyms will ensure that the participants' privacy is protected (Byrne, 2001). Ensuring participant anonymization helped to obtain research data that will answer the overarching research question. I am the only individual who has access to the actual names and pseudo names of the participants assigning pseudo names masked out the actual participant. I guarantee the participants' confidentiality through the entire research process. After the interview process occurred, I provided the participants with a paper copy of the interview to allow for the participant review. The information stored on my computer or MP3 recorders was saved on a flash drive that was encrypted with a secure password. After all, data was saved to a flash drive or printed, and then it was deleted from the computer or recording devices. Thus, after the five years of data holding, any data, including the flash media and documents, will be destroyed and shredded to protect the participants and remain compliant with the Walden University IRB process.

Data Collection

Instruments

I was the primary data collection instrument for this qualitative multi-case study. The researcher becomes the primary instrument in data collection and making sense of the collected data contributing to an understanding of the research phenomenon under evaluation (Barrett, 2007). Identifying themes and patterns to help understand the phenomenon being researched is critical to the research investigation outcome.

Researchers gather evidence through predefined research questions and act as instruments in one-on-one interviews and establish trust relationships with the participants; thus, researchers are considered the research tool (Yilmaz, 2013).

Understanding a phenomenon through data collection allows the researcher to use observations and artifacts such as documents to understand the phenomenon being researched (Barrett, 2007). I implemented a semistructured interview process that allowed for open-ended questions to help understand the participant's perspective of the research phenomenon. Open-ended questions helped triangulate the data by allowing participants to express themselves during the interview process (Tasker & Cisneroz, 2019). Semistructured open-ended questions allowed for the conversation's guiding during the interview process (Kumboyono, Hamid, Sahar, & Bardosono, 2019). Furthermore, I used a semi-structured interview approach with predefined open-ended questions that allowed the researcher to be more flexible, thus enabling the participant to answer the questions representative of their own experience.

The data collection process requires identifying common themes through the interview process to contribute to the understanding of a research phenomenon. Some methods that allow for data collection and establishment of themes are document review before the interview process is undertaken to help shed light on the organizational information contributing to the participant's overall understanding (Sutton, 2011). Researching organizations in advance of the interview process allows for the focusing of a study and can provide tremendous insight and contribute to creating themes and patterns for analysis.

The research required that I implement a semi-structured interview process to ask open-ended questions and probate the participants' experiences. The data collection method involved using documents obtained from the company's website or documents provided to me by the organization. All the interviews were conducted onsite in a conference room with the blinds shut, and the door closed to minimize distraction. Implementing a location for the interview process should be convenient for the participant and quiet (Elwood & Martin, 2000). I ensured that the participant was comfortable and that there are no distractions to the interview process and that the environment was neutral. The interview process consisted of open-ended interview questions, and the interview process spanned 30-45 minutes total time.

The study's interview data types are categorized into two groups (a) primary data obtained from the interview process. (b) However, secondary data obtained from documents related to the organization is not necessarily related to the current study (Prada-Ramallal, Fatima, Herdeiro, Takkouche, & Figueiras, 2018). The use of secondary data allows the researcher to compare different sources to verify the research findings. Combining various types of research method sources in the study of phenomena to verify the research's validity is defined as a triangulation of data Denzin, 1978). However, it is essential to note that data interpretation is still the researchers' perception of the information (Fusch et al., 2018). The use of method triangulation in this study helped to understand the overarching research question through primary and secondary data collection methods. Understanding multiple perspectives provide the researcher with a better foundation in which to help answer the research question. Data triangulation

includes collecting data from different sources to gain a multifaceted perspective of the data and contribute to data validation (Carter, Bryant-Lukosius, DiCenso, Blythe, & Neville, 2014). I implemented data triangulation in this research study to discover new and emergent themes and minimize bias within the research inherent to the researcher and the process.

Recognizing bias and minimizing the effects in research is paramount to the research; thus, I implemented member checking and data triangulation to ensure data alignment. Data triangulation allows for member checking of the results; however, for the results to be accurate, you must have all members who participated in the research to participate in the member checking process (Carter et al., 2014). A follow-up interview was scheduled with each participant and allowed them to review the transcripts' interpretation from each interview. Ensuring full member participant participation ensured help to ensure the accuracy of the interview and transcription process. Member checking allows the participant to evaluate and verify the researchers' interpretation (Harvey, 2015). Once member checking was completed, changes were made to the document if applicable by the research participant. Then an amended copy was sent back for a follow-up interview if necessary.

This study's interview protocol includes pre-interview questions, and the interview participant completes and signs the participant form before starting. A list of interview questions and pre-interview activities (see Appendix B) provides the interview process as a guide for a semi-structured interview by using preformed open-ended questions to guide the process (Harvey-Jordan & Long, 2001). Ensuring that the

interview protocol is in place will ensure that the interview process yields good results. Thus, a reliable interview protocol is linked to research data based on quality data (Yeong, Ismail, Ismail, & Hamzah, 2018). A reliable interview protocol is crucial to obtaining rich qualitative interview data to understand the research phenomena.

The interview process required various tools such as recorders and software for identifying themes and codes. I used two separate devices in this process to record the interview process. (a) Sony digital recorder (b) iPhone with a voice recording application. The recording data was processed through a speech to text program to make available in a printable format for verification. The need to ensure that the data can be verified is essential to ensuring accuracy. Sending copies of the exact transcript back to the research participant will ensure accuracy (Harvey-Jordan & Long, 2001). After the speech processing to text, it was necessary to ensure that the text is not altered or changed, thereby changing the participant's interpretation. I implemented the software NVivo to help to identify themes as well as emerging patterns. Tools such as NVivo help augment the research process and help identify themes as a data management tool (Maher, Hadfield, Hutchings, & de Eyto, 2018). The use of tools such as NVivo helped to organize the results and help establish data patterns. Establishing patterns helps identify emerging themes by transforming codes into categories, thus identifying commonalities or patterns, thus requiring the researcher to become immersed in the data during analysis (O'Neil K, 2019). Identifying patterns in the research includes both primary and secondary information is included in the process of pattern matching. Secondary sources of data that are identified as trustworthy can be used to direct the research and help to

understand the results that should be considered in the process (Zickar, 2015). Identifying patterns in research requires an objective, non-biased view of the research data and ensuring that all primary and secondary data is accounted for entirely.

Data Collection Technique

The use of an interview process in a qualitative research study provided a means to obtain an individual's perspective of the phenomenon being researched. Capturing the research participant's experience will provide insights into the daily patterns and routines and enable the researcher to pick up non-verbal communication (Denham & Onwuegbuzie, 2013). In conducting face to face interviews, I asked follow-up questions based on non-verbal communication, thereby obtaining a more rich interview experience with the participant. I created an environment for the participant that makes them feel comfortable during the interview process, allowing them to be more forthcoming with research information. External environmental stimuli can impact an interview; thus, minimizing or eliminating such distractions will contribute to a better quality interview (Drew et al., 2004). I ensured that cell phones were turned off, and the blinds were closed to remove distractions. I used face-to-face Virtual semi-structured interview to complete the data collection process. A semi-structured interview process allows the researcher to investigate a different path based on response and remain somewhat structured (Gill, Stewart, Treasure, & Chadwick, 2008). I also paid special attention to non-verbal cues and ensured that I established trust before the interview process. In the interview process, trusting the interviewer is critical to the interview results and can impact the participant (Cohen & Arieli, 2011). The importance of building trust before the interview process

and during the interview process will contribute to research data that is rich in content. The importance of ensuring the environment is comfortable will stimulate freely sharing of information. I ensured that the participant is comfortable during the interview process and ensured an absence of interruption by implementing long pauses. Ensuring the participant's comfort and the absence of interruption not to inhibit the participant's thought process is key to rich data collection (Rivard, Fisher, Robertson, & Hirn Mueller, 2014). I ensured that the interview protocol (Appendix B) was followed, thus helping the participant be comfortable and allowing the interview to stay within the allotted time frame while remaining flexible to allow for a richer interview experience.

Various data collection techniques exist that can provide the researcher with meaningful information dependent upon the research requirements. One such method that allows rigor to qualitative research is data triangulation (Kitto, Chesters, & Grbich, 2008). Member checking and data triangulation will contribute to ensuring the research is accurate and that themes emerge. Other issues that can impact the research are related to the researcher and the inherent bias brought into a research project. A qualitative research study requires method triangulation to minimize the researcher's internal bias (Tobin & Begley, 2004). It is important to note that researchers will bring internal bias to the research; however (Tobin & Begley, 2004) also indicate that method triangulation can mitigate this effect if appropriately implemented by the qualitative researcher.

One of the disadvantages of using the interview process for data collection is that it could lend to bias on behalf of the researcher. Researchers bring bias to the study through life experience and injecting bias unintentionally through the way questions are

asked (Bero, 2017). By contrast with the blind survey method of data collection, the interview process will have pros and cons; the key to mitigating these differences between the data collection methods is through the implementation of checks and balances to ensure a fair and balanced research project.

I searched the targeted institutions' websites and open-source intelligence and obtained institutional documents from the organizations that will contribute to the research. Common data collection methods include using documents and observations to allow for data analysis verification (Sargeant, 2012). I used these documents obtained from the institution to help identify patterns and themes in the research.

Once the semi-structured interview is started, I completed the process until all of the interview questions were answered while allowing for a follow up of each question if necessary, dependent upon the interview participant's response. The use of semi-structured interview questions allows for a rich participant response while adhering to an interview protocol (Bolderston, 2012). I was aware of non-verbal cues during the interview to determine if question follow up is necessary. The use of non-verbal facial indicators can indicate to the researcher and provide cues as to how to direct the interview process (Knapik, 2006). During the interview process, I ensured that I remained flexible and allowed the participant to express themselves without interruption.

I built trust before reviewing the interview process. Once the participant appears calm and all distractions are removed, I reviewed the interview process with the participant (Appendix B). I ensured that they completed the consent form and signed the pdf document. I reviewed the recording process with the participant, explained the data

retention of recorded material, identified the masking process, and ensured confidentially of the interview and all related documents. I provided the participant the opportunity to opt-out of the research. Once the introductory interview guide was completed, then I informed the participant that I started the recording.

The interviewer should ensure that they do not lead the participant while looking for specific responses (Harvey, 2011). Leading the participant would possibly skew the interview process; this sometimes occurs when individuals feel uncomfortable. Thus, if the participant responded and provided a non-verbal cue that they were uncomfortable with, I followed up with different wording questions at the end of the interview. I also used non-verbal indicators to determine if the question needs a more in-depth investigation. I also took notes that indicate response to specific questions that needed to follow up and indicate non-verbal cues that might have indicated further investigation.

Once the interview was completed, I asked the participant if there were any further questions and asked if there are any institutional documents that might benefit the research. I also explained to the research participant that I would be sending them a copy of the transcribed interview for review and then request a follow-up interview if necessary, to view any discrepancies that might arise from transcript interpretations. I also provided a copy of my notes to the participant upon request. I also reminded the participant of the data retention policy. Once the participant reviewed the transcript, I requested verification of the participant's approval, either verbal or in an email.

Data Organization Techniques

Data collection techniques are established before the start of my research to ensure the reliability of the data. An audit trail in research is achieved when the researcher provides a complete and accurate document trail, thus documenting the procedures used in obtaining the data. The process in which the interview is conducted will demonstrate the integrity of the research (Daniel, 2019). The importance of organizing the research before the process starts with proper documenting procedures will ensure my research integrity and ensure the process is organized and efficient. I used Microsoft Word, Excel, and Nvivo to organize the data collection findings for taking notes and transcription for proper organization. The use of various research tools augments the researcher's ability to organize data into meaningful results as long as the tools align with the research project (Jin Xiu Guo, 2019). The use of various research tools enhances the researcher's ability to organize data into meaningful results as long as the tools align with the research project (Weitzman, 1999). Selecting the proper tools for this research project required research in selecting software that provided the best result while being cost-effective. The software was used to take notes and track documents and the research participant's masking to protect their identity. It is the researcher's responsibility to protect the identity of the research participant (Larossa, Bennet, & Gelles, 1981). Thus, when organizing the research, it is the researcher's responsibility to protect the research participant, and one method often implemented to accomplish this is the use of identity masking. Thus, removing information when possible to identify the research participant is required for the participant (Greaney et al., 2012). The protection

of the participant's privacy is an integral element contributing to the research participant's respect. To ensure privacy, I maped the 10 participants to a set of codes. The masking codes will be as follows, research participant 1 to research participant 10, then with each participants name being assigned a code. The results of the findings were stored on a portable flash drive that is password-protected to ensure privacy. I also reminded the participant of the data retention policy in which the material will remain locked in a secure location for a period of five years then destroyed

I also maintained a journal through the research process to ensure all of the research processes are documented, and any comments or concerns can be documented and readdressed through the process. Using a journal will contribute to a more reflective research process and allow for as a tool to be self-reflective to help minimize personal bias (Ortlipp, 2008). A journal will also allow for follow-up notes when interviewing the participant and help identify other investigation areas during the interview.

Data Analysis Technique

A qualitative case study begins with gathering data from various credible sources to help answer the overarching research question. Within this study, I implemented the framework suggested by Yin (2014), in which he suggests the use of a three-phase method in which the data is obtained then (a) compiling the data, (b) disassembling the data, (c) data reassembly. Using a systematic data analysis methodology will help ensure that the research that I present follows a standardized; thus, it is logically occurring and repeatable. Data analysis in the coding process allows for revealing keywords within the interview process and helps identify keywords used frequently (Theron, 2015).

Identifying patterns and themes is crucial in helping to understand phenomena. I used documents obtained from the institution and transcribed interviews to help answer the overarching research question.

I implemented NVivo software to analyze the audio transcripts obtained from the interview process and artifacts obtained in the research. The use of NVivo allows for the coding of research material to identify a theme or patterns in the research material (Maher et al., 2018). I selected NVivio for the various tools that the software brought to the research while recognizing that it is an aid to research only and that the researcher is responsible for the research (Zamawe, 2015). Ensuring rigor in the analysis phase is critical to the study results, ensuring repeatability is vital to the study; therefore, multiple analysis methods are essential. A computer program helps to analyze the artifacts and the interviews; however, keeping a journal and using colored pens and traditional methods helps to ensure rigor in the research data analysis phase (Maher et al., 2018). Using journals and proper notetaking of facial expressions and using these as artifacts helped ensure a balanced analysis of the results. The key drawback of relying only on the transcription is that the interview's content could be lost in transcription; thus, annotation during the interview briefly allows the researcher to listen to what the participant is saying (Wainwright & Russell, 2010). Using multiple methods to analyze the data obtained from the interview process and data artifacts will ensure rigor in the research data analysis phase.

Research studies use various methods to identify the rich data that enables yielding results to identify the research phenomena. I used various coding methods to

help identify patterns in my research study. The research coding was initially developed from the list of research questions and the condensing of the research findings allowing for theme development and category refinement (Miles, Huberman, & Saldana, 1994). Identifying underlying themes from previous experience acted as a guide to initiate my research study. Qualitative coding requires the researcher to have a background in the study to identify themes in the obtained research material (Turner, Kim, & Andersen, 2013). I bring a previous background to the research to better understand the research findings and help develop themes from the research. The use of coding in a study provides a means for the researcher to bring their own experiences to the research to help identify themes (Alase, 2017). I ensured the best of my ability to use all my previous experience to organize the data to identify themes and patterns in the research obtained from interviews and company documents. I continued to research current trends to ensure that no new information applying to my research study should be included in the theme development or studies finding.

1. They have identified background data from organizational artifacts provided to the study, and Internet searches for new material for similar institutions to identify initial themes or update current themes.
2. Reviewed the transcripts and the recordings and used my research journal to help identify subtle themes and codes.
3. Identified themes and codes collected from the interview data.
4. Determined how these identified themes and codes align with the artifacts obtained from company documents.

5. Used the identified themes and codes to search for patterns in the transcripts.
6. Amended themes as new patterns become apparent as a continual process until no new themes emerge.
7. I continued this process to establish saturation until no new themes or codes are identified within the research transcripts.

Reliability and Validity

Reliability in research is critical to the study's acceptance for many reasons. There is a need in qualitative research to ensure the findings are repeatable and duplicated by another researcher investigating the same material with the same research methods (Aguinis & Solarino, 2019). Validity in research refers to various sources of evidence being evaluated to help establish a foundation. Validity refers to the research question that is being investigated and the extent to which the research question is answered by the study (Sullivan, 2011). In this study, I obtained research material from various sources to help establish validity while answering the overarching research question. I ensured that the research was trustworthy and repeatable through the interview process. To accomplish trustworthiness, a researcher should acknowledge any research bias that could impact the study's outcomes (Noble & Smith 2015). I continually ensured different perspectives in the research were represented to remain transparent in the research process. To provide credibility, a researcher should detail their personal experiences pertaining to the specific research (Cope, 2014). I followed an outline for ensuring reliability in the research as suggested that the primary researcher be consistent, truthful,

and pose neutrality and ensure applicability to research. I ensured that I was transparent in the research and truthful while remaining objective and ensuring that I followed the interview questions found in Appendix B following an interview protocol and the questions with all participants in the same manner. The importance of enabling a reader to draw the same conclusions as the study is accomplished by following the research questions and interview process with all participant interviews, thereby yielding consistent results (Yin, 2014). I ensured that all interviews follow the same process utilizing the interview protocols and interview questions as well as making notes of any non-verbal cues from the participant.

Dependability

Dependability during the study was accomplished by ensuring the study's repeatability by using the interview protocol and interview questions. Once the interview is completed, I then sent a copy of the transcript back to the participant for member checking to ensure the accuracy of interpretation. Ensuring the results obtained from interviews and artifacts are following a protocol will contribute to the study's consistency. Dependability is achieved when the study's results can be agreed upon by other individuals given the same research (Cope, 2014). I used data triangulation and member checking to ensure the dependability of the data collected and member checking by sending back the transcripts for review and approval. Data triangulation can be used as a tool to ensure the rigor of a study's research findings (Humble, 2009). Triangulation can be identified as the use of various methods for collecting data (Humble, 2009). I used various sources for data collection, such as company documents and company artifacts.

Furthermore, I implemented the use of instruments that will be standard across all interviews. The instrument included predefined interview questions with each participant. Second, I implemented member checking during the interview process to stop and check for accuracy. Member checking was also implemented after the interview process to allow the participants to review their interview transcripts by sending them back to the participant for accuracy checking. It is essential to ensure dependability. There must be measures in place to check the results of the qualitative research study and, as such, strengthen the study (Rodrigues, Alves, Silveira, & Laranjeira, 2012). I implemented various auditing and member checking methods and a proper protocol to help ensure dependability and rigor. Another method that I implement in the research study is to create an audit trail, thus allowing others to come behind my research study and repeat similar results. An auditing trail allows for transparency in the research process, thus allowing for a more rigorous study (Houghton et al., 2013). I implement an audit trail throughout the entirety of the research study documenting collection through comprehensive notes. The use of NVivo increased the rigor of the research study by also contributing to the audit trail (Houghton et al., 2013). I used NVivo as a supplemental tool to continue the audit trail as well as a journal. I reviewed the emerging themes until there was no longer new or emerging data from the research. Ensuring data saturation helped to ensure the validity of a research study (Cope, 2014). I ensured that the research is no longer yielding new themes or new research to ensure data saturation. I ensured that the study's results are confirmable, transferable, and credible (Thomas & Magilvy, 2011).

Credibility

Credibility was accomplished using member checking as well as reviewing all of the transcripts identifying patterns. I continuously was self-reflective of my perception of the research with a critical perspective of oneself. The researcher's perspective and the effort put into the research concerning the research contribute to credibility in a qualitative research study (Golafshani, 2003). Ensuring that I minimized bias while continuing to keep a critical perspective of my research interpretations will enhance the research finding's validity and richness.

Transferability

Another reliability and validity element is ensuring that other researchers that are not part of the study can recreate the research results and ensure the research results' transferability. A benchmark for determining if the research results are transferable is if other researchers can identify with the research study results based on their own similar life experiences (Cope, 2014). Thus, transferability is critical to the validity of the results of the research. Some ways suggested by Noble & Smith (2015) are to ensure that the studies' results are transferable and accurate. Furthermore, the authors also indicate that including direct quotes from the interview participants, document review of the results with the participants will also contribute to validity. The authors mention the constant review of other research case material to contrast with your current research (Noble & Smith 2015). Transferability is determined by how much of the research study can be applied either based on theory or practice to research in the future (Korstjens & Moser,

2018). I provided detail-rich accounts of the participants' interpretation of the phenomena, thus providing the research findings' transferability.

Confirmability

Trustworthiness is critical in research, and ensuring that the research is transferable is a vital tenant of a qualitative research study. To ensure the research is transferable as the primary instrument, the researcher is responsible for obtaining rich descriptions of the research data, thus allowing the potential reader to draw their conclusions in the research (Korstjens & Moser, 2018). I provided detailed thick descriptions of the research participants' descriptions of the phenomena being researched. Transferability requires that other researchers can use the findings to continue further research on the phenomena being studied. Confirmability and transferability are viewed in parallel when assessing a research study as the objective is to ensure the research is valid. Confirmability can be identified through an audit trail and helps establish the research's dependability (Korstjens & Moser, 2018). I used an audit trail to ensure the confirmability of the research. This research's findings are based on a multi-case study in which more than one educational institution is included in the research. Furthermore, to ensure that the research is transferable, it is necessary to help develop new ideas or concepts that relate to the research phenomenon (Moon, Brewer, Januchowski-Hartley, Adams, & Blackman, 2016). I ensured that all of the research was thoroughly analyzed and that the research is confirmable as well as transferable.

Transition and Summary

Section 2 covered data collection and techniques used to obtain the data. This section also covered data organization as well as data analysis methods. Section 2 identified the researcher as the primary instrument in the data collection process. This section also reviewed the need for data triangulation to create themes and patterns to ensure data saturation. And the last section of Section 2 review validity and reliability in a qualitative research study focuses on maintaining honesty, transparency, and repeatability. Section 3 will present the research findings and how the findings will benefit other organizations and society as a whole through social change.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative multiple-case study was to explore implementation strategies used by some local campus IT managers in educational institutions in the United States to secure the IoT environment. The targeted population consisted of local campus IT managers within educational institutions across the Southeast portion of the United States that have implemented strategies to secure IoT devices. The process included the use of semistructured interviews as well as interactive member checking to minimize bias. I conducted interviews with four separate educational institutions. The IT managers within these educational institutions all had experience successfully securing IoT devices within their perspective institutions. The IT managers who participated in the research had experience ranging from 2 to 31 years within the IT industry. Section 3will include research study findings that apply to secure IoT within an educational institution.

These educational institutions' research yielded rich data that provided four major themes to emerge in the research. To establish themes required a continued iteration of the data obtained from 10 semistructured interviews. Establishing themes and minimizing bias required data triangulation to ensure the company documents obtained from publicly available resources aligned with my research finding. The DOI theory of conceptual framework was implemented to understand methods used to secure the IoT environment and other security-related factors that could impact the adoption of IoT within an educational institution.

Presentation of the Findings

This study's main research question was, what security strategies do local IT managers in the Southeastern portion of the United States implement to secure IoT devices within educational institutions? Four major themes emerged from the research, indicating methods used to secure IoT devices within an educational institution. Themes were established through data analysis of semistructured participant interviews as well as publicly available institutional documents.

Four major themes were identified through this study: (a) network access restriction, (b) network isolation, (c) adoption by leadership, and (d) strong shared partnerships. Themes emerged from the research after careful triangulation of data. Triangulation included company documents and personal notes that I made during the interviews. The need to follow up with three participants became apparent after the participants' initial transcript approval. While compiling data, the need to clarify a few questions about technology types implemented by some state institutions to clarify the research. Data saturation within a qualitative research study is achieved when no new themes emerge (Lowe, Norris, Farris, & Babbage, 2018).

It became apparent that I achieved data saturation after the sixth interview. To ensure data saturation, I continued to interview four more research participants to ensure that no new themes emerged from the four participants. Once no new themes were established, I determined this aspect of the research appeared complete.

Theme 1: Restricting IoT Access to the Network

IoT security is quickly presenting challenges for small educational organizations and large institutions due to technology's pervasiveness. The first major to emerge from the research was the importance of a need to restrict IoT devices due to the devices' inability to protect themselves from attack. Participating in the research were four separate southeastern colleges and universities. Of the four separate institutions that participated in the research, all four institutions indicated that due to an absence of standardization among security standards, there is a need to segment the IoT devices to a separate virtual local area network (VLAN) isolation.

All participants within the four organizations that participated indicated unanimously that IoT security presents a unique set of challenges for all research organizations. All 10 of the participants indicated that IoT security requires serious scrutiny when managing an organization's security. In terms of implementing a separate VLAN, nine of the 10 participants indicated that a VLAN is critical to securing the local network and protecting confidentiality, integrity, and availability triad (CIA) of the network in various forms. Many of the research participants further indicated that a media access address control filter is key to securing the local network and ensuring only authorized devices can access the resources. One primary purpose of implementing (MAC) filtering is for all IoT-related devices to use a media access address to access network resources.

Three of the participants also indicated that due to the methods IoT devices connect to the network, MAC filtering allows for a minimum measure of permission

assigned to the devices. The research documents provided insight into the use of MAC filtering. Two of the research documents indicated that MAC filtering is the first defense layer in securing the network. It is important to note that participants 1 and 10 indicated advanced data encryption forms within the IoT devices. MAC filtering was one of many methods used within the institutions for securement. Table 2 demonstrates the frequency of responses for each theme.

Table 2

Minor and Major Themes Network Access Restriction

	Participant		Document	
Major/Minor Theme	Count	References	Count	References
Restricting IoT Access to the Network	10	31	4	22
VLAN Segmentation	9	20	2	16
MAC address Filtering	3	6	1	5
Hardline Connection	4	4	1	1
Access Control Lists	1	3	2	3

**Note: (MAC) Media Access Control*
**Note: (VLAN) Virtual Local Area Network*

All of the 10 participants indicated that securing the institution was the main focus of their primary job duties as an IT professional within their perspective institution. Six of the thirteen company documents appeared to support the objectives of the local IT professionals. The six combined documents had a robust security footprint within their local education sector regarding no recent breaches. Participant 3 indicated a recent cyber

breach; however, also indicated that the event was not related to any of the IoT connected devices. All of the four organizations' participants indicated in various forms that remaining vigilant in terms of IoT connected devices is critical. All of the 10 participants indicated in various forms that being aware of security is critical and that IoT is often overlooked within the network. It is important to note here that these three same participants also indicated in various forms that resources for securing the network could be improved to help support IoT devices.

Security measures implemented by the four educational institutions that participated in this research all followed NIST standards as published by the federal government. The implementation of VLANs will help ensure multi-layer security (Chandramouli, 2016). Chandramouli (2016) further indicated that VLANs could be extended beyond the virtual environment to the physical network providing the ability to isolate traffic emanating from VLANs. It becomes apparent that the adoption of IoT technology within education institutions is focused on the usability of the technology compatibility and relative advantage to the institution in securing the network.

This study's research is founded on the DOI theory, in which five primary attributes guide this research study. The relative advantage impacts the adoption of IoT related technology in securing the IoT related network components; relative advantage can also be seen in saving the institution needless, costly expenses (Vafaei-Zadeh et al., 2017). All of the institutions that participated in this research implemented both VLAN Segmentation and MAC address filtering. In terms of filtering, nine out of 10 participants actively monitored the MAC addresses connected to the network.

Participants 2 and 10 indicated that they had state-mandated systems to control the security of IoT connected devices. The participants indicated that due to other users' perceptions within their immediate network appeared to guide the adoption of the technology that the state government would adopt for use by the college systems statewide. Participants indicated that they were under specific state program regulations mandating specific technology requirements as a state college. The same participants did indicate that technology adoption occurs through peer groups in which technology is shared between various universities and colleges within the state. A shared technology adoption between institutions aligns with the theory of DOI various key elements such as observability and trialability. In many instances, according to Participants 1, 2, 6, and 10, if the technology is too complex or does not offer an advantage would not be adopted.

This occurs after the technology is observed on a trial basis. The technology at the end of the trial would be either adopted or possibly move in a different direction. Participant a provided an illustration of cellular wireless technology for underserved wireless students in which the institution was looking to implementing with other schools and colleges within their network to determine the viability to provide this as a service to the students. Many IT professionals must address issues associated with relative advantage and ease of use when implementing devices within the institution.

The four themes that have emerged in this research study were aided by using the DOI theory. A specific case study that aligns with the participant's responses regarding adapting technology through trialability and observability can be related to a particular case study (Daud et al., 2018). Daud (2018) indicated that critical elements of security

policy are based on observed influence within organizations. This first theme to be established is securing the network with MAC filtering as well as VLAN segmentation. These themes, as indicated by the participants, nine out ten are taken from collaboration with other institutions and the National Institute of Standards and Technology (NIST) recommendations, as indicated in the interview results. It became apparent in the research that the institutions were working closely with other institutions in terms of security adoption and technology implementation.

All four participant institutions indicated that compatibility in security technology was a key concern in various forms. This idea aligns with my research in which (Atzori et al., 2017) indicated that cross layering of security with various facets would help to secure the IoT. Rogers (2003) further indicated that innovation is perceived as being aligned with groups' current values or experiences. This research study identifies adopters as individuals who reach out to peers to determine what methods work best in securing the environment. An example of this is Participants 2 and 10 are working together to secure their network through data backups. Participants 2 and 10 utilize dark fiber as both institutions see the benefit of mutual data backup and recovery by sharing resources on each other’s institutional servers; it allows each institution to have a data redundancy in case of data loss. These same institutions work together by seeing what works in each other’s perspective intuitions and then, after trial implementing the technology within their own institution. The literature further pointed to leadership as being a key driving force in early adoption by leaders who are usually knowable in the subject matter

(Rogers, 2003). The coordination between partner institutions stems from management being knowledgeable in technology and ensuring that critical systems remain online.

Subthemes emerged in the data analysis while combining data from all of the resources. Participants 3, 7, 8, and 9 indicated that restricting access to IoT devices proved to provide the best method of securing the network from attack. This same perspective is also reflected in the research documents obtained from publicly available sources. Some of the documents provided insight into the security being used, such as firewalls or network monitoring appliances. However, it is essential to note that restricting access through MAC filtering, or VLAN segmentation are only a few of the methods mentioned; others are whitelisting and sticky ports on switches and separate wireless networks that only allow specific IoT devices to connect.

VLANs allow for easily monitor devices that are permitted to be connected to the network. Another subtheme is the use of hard-wired connections for IoT devices, which occurs when a few institutions have automated door controls; these networks were put on specific wired connections. One intuition also had a wireless access card read for their door control as well. Institution partisan j managed an alert system warning of emanant danger on the campus that tracked cell phones using a Bluetooth application and wireless service. Securing these various environments proves a challenge for all organizations that participated in the interview process. Concerning the CIA triad, the absence of availability or limited availability impacts the overall network security and is the primary outcome for Participants 3, 7, 8, 9, as all these participants appeared to practice air-

gapped networking for IoT devices. When securing these devices through standard methods would otherwise not prove possible.

Another perspective for IoT security in terms of observability is found in participant 10. They research the devices in advance and have more of an open-door policy to connect IoT devices to the main network. Participant 10 explained that if the institution were transparent with the users, they would be transparent with the organization. The organizations' approach to security was more relaxed than the other nine participants; however, in the background, the actual policies were more specific in terms of connecting IoT based devices to the network. Conversely, Participant 1 indicated that even to connect a smartphone to the institution's network, faculty, and staff would have to come to the IT department and have the device added.

The case study organizations that participated in the research appear to have a common theme of IoT security-related concerns. The common theme of network security for the case organizations also appears to be a key element as suggested in another case study in which the CIA triad is used as a yardstick to evaluate the security of the organization as well as a framework for evaluating security from a different perspective (de Oliveira Albuquerque et al., 2014). The same authors in this case study evaluated network security in the most basic elements related to the network, that is, layered trust that includes all security elements. The application of restricting IoT access to the network aligns well with the layer 2-3 approach of filtering the OSI model to secure the network. The approach of a high-level comparison by de Oliveira Albuquerque et al.

(2014) represented the network broken down into the most simplistic elements to understand the root cause of security threat vectors.

The conceptual framework for this study is the DOI that guides this study and helps discover new research ideas. Once tenants of the research implemented observability through the majority of the study. The concept of restricting IoT access to the network originated with peer organizations in which the idea was shared among groups through word of mouth or through governmental documents. The suggestion of how to secure IoT within the network. Rogers (2003) indicated that relative advantage or perceived advantage would be accepted or perceived as the rate of adoption. The innovation is accepted, and that it would also be viewed as better than what is currently in place. The current state of IoT security for most participant organizations is relatively new to the organizations. Observing other institutions or working closely with peer organizations helps secure the case study organizations by restricting IoT access to the network.

Theme 2: Network Isolation to Secure IoT Devices From the Network

The second theme to emerge was specific to some of the institutions in which they air-gapped individual network segments. Table 3 refers to the frequency indicating the need for an air-gapped network for isolation security. Table 3 also notes the frequency of the available company documents; Simultaneously, it is essential to mention that the security documents for the device providers and NIST mention gapping air networks; many of the publicly available documents did not mention this. In air gapping their networks, the primary reason was some of the IoT devices are medical devices, and as

such, the students need to access these devices with a portable device. The devices were not secure on the wireless network and, as such, required their isolated ad hoc network to prevent other users from attempting to access the resources and causing an unintentional denial of service. An ad hoc method of network restriction was practiced by Participants 3, 4, 5, 6, 7, 8, and 9. See Table 3 in which a theme emerged that indicated that network isolation would help secure IoT connected devices against attack and secure users within the network.

Table 3

Minor and Major Themes for Network Isolation

	Participant		Document	
Major/Minor Theme	Count	References	Count	References
Network Isolation to Secure IoT devices	10	24	2	12
Air-Gapped Network	7	12	1	2
Use of Ad-hoc networks	6	7	1	1
Network Monitoring	5	2	1	3
Firewall access isolation	5	6	1	1

Furthermore, the participants indicated that isolating the students' medical resources was a key priority for the IT professional to secure the network. They also added that this method of wireless access helped establish a secure network for these students. Furthermore, it is essential to understand that air-gapped networks still present security risks to the network (Zhou, Zhang, Li, & Yu, 2019). The research participants

unanimously indicated that constant vigilance is required to keep the network secure. An ad hoc network allows the students to use a connected medical device in an isolated network. This method enables students to connect to the training devices without concern that someone else is in the network. An ad hoc network provides peace of mind for the IT professional and the student in knowing the IoT connected devices are secure.

The CIA triad refers to confidentiality integrity and availability in terms of a benchmark for securing an organization (Sherman et al., 2018). The second theme to emerge was the need for network isolation. The term for isolation is more akin to an air-gapped network. I understood the research participants to indicate this was the only solution to solve the security challenges they must manage. One benefit as Participants 5 and 8 mentioned was that air gapping devices from the Internet allow them to be used with an isolated subnet while not permitting them to be connected to the external network. Participants 5 and 8 also indicated issues with air-gapped devices in terms of updates for the devices. Participants 5 and 8 indicated that they could no longer receive updates; and must be updated manually with a flash drive, which presents a new set of usability issues in terms of the DOI framework. Participants 1, 2, 8, and 10 indicated that these devices provide much-needed resources to the students, that is, 3D printer or CNC machine; however, they do not have the resources to protect themselves. Participants 1, 2, and 10 also indicated that the IoT devices are vulnerable to attack due to the limited nature of the computing power they pose.

The compatibility of IoT device design can be seen in the vast array of devices deployed within the educational institution. Participants 1, 2, 5, and 10 indicated the use

of CNC machines, 3D printers, medical training equipment, HVAC, and access management systems, all using different types of IoT interfaces. Participants 1, 2, 10 also indicated the absence of compatibility among the management and configuration devices. The theory of DOI (Rogers, 2003) points to compatibility based on previous experience. However, Participant 5 indicated that compatibility does not seem to be an issue with adopting the technology in securing the devices as they are managed through access controls such as MAC filtering or VLAN segmentation. The need for network isolation is ever apparent in the issues that IoT devices present to the network in terms of threat vectors. The four participant institutions present various methodologies for implementing network isolation. Participant 3, 6, and 8 indicated that a hardline cable connection for IoT enabled devices would help isolate the devices and ensure only the proper device was connected to the network, and contribute to a more robust network monitoring.

One of the five characteristics of the DOI framework is observability (Rogers, 2003) indicates that the outcome is visible and communicated to others is identified as observability. The observations by Participants 3, 4, 5, 6, 7, 8, and 9 indicated that observing other educational intuitions contributed to the decision to isolate most all IoT devices to air-gapped network completely. Other organizations have been effective in securing the network through an air-gapped security implementation. Issues indicated by the same participants come into play when updates for the devices are required to improve functionality or, in some scenarios, service the equipment by third-party vendors. The solution of an air-gapped network is more of a stop-gap, according to

Participant 8, as participants further indicated that the devices would better serve the needs of the organization are connected to the network.

In terms of the CIA triad, the absence of availability or limited availability concerning securing the IoT connected devices to the network is the primary outcome for Participants 3, 7, 8, and 9. All these participants appeared to practice air-gapped networking. Air-gapped networks were only implemented when securing the devices through standard methods would otherwise not prove possible.

Another perspective for IoT security in terms of observability is found in Participant 10, in which the organization will research the IoT devices in advance before purchasing or approving purchases. Participant 10 also indicated a more open-door policy in connecting IoT devices to the main network. Participant 10 explained that if the institution were transparent with the users, they would be transparent with the organization. The organizations indicated that their approach to security was more relaxed than other organizations; however, in the background, the actual policies were more specific in terms of connecting devices to the network that was IoT based. Conversely, Participant 1 indicated that even to connect a smartphone to the institution's network, faculty and staff would have to come to the IT department and have the device added. Participant 1 indicated that these measures might seem extreme. However, it is essential to know who is on the network while still maintaining user access to the local network.

One such case study that implemented the CIA triad as one of the research's key elements helped identify integrity and availability confidentially as key elements within

the research. Through the use of the CIA triad, concepts were able to be evaluated, such as validation of software input and helping to reduce or minimize injection attacks; furthermore, the influence of the CIA triad also helped to establish the need for network boundaries and the handling of data through the network and controlling the flow of data by ensuring the data is safe for the network (Sherman et al., 2018). My research study indicated that all of the organizations used network isolation in various forms in various forms. Examples of this are network monitoring through perimeter firewall packet inspection by all of the participating organizations. The importance of using physical security as well as virtual security is highlighted in the research by Gresham (2017), in which the need to protect the critical aspects of IoT connected devices, either physical or virtual, against target vector attacks, furthermore, ACL can provide as an extra layer of security against these critical devices.

The DOI conceptual framework includes perception or perceived benefit observability as this promotes the feeling of a secure environment to the end learner, which can be interpreted as perceived security by the student, this in effect allows the process of online or e-learning to be more effective (Tanye, 2016). When the network is perceived as more secure, the end-user could feel more secure in using the network, firewall monitoring, access controls in place, and physical security of the network, which can benefit the users of the network.

Theme 3: adoption by leadership to secure IoT inside of the network

Security leadership proves critical in securing the IoT environment, as indicated by eight of the 10 participants that participated in this research study (Table 4). Recent

security breaches appear to be linked to improper handling by third-party vendors regarding security access or personally identifiable information (Kim, Johnson, Park, & Liu, 2017). As indicated by 8 of the ten participants, leadership is critical to securing the organization from data loss or breach. Third-party vendor management falls into this category and manages the third party administrative access to your organization. Various devices present as threat vectors for the IT professionals within these organizations must be managed to prevent an attack. In terms of third-party management of resources, it was indicated by eight of the ten participants the need to either manage the access management systems, environment controls as well as many other devices that require access to a network to operate correctly. Participants 1, 3, 10 related various occasions in which they were required to contact the third-party vendor and verify some type of IoT device that was recently connected to the network and also verify that it was supposed to be whitelisted or determine the level of security that should be applied to the device. In terms of granular control of the IoT connected devices to the network. Participants 1, 3, and 10 indicated situations in which devices or third-party services have been procured without their consent or approval and has presented an issue to managing the device while maintaining security within the organization. Participant 1 indicated a scenario in which costly laboratory equipment was purchased without approval, and the software was infected with many trojans from China. Now the IT professional is put into a position of making the devices function while not contaminating the network. Participants 1, 3, 10 both indicated that the policy is to obtain permission for anything connected to the network. Participants 1, 3, and 10 indicated that this does not always occur no matter

what the policy states. Participants 4 indicated that "*security leadership provides for the organization a means to keep policies in place and ensure that the policies are effective,"* as indicated by participant. Effective leadership provides benefit to the organization in terms of early adoption of technology. Rogers, (2003) indicated that adopting a new idea can spread through interactions or social systems between groups. It is important to note that the leadership impacts the rate of adoption, and in this research study was the case between participants 1 and 10. Please see table 4 in which these themes are highlighted, representing the finding of this research.

Table 4

Minor and Major Themes Adoption by Leadership

	Participant		Document	
Major/Minor Theme	Count	References	Count	References
Adoption by Leadership to Secure IoT inside of the Network	8	31	2	21
Third-Party Vendor	7	9	2	16
Complexity	3	6	1	5
Effective Policies	4	4	1	1
Iron Fist Management	1	3	1	1
Open Door Policies	3	3	2	3
Proper Chain of Authority	5	13	1	3
Upper Management Buy-in	4	7	1	1

Relative advantage might be termed as an economic advantage or something better than the technology being replaced, as indicated by Rogers (1962). When perceiving IoT technology as adding value to the organization or replacing technology currently being used, management can align with this process of a relative advantage as a benchmark for the organization.

Strong management, as indicated by participants 1,3,4,7,8,9, which stated directly by participants 4 as “iron fist management,” can help maintain a secure network. It is interesting to note that (Karahanna & Straub, 1999) indicated that compatibility and relative advantage are linked together concerning an organization's incremental advantage. Strong management's impact on an organization in terms of securing the environment is evident by its track record of no recent security breaches. The benefit is seen by end-users and IoT connected devices remaining secure through a strong security policy enforcement perspective. Participants 1, 4, and 10 indicated that if an IoT device is purchased without prior approval of the IT department, it may not be allowed to connect to the network. IT management has a responsibility to keep the network operating correctly and securely while maintaining its policies. Participants 3 and 7 indicated the need for strong policies that were clear and understandable to the end-user in various degrees. Participants 3 suggested that the policy should be managed not overwhelming to the end-user in its various forms. A proper chain of authority and support from upper management is also vital for the organization to remain secure. Participants 2, 3,4, 5, and 10 indicated that following a proper chain of authority is key for administering the network.

Eight of the ten participants indicated that a proper chain of authority in various forms helps establish and maintain security. A recent study indicated the importance of a proper chain of authority as a benchmark for future success (Bibi & Saeed Akhtar, 2020). In various management styles and methods, participants 3, 4, 5, 6, 7, 8 indicated that they follow an internal chain of command that maintains their individual networks at each participant's perspective institution. Participants 1, 2, and 10 also follow the state mandates for each of their perspective organizations. Thereby administering policies and procedures as mandated by the state the institution resides within. It is important to note that participant 7 indicated that upper management must buy-in to the policies for them to be effective. Participant 7 also indicated that clear, concise communication is necessary for the policy to be useful when the participant indicated all stem from management buy-in. Participant 7 also stated that learning from other institutional failures and their failures was key to learning and adapting to a dynamic security environment.

The next subtheme is open-door policies. Three institutions indicated that providing an open-door policy for users is designed to encourage the user to come to the IT department for technology issues, thereby enabling them to be part of the solution. Conversely, the institutions that have the open-door policies are state intuitions. There does not appear to be a difference in the rate of exposure of these organizations based on this specific policy. There is not enough information to determine the threat exposure of these organizations concerning each other. Follow up research on this theme could benefit other institutions in terms of creating effective security policies. The last subtheme is upper management buy-in. Participants 1, 2, 3, and 10 indicated that

receiving upper management support is critical to both large- indicated that upper management buy-in is critical at the start of the project to ensure success. Participant 1 indicated that, in some scenarios, the policies and procedures are implemented backward from the normal in a business in terms of project deployment. However, participant 1 indicated that once the project is deployed, then policies and procedures are written around the project to ensure accurate alignment to the project once deployed. This method deviates from the standard of the norm for the other organizations that contributed to the research. However, it is essential to note that participant 1 also indicated that the organization had experienced no data loss or breach at this point. Participant 1 also indicated that time served on the job allowed for more flexibility in policy adherence. It was also noted by participant 1 that upper-management buy-in is still critical to the success of the project. Participant 2, 10 both also indicated upper management buy-in. Both institutions were also state colleges; thus, following a specific plan provided by the institution's state is still critical to any project deployment. Upper management buy-in was also cited by participant 3 as this participant is not part of the state institution and a private college. The participant indicated that upper management needs to support the IT department for policies and procedures to be implemented and be enforced. The upper management must be a partner in this process to be successful and for the organization to remain secure.

Theme 4: Strong, shared partnership with peer organizations through observation.

The fourth and final theme is developing a strong shared partnership with peer organizations through observation (See table 5). The importance of a robust security

stance for all organizations is key to continued success. The findings identified through this research study pointed to a shared partner relationship with various other institutions within a circle of cohorts. Regarding security policy implementation and IoT device adoption within each respective organization, all participants' organizations had one common theme: each of them looked to other organizations to determine what practices and devices worked best for each scenario. One such case study by (Carlota, Sahagún, & Selva, 2020) indicates that social interaction among peers contributes to exchanging ideas and strengthening the learning outcomes. The school of thought different methods of knowledge dissemination. One such method is informal learning, in which an individual learns on the job by doing a task. Another method mentioned in this same study was that doctors share ideas through organizational learning amongst peers. The study did indicate that the participants' level of commitment would influence the level of learning in most scenarios. The same authors also suggest that there must be an environment for this method to develop and nature.

Table 5

Minor and Major Themes Strong Shared Partnership

	Participant		Document	
Major/Minor Theme	Count	References	Count	References
Strong Shared Partnership with Peer Organizations through observation	*4*	*27*	*2*	*6*
Partner Intuitions	*3*	*22*	*2*	*16*
Security Policies	*2*	*6*	*1*	*5*
Cohort Guidance	*2*	*4*	*1*	*1*

In compiling the data, this theme appeared in all the interviews in various forms or another. It is also interesting to note that three of the public colleges' organizations were in cohorts through the state in which they serve. This same cohort allowed them to communicate with other individuals who may be in various technology adoption stages within each perspective institution.

It is interesting to note that participants 1, 2, 10 are all part of a state college system, and participant 2 and 10 work together warehousing data between each other's campuses. This collaborative effort appears to provide a symbiotic partnership between the two campuses. The idea of observation and adoption through observability is a contributing factor that Rogers (1962) indicated would be key elements to product adoption. Relative advantage and trialability, and observability all come into play

between participant 2 and 10. Participant 1 also indicated those same metrics were also used as a tool for this cohort as well.

An example of this was the adoption of wireless technology for the students. Participants evaluated the technology through local analysis and observed analysis at the other campuses to see if the technology was viable for the local college to implement. Participant 1 also indicated that in many scenarios, the organization he served provided to many other colleges within their cohort information and feedback to help other institutions make informed decisions about new technology and product adoption within their perspective institutions.

Participants 3, 5, 8, and 9 all had the same consensus regarding product adoption within the organization. Each campus is separate in terms of product adoption in many cases. Examples of this are in access door controls and environmental control systems. Each of the IT leaders within these institutions may also look to other organizations for input or within their cohorts from the same institution. Furthermore, participants 3, 5, 7, 8, and 9 indicated that they attend meetings weekly and exchange ideas with each other regarding what works and what does not. The same members also indicated that they attend professional conferences and exchange ideas between members at the conference to see what they have done on their perspective campus. Thus, these same institutions have adopted IoT devices within their institution that might otherwise not be implemented securely through observability.

Strong security policies and clearly stated objectives will help contribute to an organization's security. Another segment of a secure organization appears to come from

partner consultation or, in other terms, peer consulting with other organizations. Participant 7 stated that pulling from other people's experience and practices allows for a more informed IoT product adaption. The same participant indicated that hiring individuals from other institutions also brings the organization new skills and perspectives that will contribute to adopting IoT devices within the institution.

All of the characteristics of the DOI were applied to this research study. The DOI theory includes five key tenets, the first being compatibility in which Rogers, (2003) defined technology as perceived as being aligned with the current technology adopters. It became clear that all organizations that participated in this research in various forms look to other organizations within their cohort to determine if the technology is compatible with current standards and methods implemented within the organization. Rogers, (2003) Further indicated that compatibility could be defined as harmony between new and old technology. Participants 2, 3, 4, 5, 6, 7, 8, 9 all indicated a balance between continuing the use of older technology concerning purchasing new technology due to improved technology's capital expense. Thus, participants 4, 5 indicated that if the technology is no longer compatible with the institution's needs, it was time to look at more compatible technologies. Thus, it was essential to this same group of participants that the institution's value must be measurable. Participants 1, 5, 6, 7, 9 also indicated that the technology adopted into the organization to improve security must be compatible with previous technology and easy to manage and have standards that align with the industry. For technology to be accepted, it must align with the current adaptors or their experience, as indicated by (Zhang et al., 2010). It was noted by participants 5, 6, 7 that it would make

implementing a new IoT technology easier if it was something that they were already familiar with.

Another aspect that the theory of DOI highlighted was the concept of relative advantage. Furthermore, Rogers, (2003) identified compatibility of IoT devices would add value to the organization either by allowing it on the network or in the multicase study participants 1, 2, 5, 10 determines what the college purchases IoT devices. I observed that all of the participants in various forms mentioned that the technology being replaced must be better than the technology currently in place. Technology adoption applies not only to IoT technology but also to the same devices that monitor the network and the firewalls and IoT-based communication channels. Finally, complexity was a key element with participants 1, 5, 8, 10 in as much as if the device was overly complex to manage. The likelihood of adoption would be much less even if a faculty member wanted to procure the device. It is also important to note here that participants 5 indicated that the firewall does all of the IoT device access management within his organization, so participants are a hands-off approach to IoT device management.

A study that aligned with this research highlights IoT adoption of policies from the perspective of the organization. Chatfield & Reddick, (2019) study how a flexible organization can make decisions based on data analytics. When the data analytics are shared with other organizations that do not have the same resources, then in various forms, the shared data is provided to peer organizations such as government institutions and private organizations. The data analytics leads to policies that are also shared among these same organizations. Chatfield & Reddick, (2019) indicate in a case study that the

IoT case studies in which the policies and the current technology policies currently in place help in the creation of a more dynamic IoT policy. The case study organizations all have a common theme of implementing NIST based recommendations within each of their perspective organizations. The organizations' policy adoption is through observed compliance by peer organizations and by proxy adopted by non-governmental organizations through industry relationships.

The DOI conceptual framework used in this study highlighted observability as one of the five characteristics. Furthermore, observability had a key role in this research study as the participants in various forms worked together with cohorts to determine the best IoT security solution. The cohorts appeared to use observability, compatibility, and relative advantage as key indicators to determine a path to security within each college or university setting. The concept of cohort or peer adoption through observation was highlighted by Rogers, (2003). It indicated that adoption is indicated by the participants choosing this course of action or adoption as the most viable. The multicase research study highlighted the adoption of security practices that were observed or recommended by peer organizations that suit the network's security needs in terms of securing IoT devices within the network.

Applications to Professional Practice

This study aimed to explore security implementations strategies that IT managers in the Southeastern portion of the United States use to secure IoT devices within educational institutions. The participants provided many different security practices that benefit their perspective organizations and possibly help educational organizations

globally adopt these same security practices procedures. Of the organization that participated, it became evident that they chose to work together. An example of this was in data warehousing to maintain critical data for each other's institutions. Other examples of peer sharing are in some state colleges where they share ideas on various platforms.

The largest sector of these participants all indicated that upper management buy-in is critical to all deployments' success within the educational intuitions. The participants also suggested that they monitor other peer organizations to determine if they are using new technology and if the same technology could benefit their organization. Many participants indicated that the key to security is working together to see what works and what does not. One participant noted that it was essential to communicate with other campuses within the state intuitions to determine what works and what has not worked due to a limited budget. The reasoning was that larger budgets help those educational institutions with smaller budgets keep costs down while still providing a secure environment for the students.

IT professionals require cutting-edge technology within a budget that makes financial sense. Implementing technology that provides the greatest return on the investment is critical to any organization's continued success. Issues associated with IoT technology are defined in this research. Standardization between IoT device vendors and limited computing associated with the IoT devices lending to the inability for the device to be appropriately secured has contributed to IoT threat vectors that must be addressed. In this research study, the educational institutions have provided methods and means of

securing their perspective organizations by ensuring confidentially, integrity, and availability (CIA) by following basic practices.

The organizations implemented various techniques to protect the network and minimize threat vectors. Securing IoT devices at the endpoint is not as practical as minimizing the IoT device's footprint to the network appears to be a common thread among all participating intuitions. Another key element is a basic question being asked if the device cannot be put into an air-gapped network? Various valid reasons for not using an air-gapped network are required real-time updates or external access. If the device cannot be secured within an air-gapped network, it would be appropriate for access restrictions to be put in place with monitoring and constant vigilance with the network. This vigilance would include monitoring the network and actively creating a culture within the organization that the organization's security starts with the end-user, which includes the IoT devices.

This research study used the DOI theory to help to guide the research. The first element was compatibility. This particular aspect provided insight into the colleges and universities that were part of different educational systems. Furthermore, security policies were usually adopted from the state or parent campus regarding the security policies. This concept ensures the compatibility of the policies before they are adopted at a local level. This same approach ensured that adopting the technology and implementation of IoT security methods would work and serve the institution in the best fashion.

The DOI attributes are the key foundational element of relative advantage and observability; these were both a cornerstone of this research study. Relative advantage

allowed for the question to be asked, does this technology provide to other organizations benefit? Rogers, (2003) indicated a need to evaluate if the technology being considered for adoption is better than the current technology. Is the technology in place currently more suited for the organization's needs? All the participating organizations consulted with other organizations within their cohort or organizational peers from other institutions from past employment.

Compatibility, as defined by (Rogers, 2003), looks at the previous experience in adoption. The IoT landscape is changing so quickly and presenting new threat vectors continuously, and the compatibility of the device to be managed is key to endpoint security. The educational institutions that participated indicated that they are working to secure IoT in a wholistic method. All the various elements of IoT security are being considered. Examples of this are end-user devices or stand-alone IoT devices. For the network to remain secure, it is suggested that all of the IoT devices should have MAC address filtering and VLAN segmentation applied. If the device is not required to have Internet access, the device may be assigned an air-gapped network unless updates were needed, as is the example in some of the more advanced medical training devices.

Some participants' organizations stated one final observation was researching the IoT device firmware before connecting to the network. When this approach was not possible in some scenarios, the device being considered for adoption would be tested inside the sandbox environment before being approved for purchase or connection to the network. The last comment made by one of the participants was to review the driver

associated with the device. The same participants indicated that before approving an IoT device, the device driver is downloaded and then checked for vulnerabilities.

When applied to the above research, the benefit of the DOI theory helped clarify the research and provide a practical application to society for the implementation of IoT devices within not only educational intuitions but hopefully other intuitions and individual users.

Implications for Social Change

The exploration of IoT security strategies can impact other organizations aside from educational institutions and provide benefits on a global scale. Educational institutions offer benefits to the students and the community at large due to the active involvement in the local community. Other educational institutions provide benefits in research either in medical or farm and land management, just a few of the segments that IoT technology currently impacts. A more secure IoT environment within educational institutions allows for the deployment and adoption of IoT technology within these environments. It provides benefit by providing institutions and communities with a clearly defined best use practice for securing IoT that has worked for industry professionals. Within the organizations that participated in this study. Another benefit is provided to end-users enabling them to feel more comfortable adopting IoT technology within their home or business.

Educational institutions are refraining from fully adopting IoT technology to serve the students in the classroom due to security issues associated with the current technology. This multi-case study has provided various methods to ensure that the device

considered should be evaluated before adoption. Some of the participants' methods include downloading the firmware and drivers and scanning them for malware or backdoors before adoption. These methods do not always apply to smaller organizations with limited resources; however, a good search in some scenarios will yield the same results from credible organizations. Some of the participants recommended that due diligence be applied before adoption. Your current organization may select a different course for evaluation; however, some type of due diligence needs to be completed before adoption to minimize organizational threat vectors.

The DOI theory provided a key foundation for this research study to apply the research to a real-world example. The theory applied and centered around the user and organization and perceived value to the end-user. This research study's main focus was on securing IoT to make the technology more suitable for adoption within the institution. This multi-case study identified various methods through the use of the DOI framework. Furthermore, these methods of securing the institution will allow the adoption of IoT technology on a global scale. IoT adoption will occur within an educational environment and home monitoring management systems for the aging elderly. Another area that IoT adoption will benefit is farmland management in underserved countries where resources are scarce. There is a need to maximize the most significant yield from the production of food.

Recommendations for Action

This research multi-case study revealed four primary key foundational elements to secure an educational institution. This study further indicated the need for a shared

partnership within the community—the study also indicated that institutions need to work together to achieve a common goal. Organizational leaders should include the restriction of IoT access to the network in their IoT device deployment to ensure a layer of protection for the IoT devices as well as the network these devices are connected to. Another actionable recommendation for IT professionals is network isolation to secure IoT devices from the network if the devices need to connect to the network for management and monitoring, then isolation of the devices to provide for continuous monitoring of the devices to minimize threat vectors to the network.

Another recommendation is adoption by leadership to support the security IoT connected devices within the organization. All of the institutions that participated in this multi-case research study indicated that leadership support in all facets of device procurement and deployment was critical to the network's security. The recommendations from the IT professionals are the upper management must support them for the process to work. This support includes before device procurement that the device must be researched by the IT professional or an outside trusted organization to ensure the device is secure.

IT professionals within educational organizations need a robust shared partnership with peers within the organizational structures. Strong organizational structures provide a more robust cohort of organizations that will help the community remain secure and help new organizations and individuals remain secure.

This study will also benefit community leaders to help fortify the local educational institutions by disseminating this research material and continued vigilance

of IoT security as a primary focus within the educational institution. To this end, I will create an executive-level overview of this study. Once completed, I will send it to community leaders within the Southeast. as well as participants of the research study, to allow for a deeper understanding of methods that are being implemented by peer organizations within their perspective communities.

Organizational IT leaders should ensure that the organization, before adopting an IoT device to experiment with the device to determine if the device provides benefit to the organization more than what current technology is already in place. Another suggestion would be a trial period of the technology in a sandbox environment before adoption to ensure the device is secure and benefit the organization. The IT professional should remove the need for the end-user within the institutions to manage the security of the IoT connected device by anyone other than the IT professional to minimize complexity in device management. This administration can be done through the use of firewall management and monitoring of the device. IT professionals need to ensure that the network's security is not left to the end-user of the IoT devices; thus, the need to use creative methods to ensure the device management interface's complexity is not the only security mechanism in place.

Recommendations for Further Study

This research study focused on IoT security within the educational institution, and as such, the research uncovered a vibrant research topic of peer organization collaboration. There is a tremendous amount of information and benefit to other educational institutions that could be gained from further research in understanding how

this relationship is established between peer organizations. Another rich area is understanding how to create a more robust relationship between peer organizations beyond the context of the current peer groups.

Other areas for further recommendations for further research would be due to the nature of qualitative research. I would recommend that this research be paired with a quantitative study to help guide qualitative data research. A quantitative study would help to minimize the bias that is inherent in a qualitative study. Using a larger sample size normally found in a quantitative study would help steer future qualitative research and help minimize the inherent bias. Finally, based on the literature review, there is a need to explore standardization between IoT device vendors. The current study addressed issues with the absence of standardization. However, a research study helps understand why this void exists and what can be done, if anything, to fill the void of absence in IoT device standardization. Another area from the literature review that needs to be addressed is why do so many variations in firmware cores exist?

Reflections

During this research process, I understood qualitative research and a deeper understanding of a living document. Honestly, I was in awe of the process once it started as with each interview and transcription, my preconceived notions and ideas melted away with each memo and note that I attached to each transcript. I honestly have to admit that if I were asked what the study result would be that I could predict the outcome, I was wrong. It was essential to keep an open mind and reduce the internal bias inherent to researchers. Minimizing my internal bias was required to listen to the facts and report

them as they appeared in the research. After writing the memos and creating themes from these memos, it was essential to go back over the previous interview and use the documentation to verify the finding and add validity to the research results. I was honestly concerned with gaining access to my research participants. This research was conducted through one of the darkest periods in human history COVID 19; however, institutions were willing to step up and help me complete the research. I am a faculty member at campus covered by the research.

I would not use any of the participants within my institution to minimize. I have been doing computers and electronics since 1984 and currently hold a certified ethical hacker certification along with a Security Plus and other cloud certification. I was able to draw on this knowledge to help with the research and help minimize the bias. The (CEH) allowed me ask myself questions that directly related to the research. This approach helped to minimize bias as I would refer to formal certification, not my own opinion.

This multi-case research study required me to view the research through the eyes of the research participant. Overall, this has been an amazing journey, and at the end of it, I am grateful for this opportunity to contribute to IoT security within educational institutions.

Summary and Study Conclusions

Security will be an ongoing issue for society; new technology will be continuing to expand the minds and capabilities of humanity. Maintaining an acceptable level of security within the educational institution and society is kept to accepting new IoT technology. The error of society would be not to adopt IoT technology because there is a

fear that it could impact network security. This stance would be a travesty as this study identified various methods to adopt IoT technology and remain secure. The specific IT problem is that some IT professionals in educational institutions in the Southeastern portion of the United States lack security implementation strategies for securing IoT environments. This study answered this question that was posed at the beginning of this research. The semi-structured interviews presented findings that identified four primary themes that clearly stated strategies that could benefit educational institutions, as identified below.

- restricting IoT access to the network
- network isolation to secure IoT devices from the network
- adoption by leadership to secure IoT inside of the network
- strong shared partnership with peer organizations through observation

There is a need for continued vigilance in IoT security deployment. Furthermore, not adopting IoT technology because of fear of the unknown is not acceptable. These concerns are valid; however, this study's findings should help steer potential adopters of this new and exciting technology that is sure to change the way society interacts with technology daily. There is a need for continued vigilance to secure the institution from attack from outside threat actors. An increase in partner institutions' knowledge can be gained from peers based outside of your normal circle of activity. This cohort realm of IT security can make for a more vital institution in terms of security and society as a whole.

References

Aftab, H., Gilani, K., Lee, J., Nkenyereye, L., Jeong, S., & Song, J. (2019). Analysis of identifiers on IoT platforms. *Digital Communications and Networks*. doi:10.1016/j.dcan.2019.05.003

Aguinis, H., & Solarino, A. M. (2019). Transparency and replicability in qualitative research: The case of interviews with elite informants. *Strategic Management Journal*, *40*(8), 1291–1315. doi:10.1002/smj.3015

Alase, A. (2017). The interpretative phenomenological analysis (ipa): A guide to a good qualitative research approach. *International Journal of Education and Literacy Studies*, *5*(2), 9–19. Retrieved from ERIC

Albuquerque, R., Villalba, L., Orozco, A., & Buiati, F., & Tai-Hoon, K. (2014). A layered trust information security architecture. *Sensors*, *14*(12), 22754–22772. doi.org/10.3390/s141222754

Ali, B., & Awad, A. I. (2018). Cyber and physical security vulnerability assessment for IoT-based smart homes. *Sensors, 18*(3), 817. doi:10.3390/s18030817

Almeida, V. A. F., Doneda, D., & Abreu, J. de S. (2017). Cyberwarfare and digital governance. *Ieee Internet Computing*, *21*(2), 68–71. Retrieved from Ebscohost

Araujo, V., Mitra, K., Saguna, S., & Åhlund, C. (2019). Performance evaluation of FIWARE: A cloud-based IoT platform for smart cities. *Journal of Parallel and Distributed Computing*, *132*, 250–261. doi:10.1016/j.jpdc.2018.12.010

Atzori, L., Iera, A., & Morabito, G. (2017). Understanding the Internet of Things: Definition, potentials, and societal role of a fast-evolving paradigm. *Ad Hoc Networks*, *56*, 122–140. doi:10.1016/j.adhoc.2016.12.004

Bajracharya, B., Blackford, C., & Chelladurai, J. (2018). Prospects of Internet of Things in Education system. CTE Journal, 6(1), 17. 17–24. Retrieved from https://search-ebscohost-com.ezp.waldenulibrary.org/login.aspx?direct=true&db=eue&AN=131387299&site=eds-live&scope=site

Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications, 58*(1), 49–69. doi:10.1007/s11277-011-0288-5

Barrett, J. (2007). The researcher as instrument: Learning to conduct qualitative research through analyzing and interpreting a choral rehearsal. *Music Education Research, 9*(3), 417–433. doi:10.1080/14613800701587795

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation. *Qualitative Report, 13*(4), Art. 2. Retrieved from https://nsuworks .nova.edu/cgi/viewcontent.cgi?article=1573&context=tqr

Belhekar, P., Thakare, A., Budhe, P., Shinde, U., & Waghmode, V. (2018). Decision support system for Smart Farming with hydroponic style. *International Journal of Advanced Research in Computer Science; Udaipur, 9*(1). Retrieved from https://search-proquest-com.contentproxy.ix.edu/docview/2007415592/abstract/6CCF13DAA1034597PQ/1

Bero, L. (2017). Addressing bias and conflict of interest among biomedical researchers. JAMA, 317(17), 1723–1724. doi:10.1001/jama.2017.3854

Berte, D. R. (2018). Defining the IoT. *Proceedings of the International Conference on Business Excellence, 12*(1), 118-128. doi:10.2478/picbe-2018-0013

Bhattarai, S., & Wang, Y. (2018). End-to-end trust and security for Internet of things applications. *Computer, 51*(4), 20–27. doi:10.1109/MC.2018.2141038

Bibi, N., & Saeed Akhtar, M. M. (2020). Relationship between organizational structure and job performance of teaching faculty at higher education level. *Journal of Research & Reflections in Education, 14*(1), 113–122. Retrieved from EBSCOhost

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking. *Qualitative Health Research, 26*(13), 1802–1811. doi:10.1177/1049732316654870

Blackwell, C. K., Lauricella, A. R., & Wartella, E. (2014). Factors influencing digital technology use in early childhood education. *Computers & Education, 77,* 82–90. doi:10.1016/j.compedu.2014.04.013

Bolderston, A. (2012). Conducting a research interview. *Journal of Medical Imaging and Radiation Sciences*, *43*(1), 66–76. doi:10.1016/j.jmir.2011.12.002

Boukerch, A., Xu, L., & EL-Khatib, K. (2007). Trust-based security for wireless ad hoc and sensor networks. *Computer Communications, 30*(11), 2413–2427. doi:10.1016/j.comcom.2007.04.022

Broström, T., Zhu, J., Robucci, R., & Younis, M. (2018). Internet of Things boot integrity

measuring and reporting. *SIGBED Rev., 15*(5), 14–21. doi:10.1145/3292384.3292387

Buabeng-Andoh, C. (2018). Predicting students' intention to adopt mobile learning: A combination of theory of reasoned action and technology acceptance model. *Journal of Research in Innovative Teaching & Learning*, (2), 178. doi.org/10.1108/JRIT-03-2017-0004

Burgess, M. (2003). On the theory of system administration. *Science of Computer Programming*, *49*(1–3), 1. Retrieved from EBSCOhost

Byrne, M. (2001). The concept of informed consent in qualitative research. *AORN Journal*, *74*(3), 401–403. doi:10.1016/S0001-2092(06)61798-5

Cahill, J., Portales, R., McLoughin, S., Nagan, N., Henrichs, B., & Wetherall, S. (2019). IoT/sensor-based infrastructures promoting a sense of home, independent living, comfort and wellness. *Sensors, 19*(3). doi:10.3390/s19030485

Cao, Y., Ajjan, H., Hong, P., & Le, T. (2018). Using social media for competitive business outcomes: An empirical study of companies in China. *Journal of Advances in Management Research*, *15*(2), 211–235. doi:10.1108/JAMR-05-2017-0060

Carlota, C., Sahagún, M., & Selva, C. (2020). Peer and informal learning among hospital doctors: An ethnographic study focused on routines, practices and relationships. *Journal of Workplace Learning*, *32*(4), 285–301. doi:10.1108/JWL-11-2018-0141

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. J. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*(5), 545–

547. doi:10.1188/14.ONF.545-547

Castillo, A., & Thierer, A. D. (2015). Projecting the growth and economic impact of the Internet of things. *SSRN Electronic Journal.* doi:10.2139/ssrn.2618794

Chacko, A., & Hayajneh, T. (2018). Security and privacy issues with IoT in healthcare. EAI Endorsed Transactions on Pervasive Health and Technology, 0(0), 155079. doi:10.4108/eai.13-7-2018.155079

Chandramouli, R. (2016). *Secure Virtual Network Configuration for Virtual Machine (VM) Protection* (No. NIST SP 800-125B) (p. NIST SP 800-125B). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-125B

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. Federal Government. Government Information Quarterly, 36(2), 346–357. doi:10.1016/j.giq.2018.09.007

Chen, H., Duan, W., & Zhou, W. (2017). The interplay between free sampling and word of mouth in the online software market. *Decision Support Systems*, *95*, 82–90. doi:10.1016/j.dss.2017.01.001

Cheng, H. K., & Tang, Q. C. (2010). Free trial or no free trial: Optimal software product design with network effects. *European Journal of Operational Research*, 205(2), 437–447. doi:10.1016/j.ejor.2010.01.014

Choi, S. (2018). What promotes smartphone-based mobile commerce? Mobile-specific and self-service characteristics. *Internet Research*, *28*(1), 105–122. doi:10.1108/IntR-10-2016-0287

Cohen, N., & Arieli, T. (2011). Field research in conflict environments: Methodological challenges and snowball sampling. *Journal of Peace Research*, 48(4), 423–435. doi:10.1177/0022343311405698

Cope, D. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. *Oncology Nursing Forum*, (1), 89. doi.org/10.1188/14.ONF.89-91

Creswell, J. W., Hanson, W. E., Clark, V. L., & Morales, A. (2007). Qualitative Research Designs: Selection and implementation. *The Counseling Psychologist*, 35(2), 236–264. doi:10.1177/0011000006287390

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

Cruz, B., Gómez-Meire, S., Ruano-Ordás, D., Janicke, H., Yevseyeva, I., & Méndez, J. R. (2019). A practical approach to protect IoT devices against attacks and compile security incident datasets. *Scientific Programming*, 1–11. doi.org/10.1155/2019/9067512

Cruz-Jesus, F., Pinheiro, A., & Oliveira, T. (2019). Understanding CRM adoption stages: Empirical analysis building on the TOE framework. *Computers in Industry*, *109*, 1–13. doi.org/10.1016/j.compind.2019.03.007

Cunningham, J., Menter, M., & Young, C. (2017). A review of qualitative case methods trends and themes used in technology transfer research. *Journal of Technology*

Transfer, 42(4), 923–956. doi:10.1007/s10961-016-9491-6

Curtis, S. R., Carre, J. R., & Jones, D. N. (2018). Consumer security behaviors and trust following a data breach. *Managerial Auditing Journal*, *33*(4), 425–435. doi:10.1108/MAJ-11-2017-1692

Cypress, B. S. E. (2017). Rigor or reliability and validity in qualitative research: Perspectives, strategies, reconceptualization, and recommendations. Dimensions of Critical Care Nursing, 36(4), 253–263. doi:10.1097/DCC.0000000000000253

Dang, C. C., & Li, Y. G. (2014). Application of IoT in physical teaching of ethnic colleges. *Applied Mechanics and Materials*; *Zurich*, 672–674, 2257–2260. doi:10.4028/672-674.2257

Daniel, B. K. (2019). Using the tact framework to learn the principles of rigour in qualitative research. *Electronic Journal of Business Research Methods*, *17*(3), 118–129. doi:10.34190/JBRM.17.3.002

Daud, M., Rasiah, R., George, M., Asirvatham, D., & Thangiah, G. (2018). Bridging the gap between organisational practices and cyber security compliance: Can cooperation promote compliance in organisations? *International Journal of Business & Society*, *19*(1), 161–180. Retrieved from EBSCOhost

Davar, P. (2017). IoT: Their conveniences, security challenges and possible solutions. *Advances in Science, Technology and Engineering Systems*, (3), 1211. doi:10.25046/aj0203153

Dearing, J. W., & Cox, J. G. (2018). Diffusion of innovations theory, principles, and practice. *Health Affairs; Chevy Chase*, *37*(2), 183–190. doi.org.contentproxy.phoenix.edu/10.1377/hlthaff.2017.1104

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of Cyberspace security. *International Political Sociology*, 4(1), 15–32. doi:10.1111/j.1749-5687.2009.00088.x]

Denham, M. A., & Onwuegbuzie, A. J. (2013). Beyond Words: Using Nonverbal Communication Data in Research to Enhance Thick Description and Interpretation. *International Journal of Qualitative Methods*, *12*(1), 670–696. doi:10.1177/160940691301200137

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

Department of Education. (2013). 3D printers in schools: Uses in the curriculum. 24. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/251439/3D_printers_in_schools.pdf

Dinculeană, D., & Cheng, X. (2019). Vulnerabilities and limitations of MQTT protocol used between IoT devices. Applied Sciences, 9(5), 848. doi:10.3390/app9050848

Ding, Y., Shi, Y., Wang, A., Zheng, X., Wang, Z., & Zhang, G. (2019). Adaptive chosen-plaintext collision attack on masked AES in Edge Computing. IEEE Access, 7, 63217–63229. doi:10.1109/ACCESS.2019.2916553

Doyle, L., Brady, A. M., & Byrne, G. (2016). An overview of mixed methods research revisited. *Journal of Research in Nursing, 21*(8), 623–635.

doi:10.1177/1744987116674257

Drew, B. L., Mion, L. C., Meldon, S. W., Khalil, M. Y., Beaver, A., & Ghazal-Haddad, L. (2004). Effect of environment and research participant characteristics on data quality. *Western Journal of Nursing Research*, 26(8), 909–921. doi:10.1177/0193945904267709

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, 50, 25-32. doi:10.5465/amj .2007.24160888

Ellis, T. J., & Levy, Y. (2009). Towards a guide for novice researchers on research methodology: Review and proposed methods. Issues in Informing Science & Information Technology, 6, 323–337. doi:10.28945/1062

Elwood, S. A., & Martin, D. G. (2000). "Placing" interviews: Location and scales of power in qualitative research. *Professional Geographer,* 52(4), 649. doi:10.1111/0033-0124.00253

Erlen, J. A., Sauder, R. J., & Mellors, M. P. (1999). Ethics. Incentives in research: Ethical issues. *Orthopaedic Nursing, 18*(2), 84–87. Retrieved from EBSCOhost

Farrell, S. (2008). Password policy purgatory. IEEE Internet Computing, 12(5), 84–87. doi:10.1109/MIC.2008.108

Fattah, S. M. M., Sung, N.-M., Ahn, I.-Y., Ryu, M., & Yun, J. (2017). Building IoT services for aging in place using standard-based IoT platforms and heterogeneous IoT products. *Sensors; Basel,* 17(10), 2311. doi:10.3390/s17102311

Fawaz, K., & Shin, K. G. (2019). Security and privacy in the Internet of things. Computer

(New York), 52(4), 40–49. doi:10.1109/MC.2018.2888765

FBI. (2017). Internet crime complaint center (ic3) | Internet-connected toys could present privacy and contact concerns for children. Retrieved January 27, 2019, from https://www.ic3.gov/media/2017/170717.aspx

Federal Communications Commission. (2017). Cybersecurity planning guide. Retrieved from https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/SurveyCertEmergPrep/Downloads/CyberSecurity-Planning-Guide-FCC.pdf

Fournaris, A. P., Fraile, L. P., & Koufopavlou, O. (2017). Exploiting hardware vulnerabilities to attack embedded system devices: A survey of potent microarchitectural attacks. *Electronics,* 6(3). doi:10.3390/electronics6030052

FTC Staff. (2015). Internet of things; privacy & security in a connected world. Retrieved from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

Funk, M., Lin-Lin, C., Shao-Wen, Y., & Yen-Kuang, C. (2018). Addressing the need to capture scenarios, intentions and preferences: Interactive intentional programming in the smart home. *International Journal of Design*, *12*(1), 53–66. Retrieved from EBSCOhost

Fusch, P., Fusch, G., & Ness, L. (2018). Denzin's Paradigm Shift: Revisiting Triangulation in Qualitative Research. *Journal of Social Change*, *10*(1). Retrieved from https://scholarworks.waldenu.edu/jsc/vol10/iss1/2

Garcia, G. C., Ruiz, I. L., & Gomez-Nieto, M. A. (2016). State of the art, trends and future of bluetooth low energy, near field communication and visible light communication in the development of smart cities. *SENSORS*, *16*(11). doi:10.3390/s16111968

Gary, J. I. (2017). Fostering the advancement of the Internet of Things. Retrieved from https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf

Gene, L., Nguyen, A., & Kanji, Z. (2006). Implementing and assessing the benefits and feasibility of a "safe sampling" pilot project. *Canadian Pharmacists Journal*, *139*(3), 42. Retrieved from EBSCOhost

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal; London*, *204*(6), 291–295. doi:10.1038/bdj.2008.192

Gloria, D. (2016). Strategic principles for securing the internet of things (IoT). DHS, Ver 1.0, 17. Retrieved from https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 597–606. Retrieved from https://nsuworks.nova.edu/tqr/vol8/iss4/6

Goldenberg, D., & Laschinger, H. (1991). Attitudes and normative beliefs of nursing students as predictors of intended care behaviors with AIDS patients: A test of the

Ajzen-Fishbein Theory of Reasoned Action. *Journal of Nursing Education*, *30*(3), 119–126.

Greaney, A.-M., Sheehy, A., Heffernan, C., Murphy, J., Mhaolrúnaigh, S. N., Heffernan, E., & Brown, G. (2012). Research ethics application: A guide for the novice researcher. *British Journal of Nursing,* 21(1), 38–43. doi:10.12968/bjon.2012.21.1.38

Greene, J. C., Caracelli, V. J., & Graham, W. F. (1989). Toward a conceptual framework for mixed-method evaluation designs. Educational evaluation and policy analysis, 11(3), 255–274. doi:10.2307/1163620

Gresham, T. P. (2017). Critical infrastructures critical vulnerabilities. ITNOW, 59(1), 26–27. doi:10.1093/itnow/bwx012

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

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *J. of Management Information Systems*, *28*, 203–236. doi:10.2753/MIS0742-1222280208

Haddud, A., DeSouza, A., Khare, A., & Lee, H. (2017). Examining potential benefits and

challenges associated with the Internet of Things integration in supply chains. *Journal of Manufacturing Technology Management,* 28(8), 1055–1085. doi:10.1108/JMTM-05-2017-0094

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in internet of things (IoT): A review. *Journal of Computer Networks & Communications*, 1–14. doi:10.1155/2019/9629381

Hammarberg, K., Kirkman, M., & de Lacey, S. (2016). Qualitative research methods: When to use them and how to judge them. Human Reproduction, 31(3), 498–501. doi:10.1093/humrep/dev334

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research & Method in Education*, 38(1), 23–38. (Routledge. Available from: Taylor & Francis, Ltd. 325 Chestnut Street Suite 800, Philadelphia, PA 19106. Tel: 800-354-1420; Fax: 215-625-2940; Web site: http://www.tandf.co.uk/journals).

Harvey, W. S. (2011). Strategies for conducting elite interviews. Qualitative Research, 11(4), 431–441. doi:10.1177/1468794111404329

Harvey-Jordan, S., & Long, S. (2001). The process and the pitfalls of semi-structured interviews. *Community Practitioner; London*, 74(6), 219. Retrieved from http://search.proquest.com/docview/213313284/citation/9BFA67D168574984PQ/

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: How many interviews are enough? Qualitative Health Research, 27(4),

591–608. doi:10.1177/1049732316665344

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47(2), 154–165. doi:10.1016/j.dss.2009.02.005

Hernández-Ramos, J. L., Pérez, S., Hennebert, C., Bernabé, J. B., Denis, B., Macabies, A., & Skarmeta, A. F. (2018). Protecting personal data in IoT platform scenarios through encryption-based selective disclosure. *Computer Communications*, *130*, 20–37. doi.org/10.1016/j.comcom.2018.08.010

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, (4), 12. Retrieved from EBSCOhost

Humble, Á. M. (2009). Technique triangulation for validation in directed content analysis. *International Journal of Qualitative Methods*, 8(3), 34–51. doi:10.1177/160940690900800305

Hwang, Y. M., Kim, M. G., & Rho, J.-J. (2016). 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

Irawan, J. D., Adriantantri, E., & Farid, A. (2018). RFID and IoT for attendance monitoring system. MATEC Web of Conferences; Les Ulis, 164. doi:10.1051/matecconf/201816401020

Jin Xiu Guo. (2019). Measuring information system project success through a software-assisted qualitative content analysis. Information Technology & Libraries, 38(1),

53–70. doi.org/10.6017/ital.v38i1.10603

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. Educational Researcher, 33(7), 14-26. doi:10.3102 /0013189X033007014

Karahanna, E., & Straub, D. W. (1999). The psychological origins of perceived usefulness and ease-of-use. Information & Management, 35(4), 237–250. doi:10.1016/S0378-7206(98)00096-2

Karahanna, Agarwal, & Angst. (2006). Reconceptualizing compatibility beliefs in technology acceptance research. MIS Quarterly, 30(4), 781. doi:10.2307/25148754

Kassab, M., DeFranco, J., & Voas, J. (2018). Smarter education. *IT Professional, IT Prof.*, *20*(5), 20–24. doi:10.1109/MITP.2018.053891333

Khan, Z. A., & Herrmann, P. (2019). Recent advancements in Intrusion Detection Systems for the Internet of Things. Security & Communication Networks, 1–19. doi:10.1155/2019/4301409

Khera, M. (2017). Think like a hacker: Insights on the latest attack vectors (and security controls) for medical device applications. *Journal of diabetes science and technology,* 11(2), 207–212. doi:10.1177/1932296816677576

Killingback, C., Tsofliou, F., & Clark, C. (2017). Older people's adherence to community-based group exercise programmes: A multiple-case study. BMC Public Health, 17(1), 1–12. A doi:10.1186/s12889-017-4049-6

Kim, B., Johnson, K., Park, S.-Y., & Liu, S. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management*, *4*(1), 1-N.PAG. Retrieved from EBSCOhost

Kimani, K., Oduol, V., & Langat, K. (2019). Cyber security challenges for IoT-based smart grid networks. *International Journal of Critical Infrastructure Protection*, *25*, 36–49. https://doi.org/10.1016/j.ijcip.2019.01.001

Kitto, S. C., Chesters, J., & Grbich, C. (2008). Quality in qualitative research. *The Medical Journal of Australia*, *188*(4), 4. Retrieved from https://www.mja.com.au/system/files/issues/188_04_180208/kit10137_fm.pdf

Knapik, M. (2006). The qualitative research interview: Participants' responsive participation in knowledge-making. *International Journal of Qualitative Methods,* 5(3), 77–93. doi:10.1177/160940690600500308

Kolasińska-Morawska, K., Sułkowski, Ł., & Morawski, P. (2019). New technologies in transport in the face of challenges of economy 4.0. *Scientific Journal of Silesian University of Technology*. Series Transport, 102, 73.

Korstjens, I., & Moser, A. (2018). Series: Practical guidance to qualitative research. Part 4: Trustworthiness and publishing. *European Journal of General Practice,* 24(1), 120–124. doi:10.1080/13814788.2017.1375092

Kreindler, G. E., & Young, H. P. (2014). Rapid innovation diffusion in social networks. Proceedings of the National Academy of Sciences of the United States of America, 111, 10881–10888.

Kumboyono, K., Hamid, A. Y. S., Sahar, J., & Bardosono, S. (2019). Community response to the initiation of smoking in indonesian early adolescents: A qualitative study. *International Journal of Adolescence and Youth*. doi:10.1080/02673843.2019.1608273

Larossa, R., Bennet, L. A., & Gelles, R. J.(1981). Ethical dilemmas in qualitative family research. *Journal of Marriage & Family,* 43(2), 303. doi:10.2307/351382

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, J. (2018). Patch Transporter: Incentivized, Decentralized software patch system for WSN and IoT environments. *SENSORS*, *18*(2). doi.org/10.3390/s18020574

Lee, J., & Runge, J. (2001). Adoption of information technology in small business: Testing drivers of adoption for entrepreneurs. *Journal of Computer Information Systems*, *42*(1), 44–57. doi:10.1080/08874417.2001.11647038

Leiba, O., Bitton, R., Yitzchak, Y., Nadler, A., Kashi, D., & Shabtai, A. (2019). IoT patchpool: Incentivized delivery network of IoT software updates based on proofs-of-distribution. *Pervasive and Mobile Computing*, *58*. doi.org/10.1016/j.pmcj.2019.04.010

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

Lien, A. S., & Jiang, Y. (2017). Integration of diffusion of innovation theory into diabetes care. *Journal of Diabetes Investigation*, *8*(3), 259–260. doi:10.1111/jdi.12568

Lin, H., & Bergmann, N. (2016). Iot privacy and security challenges for smart home environments. *Information (Basel), (3)*, 44. doi:10.3390/info7030044

Liu, Y., Han, W., Zhang, Y., Li, L., Wang, J., & Zheng, L. (2016). An internet-of-things solution for food safety and quality control: A pilot project in China. *Journal of Industrial Information Integration,* 3, 1–7. doi:10.1016/j.jii.2016.06.001

Lowe, A., Norris, A. C., Farris, A. J., & Babbage, D. R. (2018). Quantifying thematic saturation in qualitative data analysis. *FIELD METHODS*, *30*(3), 191–207. doi:10.1177/1525822X17749386

Lowe, B., & Alpert, F. (2015). Forecasting consumer perception of innovativeness. Technovation, 45-46, 1-14. doi:10.1016/j.technovation.2015.02.001

Macur, M. (2013). Quality in health care: Possibilities and limitations of quantitative research instruments among health care users. *Quality and Quantity; Dordrecht*, *47*(3), 1703–1716 .doi.org.ezp.waldenulibrary.org/10.1007/s11135-011-9621-z

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods,* 17(1), 1609406918786362. doi:10.1177/1609406918786362

Malina, L., Hajny, J., Fujdiak, R., & Hosek, J. (2016). On perspective of security and privacy-preserving solutions in the internet of things. Computer Networks, 102, 83–95. doi:10.1016/j.comnet.2016.03.011

Malone, H., Nicholl, H., & Tracey, C. (2014). Awareness and minimisation of systematic bias in research. *British Journal of Nursing*, *23*(5), 279–282. Retrieved from EBSCOhost

Marak, Z. R., Tiwari, A., & Tiwari, S. (2019). Adoption of 3d printing technology: An innovation diffusion theory perspective. *International Journal of Innovation*, (1), 87. doi:10.5585/iii.v7i1.393

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

Matua, G. A., & Van der Wal, D. M. (2015). Differentiating between descriptive and interpretive phenomenological research approaches. Nurse Researcher, 22(6), 22-27. doi:10.7748/nr.22.6.22.e1344

Mershad, K., & Wakim, P. (2018). A learning management system enhanced with internet of things applications. *Journal of Education and Learning*, 7(3), 23. doi:10.5539/jel.v7n3p23

Meyer, D., Haase, J., Eckert, M., & Klauer, B. (2017). New attack vectors for building automation and IoT. *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, 8126–8131. https://doi.org/10.1109/IECON.2017.8217426

Miles, M., Huberman, M., & Saldana, J. (1994). *Qualitative data analysis*. (3rd ed.). Thousand Oaks California: Sage.

Min, S., So, K. K. F., & Jeong, M. (2019). Consumer adoption of the Uber mobile application: Insights from diffusion of innovation theory and technology

acceptance model. *Journal of Travel & Tourism Marketing*, *36*(7), 770–783. doi.org/10.1080/10548408.2018.1507866

Mollah, M. B., Azad, A. K., & Vasilakos, A. (2017). Security and privacy challenges in mobile cloud computing: Survey and way ahead. *Journal of Network and Computer Applications*, *84*, 38–54. doi.org/10.1016/j.jnca.2017.02.001

Moon, K., Brewer, T., Januchowski-Hartley, S., Adams, V., & Blackman, D. (2016). A guideline to improve qualitative social science publishing in ecology and conservation journals. Ecology and Society, 21(3). doi:10.5751/ES-08663-210317

Morgan, L., & Conboy, K. (2013). Key factors impacting cloud computing adoption. Computer (New York), 46(10), 97–99. doi:10.1109/MC.2013.362

Morgan, L., & Finnegan, P. (2007). *How perceptions of open source software influence adoption: an exploratory study.* Retrieved from ulir.ul.ie

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *The European Journal Of General Practice,* 24(1), 9–18. doi:10.1080/13814788.2017.1375091

Mullan, J., Bradley, L., & Loane, S. (2017). Bank adoption of mobile banking: Stakeholder perspective. *International Journal of Bank Marketing*, (7), 1154. doi.org/10.1108/IJBM-09-2015-0145

Ngozwana, N. (2018). Ethical Dilemmas in qualitative research methodology: Researcher's reflections. *International Journal of Educational Methodology*, *4*(1), 19–28. https://doi.org/10.12973/ijem.4.1.19

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research.

Evidence-Based Nursing, 18(2), 34–35. doi:10.1136/eb-2015-102054

Oğüt, H., Raghunathan, S., & Menon, N. (2011). Cybersecurity risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection. Risk Analysis: An Official Publication Of The

Ojo, M. O., Giordano, S., Procissi, G., & Seitanidis, I. N. (2018). A review of low-end, middle-end, and high-end IoT devices. IEEE Access, 6, 70528–70554. doi:10.1109/ACCESS.2018.2879615

O'Neil, K. (2019). How qualitative data analysis happens: Moving beyond 'themes emerged'. *Forum: Qualitative Sozialforschung*, *20*(3), 1–8. doi:10.17169/fqs-20.3.3388

O'Neill, M. (2016). Insecurity by Design: Today's IoT device security problem. Engineering, 2(1), 48–49. doi:10.1016/J.ENG.2016.01.014

O'Reilly, M., & Parker, N. (2013). 'Unsatisfactory saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. Qualitative Research, 13(2), 190–197. doi:10.1177/1468794112446106

Ortlipp, M. (2008). Keeping and using reflective journals in the qualitative research process. The Qualitative Report, 13(4), 695–705. Retrieved from https://nsuworks.nova.edu/tqr/vol13/iss4/8

Padilla, F. J. A., Baccelli, E., Eichinger, T., & Schleiser, K. (2016). *The future of IoT software must be updated*. (IAB Workshop on Internet of Things Software Update (IoTSU)), 5. Retrieved from https:// hal.inria.fr/hal-01369681/document

Padilla-Díaz, M. (2015). Phenomenology in educational qualitative research: Philosophy

as science or philosophical science ? 1, 1–10. Retrieved from https://pdfs.semanticscholar.org/1c75/935d3682047beb9723ce467a136b8456e794.pdf

Palinkas, L. A. (2014). Qualitative methods in mental health services research. *Journal of Clinical Child and Adolescent Psychology* : The Official Journal for the Society of Clinical Child and Adolescent Psychology, American Psychological Association, Division 53, 43(6), 851–861. doi:10.1080/15374416.2014.910791

Pantano, E., & Vannucci, V. (2019). Who is innovating? An exploratory research of digital technologies diffusion in retail industry. *Journal of Retailing and Consumer Services*, *49*, 297–304. doi.org/10.1016/j.jretconser.2019.01.019

Papp, D., Ma, Z., & Buttyan, L. (2015). Embedded systems security: Threats, vulnerabilities, and attack taxonomy. 2015 13th Annual Conference on Privacy, Security and Trust (PST), 145–152. doi:10.1109/PST.2015.7232966

Pering, T., Farrington, K., & Dahm, T. (2018). Taming the IoT: Operationalized testing to secure connected devices. *Computer (New York)*, *51*(6), 90–94. doi.org/10.1109/MC.2018.2701633

Petac, E., & Duma, P. (2018). Exploring the new era of cybersecurity governance. *Ovidius University Annals: Economic Sciences Series*, *XVIII*(1), 358–363 Retrieved from https://doaj.org

Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The quest for privacy in the internet of things. IEEE Cloud Computing, 3(2), 36–45. doi:10.1109/MCC.2016.28

Prada-Ramallal, G., Fatima, R., Herdeiro, M., Takkouche, B., & Figueiras, A. (2018). Primary versus secondary source of data in observational studies and heterogeneity in meta-analyses of drug effects: A survey of major medical journals. *BMC Medical Research Methodology*, (1), 1. doi.org/10.1186/s12874-018-0561-3

Qi, X., & Liu, C. (2018). Enabling deep learning on IoT edge: Approaches and evaluation. 2018 IEEE/ACM Symposium on Edge Computing (SEC), 367–372. doi:10.1109/SEC.2018.00047

Qu, S., & Dumay, J. (2011). The qualitative research interview. *Qualitative Research in Accounting & Management*, *8*(3), 238–264. doi:10.1108/11766091111162070

Ravindranath, N. H., Chaturvedi, R. K., & Kumar, P. (2017). Paris agreement; research, monitoring and reporting requirements for India. Current Science, 112(05), 916. doi:10.18520/cs/v112/i05/916-922

Reid, R., & Niekerk, J. V. (2014). From information security to cyber security cultures. 2014 Information Security for South Africa, 1–7. doi:10.1109/ISSA.2014.6950492

Rempel, H. G., & Mellinger, M. (2015). Bibliographic management tool adoption and use: A qualitative research study using the UTAUT model. *Reference & User Services Quarterly*, (4), 43.

Richards, R. J., Ratliff, L. J., Dong, R., Beaulieu, R., Shors, D., Smith, J., … Wingers, L. (2016). Next wave: the national security review of emerging technologies. Retrieved from https://www.hsdl.org/?abstract&did=799681

Rivard, J. R., Fisher, R. P., Robertson, B., & Hirn Mueller, D. (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

Rivas, M. L., & Kliarsky, A. (2017). Securing the home IoT network. *SANS Institute*, 38. Retrieved from https://www.sans.org/reading-room/whitepapers/hsoffice/securing-home-iot-network-37717

Rodrigues, G. N., Alves, V., Silveira, R., & Laranjeira, L. A. (2012). Dependability analysis in the Ambient Assisted Living Domain: An exploratory case study. *Journal of Systems and Software,* 85(1), 112–131. doi:10.1016/j.jss.2011.07.037

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

Rogers, E. (1995). Diffusion of innovations (4th ed). New York: Free Press.

Rogers, E. (2003). *Diffusion of innovations.* (5th ed.). Thousand Oaks, CA: New York: Free Press.

Rogers, E. (2010). *Diffusion of innovation* (5th ed.). New York, NY: The Free Press.

Rogers, E., Quinlan, M., & Singhal, A. (2004). *Diffusion of Innovations*. Retrieved from http://utminers.utep.edu/asinghal/Book%20Chapters/Rogers-Singhal-Quinlan-2009-DOI-Stack%20and%20Salwen.pdf

Rossman, C., & Marshall, G. (2016). *Designing qualitative research.* (6th ed.). Retrieved from https://read.amazon.com/

Roy, S. K., Misra, S., & Raghuwanshi, N. S. (2019). Senspnp: Seamless integration of heterogeneous sensors with iot devices. *IEEE Transactions on Consumer*

Electronics, Consumer Electronics, IEEE Transactions on, IEEE Trans. Consumer Electron., *65*(2), 205–214. doi:10.1109/TCE.2019.2903351

Sargeant, J. (2012). Qualitative research part II: Participants, analysis, and quality assurance. *Journal of Graduate Medical Education*, 4(1), 1–3. doi:10.4300/JGME-D-11-00307.1

Schiller, J. (2003). Working with ICT: Perceptions of Australian principals. *Journal of Educational Administration; Armidale*, *41*(2), 171–185. Retrieved from http://search.proquest.com/docview/220428612/abstract/38267FE523F74B18PQ/1

Scrutton, R., & Beames, S. (2015). Measuring the unmeasurable: Upholding rigor in quantitative studies of personal and social development in outdoor adventure education. Retrieved January 14, 2019, from doi:10.1177/1053825913514730

Shaw, J. (2018). How Can research mediators better mediate? : The importance of inward-looking processes. Evidence & Policy: *A Journal of Research, Debate and Practice,* 14(1), 143–153. (Policy Press. University of Bristol, 1-9 Old Park Hill, Bristol BS2 8BB, UK. Tel: +44-117-954-5940; e-mail: pp-info@policypress.co.uk; Web site: https://policypress.co.uk/journals/evidence-and-policy).

Sheng, Z., Mahapatra, C., Zhu, C., & Leung, V. C. M. (2015). Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT. *IEEE Access*, *3*, 622–637. doi:10.1109/ACCESS.2015.2435000

Sherman, A. T., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., … Thompson, J. (2018). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia*, *42*(4), 337–377. doi.org/10.1080/01611194.2017.1362063

Sims, J. M. M. (2010). A brief review of the Belmont report. Dimensions of critical care nursing, 29(4), 173–174. doi:10.1097/DCC.0b013e3181de9ec5

Sullivan, G. M. (2011). A primer on the validity of assessment instruments. *Journal of Graduate Medical Education*, *3*(2), 119–120. doi.org/10.4300/JGME-D-11-00075.1

Sun, J., Huang, G., Sangaiah, A. K., Zhu, G., & Du, X. (2019). Towards supporting security and privacy for social IoT applications: A network virtualization perspective. *Security & Communication Networks*, 1–15. https://doi.org/10.1155/2019/4074272

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. *Qualitative Research Journal (RMIT Training Pty Ltd Trading as RMIT Publishing)* doi:10.3316/QRJ1102063

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy*, *68*(3), 226–231 Retrieved from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4485510/

Sutton, S. R. (2011). The preservice technology training experiences of novice teachers. *Journal of Digital Learning in Teacher Education*, 28(1), 39–47. doi:10.1080/21532974.2011.10784678

Tang-Mui, J., & Teng, C.-E. (2017). Impacts of social media (facebook) on human communication and relationships: A view on behavioral change and social unity. *International Journal of Knowledge Content Development & Technology; Chungju*, *7*(4), 27–50. doi.org.ezp.waldenulibrary.org/10.5865/IJKCT.2017.7.4.027

Tanye, H. A. (2016). Perceived attributes of innovation: Perceived security as an additional attribute to Roger's diffusion of innovation theory. *International Journal of Multicultural and Multireligious Understanding*, *3*(6), 6–18. doi:10.18415/ijmmu.v3i6.57

Tasker, T. J., & Cisneroz, A. (2019). Open-ended questions in qualitative research. *Curriculum & Teaching Dialogue*, *21*(1/2), (Sp)119-(Sp)122. Retrieved from EBSCOhost

Taufique, K. M. R., Siwar, C., Chamhuri, N., & Sarah, F. H. (2016). Integrating general environmental knowledge and eco-label knowledge in understanding ecologically conscious consumer behavior. *Procedia Economics and Finance*, *37*, 39–45. doi.org/10.1016/S2212-5671(16)30090-9

Tew, Y., Tang, T. Y., & Lee, Y. K. (2017). A study on enhanced educational platform with adaptive sensing devices using IoT features. In 2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC) (pp. 375–379). doi:10.1109/APSIPA.2017.8282061

Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Generation Computer Systems,

S0167739X17321003. doi:10.1016/j.future.2018.04.027

Theron, P. M. (2015). Coding and data analysis during qualitative empirical research in practical theology. *In Die Skriflig/In Luce Verbi*, *49*(3), 9. doi:10.4102/ids.v49i3.1880

Thomas, E., & Magilvy, J. K. (2011). Qualitative Rigor or Research Validity in Qualitative Research. *Journal for Specialists in Pediatric Nursing*, *16*(2), 151–155. doi.org/10.1111/j.1744-6155.2011.00283.x

Tobin, G. A., & Begley, C. M. (2004). Methodological rigour within a qualitative framework. *Journal of Advanced Nursing*, *48*(4), 388–396. doi:10.1111/j.1365-2648.2004.03207.x

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The processes of technological innovation*. Lexington, Mass.: Lexington Books.

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

Tsai, M.-C., Lee, W., & Wu, H.-C. (2010). Determinants of RFID adoption intention: Evidence from Taiwanese retail chains. *Information & Management*, *47*(5–6), 255–261. doi.org/10.1016/j.im.2010.05.001

Tsai, T.-H., Chang, H.-T., Chen, Y.-J., & Yung-Sheng, C. (2017). Determinants of user acceptance of a specific social platform for older adults: An empirical examination of user interface characteristics and behavioral intention. PLoS One; San Francisco, 12(8), e0180102. doi:10.1371/journal.pone.0180102

Tu, M. (2018). An exploratory study of internet of things (IoT) adoption intention in logistics and supply chain management: a mixed research approach. *The International Journal of Logistics Management*, *29*(1), 131–151. doi:10.1108/IJLM-11-2016-0274

Turner, B. L., Kim, H., & Andersen, D. F. (2013). Improving coding procedures for purposive text data: Researchable questions for qualitative system dynamics modeling. SYSTEM DYNAMICS REVIEW, 29(4), 253–263. doi:10.1002/sdr.1506

Umek, A., Zhang, Y., Tomažič, S., & Kos, A. (2017). Suitability of strain gage sensors for integration into smart sport equipment: A golf club example. Sensors (Basel, Switzerland), 17(4). doi:10.3390/s17040916

Ünver, M. B. (2018). Turning the crossroad for a connected world: Reshaping the European prospect for the Internet of Things. *International Journal of Law & Information Technology*, *26*(2), 93–118. doi:10.1093/ijlit/eay003

Ursutiu, D., Samoila, C., & Bergmans, J. (2013). Labsocket: A new trend in remote labs. *International Journal of Online Engineering*, *9*, 56–60. doi:10.3991/ijoe.v9iS5.2787

Vafaei-Zadeh, A., Ramayah, T., Wong, W. P., & Hanifah, M. H. (2017). Modeling internet security software usage among undergraduate students: A necessity in an increasingly networked world. *VINE Journal of Information and Knowledge Management Systems*, 48, 2-20. doi:10.1108/vjikms-09-2016-0052

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting

mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, *17*(7), 435–495. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=117082888&site=eds-live&scope=site

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425–478.

Wainwright, M., & Russell, A. (2010). Using NVivo audio-coding: Practical, sensorial and epistemological considerations. Social Research Update, (60), 1–4

Wan, J., Al-awlaqi, M., Li, M., O'Grady, M., Gu, X., Wang, J., & Cao, N. (2018). Wearable IoT enabled real-time health monitoring system. *EURASIP Journal on Wireless Communications and Networking*, *2018*(1), 298. https://doi.org/10.1186/s13638-018-1308-x

Wang, D., Zhang, X., Ming, J., Chen, T., Wang, C., & Niu, W. (2018). Resetting your password Is vulnerable: A security study of common sms-based authentication in iot device. *Wireless Communications & Mobile Computing*, 1–15. doi:10.1155/2018/7849065

Weitzman, E. A. (1999). Analyzing qualitative data with computer software. Health Services Research, 34(5 Pt 2), 1241–1263.

Williamson, K. (2006). Research in constructivist frameworks using ethnographic techniques. (1), 83. doi:10.1353/lib.2006.0054

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial

populations in Malaysia. The Qualitative Report; Fort Lauderdale, 23(11), 2700–2713.

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

Zamawe, F. C. (2015). The implication of using nvivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal*, *27*(1), 13–15. Retrieved from PubMed Central

Zandberg, K., Schleiser, K., Acosta, F., Tschofenig, H., & Baccelli, E. (2019). Secure firmware updates for constrained IoT devices using open standards: A reality check. *IEEE Access, Access, IEEE*, *7*, 71907–71920. doi:10.1109/ACCESS.2019.2919760

Zeadally, S., Siddiqui, F., & Baig, Z. (2019). 25 Years of bluetooth technology. *Future Internet*, *11*(9), 194. Retrieved from EBSCOhost

Zhang, L., Wen, H., Li, D., Fu, Z., & Cui, S. (2010). E-learning adoption intention and its key influence factors based on innovation adoption theory. Mathematical and Computer Modelling, 51(11), 1428–1432. doi:10.1016/j.mcm.2009.11.013

Zhang, W., Lin, Y., & Qi, G. (2018). Catch you if you misbehave: Ranked keyword search results verification in cloud computing. IEEE Transactions on Cloud Computing, 6(1), 74–86. doi:10.1109/TCC.2015.2481389

Zhou, Z., Zhang, W., Li, S., & Yu, N. (2019). Potential risk of IoT device supporting IR remote control. *Computer Networks*, *148*, 307–317. doi:10.1016/j.comnet.2018.11.014

Zhu, Z.-T., Yu, M.-H., & Riezebos, P. (2016). A research framework of smart education. Smart Learning Environments, 3(1), 4. doi:10.1186/s40561-016-0026-2

Zickar, M. J. (2015). Digging through dust: Historiography for the organizational sciences. *Journal of Business and Psychology*, *30*(1), 1–14. doi:10.1007/s10869-013-9339-0

Zikria, Y. B., Yu, H., Afzal, M. K., Rehmani, M. H., & Hahm, O. (2018). Internet of things (iot): Operating system, applications and protocols design, and validation techniques. *Future Generation Computer Systems*, *88*, 699–706. doi:10.1016/j.future.2018.07.058

Appendix A: NIH Certificate of Compliance

Certificate of Completion

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

Date of completion: 09/15/2017.

Certification Number: 2488136.

Appendix B: Interview Protocol

- Greet the participant with a smile to help them feel at ease.
- Thank the participant for their time.
- I will ensure the participant is aware that they can withdraw from the interview at any time without penalty.
- Provide the consent form before interview and ensure signed.
- Remind the participant about the recording process as well as ensure strict confidentiality of the recorded content. Review archival process with participant
- Inform participant that the interview process will be between 30-45 minutes
- I will inform the participant that I am going to start the recording and identify the participants ID mask code as well as date of interview.
- I will then conduct the interview based on the questions provided.
- During the process I will ensured that the interviewee is comfortable.

Interview/Survey Questions

What security implementation strategies do local IT managers in the Southeastern portion of the United States implement to secure IoT devices within educational institutions?

1. What IoT strategies have you used within your institution to implement IoT technology?
2. What method did you use within your institution to adopt policies that allowed for the implementation of IoT strategies?
3. What method did you use within your institution to adopt practices that allowed for the implementation of IoT strategies?
4. What strategies did you use within your institution to ensure that IoT policies and practices are effective?
5. What methods provided the best results when implementing practices and policies within the institution?
6. How has the adoption of IoT within other institutions impacted the adoption within your institution?

7. How did your organization address the issues associated with the complexity of IoT devices?
8. What security implementation strategies do you feel work best overall regarding policies and practices?

Appendix C: Consent Form

Consent Form

You are invited to take part in a research study about the Security of Internet of Things Connected devices and security implementation. The researcher is inviting individuals who administer networks for educational institutions and have some experience in securing a network to be in the study. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to take part.

This study is being conducted by a researcher named James Clapp, who is a doctoral student at Walden University. You might know the researcher as James Clapp, but this research study is a separate role from that as an instructor or member in the community.

Background Information:

The purpose of this study is to investigate methods that are used to help secure IoT connected devices within the educational institution

Procedures:

If you agree to be in this study, the following describes what you will be asked to:

- The interview process will be a 30-minute audiotaped interview, and you will be advised before the recording starts.
- The follow-up interview process will only take about 20 minutes to ensure that what was presented from the first interview is accurate and if there are any other details or points that may have been omitted.
- This summation will be sent back to the participant within a week of the interview for consideration. This process should only take 20 minutes.

Voluntary Nature of the Study:

This study is voluntary. You are free to accept or turn down the invitation. No one at your educational institution will treat you differently if you decide not to be in the study. If you choose to be in the study now, you can still change your mind later. You may stop at any time. I, James Clapp, the student researcher, will be following up with each participant once selected for the study. You may choose to withdraw from the research at any point in the process or if you are not comfortable with any aspect of the research. You may also refuse to answer any question that you do not agree with or upsets you without penalty. If for any medical reason your doctor deems it necessary to withdraw you from this research, you will be withdrawn immediately. If the study staff finds evidence of illegal information or child abuse or neglect, it will be reported to local law authorities as required by law.

Risks and Benefits of Being in the Study:

Being in this type of study involves some risk of the minor discomforts that can be encountered in daily life, such as The interview process will take about 30 minutes and

might cause some fatigue on the part of the participant. Being in this study would not pose a risk to your safety or wellbeing. Although it is unlikely there is a risk of confidentiality in the participation in this research study.

The results of this study will benefit organizations in education as well as others that implement IoT connected devices within an institution or organization.

Payment:
There will not be any payments or incentives for participating in this study.

Privacy:
Reports coming out of this study will not share the identities of individual participants. Details that might identify participants, such as the location of the study, also will not be shared. The researcher will not use your personal information for any purpose outside of this research project. Data will be kept secure by James Clapp as all information will be kept in a locked box for the duration of 5 years the flash drive will be encrypted with a password to protect the data and the identity of the participants' data will be kept for a period of at least five years, as required by the university.

Contacts and Questions:
You may ask any questions you have now. Or if you have questions later, you may contact the researcher via 828-527-8443 james.clapp@waldenu.edu. If you want to talk privately about your rights as a participant, you can call the Research Participant Advocate at my university at 612-312-1210. Walden University's approval number for this study is 2488136.