2021

Strategies to Protect Against Security Violations During the Adoption of the Internet of Things by Manufacturers

Sixtus Anayochukwu Ekwo
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Sixtus Ekwo

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. Donald Carpenter, Committee Chairperson, Information Technology Faculty
Dr. Jodine Burchell, Committee Member, Information Technology Faculty
Dr. Gail Miles, University Reviewer, Information Technology Faculty

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

Walden University
2021

Abstract

Strategies to Protect Against Security Violations During the Adoption of the Internet of Things by Manufacturers

Sixtus Ekwo

MS, Strayer University, 2016

BS, Enugu State University, Nigeria, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Abstract

Security violations have been one of the key factors affecting manufacturers in adopting the Internet of Things (IoT). The corporate-level information technology (IT) leaders in the manufacturing industry encounter issues when adopting IoT due to security concerns because they lack strategies to protect against security violations. Grounded in Roger's diffusion of innovations theory, the purpose of this qualitative multiple case study was to explore strategies corporate-level IT leaders use in protecting against security violations while adopting IoT for manufacturers. The participants were senior IT leaders in the eastern region of the United States. The data collection process included interviews with corporate-level IT leaders (n = 6) and examination of company documents (n = 10). The data analysis process involved searching patterns for words, codes, or themes and their relationships to confirm the findings. During analysis, four major themes emerged: relevance of securing IoT devices in IoT adoption, identifying and separating personal and confidential data from analytical data, adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption, and risk mitigation policy relevant to securing IoT devices. The implications for positive social change include the potential for corporate-level IT leaders to develop tools that will detect threats, prevent malicious attacks, and monitor IoT networks for any IoT device vulnerabilities. Improved protection from security violations may result in more efficient ways for people to use natural resources. Additionally, there may be a wider usage of smartphones connected to IoT to simplify people's lives.

Strategies to Protect Against Security Violations During the Adoption of the Internet of Things by Manufacturers

by

Sixtus Ekwo

MS, Strayer University, 2016

BS, Enugu State University, Nigeria, 1996

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

August 2021

Dedication

I dedicate this work first to my God for making it possible for me to get to this stage of my career despite my poor beginning in life. Father Lord, I thank you and I give you all the adoration and glory! I also dedicate this work to my four children (Chinenye, Chukwuemeka, Chikaodinaka, and Chidera) for bearing with me when I could not give them all the attention that they needed from a parent. However, if I could get to this stage in my life, I encourage everyone to work hard because nothing is impossible. I believe in the acronym PUSH (Press Until Something Happens). Let no one give up; it is never easy, but the end justifies the means. Last, I want to dedicate this to my late mother, Mrs. Veronica Ekwo; wherever you are, I know that this accomplishment will make you proud.

.

Acknowledgments

One page is not enough to thank all the people who supported me in my journey to a doctorate. I will start by thanking my committee chair, Dr. Donald Carpenter; I dough my hat for you, because your mentorship was second to none. You were so encouraging and thorough at the same time; I appreciate all you have done for me to get to the final stage of this study. Many thanks to the committee members, Dr. Burchell and Dr. Miles, for your encouragement and guidance. This journey has not been easy, but consistency and perseverance were what kept me going. Also, thank you to Walden's chief academic officer, Dr. Sue Subocz, and some faculty members at Walden University that I interacted with these past few years. I also want to thank my participants in this research for making out time for me despite their busy schedules, especially during the period of the COVID-19 pandemic. I sincerely appreciate your participation in my study. Finally, I do appreciate the support, understanding, and encouragement that I got from my friends like Edith Ubaka and well-wishers.

God bless all of us!

Table of Contents

List of Tables

Section 1: Foundation of the Study

Background of the Problem

The Internet of Things (IoT) can be used in everyday life and in industries using devices such as smartphones, household appliances, sensors, multimedia devices, control devices, machines used in manufacturing plants, and other electronics that have a sensor (Coskun et al., 2018). IoT offers services relevant to manufacturing, such as provisioning manufacturing assets, maintenance and repair, and operations (Ehret & Wirtz, 2017). In the manufacturing industry, IoT can be used in determining machine health, facilitating predictive maintenance, and performing data analysis for an entire production line (Lade et al., 2017).

IoT may be a suitable technology for the manufacturing industry in increasing production and preventive maintenance. Still, security violations are a big concern in achieving the full benefits of that solution. According to Zalewski (2019), the heterogeneity and complexity of IoT devices have made stakeholders concerned that IoT may open the door to security breaches. Heterogeneity is an inherent characteristic of IoT, which has given rise to many security issues (Yousuf & Mir, 2019). Therefore, there is a need to have IoT devices protected against sophisticated attacks in the manufacturing process (Simranjeet et al., 2019). In this study, I explored strategies that corporate-level IT leaders use to protect against security violations when manufacturers adopt IoT.

Problem Statement

Security issues hinder the implementation of IoT in the manufacturing sector (Ahanger & Aljumah, 2019). Ninety-four percent of risk management professionals believe that IoT security incidents in organizations represent an issue, and 48% of organizations have already experienced an IoT security breach at least once with consequences (Feit, 2017). The general information technology (IT) problem is that many organizations encounter issues when adopting IoT due to security concerns. The specific IT problem is that corporate-level IT leaders lack strategies to protect against security violations while adopting IoT in the manufacturing industry.

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry. The population consisted of at least two corporate-level IT leaders who had been involved in strategies to protect against security violations while adopting IoT in at least three manufacturers in the eastern United States. The study's implications for positive social change include corporate-level IT leaders having strategies to protect against security violations in IoT devices. The findings of this study may lead to increased trust by the public that personal data will not be compromised, leading to greater IoT use. Greater use of IoT will have myriad societal benefits, including fuel and cost savings resulting from greater use of smart cars (Aekarat et al., 2019; Miller, 2018) and more efficient resource consumption through increased use of smart meters (Spano et al., 2015).

Nature of the Study

I considered three methods for this research project and chose a qualitative methodology. The qualitative methodology involves informal and in-depth interviews for collecting data (Fuller et al., 2019). The qualitative methodology is a rigorous method that ensures quality and trustworthiness (Kallio et al., 2016). I chose the qualitative methodology because I intended to conduct in-depth interviews to gain high-quality, reliable results on strategies to protect against security violations while adopting IoT in the manufacturing industry.

Quantitative methods involve the use of a deductive process to test prespecified concepts, constructs, and hypotheses that make up a theory (Sabet & Minaei, 2017). Quantitative methods largely depend on the measurement device or instrument used and the characteristics of the data being collected (Sabet & Minaei, 2017). Quantitative methods involve testing hypotheses and depend on some statistical analysis (Burrows et al., 2016). I did not intend to test hypotheses in this research, and I was not carrying out a deductive process, so quantitative methods were not appropriate.

The mixed method is a hybrid of qualitative and quantitative methods (McCusker & Gunaydin, 2015). The mixed method involves exploring complex research questions and combines inductive and deductive thinking and reasoning (McCusker & Gunaydin, 2015). Mixed methods were not appropriate for this study because such a methodology would have been a hybrid of qualitative and quantitative approaches, and quantitative methods had already been ruled out.

I chose qualitative methods over other methods because I sought to use a semi

structured interview process for data collection. Qualitative methods helped me explore the strategies that corporate-level IT leaders use to protect against security violations while adopting IoT in the manufacturing industry and were therefore most suitable for my research study.

I considered several research designs and chose a multiple case study for this research project. Multiple case study design involves exploration of multiple real-life cases over time and includes procedures for collecting detailed and in-depth data from multiple sources (Alpi & Evans, 2019), with a focus on analyzing one individual, several individuals, a group, an entire program, or an activity (Guetterman & Fetters, 2018). I chose multiple case study design because it allowed me to develop an in-depth understanding of strategies used to protect against security violations. The multiple case study design helped me in the collection of detailed and in-depth data on procedures from multiple sources. It enabled me to analyze various activities and address multiple themes in the interview results.

Narrative research explores social, cultural, and familial phenomena based on individual experiences and uses various analytical practices (Heilmann, 2018). Narrative research was not appropriate for this study because a narrative design centers on procedures for capturing and analyzing social, cultural, and familial phenomena based on experiences of one or two individuals. Phenomenological research design deals with gaining an understanding of the essence of an experience (Wong, 2018). In phenomenological research, findings are integrated into a detailed description of the phenomenon (Wong, 2018). Phenomenological research was not appropriate for this

study because understanding the essence of the experience and integrating findings into an exhaustive description of the phenomenon were not needed. Last, ethnographic research is used when the researcher is interested in studying behavior patterns and interpreting them accordingly (Walford, 2018). Ethnographic research was not appropriate for this study because studying and interpreting patterns were not needed. Because multiple case study design provides an in-depth analysis of cases, bounded by time and activity, and afforded me the opportunity of collecting data through different procedures, multiple case study design was most appropriate for this study.

Research Question

What are the strategies that corporate-level IT leaders in the manufacturing industry use to protect against security violations while adopting IoT in the manufacturing industry?

Interview Questions

1. What are your position and job functions?
2. How long have you been in that role?
3. How long have you used IoT?
4. How many security breaches have you had since IoT implementation?
5. How do you protect against security violations of IoT heterogeneous devices and IT infrastructure in adopting IoT?
6. What kind of security policy do you have in place? If you have one, can you describe it?
7. How does creating a relative advantage over competitors impact your security

activities when adopting IoT?

8. How does the compatibility of IoT devices with existing technology impact your security activities when adopting IoT?
9. How does the complexity of IoT devices impact your security activities when adopting IoT?
10. What impact will the trialability of IoT devices have on your security activities when adopting IoT?
11. How do you observe that protecting against security violations will help in making IoT a viable solution?
12. How do you ensure that there is an adequate budget for protecting against security violations in adopting IoT?

Conceptual Framework

In 1962, Rogers developed diffusion of innovations (DOI) theory (Dibra, 2015). DOI theory indicates that there are five main factors that influence the adoption of an innovation: relative advantage, compatibility, complexity, trialability, and observability (Rogers, 1962). Relative advantage deals with what will be gained with modern technology or innovations (Scott & McGuire, 2017). Compatibility involves the modern technology adapting to the legacy of existing technology (Scott & McGuire, 2017). Complexity is about how difficult it is to learn modern technology (Pan & Yang, 2019). Trialability refers to testing a modern technology or solution (Al-Habaibeh et al., 2017). Last, observability refers to the extent to which the technology provides a result (Dohmen & Raman, 2018).

The reason for my selection of DOI theory as my research study's conceptual framework was that DOI theory's five characteristics are in line with strategies for protecting against security violations while adopting IoT in the manufacturing industry. The purpose of having strategies for protecting against security violations in adopting IoT is to ensure that IoT has a relative advantage over other existing technology through the interconnection of IoT devices using sensors. The relative advantage will promote smarter ways of doing business and may help corporate-level IT leaders achieve a return on investment in IoT solutions. Second, having strategies for protecting against security violations in IoT technology makes the solution compatible with all legacy and existing systems. IoT adoption should not necessitate corporate-level IT leaders facing security violations because of the adoption. Third, having strategies for protecting against security violations makes IoT complexity minimal so that corporate-level IT leaders can easily adopt the solution. Fourth, having strategies for protecting against security violations in IoT solutions makes IoT a trialability solution to be tested as a pilot before the overall solution is finally deployed. Corporate-level IT leaders should test their strategies in protecting against security violations because of IoT adoption. Fifth, having strategies for protecting against security violations in an IoT solution makes it measurable by corporate-level IT leaders by observing the extent to which the solution has been able to meet business objectives. Therefore, DOI theory allows manufacturing corporate-level IT leaders to have insight into strategies for protecting against security violations.

Definition of Terms

Corporate-level IT leader: A corporate-level IT leader could be a person

appointed to a senior IT position, such as chief information security officer (CISO), senior IT manager, or chief information officer (CIO), or may sit on the organization's board (Sohel & Quader, 2017).

Internet of Things (IoT): IoT is the network interconnection of uniquely addressable devices based on standard and interoperable communication protocols with self-configuring capabilities (Lampropoulos et al., 2019).

Assumptions, Limitations, and Delimitations

Assumptions

In a qualitative research study, assumptions consist of what the researcher presumes to be true, usually only temporarily or for a particular purpose (Haines-Saah et al., 2019). The first assumption related to this study was that the participants would be honest in answering the interview questions. Member checking can be a valuable tool for achieving transactional validity by following up with participants based on responses from interviews (Caretta & Pérez, 2019). As part of this study, I employed member checking to summarize the findings in a few short bullets and asked the interviewees to verify the bullets before including the data into my research study.

A second assumption was that the criteria that would be used for the sample were appropriate for the study. Using a sampling plan is one way of ensuring that the criteria being used for a sample are appropriate because the plan specifies the procedure for recruiting participants and how many interviews or cases are needed to ensure that the findings will provide the needed data (Moser & Korstjens, 2018). In this study, I used a sampling plan to select the sample unit from participants who had implemented IoT and

were knowledgeable regarding security violations.

The third assumption was that participants were experienced in the phenomenon of interest in the study. In a qualitative study, participants who are knowledgeable and experienced in the phenomenon under study help in answering the research question and influence the resulting outcome (Kirkegaard et al., 2018). The interviews used for this study included two corporate-level IT leaders in at least three manufacturing industries in the eastern United States who had developed strategies to protect against security violations while adopting IoT in the manufacturing industry.

The fourth assumption was that participants were willing to take part in the study without any pressure or incentives. Informed consent is an effective tool that includes a detailed description of the research procedure and a statement that participation is voluntary without fear of reprisal if the participant refuses to participate (Miracle, 2016). I used an informed consent form to ensure that my study adhered to Belmont Report principles so that participants were willing to participate without any pressure or incentives.

The fifth assumption was that I would have access to at least two corporate-level IT leaders in at least three manufacturers in the eastern United States who had been involved with strategies to protect against security violations while adopting IoT.

Limitations

Limitations in qualitative research are those issues that cannot be avoided, over which researchers do not have any control; researchers still conclude their findings even when they exist (Munthe-Kaas et al., 2019). One limitation was that participants might

not fully provide the data necessary to answer the research question. That limitation could have been present because of the interviewees' bias toward IoT or IoT security strategies. One effective way to eliminate interviewees' bias toward the phenomenon under study is to use an interview protocol (Castillo-Montoya, 2016). An interview protocol is used in qualitative research to help in improving the quality of data obtained from research interviews and ensure that interview questions align with research questions (Castillo-Montoya, 2016). In this study, I structured the interview protocol to help me eliminate interviewees' bias toward the phenomenon under study.

The next limitation was that the responses to the interview questions might not align with other industries such as healthcare or logistics. One of the effective ways to eliminate interview questions that might not align with other industries, such as healthcare or logistics, is to refine the interview protocol to produce data that will answer research questions across different industries (Castillo-Montoya, 2016).

Finally, having corporate-level IT leaders as participants did not provide other users' perceptions of the IoT solution. To deal with that limitation required having participants who had a wealth of experience in the phenomenon. Participants with experience can provide useful and vast information about the subject of study (Mitchell et al., 2018).

Delimitations

Researchers use delimitations to limit the scope and set the boundaries in a research study. Delimitations are in the researcher's control and may include the choice of research questions and the population to be used (Alpi & Evans, 2019). Participants in

this study consisted of corporate-level IT leaders who had knowledge and experience in protecting against security violations while adopting IoT in their organizations. Corporate-level IT leaders have the knowledge and responsibility to implement strategies in the day-to-day running of their organization's business (Sohel, & Quader, 2017). Finally, I conducted the research study by interviewing two corporate-level IT leaders in the IT organizations of three manufacturing companies in the eastern United States.

Significance of the Study

Contribution to Information Technology Practice

IoT has become an emerging trend in IT, and security violations have affected its widespread adoption. According to Brous et al. (2019), IoT adoption generates a great deal of essential data, and there is a need to ensure that security violations are addressed. This study may provide deep insight into the strategies that corporate-level IT leaders in the manufacturing industry use in protecting against security violations to facilitate the adoption of IoT. The outcome of this research study may provide manufacturing industry corporate-level IT leaders some security violation issues to be considered in adopting IoT. Corporate-level IT leaders in other industries such as transportation, health, human services, eco-systems, and aviation may also benefit from the result of this study. There may be a lot of improvement in IT practice because the knowledge gained might make the manufacturing industry's IT practitioners foresee ways of protecting against security violations that come with IoT adoption and may provide practical strategies to protect them.

Furthermore, the adoption of IoT with good strategies for protecting against

security violations may enable businesses to perform data analytics and give some good insight into data generated from IoT solutions or environments (Al-Turjman et al., 2019). Again, IoT may help users and consumers in information sharing (Yu et al., 2017). A secured IoT solution through device authentication may also lead to a high increase in the usage of mobile technologies and apps (Jang et al., 2016). More so, the extensive usage of IoT devices may lead to the low cost of connected sensors and devices that can help IT practitioners develop more sensor-driven applications (Tresanchez et al., 2018). Last, as technology continues to grow, corporate-level IT leaders from manufacturing and other sectors may have the necessary strategies to protect against security violations because of IoT adoption (Li et al., 2016).

Implications for Social Change

This research study's positive social change implication is that corporate-level IT leaders may gain valuable strategies to protect against security violations while promoting IoT adoption. IoT adoption may enhance the usage of IoT devices in manufacturing and other industries (Saez et al., 2018). Second, the protection of IoT devices may enhance broader usage of smart cars, helping consumers save money on gas and efficient parking systems. IoT devices may help people working in cities by offering an easier way of parking by detecting available parking spaces (Aekarat et al., 2019). The third social implication is that the study might help industrial manufacturing by providing an efficient way of using natural resources. For example, remote-control thermostats in industrial manufacturing might help to improve natural resources (Miller, 2018). Fourth, the social implication of security strategies for protecting IoT devices is that it might help

organizations' employees use smartphones to share information about their products. IoT may help smartphone users to share product information and promotions using social media and other forms of social networking (Erhan et al., 2019). Fifth, energy and utility companies may have a better way of remotely monitoring their customers' meters. IoT may increase the usage of smart meters by utility companies for a more efficient way of monitoring and billing customers (Spano et al., 2015). Last, social networking and family relationships may improve if IoT consumers understand that their personal information is not compromised by using IoT devices. Social relationships may attract rural residents to IoT cities with an IoT-based infrastructure (Hassan & Awad, 2018).

A Review of the Professional and Academic Literature

Overview

Researchers use literature reviews to identify other research on a phenomenon under study (Bressanelli et al., 2019). A literature review addresses other challenges that could be found in developing a framework and what organizations may pursue to overcome those challenges (Bressanelli et al., 2019). A qualitative multiple case study explores strategies that corporate-level IT leaders use to protect against security violations while manufacturers adopt IoT. This literature review provided a critical analysis and synthesis of the professional and academic literature to support all aspects of that exploration.

The research databases that were used for this literature review were IEEE Xplore, Digital Library, EBSCOhost Computers, ScienceDirect, ACM Digital Library, ProQuest Dissertations, and Applied Sciences Complete. Search keywords included

Internet of Things, *the security of IoT*, *Internet of Things adoption*, *security violations*, *privacy violations*, and *IoT strategies*.

This study's literature review contains references from journals and articles that were drawn from different databases. I used Ulrich's Global Serials Directory to verify whether the journals or articles were peer reviewed. I reviewed 410 sources; 228 sources were in the literature review, 391 (96%) were peer reviewed, and 397 (97%) were published within 5 years before the anticipated approval of this study by Walden University's Chief Academic Officer.

This literature review begins with an overview of the process. In the next subsection, I explain the conceptual model, DOI, examining five characteristics of DOI theory, then the DOI theory's five characteristics, focusing on security violations while adopting IoT. The literature review further includes a critical analysis of DOI theory, the use of DOI in research, limitations of DOI theory, analysis of supporting theories, analysis of contrasting theories, an explanation of IoT, a definition of IoT, organizational reasons and benefits for adopting IoT, and IoT security strategies. Additionally, the literature review contains a discussion of the applied IT problem, the need for IoT security strategy, IoT security policy strategies, and security strategies for implementing IoT in the manufacturing industry. Last, I describe the relationship of the literature to this study.

Diffusion of Innovations Theory

Rogers developed DOI theory in 1962 (Hassan et al., 2017). DOI theory indicates that there are five main factors that influence the adoption of an innovation: relative

advantage, compatibility, complexity, trialability, and observability (Rogers, 1962). Relative advantage deals with what will be gained with modern technology or innovations (Scott & McGuire, 2017). Compatibility involves the modern technology adapting to the legacy of existing technology (Scott & McGuire, 2017). Complexity is about how difficult it is to learn modern technology (Pan & Yang, 2019). Trialability refers to the ability to test a modern technology or solution (Al-Habaibeh et al., 2017). Observability refers to the extent to which the technology provides a result (Dohmen & Raman, 2018). I used the DOI theory's five characteristics to highlight IoT technology and gaps that corporate-level IT leaders need to be aware of when developing strategies to protect against security violations while adopting IoT. The results of this research may provide corporate-level IT leaders with security violation information to consider while adopting IoT.

Relative Advantage

Relative advantage deals with what will be gained with modern technology or innovations (Hassan et al., 2017). Organizations need to adapt to new ways of doing business to have a competitive advantage over their competitors. Organizations may have a relative advantage over their competitors if customers feel better than those already in the market (Chen & Zhang, 2016). Chen and Zhang (2016) also stated that gaining relative advantage and reducing privacy concerns are challenges for organizations. For example, manufacturing industries must reduce the security violation concerns of their customers by ensuring that they are protected from security and privacy vulnerabilities (Preuveneers et al., 2017). Reduction of security violations will enhance the rate of use

for manufacturing products such as smart cars and improve the adoption rate for vehicles, thereby providing a relative advantage for users. Corporate-level IT leaders in various organizations consider security violations in adopting IoT because ignoring them could lead to competitors gaining relative advantage over them. A study conducted by Padyab et al. (2019) to explore IoT adoption barriers in four large-scale pilots (LSPs) in Europe indicated that privacy and security are common concerns in organizations in having the relative advantage value of using an innovation.

Relative Advantage and IoT Security

Relative advantage is a crucial DOI characteristic for corporate-level IT organization leaders when considering security violation challenges while adopting IoT. The relative advantage characteristic of DOI is beneficial economically, socially, and competitive advantage of using an innovation (Rogers, 1962). Boamah (2018) described how key stakeholders can be motivated to contribute and support digital preservation management over traditional heritage management in developing countries using DOI's relative advantage. Potential adopters can use the DOI's relative advantage to consider whether digital preservation management is relatively better than other traditional systems for managing cultural heritage resources (Boamah, 2018). Security concerns affect the adoption of innovation and users' perceptions of an innovation's relative advantage over others (Johnson et al., 2018). According to Vaibhav et al. (2019), one of the factors affecting the adoption of IoT and cloud technology is privacy concerns, which affects the relative advantage of these solutions over competing innovations.

Pal et al. (2019) used DOI's relative advantage to test the influence of mobility

and usability in promoting users' trust in the usage of IoT smart wearables. Further, they asserted that security and privacy concerns are two key elements that strongly influence consumers' trust in the wearable platform. For example, security and privacy concerns are among the factors that have affected the end-user penetration of wearable devices, which are predicted to climb from 526 million in 2017 to over 1.1 billion by 2022 as telecom technology transits from 4G to 5G (Pal et al., 2019). In the adoption of IoT in smart cities, privacy and security are common concerns; therefore, the relative advantage of using the innovation needs to be communicated and related to users' situational use (Padyab et al., 2019).

Privacy concerns are another factor that influences DOI's relative advantage. They are among the security violations that necessitate a protection strategy while adopting IoT. According to Padyab et al. (2019), the relative advantage of innovation is personal data protection because privacy is one of the adoption barriers. One of the reasons is that consumers are willing to provide their personal information at the risk of privacy breaches because of their interest in adopting an innovation (Kim et al., 2019). A study by Martín-Ruíz et al. (2018) about using a prototype of smart toys to detect development difficulties in children indicated the benefits of IoT. It emphasized that privacy is a concern, and innovation design must guarantee privacy. Due to rapid growth in innovations such as IoT, addressing the need for privacy to protect personal data should be an important regulatory requirement so that innovations will support an organization's stakeholders (Lodge & Crabtree, 2019). An organization's security and privacy policies will help in making sure that users cooperate in adopting innovation, and

that will build competitiveness and relative advantage over other organizations (Eskridge, 2019).

Compatibility

There is a need to have strategies for protecting against security violations in IoT technology because these strategies make the solution compatible with all of the legacy and existing systems for it to be adopted. The compatibility characteristic of DOI is used to understand how innovation will be assimilated into adopters' lives based on past experiences, existing beliefs and values, behaviors, and what needs are during the adoption of the innovation (Rogers, 1962). Consumers' existing beliefs influence how they accept a solution and their perceived benefit in using the designed technology (Cocosila & Turel, 2019). Gessl et al. (2019) studied the acceptance of artificially intelligent robotics and the psychology of the future elderly. One of the factors affecting adults' acceptance of technology is their experience with other technologies. Therefore, organizations will not be willing to adopt a solution if their experience has been negative. Finally, organizations need requirements while considering adopting innovation, and they must be specific and easily tested (Xi et al., 2016).

Compatibility is one of the critical DOI characteristics when considering security violation strategies while adopting IoT devices because it ensures that technical and functional requirements are designed to include security violation strategies while adopting IoT. Compatibility refers to users' satisfaction in adopting modern technology and includes adapting changes and advancements to information systems (Sebetci, 2018). In the manufacturing industry, manufacturing systems and IT must be compatible with

having positive direct effects on production processes and total impact on the organizational performance of manufacturing systems (Realyvásquez et al., 2019). For example, compatibility plays a significant role in consumers' adoption decisions concerning mobile payment technology acceptance (Ozturk et al., 2017). IoT comes with heterogeneous devices with security violations, and organizations need some security strategies to protect these devices. The heterogeneous IoT devices communicate with each other by exchanging information or data without dedicated hardware (Chen et al., 2019). As organizations introduce strategies to protect against security violations while adopting IoT, compatibility of IoT with existing technologies becomes increasingly important.

Compatibility and IoT Security

Organizational leaders who are considering IoT adoption should consider the compatibility of the innovation and strategies to protect IoT devices against security violations. IoT devices should be compatible with existing nodes; however, the constant connectivity and increasing number of smart devices expose users' privacy and security vulnerabilities (Celic & Magjarevic, 2020). For example, Singh and Shrimankar (2018), in their study about privacy-preserving authentication protocol with secure handovers for the Long-Term Evolution/Long-Term Evolution Advanced (LTE/LTE-A) networks, indicated that LTE/LTE-A standards are compatible with the heterogeneous networks; still, they create new security challenges in the LTE/LTE-A networks. Some solutions, such as physical unclonable functions (PUFs) compared to the current classical cryptographic solutions, are compatible with IoT and can be used to secure IoT devices

(Babaei & Schiele, 2019). According to Guo et al. (2019), having an efficient data protection mechanism is a big issue in having a complex and heterogeneous IoT infrastructure; therefore, security is still a huge challenge as large volumes of data are collected and processed in IoT systems. Therefore, the compatibility of IoT with the existing infrastructure is vital to organizations because it helps in tackling security challenges that come with the adoption of the solution.

Innovations should be compatible with the existing technology while the privacy of IoT users is preserved. Innovations such as IoT, coupled with the integration of heterogeneous devices, solve the compatibility issues but raise IoT users' privacy concerns because of vulnerabilities of their personal information (Celic & Magjarevic, 2020). IoT is compatible with a solution such as a cloud storage environment; however, there is a need to shield the privacy of personal information being retrieved (Riad & Ke, 2018). Organizations adopting IoT have many IoT applications developed and deployed using different IoT standards. However, there should be security mechanisms where issues related to security and privacy are addressed (Ammar et al., 2018).

Complexity

Complexity in DOI highlights the difficulty of adopters learning and using an innovation (Rogers, 1962). Innovation adopters primarily deal with the acceptance of IT and information systems based on perceived ease of use and complexity (Al-Rahmi et al., 2019). For example, Al-Rahmi et al. (2019), in their study of students' intention to use e-learning systems, indicated that when end-users perceive an e-learning system as complex, they tend to have a low intention to use the system. Strategies for protecting

against security violations make IoT complexity minimal so that corporate-level IT leaders can easily adopt the solution. Weidinger et al. (2018), in their study about the context of emergency response processes, indicated that emergency response processes have specific characteristics such as complexity, which result in specific factors that influence the acceptance of the latest information technologies in the firefighting domain. In cloud solution adoption, the complexity of the cloud innovation and diffusion process could make seamless adoption difficult (Choi et al., 2018). This research supports the need for organizations and potential adopters of innovations such as IoT to understand its capabilities and features to avoid any associated complexity, primarily in relation to security violations.

Complexity and IoT Security

IoT security violations, which include the vulnerabilities of IoT devices, make complexity a significant DOI characteristic in this study. Complexity, combined with security challenges, affects the adoption of an innovation (Stieninger et al., 2018). The security requirements that contribute to data exchange between devices make IoT security difficult when being designed as a single solution (Aldosari et al., 2016). Aldosari et al. (2016) further indicated that IoT solutions integrating with cloud and other ubiquitous computing makes privacy issues an urgent concern.

Complexity is related to the user's privacy because of the difficulty in designing a security mechanism to protect the personal information of innovation adopters. According to Ioannou and Vassiliou (2019), the complexity and overhead of security mechanisms make it difficult for security agents to monitor or receive the whole

network's activity in IoT networks, making it easy for attackers to have access to devices on the networks and invade the users' privacy. For example, IoT smart cities have a complex network infrastructure that is prone to security and privacy violations through attacks, such as side-channel, man in the middle, botnets, and cold boot attacks (Shoaib & Shamsi, 2019). Shoaib and Shamsi (2019) further stated that most of these attacks are directed toward user privacy, such as identity theft, inferring sensitive information, and violation of location privacy, creating the need for an effective strategy to address these privacy issues. Therefore, organizations should have a security mechanism to protect themselves from these malicious attacks despite the complexity of IoT solutions (Nurse et al., 2017).

Trialability

Trialability is also an essential characteristic of DOI theory. Trialability defines how easily potential innovation adopters can explore innovation and test-run a solution before adoption (Rogers, 1962). Trials are used to show that the technology functions as expected and meets all the requirements (Elizabeth et al., 2019). Trialability also refers to testing a modern technology or solution (Al-Habaibeh et al., 2017). Having strategies for protecting against security violations in IoT solutions makes it a trialability solution to be tested as a pilot before the overall solution is finally deployed. In Dellinger et al.'s (2018) study about a software program (app) to perform a risk assessment based on data from communities using mobile technology, a pilot test was used to confirm the solution's functionalities before its full acceptance. Kobrakov et al. (2017) had a pilot test of technologies for introducing nanosized silver particles into fibrous materials of

composites with biocidal properties in the manufacturing industry to confirm their acceptance. Organizations that test innovations before adopting them have the benefits of foreseeing the risks in advance and making some conscientious efforts toward mitigating them.

Trialability and IoT Security

Organizations need to test solutions before they are fully adopted, thereby reducing the risk of security violations while adopting technology (Karahoca et al., 2018). Trialability, security, and privacy risk impact perceived ease of use of innovation by adopters, and trialability could be described as the extent to which an innovation may be tested without bias (Karahoca et al., 2018). The trialability of an innovation positively influences how individuals perceive security, and privacy risks negatively influence perceptions of security (Johnson et al., 2018). In IoT security, security mechanism has some challenges that should be tested at different layers of the infrastructure or architecture for security to ensure that the solution meets the requirements (Aldosari et al., 2016). This research supports the need for corporate-level organization IT leaders to ensure that IoT strategies and security mechanisms have trialability.

Observability

Observability is the final characteristic of the DOI theory. Rogers (1962) defined observability as the extent to where innovation results are visible to potential adopters, such as stakeholders. An observability characteristic of DOI is an essential component in adopting innovation because it shows users' perception of the innovation (Rogers, 1962). The need for having strategies for protecting against security violations in the IoT

solution makes it measurable by corporate-level IT leaders as they observe the extent to which the solution has been able to meet business objectives. Observability refers to the extent to which the technology provides the result and the implication (Dohmen & Raman, 2018). Al-Rahmi et al. (2019) stated that observability in innovation such as IoT allows adopters to provide feedback and the visibility to discuss the latest ideas. Karahoca et al. (2018) used DOI observability characteristics to see how the results of adopting IoT in healthcare technology products were made visible to other adopters.

Observability and IoT Privacy

Organizations' corporate-level IT leaders need to use DOI observability to see the extent to which the strategies for protecting against security violations are visible to stakeholders. With the rapid growth of sensor networks, information security and privacy issues are growing. Using DOI observability characteristics, Wang et al. (2019) observed how individual users could see the design-for-testability (DFT) technique that ensures the security of cryptographic chips for sensor networks with extremely low area penalty are performing. Observability creates awareness about certain security violations in organizations. Indrianto et al. (2019) studied smart taxis, highlighted one of the benefits of using IoT as a modification security technique on the taxi helps to secure the taxi and the driver of a crime committed by a person benefits were made visible to stakeholders.

Therefore, the DOI theory supports the need for manufacturing corporate-level IT leaders to have insight into strategies for protecting against security violations and has five components of the theory that align with my research question.

A Critical Analysis of Diffusion of Innovations Theory

This section begins with a discussion of the usage of DOI theory in research. That will include comments about Doi's adaptability to many settings. This section concludes with a discussion on the limitations of the DOI theory.

Usage of Diffusion of Innovations Theory in Research

DOI has been applied in different areas and has gone through many development changes since it was initially developed. Rogers initially developed his theory of how individual decision-making characteristics affect the adoption of innovation around sociology (Abdullah, 2018). IT developers can use DOI to understand how people will accept modern technology such as mobile shopping applications (Natarajan et al., 2018). Similarly, Nehme et al. (2016) used DOI to study the perception of transportation cycling adoption in terms of consistency with existing values, norms, past experiences, and self-perception of future adopters. The authors of that study noted that behavioral and social change might be relevant to transportation cycling for its adoption; therefore, future adopters in a social system should be aware of it because that can as well lead to either acceptance or rejection. Over time, DOI as the unit of adoption has been expanded to include organizations and other social communities. For example, DOI has helped the Organization for Economic Cooperation and Development (OECD) to recognize information systems (IS) as an example of a transformative eco-innovation (Zheng & Jia, 2017). DOI can now be applied heavily in IS regarding quality management. For instance, in the adoption of Enterprise Resource Planning (ERP) in the North American automotive business network, technical compatibility, technical complexity, and relative

advantage facilitated its adoption (Kim & Chai, 2017). DOI is now used to distribute or disseminate information about an innovation or adoption process through mass media channels to reach a large audience of potential adopters (Scott & McGuire, 2017). In the medical field, DOI can implement value-added clinical systems (Gonzalo et al., 2018). The evolution of DOI has been applied in multiple disciplines in both the social sciences and natural sciences. Most importantly, it allows a researcher to see how humans interact with technology and how different social systems are maintained, and privacy violations, which could affect the adoption of the technology (Liu et al., 2017).

DOI is easily applicable and dynamic, thereby making it easy to be adapted in any discipline. As DOI has evolved, it has been used as a lens by other researchers to describe innovation being communicated through different channels to adopters in a social system (Dearing & Cox, 2018). The theory was necessary for this study because strategies for protecting against security violations considered some social and organizational culture that could impact IoT acceptability and adoption. Currie and Spyridonidis (2019) discussed how DOI should align with organizational culture to ensure that employees are engaged in implementing the innovation. The authors further stated that shared leadership in organizations helps develop the necessary skills needed for innovation and promotes its acceptance. Given the similarity to IoT, DOI offers a framework that allows for understanding how heterogeneous IoT devices could be protected against security violations.

Limitations of Diffusion of Innovations Theory

DOI theory is a practical conceptual framework that enables the adaptation of

innovation across different sectors (Allen et al., 2017). Despite these benefits, there are several drawbacks to researchers and organization IT leaders who might consider applying the DOI theory. The criticism of the theory started in the 1970s in international development projects (Rogers, 2003). First, the DOI theory does not consider the factors that affect technology and infrastructure user's acceptability, such as user demographics and psychographic factors (Blut et al., 2016). Second, DOI theory is faced with perceived risks such as loss from users in adopting technical innovation, thereby making their user experience uncertain and anxious (Hubert et al., 2019). Third, DOI theory depends on user perception as one factor driving the acceptance of innovation, which could negatively affect its relative advantage (Wang, Y.-Y., Lin, et al., 2018). Fourth, the DOI theory is dependent on organizations' strategy and beliefs in adopting it (Upadhaya et al., 2018). Fifth, DOI theory adopters are not explicitly designed for an industry like manufacturing; therefore, it does not have specific strategies for organization IT leaders to address security violations while adopting the innovation. According to Rekers (2016), the organizations' settings are different from each other and negatively impact adopting the DOI theory. Sixth, the DOI theory does not address product and location differences that could affect the adoption of an innovation (Rekers, 2016). Seventh, compliance and regulations standards differ between organizations, and DOI theory does not address how compliance and regulations standards could affect the adoption of an innovation. Blind et al. (2017), in their study about the impact of standards and regulation on innovation in uncertain markets based on the German community innovation survey (CIS), stated that standards and regulations have different effects on innovation, which was not addressed

in DOI theory. Therefore, manufacturing industries with effective and efficient IoT standards and regulations may find it easier to diffuse IoT.

In contrast, healthcare industries could struggle to adopt IoT because of a lack of ineffective standards. Eighth, DOI theory was initially targeted to innovators and early adopters without getting to the entire population and nonadopters (Talebian & Mishra, 2018). Nineth, Rogers (2003) highlighted that DOI theory is biased in terms of pro-innovation bias, individuals being blamed for their lack of response in adopting the innovation, lack of consideration of the negative impacts of the theory, and innovation adopters targeting successful innovators. Tenth, DOI theory originated from research institutes rather than the actual adopters, and the research process is not being separated from the innovation process; hence it is process-oriented (Nath et al., 2016). Finally, the DOI theory does not focus on social changes; instead, it focuses on technical changes, individuals, and group changes (Nath et al., 2016).

Analysis of Supporting Theories

There are other theories like DOI that are being used in various research studies. This section discusses three supporting theories: Theory of Reasoned Action; Technology Acceptance Model; and the Technology, Organization, and Environment Framework.

Theory of Reasoned Action

The Theory of Reasoned Action (TRA) was first developed by Martin Fishbein and Icek Ajzen to identify the fundamental relationship between perceived ease of use, users' attitudes, subjective norms, intentions, and actual use of technology and to predict and explain behavior across different areas (Ajzen & Fishbein, 1980). Researchers have

used TRA for identifying the fundamental relationship between perceived ease of use, users' attitudes, subjective norms, intentions, and actual use of technology and to predict and explain behavior across different areas (Buabeng-Andoh, 2018). The first construct of the theory is perceived ease of use because adopters want an IT innovation to be easy to use (Riki - Riki, 2019). Modern technology should not be complex to be adopted by users because that diminishes its relative advantage. In TRA, the intentions and actual use of technology constructs are based on the behavior of the users, and several factors influence such behavior (Hwang et al., 2016). For example, a user who has strong intentions influences his or her intentions to adopt a solution. The attitude construct of the theory determines how the user negatively or positively perceives the innovation (Hwang et al., 2016). Last, the subjective norm refers to the social influence that affects the behavior (Hwang et al., 2016). For example, the wide usage of social media has influenced the adoption of mobile technology.

DOI has some similarities with TRA because both theories have common constructs such as attitudes, subjective norms, and intentions to use a particular technology. A study conducted by Jamshidi and Hussin (2018) about religious obligation and customer awareness in explaining behavior intention and usage behavior of Islamic credit card (ICC) indicated the relationships between DOI and TRA such as relative advantage, compatibility, trialability, observability, attitude, the customer awareness, and acceptance as stronger predictors of intention and adoption of ICC. TRA was not suitable for this study because it does not have complexity characteristics to test the security violation strategies that corporate-level IT leaders use while adopting IoT in

manufacturing organizations.

Technology Acceptance Model

Based on TRA, Fred Davis proposed the Technology Acceptance Model (TAM) for explaining an individual's technology adoption behavior; that perceived usefulness (PU) and perceived ease-of-use (PEU) are the main determinants of an individual's intention to use technology to improve their life and consumption (Davis, 1989). Researchers have used TAM theory for explaining an individual's technology adoption behavior (Sun & Ting, 2019). Perceived usefulness (PU) and perceived ease-of-use (PEU) are the main determinants of an individual's intention to use technology to improve their life and consumption (Sun & Ting, 2019). PU and PEU constructs of TAM theory are further influenced by other external variables such as system features and capabilities of the system (Chen et al., 2017). According to Davis (1989), PU refers to the extent that users believe that a particular innovation will improve their job performance, while PEU refers to the extent to which a user would use the innovation with minimal effort. The two constructs of the theory state that organizations would be willing to adopt a technology that enhances employees' job performance and easy to use.

TAM and DOI focus on user acceptance and adoption of an innovation, and the PEU is like the complexity characteristic of DOI. At the same time, PU is like the relative advantage of DOI. TAM is different from DOI as it is based on the individual user of innovation in line with PU (Sun & Ting, 2019). However, because TAM does not have all the five DOI characteristics that corporate-level IT leaders need in mapping out strategies for protecting against security violations while adopting IoT in manufacturing

organizations, it was not suitable for my study. Hence, I used the DOI theory to address security violations while adopting IoT because the five characteristics highlighted the security violations.

Technology, Organization, and Environment

Tornatzky and Fleischer developed the Technology, Organization, and Environment (TOE) framework to identify the factors that influence innovation adoption at the organization level (Tornatzky & Fleischer, 1990). Researchers have used the Technology, Organization, and Environment (TOE) framework for identifying the factors that influence innovation adoption at the organization level. (Al-Shura et al., 2018). TOE framework was classified into these main groups for innovation adoption, namely technological, organizational, and environmental factors (Kang et al., 2019). The technology construct of the theory refers to the internal and external technologies that might be important in improving the organizations' productivity, and the organizational construct refers to the size of the firm and the complexity of the management structure that affects the adoption of the solution (Kang et al., 2019). The environment construct refers to how the organizations deal with their business partners and competitors (Al-Shura et al., 2018) because it influences the adoption of an innovation.

The TOE framework is like DOI theory because the technology context is similar to DOI relative advantage, complexity characteristics are similar to the adoption of technology, the environment context is similar to compatibility characteristic of DOI, and the organizational context is similar to the relative advantage based on top management support (Al-Shura et al., 2018). The fundamental similarity is that the TOE technology

context is the same as DOI's technology acceptance characteristic and is connected to the five characteristics of DOI. TOE and DOI vary based on their TOE emphasis on the environmental context, including competitive pressure and trading partner pressure factors (Al-Shura et al., 2018); hence, it was not suitable for this study. DOI theory was suitable for this study because this study aimed to explore strategies that organizations corporate-level IT leaders use in protecting against security violations while adopting IoT and did not require the environmental context of the TOE, such as competitive pressure and trading partner pressure factors.

Analysis of Contrasting Theories

This section analyzes other contrasting theories to DOI. The focus is on the Theory of Planned Behavior and The Unified Theory of Acceptance and Use of Technology.

Theory of Planned Behavior

Theory of Planned Behavior (TPB) was proposed by Icek Ajzen and focused on factors that influence individual decision making (Ajzen, 1991). TPB has been used in research to focus on factors that influence individual decision-making (Si et al., 2019). TPB theory can help understand individuals' behavior in adopting modern technology and describes how constructs are related and expose some factors that can hinder the adoption and use of innovation (Hadadgar et al., 2016). The TPB constructs are attitudes, subjective norms, perceived behavioral control, and intentions (Lo et al., 2019). Attitudes influence the behavioral intentions of users adopting a technology. Subjective norms help predict how adopters will use the technology, and perceived behavioral control

determines the ability of adopters to use the technology (Cheng, 2019).

These four constructs relate to four characteristics of DOI theory except the complexity characteristic of DOI used by innovation adapters to determine the acceptance of IT and information systems based on perceived ease to use (Al-Rahmi et al., 2019). Therefore, TPB was not suitable for this study because it does not have complexity characteristics for testing corporate-level IT leaders' strategies while adopting IoT in manufacturing organizations.

The Unified Theory of Acceptance and Use of Technology

The Unified Theory of Acceptance and Use of Technology (UTAUT) has been used extensively in information systems (IS) and other disciplines to study individual technology acceptance across a variety of settings such as organization types and several types of technologies (Venkatesh et al., 2016). UTAUT stated four moderators: gender, age, experience, and voluntariness, and has been used so much in explaining the adoption of technologies by individuals (Dwivedi et al., 2019). For example, organizations may force all employees to use an adopted innovation, but such a mandate will not apply to voluntariness as a moderator (Dwivedi et al., 2019). Furthermore, UTAUT is focused on performance expectancy, effort expectancy, social influence, and facilitating conditions (Dwivedi et al., 2019). The performance expectancy construct refers to the degree that users will have confidence that the technology will offer performance gains during usage (Iskandar et al., 2020). Effort expectancy refers to the ease of use of the technology to reduce time spent in activities (Iskandar et al., 2020). Social influence and facilitating conditions refer to the level of trust in the society that convinces adopters to use the

technology (Iskandar et al., 2020).

DOI was suitable for my research study because it was focused on five characteristics for innovation, namely: relative advantage, compatibility, complexity, trialability, and observability for strategies to protect against security violations while adopting IoT. Another reason UTAUT was not suitable for this study was that it was focused on individual experience. In contrast, DOI was focused on an organizational level that does not need voluntariness as a moderator for accepting the strategies to protect against security violations while adopting IoT (Dwivedi et al., 2019). Finally, there is a lack of integration of the UTAUT moderating variables, which affects the adoption of an innovation.

Analysis of Internet of Things

This section begins with an explanation of IoT. Then, the focus is on defining IoT and the organizational reasons or benefits for adopting IoT. The section further discusses IoT security strategies focusing on the need for IoT security strategy, IoT security policy strategies, and security strategies for implementing IoT in the manufacturing industry.

Explanation of IoT

IoT is an emerging technology where devices are connected to exchange data using embedded sensors. This research defines IoT and the organizational reasons or benefits for adopting IoT. IoT as modern technology provides services to many organizations and different sectors of the economy with the seamless integration and connection of devices over the internet (Čolaković, & Hadžialić, 2018). The IoT can be used in everyday life with smartphones, wearing devices, household appliances, sensors,

multimedia devices, and control devices (Coskun et al., 2018). IoT offers services in manufacturing, such as provisioning of manufacturing assets, maintenance and repair, and operations (Ehret & Wirtz, 2017). IoT devices that provide these services are heterogeneous, giving rise to many security issues (Yousuf & Mir, 2019). Therefore, there is a need for corporate-level IT leaders to have strategies that may help these IoT devices to be protected against sophisticated attacks in the manufacturing process while adopting IoT (Simranjeet et al., 2019). Understanding the concept of IoT explains the need for exploring the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry.

Definition of IoT

IoT is a technology where devices relate to each other to exchange data using embedded sensors. According to Bendavid et al. (2018), the IoT concept finds its roots in the last decade of the 20th century with the vision of ubiquitous computing and the underlying idea that any object can be equipped with technology to become a computing device. IoT is described as an ecosystem where ordinary objects around us like phones, cars, clothing, appliances, and even food are communicated and connected through the internet using smart processors to collect and exchange data (Roxana & Mircea, 2016). IoT, coupled with digitalization and automation of industrial manufacturing, has initiated the latest industrial revolution, and the purpose is to transform existing industries' intelligence by introducing self-maintainability, self-optimization, self-cognition, and self-customization into the industry (Lampropoulos et al., 2019). IoT refers to internet connectivity beyond devices and includes radio-frequency identification (RFID) tags,

smartphones and tablets, and other heterogeneous devices (Atzori et al., 2017). Many IoT devices operate with WiFi or similar technology and other industrial, scientific, and medical equipment operating at different frequencies (Chi et al., 2019). IoT devices are interconnected to the network, and the historical information of these devices is stored in the database (Noguchi et al., 2019). IoT devices on the network use Internet Protocol (IP) addresses to communicate and transfer data over the network without human intervention to generate integrated data (Kokila et al., 2019). Understanding the definition of IoT explains the need for exploring the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry.

Multiple technologies and frameworks may be used for IoT. IoT is a technology that enables the interaction of different devices for the exchange of data and information (Andriole, 2019). IoT includes IoT devices that are connected and embedded with sensors or communication devices through the internet, such as smartphones, smart car and mobility, smart homes, smart industries, and applications that help individuals or organizations effectively and efficiently (Roopa et al., 2019), and the inclusion of smart healthcare services coupled with smart computed tomography scanners can be employed to produce a considerable flow of statistics for investigation and visualization purposes (Dobson-Lohman, 2019). According to Das et al. (2018), IoT is a physical system and virtual objects connected to exchange data and information over the internet. IoT is a paradigm where wireless sensors or wireless technologies and actuators connect to provide the connectivity of various fixed and mobile system components to achieve desired goals (Burg et al., 2018). Some of the characteristics of IoT include the

integration of various heterogeneous devices for identifying, sensing, networking, and computation processes (Čolaković & Hadžialić, 2018) and works well in a cross-technology environment that has ubiquitous and pervasive computing (Jiang et al., 2019). IoT includes Internet eco-system devices that the sensors are divided into hardware, software, development, and data integration environments (Lu, 2018). Organizations could decide to adopt IoT because of the rapid growth of smart devices connected over the internet.

IoT is built on several standards that inform the decisions of some organizations to adopt it or not. IoT device manufacturers and the research community introduced some standards that will enhance their efficiency and effectiveness; however, adopting these standards in different IoT applications may pose some challenges (Nikoukar et al., 2018). Nonetheless, Nikoukar et al. (2018) noted that applying these standards in various application domains is suitable and meets the requirements of IoT applications. The whole idea is to have a common platform where heterogeneous IoT devices can communicate with each other. For a broader adoption of IoT, there is a need to standardize key interoperability to tackle the challenges concerning multiple layers of the end-to-end protocol (Gazis, 2017). Therefore, it is necessary for organizations that want to adopt IoT to implement the standards required for its adoption.

IoT comes with various standards that organizations may use for its successful adoption, and it has standards for different layers in the overall architecture. The IoT structure is as follows: perception layer standards, transmission layer standards, computation layer standards, application layer standards (Trappey et al., 2017).

Organizations considering adopting IoT need to consider these established standards based on these layers. Organizations have been using standards like radio frequency identification (RFID) technology supported by Electronic Product Code EPC Class1 Gen2 standard to track assets and products and identify electronic tags in real-time (Segarra et al., 2017). Other standards like Long Range Wide-Area Network (LoRaWAN) and DASH7 use unlicensed frequencies and are available globally (Ayoub et al., 2019). Despite the standards, IoT using IoT device sensors has been a valuable tool in tracking assets and products using barcodes and electronic tags.

Organizations consider IoT when they are interested in having IoT devices that may help in information transmission and communication. IoT is a powerful technology that contains these crucial factors: information recognition, the transmission of confidence, and application of information, recognition use of RFID, sensors, QR codes to capture the dynamic information of objects wherever they are (Pan & Yang, 2019). IoT, with the functions of sensing, identification, transmission, monitoring, can be applied to achieve intelligent, scientific, and efficient outcomes (Chen & Yang, 2019). Another determinant factor for organizations in considering the technology that communicates between IoT devices is location. To address network onboarding schemes of IoT devices is the use of WiFi Alliance as a standard for organizations (Lee et al., 2019). Managing network onboarding issues may require some organizations to limit the number of devices to the IoT network; however, organizations may derive the full potentials of IoT by ensuring its availability through the internet.

IoT's ability to connect is one of the things organizations must keep in mind while

adopting IoT. That connectivity should be flexible and agile to ensure robust and scalable network performance (Silva et al., 2019). IoT interconnected devices can be managed locally by having the IoT platform run in the same environment as the devices or remotely. The platform controls the devices in different networks and requires registration of those devices during connection (Silva et al., 2019). IoT uses identifiers to uniquely assign addresses to the connected heterogeneous devices on the network. These identifiers are grouped into object identifiers, communication identifiers, and application identifiers (Aftab et al., 2019). IoT devices use object identifiers (OIDs) to be uniquely identified, and it is equivalent to a MAC address for a computer. Global standard-driven connectivity helps manage these IoT devices from different manufacturers (Yun et al., 2016). The OIDs are the physical or virtual objects that include barcodes and RFID identifiers but cannot address or communicate (Aftab et al., 2019). However, the OIDs are used to address the interoperability issues of heterogeneous interindustry identification systems as they have other product information (Aftab et al., 2019; Yun et al., 2016). OIDs are managed in a tree-like hierarchical manner to assign unique numbers, thereby ensuring no duplicates (Yun et al., 2016). In the area of IoT devices, IPv6 is a communication protocol and an enabler for IoT. It uses application protocols like multicast Domain Name System (mDNS), Remote Procedure Call (RPC), and Message Queue Telemetry Transport (MQTT) protocol to communicate and exchange data among each other (Feldner & Herber, 2018). Therefore, connectivity between IoT devices is like computers connected in a local area network (LAN) environment.

The adoption of IoT for organizations depends on the devices and the extent to

which they intend to use the technology because it has many advantages and capabilities. IoT devices have embedded sensors, actuators, processors, and transceivers that can sense, track, automate, and control objects (Sethi & Sarangi, 2017). IoT is being used in many organizations and applications for intelligent transportation systems (ITS), location-based services (LBS), and sensing techniques and applications (Chen & Lo, 2018). IoT utilizes the heterogeneous road monitoring tools that measure, and send the traffic information, vehicle speed to the traffic management entity (Abualsaud et al., 2019). Smartphones are widely used as a device in IoT because they can be effectively used in diverse ways. For example, the IoT applications have utilized the proposed IoT platform to provide smart IoT services in the areas of smart manufacturing for the manufacturing industry by using smartphones and other devices to drive manufacturing efficiency in factories and supply chains (Georgakopoulos & Jayaraman, 2016). Therefore, organizations protecting against security violations may drive efficiency while adopting IoT.

Organizational Reasons for or Benefits of Adopting IoT

There is a rapid growth of IoT technology. While some IoT consumers are excited about that solution, others still doubt its acceptance, primarily due to security violation concerns. It is estimated that IoT will be worth $3 trillion by 2025, with over billions of heterogeneous devices connected to the Internet (Hoffman & Novak, 2018). IoT devices may affect people's lifestyles and industry practices. IoT will impact the way people live and work, and it will get into smart cities, smart car and mobility, smart homes, assisted living, smart industries, public safety, manufacturing, energy consumption, location of

incidents, agriculture, tourism, and other ecosystems (Hassan & Awad, 2018). Many business sectors may use IoT devices for tracking assets, security monitoring, supply chain management activities, energy conservations, and building the database of customers (De Cremer et al., 2017). For example, in manufacturing, the IoT has helped the industry create business opportunities by making their products, services, and customer data available because of interconnected devices over the Internet (Sayar & Er, 2018). IoT is a new trend in technology and has proven to positively impact our society, personal lives, and industries and transform a lot of technologies.

Many industries have so far adopted IoT because it provides opportunities to improve efficiency and productivity, ensuring real-time tracking of assets, helping with data analytics to make informed decisions and proper monitoring of activities.
The manufacturing industry is now focusing on data analysis from the entire production line based on the amount of data generated by IoT to make informed decisions (Lade et al., 2017). Also, when data are collected from various IoT sources and combined with data from other sources of big data analytics, strategic decisions are made that may have some economic, social, ecological, and environmental implications (Kshetri, 2017). In many organizations, having IoT-based software coupled with IoT sensors may help deliver enhanced customer service and improve business management procedures by monitoring business operations and the ability to track products and employees (Antoniou & Andreou, 2019). Therefore, IoT may help organizations improve efficiency and productivity, big data analytics, and monitor business operations.

IoT offers many benefits in other sectors such as agriculture and healthcare

through its interconnected devices. IoT may enhance the efficiency and safety of production and management of modern agriculture and provide a monitoring system for agricultural products (Liu et al., 2019) and enhance the usage of health management systems through the supply of smart healthcare services by providing healthcare facilities to the patients residing in secluded regions (Dobson-Lohman, 2019). IoT also provides the opportunity to remotely manipulate home appliances such as heating systems, ovens, and blinds using computers and mobile devices (Cruz et al., 2019). Furthermore, based on big data collected from medical IoT called smart health, there is the potential of diagnosing gallbladder stones through their characteristics, and treatment of gallbladder stones can be recommended (Yao et al., 2019). Organizations that engage in civil infrastructure management may benefit from IoT adoption by understanding organizational, and business process changes, developing new capabilities, data provenance and standardization, and proper interpretation of data generated by the technology (Brous et al., 2019). IoT, coupled with smart objects interacting with other objects and possess information processing abilities, may help organizations foster relationships and trustworthiness between employees and management through information sharing and reliable and trustworthy networking solutions utilizing the social network of friend objects (Roopa et al., 2019). IoT's smart cities enable urban development, and organizations will have more automated processes and efficient ways of conduction their businesses.

The manufacturing industry data generated from connecting IoT devices can provide the information needed to stay competitive by applying analytics and artificial

intelligence to improve operations' efficiency, safety, and flexibility (Stracener et al., 2019). Those factors may be further achieved by connecting IoT sensors and computing infrastructure in the manufacturing industry shopfloor to automate processes (Upasani et al., 2017). For example, IoT will make it possible for the manufacturing industry to create a range of independent products by having production interconnected with other devices (Caputo et al., 2016). Smart services, being a data-driven service used in IoT, can be used for the manufacturing industry to improve value creation and profitability for both the business and customers (Kaňovská, & Tomášková, 2018), thereby promoting the need to have intelligent manufacturing environments and smart factories (Lampropoulos et al., 2019). Other benefits of IoT include manufacturing assets, maintenance, and repair (Ehret, & Wirtz, 2017). More benefits of IoT include operation efficiency, having innovative information and analytical services, and new services aimed at end-users by unifying them with the manufacturing and supply chain ecosystem (Ehret, & Wirtz, 2017). With the use of data extracted from machines connected to IoT, the manufacturing industry can monitor discrete variables of different machines to analyze performance using a virtual environment running synchronous to plant floor equipment (Saez et al., 2018). IoT enables real-time monitoring of energy efficiency on manufacturing shop floors and data envelopment analysis techniques to detect abnormal energy consumption patterns and quantify energy efficiency gaps (Tan et al., 2017). IoT will further reduce waste on the manufacturing shop floor through real-time waste monitoring and analysis, thereby increasing efficiency (Yen Ting et al., 2017). The ability to drive efficiency optimization to offer better products, quality, and services by

connecting services and operations globally contributes to the numerous IoT-related manufacturing solutions.

In many cases, organizations using IoT may improve efficiency and productivity, especially in the manufacturing industry. Plant managers in manufacturing may spend time on other plant operations because IoT performs real-time resource status monitoring and dynamic scheduling that manipulates production schedules dynamically to maximize production outputs with limited resources (Yang et al., 2019). The IoT-enabled real-time scheduling in the manufacturing process helps in the predictive-reactive approach and ensures information about manufacturing resources on the shop floor (Wu et al., 2019). IoT may offer plant workers a reduction in unplanned downtime and offers real-time condition monitoring of machines, thereby detecting early any unwanted deviation to shift the failure category from unplanned to planned (Seetharaman et al., 2019). IoT will help in addressing some production deficiencies in the manufacturing process that would have required human interventions. IoT will help in acquiring data and information in real-time to facilitate dynamic just-in-time (JIT) manufacturing to enhance manufacturers' competitiveness through inventory and lead time reduction (Xu, & Chen, 2016) and will enhance intelligent processing and optimal control of manufacturing resource information and product information by enabling quality information of the service, such as response time, cost, reputation and success rate (Dong et al., 2018). The IoT as advanced technology has helped manufacturing industries in cost reduction, such as operations cost, through efficient manufacturing and supply chain process. It takes a shorter time for products to get to the market. Also, the technology ensures in the

manufacturing industry that products get to people who need them through analysis of data collected from IoT connected sensors and enhances safety in the workplace through wearing devices that monitors worker's health state.

Internet of Things Security Strategies

IoT network has wireless technology with wireless sensor networks (WSNs) that enable IoT devices to communicate remotely. These WSNs are essential components of the IoT for event monitoring and information gathering (He et al., 2019). However, these wireless networks are often vulnerable to security issues such as a denial of service (DoS) through man-in-the-middle (Burg et al., 2018). These vulnerabilities are like the ones found in most computer networks. Since IoT is an emerging trend in technology that generates big data, these vulnerabilities are higher and pose a big challenge for organizations to mitigate security violations. Strategies that will be needed to protect the WSNs from security violations include but not limited to changing the administrator default passwords of the wireless access points, restrict access to only allow authorized users of IoT networks, and encrypting the wireless data to prevent anyone on the IoT network with viewing access, except it is decrypted (Cybersecurity and Infrastructure Security Agency, 2019). Therefore, there is a need for corporate-level IT leaders in the manufacturing industry to consider those strategies to protect WSNs on IoT networks against security violations while adopting IoT.

In the manufacturing industry, physical IoT security issues such as theft of the IoT devices in an IoT-enabled environment include employee's removal of storage media, and sometimes terrorist attack poses a significant risk. As more data are stored in IoT

embedded devices, it increases the effectiveness of physical attacks such as loss of embedded devices like mobile phones and personal computers (Zhang &Yang et al., 2019). According to Makhdoom et al. (2019), IoT devices' vulnerabilities could be a lack of physical security, host-based defense, software updates, and security patches. According to the authors, other devices' vulnerabilities are lack of access control measures, cross-device dependencies, lack of IoT-focused attack signatures, and physical compromise by unauthorized employees. Exposure of the IoT devices to these attacks affects the manufacturing industry from adopting IoT. Strategies such as having an effective access system and video might help corporate-level IT leaders to protect against that kind of security violations while adopting IoT in the manufacturing industry.

IoT is faced with cybersecurity violations that could be classified into data privacy and anonymity, identity verification and authentication, and confidentiality, data integrity, and availability (CIA) (Alotaibi, 2019). Strategies such as data privacy and anonymity will ensure no access to confidential information by the public or malicious attacker (El-hajj et al., 2019). The second strategy has access control or authorization that determines whether an entity such as a user or device can access resources and control the devices or actuators and identity verification to identify an entity (Kim, & Lee, 2017). The third strategy is having a confidentiality, integrity, and availability triad. Confidentiality entails having a set of rules to limit unauthorized access to certain information. Integrity involves providing reliable and trustworthy data, and availability ensures that a fully functioning internet-connected environment is in place and devices are available for collecting data, thereby preventing service interruptions (Mosenia, &

Jha, 2017). The fourth strategy is preventing unauthorized access to the IoT device, which is necessary to prevent most of the security violations in the IoT environment. Therefore, corporate-level IT leaders need proper access management protocol as a security strategy while adopting IoT in the manufacturing industry.

As IoT technology continues to grow and is an emerging trend in technology, many security violations come with it. IoT adoption suffers from several security violations that are challenging when compared to other technologies because of its complex environment and resource-constrained IoT devices (Kouicem et al., 2018). These security violations have been a deterrent factor for corporate-level IT leaders to adopt IoT in the manufacturing industry. One of the reasons is the lack of strategy to protect against these security violations, hence the need for strategy.

The Need for IoT Security Strategy

Manufacturing industry corporate-level IT leaders who need to adopt IoT should explore so many strategies to ensure no security violations. For example, Zarpelão et al. (2017), in their survey of intrusion detection systems (IDS), classified IDS according to the following attributes: detection method, IDS placement strategy, and security threat and validation strategy. Harbi et al. (2019) proposed addressing authentication and key management security issues such as replay attack, denial of service attack, impersonation attack, and lack mutual authentication and session key agreement. In the health sector, to ensure the security of client data such as Electronic Patient Records (EPR), Kaw et al. (2019) proposed having a reversible data hiding approach as a strategy for securely embedding EPR within the medical images using Optimal Pixel Repetition (OPR).

Kshetri (2017) highlighted the need to use blockchain to contain an IoT security breach in a targeted way after it is discovered. Bendavid et al. (2018) highlighted the need to increase security and prohibit unauthorized access in IoT applications through tag-reader mutual authentication protocol with various security techniques such as cryptosystems commonly divided into two groups: one-way and two-way. The application of these strategies might help corporate-level IT leaders in adopting IoT in the manufacturing industry.

Compared to computers and other peripherals on the network, IoT devices are more vulnerable to security violations because of the number and their heterogeneous nature. There is a need to have robust, secured strategies to detect any data injection or malicious attack before it causes some data breach and affects data integrity (Arwa et al., 2018). A data breach involves the malpractice of having unauthorized access to personal information belonging to various stakeholders within the organization, thereby compromising the confidentiality, integrity, and availability of sensitive data (Wei et al., 2019). Security breaches and violations have been serious concerns to organizations because of the negative consequences that come with it, like reputational effects. Data security breaches are on the rise and impact an organization's financial performance, and management must ensure that they have a strategy to mitigate these effects. (Xu et al., 2019). Xu et al. (2019) referenced a study that stated there were 1,776 reported data breach incidents in the United States of America and many more that were not disclosed. Those data show that the need for corporate-level IT leaders to have a strategy to protect against security violations while adopting IoT cannot be overemphasized.

IoT Security Policy Strategies

Organization corporate-level IT leaders have a security policy as a guide to prevent and mitigate security breaches (Amankwa et al., 2018). Security policy in an organization is a document that contains the requirements or rules that are applied to prevent IT infrastructure from threats or attacks (Amankwa et al., 2018). Effective security policy requires employees' commitment to compliance; therefore, information security awareness and education will be required and help mitigate information security issues (Sohrabi et al., 2016). Protecting the IT infrastructure requires humans and technology to work together to ensure that is accomplished. For example, an employee who refuses to comply with organization's policy on avoiding scam emails or use strong passwords may expose or endanger his or her organization's data assets to attacks or threats; therefore, any technical measure put in place will be ineffective if such an employee exists within the organization (Ifinedo, 2016). Thus, for effective IoT adoption, corporate-level IT leaders should have a security policy as one of the strategies that will limit IoT devices' vulnerabilities. Also, there is a need to train employees on the importance of security policy.

Effective security policy requires some enforcement from the management. Paliszkiewicz (2019) surveyed how leadership and trust influence the enforcement of security policy. The study found out that trust based on competence, benevolence, and integrity map helps leaders enforce an organization's information security policy compliance. Also, Ifinedo (2016) study revealed that top management support and beliefs, sanction severity, and cost-benefit analysis play substantial roles in how

employees comply with information systems security policy. Therefore, organization corporate-level IT leaders in the manufacturing industry considering IoT adoption must consider the adoption and enforcement of security policy to ensure enforcement of the strategies that are needed for preventing security violations in their organizations.

Security Strategies for Implementing IoT in the Manufacturing Industry

IoT has already made its way into the manufacturing industry with a high rate of embedded sensor devices connected to the Internet that enhance real-time monitoring of machine activities. Despite these benefits, there are still some security challenges. For example, according to Cruz et al. (2019), many manufacturers have hundreds of devices on the IoT network that have ignored patching these devices, which has led to some security issues that cannot be addressed after the devices have been deployed. The strategy that corporate-level IT leaders can use to protect against those security violations is to periodically check IoT device manufacturers' websites to ensure that IoT device patches are current and run the latest and most secure firmware updates (U.S. Department of Justice, 2017).

The widespread IoT devices in manufacturing IoT networks expose the critical infrastructure and customer data to security threats and attacks by malicious attackers (Preuveneers et al., 2017). The strategy that corporate-level IT leaders can use to protect against such security violations is to keep passwords complex and unique for each device and router and segment the entire IoT network (U.S. Department of Justice, 2017). Also, the corporate-level IT leaders can adopt user and device authentication techniques as another strategy that will help ensure that the IoT data in the systems are only accessible

to authorized individuals (Sun et al., 2019).

Manufacturing industry corporate-level IT leaders during the adoption of IoT are exposed to attackers causing unsafe remote monitoring systems for machine tools through IoT devices (Tedeschi et al., 2016). The security violation strategy is having the IoT network's routers equipped with a built-in firewall that should be enabled (U.S. Department of Justice, 2017). IoT devices are exposed to security violations during acquisition in the manufacturing industry because some are not embedded with security features; hence they are exposed to vulnerabilities and risks (Hoffman, 2019). Corporate-level IT leaders should ensure that they acquire IoT devices from the manufacturer who takes cybersecurity seriously; for example, if the IoT device uses a password, they should make sure that the password can be changed (U.S. Department of Justice, 2017).

The manufacturing industry's adoption comes with big data coming from the devices that could create data integrity issues. The interconnection of machines using computer integrated manufacturing (CIM) to the IoT could lead to big data vulnerable to malicious attacks (Shafiq et al., 2018). Corporate-level IT leaders should ensure that they purchase IoT devices from manufacturers that are EU General Data Protection Regulation compliant; that regulation makes sure that manufacturers build data protection into their devices in the design process (Tedeschi et al., 2016). Again, having another strategy such as a security solution well designed to force the hackers to give up before they succeed, such as having a security guarantee of RFID from vendors that will ensure the privacy of RFID and WSNs devices (Li et al., 2016) will be needed by corporate-level IT leaders to protect against that kind of security violation. For example, according

to Hassan and Awad (2018), when considering the social impact of IoT security violations, there is a need to have legislation and international laws to ensure the personal right to privacy.

Manufacturing organizations' IoT adoption comes with heterogeneous devices and sensors connected that could open the door to eavesdropping, malware, denial of service (DoS) attacks, and user profiling (Sun et al., 2019). As a strategy, corporate-level IT leaders should ensure that they have antivirus and intrusion detection software products to protect IoT devices (U.S. Department of Justice, 2017).

IoT adoption comes with real-time information that helps organizations decide based on big data generated by IoT sensors and systems (Gutschow, 2019). Some real-time privacy-preserving approaches in sensors like blob sensors that collect shared data can be counter-productive in organizations because they put computation overhead to the ambient sensors (Ding et al., 2019). Therefore, organization corporate-level IT leaders need a strategy that will ensure that manufacturing industries focus more on privacy-preserving sensors despite the computational costs associated with them, depending on the shared information (Ding et al., 2019) protect against security violations.

Manufacturing industry corporate-level IT leaders adopting IoT are engaged in integrating applications as part of the solution, which comes with security challenges (Henk-Jan van Roekel, & Martijn van der Steen, 2019). There is a need for corporate-level IT leaders to have a strategy for managing the complexity encountered during the integration of applications to protect against security violations (Henk-Jan van Roekel, & Martijn van der Steen, 2019).

Manufacturers adopting IoT adoption might need to be transmitting sensitive information between different entities of IoT, and there could be security violations while performing such transmission (Wang et al., 2018). Having a strategy such as attribute-based encryption to protect the associated data based on users' preferences to protect user's privacy and getting individual consent before disclosing their data is essential (Hernández-Ramos et al., 2018).

In general, manufacturing industry corporate-level IT leaders, while adopting IoT and protecting against security violations, should ensure that their employees have advanced cybersecurity education and training programs to defend critical systems and sensitive data against emerging security threats and attacks (Ficco & Palmieri, 2019). Employees should be trained on security violations at least once a year to create awareness of the need for protecting against them. Last, corporate-level IT leaders should ensure full enforcement of access management policy so that the attackers will not have unauthorized access to employees' personal information and organizations' sensitive data.

Relationship of Literature to This Study

This research study included the literature review relating to corporate-level IT leaders' strategies to protect against security violations while adopting IoT in the manufacturing industry. IoT concept found its way in the last decade of the 20th century and still an emerging technology that offers so many benefits to consumers and adopters in various industries. IoT benefits include expanded usage of smart cars, smart industries, and smart meters that enable the public to save on fuel and preserve natural resources.

However, vulnerabilities in IoT devices are a concern, and the research supports the need for effective strategies to protect against security and privacy violations.

According to the research, some manufacturing industries have hundreds of devices on the IoT network that are not being regularly patched, leading to some security issues. The widespread use of IoT devices in manufacturing IoT networks exposes the critical infrastructure and customer data to security threats and attacks by malicious attackers (Preuveneers et al., 2017). According to researchers, organizations that are considering adopting IoT need to develop strategies that will protect against security violations to ensure that the security and privacy risks that come with the adoption are mitigated. IoT devices' vulnerability leads to security threats causing customers' personal information to be compromised (Wei et al., 2019). If these security threats and violations are not addressed, organizations could suffer some reputational loss, and competitors may take full advantage of their situation (Xu et al., 2019). Therefore, there is a need for corporate-level IT leaders to have a firm security violation strategy that will enhance IoT adoption. Some of the strategies identified in research studies are having a security policy that the management will enforce to limit the vulnerabilities of IoT devices, having IDS placement and validation strategies such as firewalls and DMZ, employee training on information security and IoT devices regulations that are meant to protect employees' privacy violations on the shop floor and other areas in the manufacturing process.

The conceptual framework in this literature review is DOI theory because the five characteristics align with the benefits and challenges of having strategies to protect against security violations while adopting IoT. The benefits include the relative

advantage of having the IoT security violation strategy for a new IoT innovation. The compatibility characteristic benefit is that the strategy aligns with existing security policies. Next is the complexity characteristic by having the security strategy that will not be difficult to learn while adopting IoT. The trialability characteristic benefit is testing the security violation strategy on the adopted IoT solution. Finally, the observability characteristic will be beneficial to examine the extent to which the security violation strategy provides the result and the implication. There are some limitations to DOI theory, like DOI theory not considering the factors that affect technology and infrastructure, but it aligns well with my research question. Some theories are like DOI theory, such as TRA, TAM, and TOE, and some contrasting theories like TPB and UTAUT. The various components of the literature review highlighted the need for organizational corporate-level IT leaders in manufacturing to have a workable strategy that will protect security violations while considering IoT adoption.

Transition and Summary

Section 1 included the background of the problem that described the benefits of IoT and the security violations associated with IoT adoption in the manufacturing industry. It also stated the problem, the purpose, and the relevance of this study in exploring the strategies that corporate-level IT leaders use to protect against security violations while adopting IoT in the manufacturing industry. I included the literature review relating to corporate-level IT leaders' strategies to protect against security violations while adopting IoT in the manufacturing industry.

Section 2 includes the role of the researcher that describes the expectations of the

researcher in this study, the participants, the research method and design, population and sampling, ethical research as it relates to this study, data collection and analysis techniques that will be used in this study on security violation strategies while adopting IoT and how to ensure the reliability and validity of the collected data.

Topics to be discussed in Section 3 are the overview of this study, presentation of the findings, applications to professional practice, implications for social change, recommendations for action, recommendations for further study, reflections, and summary, and the conclusions of this study.

Section 2: The Project

Purpose Statement

The purpose of this qualitative multiple case study was to explore the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry. The population consisted of at least two corporate-level IT leaders who had been involved in strategies to protect against security violations while adopting IoT in at least three manufacturers in the eastern United States. The implications for positive social change include corporate-level IT leaders having strategies to protect against security violations in IoT devices. This study may lead to increased trust by the public that personal data will not be compromised, leading to greater use of IoT. Greater use of IoT will have myriad societal benefits, including fuel and cost savings resulting from greater use of smart cars (Aekarat et al., 2019; Miller, 2018) and more efficient resource consumption through increased use of smart meters (Spano et al., 2015).

Role of the Researcher

I was the primary instrument for data collection for this study. In qualitative research, the researcher is often the main instrument in the data collection process (Pezalla et al., 2012). In a multiple case study, researchers are responsible for (a) choosing the study design, (b) developing interview questions, (c) creating rapport with the participants, (d) using open-ended questions during semi structured interviews, (e) clarifying participant responses, and (f) not allowing personal bias in data collection and analysis (Karagiozis, 2018; Springer et al., 2018). As the primary researcher in this

qualitative multiple case study, I had the role of exploring differences within and between cases, designing the study, developing interview questions that would address my research question, collecting and organizing data, and analyzing and interpreting data.

As the primary instrument, I mitigated bias by focusing on my sources of bias, presented my findings from the participants' perspectives, and ensured that results met the standard expected of a qualitative research study. A researcher should recognize and monitor bias, be transparent about the phenomenon being studied, and not exert undue influence on participants and processes (Peterson, 2019).

I have been an IT professional for more than 15 years without any considerable experience in IoT. However, having worked in the manufacturing industry for 2 years as an IT professional, I have been exposed to IoT concepts and have developed an interest in this topic after reading scholarly journals about IoT devices and lack of security. I developed an interest in this topic because I visited five manufacturing plants and noticed how their IoT devices were connected. I asked how some of the plant managers had managed to protect against security violations while adopting IoT. The responses showed that they did not have enough strategies in place. The managers to whom I talked in those five plants were not participants in this study. Researchers' experience in the phenomena of interest in their studies can bring deeper insights into the work and introduce bias in qualitative research (Pagan, 2019). Because I had little knowledge and experience in IoT, my prior IT experience did not introduce bias, in that I did not fully understand the strategies needed to protect against security violations during IoT adoption.

Before proceeding with this study, I received approval from the Walden

University Institutional Review Board (IRB), which ensures that research is conducted ethically. The IRB handles full compliance with the relevant regulations and ensures that no financial conflict of interest exists between researcher and participants (Clapp et al., 2017). Having a good rapport and relationship with participants helps a researcher ensure that reliable data are gathered (Pinnegar & Quiles-Fernández, 2018). My participants were corporate-level IT leaders working in manufacturing organizations other than the one I work for, which further mitigated the possibility of bias in my study.

I observed all relevant ethical rules in this research during the interview and data collection processes. There is a need to consider ethical issues in research study design and data collection, as well as to assure that participants are fully informed and protected (David, 2017). The Belmont Report has three basic ethical principles and guidelines for researching human subjects (U.S. Department of Health & Human Services, 1979). As a researcher, I understood and followed those ethical principles during data collection. The ethical principles for researchers are (a) respect for persons, which is based on allowing individuals to make their own decisions and accommodating vulnerable persons who need additional protection; (b) ensuring that participants are not harmed; and (c) making sure that all participants are treated equally and fairly (Miracle, 2016). I completed the National Institutes of Health Office of Extramural Research training course (Certification Number 2822658) to protect human research participants (Appendix A).

I used an informed consent form to ensure that my study adhered to The Belmont Report principles. The informed consent form was a measure to protect research participants based on Belmont Report principles, and the participants signed it. The

consent form included a detailed description of the research procedure and a statement that participation was confidential, voluntary, and without reprisal if the individual chose not to participate at any point. An informed consent form should include a research procedure and the right of participants to withdraw at any time without reprisal (Miracle, 2016).

Researchers can have various intentional or unintentional biases that can influence the outcome of a qualitative research study and result in misrepresentation of the true experiences of participants (Wadams & Park, 2018). Research outcomes must represent the participants' perspectives and experiences based on the research questions and not on the researcher's conscious and unconscious biases, perceptions, and perspectives (Buetow, 2019). Bias in a qualitative research study can undermine the study's credibility and compromise the integrity of the data being collected (O'Boyle, 2018). I mitigated my personal bias in this study by ensuring that my experiences, perceptions, and perspectives did not affect my interview questions or interactions with my participants. To further reduce bias, I used open-ended interview questions to inquire about the participants' experiences. I did not convey my understanding of the topic to avoid influencing the interview participants' responses during data collection.

An interview protocol helped me when conducting interviews (Appendix B). Interview protocols are used in qualitative research to improve the quality of data obtained from research interviews, ensure that interview questions align with research questions, and allow for feedback from interview participants (Castillo-Montoya, 2016). An interview protocol can help in gathering all necessary information from participants

within the allocated time for interviews (Yeong et al., 2018). The use of an interview protocol helps in establishing rapport between researcher and participants and allows participants to answer interview questions without being influenced (Majid et al., 2017). Interview protocols involve the following: building rapport with participants, allowing the participants to have a positive response to open-ended questions, letting the researcher explain the ground rules, helping the researcher raise the topic of concern, and providing an opportunity for follow-up questions (Hamilton et al., 2017). The interview protocol used in this research followed all those best practices.

Participants

Eligibility Requirements

The purpose of this qualitative multiple case study was to explore the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry. I followed the eligibility criteria for selecting participants for my study. Participant selection is vital in research because it helps in data collection and ensures that the study's outcome is credible (Bendixen et al., 2016). In qualitative research, the participant's experience as it relates to the phenomenon of interest is a fundamental criterion for selecting study participants (Koskey, 2016). The participants for this study consisted of two corporate-level IT leaders who had 5 years of involvement in strategies for protecting against security violations during IoT adoption in at least three manufacturing companies in the eastern United States. However, if one of the corporate-level IT leaders had played the role of a gatekeeper, the corporate-level leader would not have been a participant, and I would have needed two corporate-level IT

leaders as my participants. Corporate-level IT leaders' positions include CIO, CISO, and senior manager (Hickman & Akdere, 2018). The participants' job titles helped to identify that they were manufacturing organization corporate-level IT leaders who were directly involved in strategies for protecting against security violations during IoT adoption.

Strategies for Gaining Access to Participants

I looked for contacts within organizations, including employees or managers of the organization who were my gatekeepers and helped me identify and have access to potential participants. Gaining access to participants involves providing a list of people who can be contacted for research (Peticca-Harris et al., 2016). Gaining access is a precondition for research to be conducted and can be achieved by sharing personal stories and contacting informants, gatekeepers, or mediators (Peticca-Harris et al., 2016). The gatekeepers helped me to locate and gain access to documents that were essential to my study. Researchers may need to gain trust and build rapport with gatekeepers to access an organization (Lim et al., 2018).

Strategies for Establishing Working Relationship With Participants

The first thing I did to establish a working relationship with participants was to ask the gatekeepers, through telephone calls and email, for the contact information of the potential participants so that I could send them an email invitation (see Appendix D) and consent form. Gatekeepers act as intermediaries between researchers and potential participants (Abbott et al., 2018). Once I got the contact information of the potential participants, I sent them an email invitation through Walden's email. The email invitation included information about the study so that potential participants could familiarize

themselves and be comfortable with my research question. That method helped to ensure that my participants' responses aligned with the overarching research question. When researchers send information about their studies to participants, the body of their messages should have clear and concise content about the research so that participants are well informed (Marks et al., 2017).

After receiving responses from the participants indicating that they were willing to participate voluntarily, I contacted participants through Walden's email and established rapport with them. Good rapport can be established with participants by being sensitive to the ethical issues, developing trustful relationships, acknowledging and respecting the individuality of each participant, and understanding participants' perspectives (Karagiozis, 2018). I emailed eligible participants the consent form, explained the relevance of the consent form to my research study, and described the voluntary nature of participation. I let potential participants know that there was no risk in participating and that their personal information would remain confidential. The purpose of signing the consent form was to ensure that my study adhered to Belmont Report principles, as researchers must adhere to all applicable ethical guidelines. A consent form should inform participants that their privacy will be protected. A consent form shows participants what information is provided and how it is formulated (Salman et al., 2016).

I followed up via Walden email or telephone to ask for a meeting time that would be convenient for the interview after each participant signed the consent form. If potential participants did not sign the consent form before our meeting, I asked them to sign it

before the interview and reminded them of the purpose, benefits, and risks of the study, as well as measures for privacy. To further align participants with the overarching research question, I used a semistructured interview process. A semistructured interview process offers the opportunity to ask flexible questions leading to new topics, and the researcher should prepare and listen well during interviews (Oplatka, 2018). Another method to align with the participants was to have a suitable interview protocol to ensure that the interview process was on track. Interview protocols help in identifying new themes, and capturing participants' perception (Oplatka, 2018). I assured that I summarized my interview protocol for my participants so that any ambiguity would be taken care of ahead of time. I ensured that the interview environment was comfortable for the participants while answering the in-depth interview questions. Interviewees or research participants need to express themselves clearly and share their experiences in the manner that they see them, without any distortion (Alase, 2017). That approach gave the participants the desired freedom and comfort to provide feedback during the interview and answer follow-up questions, thereby ensuring that the participants' responses aligned with my research study's question.

Research Method and Design

Method

To select the research method for this study, I reviewed several research methods and how they would help in addressing my research question. Three research methodologies help researchers understand the fundamentals of developing a research study: qualitative, quantitative, and mixed methods (Totawar & Prasad, 2016).

Qualitative methods can be easily adapted, and they provide the ability to explore and gain an in-depth understanding of how different study components can work together (Randall et al., 2019). I selected a qualitative method because it gave me an in-depth understanding of corporate-level IT leaders' strategies to protect against security violations in adopting the IoT. The qualitative method is exploratory, provides opportunities for further research (Rolfe et al., 2018), and includes procedures for data gathering, such as interviewing and participant observation (Gibson & Sullivan, 2018). I selected the qualitative method because it helped me to explore and gather data on corporate-level IT leaders' strategies to protect against security violations in adopting the IoT through interviews by asking some open-ended questions.

Exploring participants' perspectives and experiences is vital for a researcher to develop further and improve the outcome of a research study (Lundgren et al., 2018). I explored participants' experiences and perspectives using the qualitative method to answer my research question. Researchers adopting the qualitative research seek in-depth understanding of how individual participants see the world through observational studies, semistructured interviews, focus group discussions, consensus methods, and the analysis of documents and images (Kennedy, 2019). I selected the qualitative method because it helped me use semistructured interviews that ensured that interview questions were prepared ahead of time and allowed me to be well prepared and competent during the interview so that corporate-level IT leaders could provide the strategies that they used to protect against security violations in adopting IoT. The qualitative method comes with the ability for researchers to ask open-ended questions that are then coded into categories

(Johansson, 2019). I chose a qualitative method because I explored the strategies that corporate-level IT leaders used in protecting against security violations while adopting IoT in the manufacturing industry with open-ended questions. Qualitative research may be conducted as multiple case studies using semistructured interviews as the primary means of data collection and coding for data analysis (Hoeber & Shaw, 2017). I used the qualitative method because data collected using semistructured interviews helped in answering my research question. A researcher in a qualitative study collects data using semistructured interviews to answer a research question (Castillo-Montoya, 2016). Furthermore, researchers in qualitative studies use inductive reasoning to develop conclusions from the collected data by combining the latest information into theories. Researchers in quantitative studies use deductive reasoning to look for predetermined, existing subjects by testing hypotheses or principles (Bengtsson, 2016).

I did not use a quantitative method in this study because I applied inductive reasoning to explore the strategies that corporate-level IT leaders use in protecting against security violations in adopting IoT. Quantitative methods test hypotheses and depend on some statistical analysis (Burrows et al., 2016). I did not intend to test hypotheses in the research, so quantitative methods were not appropriate. Quantitative research involves discovering patterns, using statistical analysis, making inferences and decisions about individuals and real-world problems, and generating numerical data that must conform to scientific measurement (Uher, 2018). This research study explored participants' experiences and perspectives about the strategies that corporate-level IT leaders use in protecting against security violations in adopting IoT. Therefore, numerical data would

not have provided me with deep insight into the participants' experience with strategies to protect against security violations while adopting IoT.

The mixed method is a hybrid of qualitative and quantitative, and it involves exploring complex research questions and combines inductive and deductive thinking and reasoning (Murray, 2016). This research study applied only inductive reasoning by collecting data on corporate-level IT leaders' strategies in protecting against security violations in adopting IoT. Also, the hypothesis is attributed to a quantitative study, and a hypothesis is not needed for this study. Mixed methods were not appropriate for this study because it is a hybrid of qualitative and quantitative, and quantitative methods have already been ruled out. The mixed method interpretation of the findings can be unclear and time-consuming (Almalki, 2016). In contrast, the qualitative method allowed me to interpret the findings of my study in a clear and less time-consuming manner. The mixed method is essential when a researcher wants to corroborate the results obtained from other methods, making it difficult to plan and implement (Venkatesh et al., 2016). I did not need results from another method to corroborate my findings from qualitative research in interpreting the strategies that I need to protect against security violations in adopting IoT. Results from the participants' interviews and document analysis were enough for my study.

Research Design

I used multiple case studies for this qualitative research study. The qualitative design approaches are ethnography, narrative, phenomenology, case study, and grounded theory (Korstjens & Moser, 2017). Multiple case studies provide an in-depth and proper

understanding of the participants' experiences (Atout et al., 2019). I chose multiple case studies because it allowed me to develop an in-depth understanding of strategies that corporate-level IT leaders use to protect against security violations and allowed me to address multiple themes in interview results. The use of multiple case studies will help ensure the credibility of the qualitative research study during the data collection method using member checking (Birt et al., 2016). I used multiple case studies because the collected data were interpreted correctly. The findings were shared with my participants, allowing them to clarify their perspectives, correct errors, and provide additional information, if necessary, to ensure the credibility of the research study. Multiple case studies focus on understanding the participants' perspectives and the phenomena under the study (Dewilde et al., 2018). Researchers use in-depth and face-to-face interviews, and semistructured interviews contain several open-ended questions (Lekunze & Strom, 2017). I used multiple case studies because I explored corporate-level IT leaders' perspectives on the strategies they use to protect against security violations while adopting IoT, using face-to-face interviews and semistructured interview methods. Multiple case studies are also helpful when the researcher attempts to explain the mechanisms and outcomes of a phenomenon (Alshehry, 2018). I used a multiple case study to explore the complex phenomenon related to corporate-level IT leaders' strategies to protect against security violations while adopting IoT in the manufacturing industry.

Narrative research explores social, cultural, and familial, based on individual experiences, and uses different analytical practices (Chrismas, 2018). Narrative research was not appropriate for this study because it centers on capturing and analyzing an in-

depth story told. Narrative research is well used in studying one or two individuals and gives a broader meaning to a story while interpreting data based on human perceptions in the participants' responses (Grysman & Lodi-Smith, 2019). However, I used a direct interpretation of data based on what I learned from the participants on protecting against the security violation in adopting IoT by having my data organized and classified into codes and themes. Narrative research, being more like storytelling, could be subjective because the participants tell their stories from different viewpoints (Berg, 2016), and multiple case studies will make my study distinct. The data collected from in-depth interviews makes it more objective.

Phenomenological research design deals with the proper understanding of the essence of the experience, and findings are integrated into a detailed description of the phenomenon (Wong, 2018). I used multiple case studies because it helped me carry out a deep inquiry into the complex phenomenon about the strategies to protect against security violations used to adopt IoT. Phenomenological research design allows researchers to collect data from interviews but not from public documents (Bustard et al., 2019). I used multiple case studies because data can be collected using interviews or organizational documents on the various strategies that corporate-level IT leaders use to protect against security violations while adopting IoT in the manufacturing industry, and recorded data could be easily analyzed. Phenomenological research design describes the essence of a lived experience and does not provide an in-depth understanding of a case or multiple-case (Groenewald, 2018). I used multiple case studies because I was exploring an in-depth and detailed investigation of the strategies that corporate-level IT leaders need to

protect against security violations while adopting IoT in the manufacturing industry. For all the above reasons, the phenomenological design was not appropriate for this study

Last, ethnographic research is used when the researcher is interested in studying behavior patterns and interpreting them accordingly (Walford, 2018). I used multiple case studies because I explored the strategies used in protecting against security violations while adopting IoT and not studying the patterns of behaviors of those security violations. Ethnographic research design studies a group that shares the same culture, thereby engaging cultural participants and not an event or an activity (Uttaran, 2019). I used multiple case studies because I was not describing and sharing patterns of a culture of a group of corporate-level IT leaders as relates to the security violations. Instead, I was exploring the strategies that they use in protecting against security violations. Ethnographic research design describes and interprets the shared patterns of a culture of the group and makes the researcher deeply involved in the participants' lives through participant observation and data collected through observations (Plowman, 2017). I used multiple case studies because I did not need to be deeply involved in the lives of my participants and observe them. Instead, I asked open-ended questions through interviews to understand the strategies that they use to protect against security violations while adopting IoT. For all the above reasons, the phenomenological design was not appropriate for this study.

Data from multiple sources were included in this study to achieve data saturation. Data saturation can also be achieved based on adding new participants until there is no latest information from the participants (Tran et al., 2016). Data saturation can further be

achieved using face-to-face interviews and in-depth interviews so that the same set of questions being asked will facilitate that (Moser, & Korstjens, 2018). The multiple-case designs for this study were for at least two participants from at least three manufacturing organizations who contributed to the study through face-to-face interviews on the strategies used to protect against security violations while adopting IoT, and the interview continued until no more information was needed. I interviewed two corporate-level IT leaders from one manufacturing organization. If there was no latest information from the two corporate-level IT leaders, then I have reached saturation. If the two corporate-level IT leaders revealed the latest information, I added another corporate-level IT leader from the first organization until there was no updated information to reach saturation. I collected data from the organizations in the form of documents relating to my research question. I collected data from multiple sources, including member checking, until no other information was needed for my study, which was how I achieved data saturation.

Member checking was used after my initial interview by scheduling either Skype or Zoom for follow-up interviews with the participants to review a summary of the transcript to confirm my understanding of their responses. One aspect of member checking is for the researcher to have an opportunity to add more information and ask additional questions that will accurately reflect the participant's experiences, meanings, and perspectives (Brear, 2019; Madill & Sullivan, 2018). If any information was not clear to me at the initial interview, I asked the participant some follow-up questions to clarify my data. Member checking helps eliminate the possibility of the researcher misinterpreting the data in a qualitative method and ensuring that participants' responses

are represented accurately by asking follow-up questions (Brear, 2019). Member checking is a quality control technique used by researchers to increase the credibility and accuracy of what was recorded during the interview (Holt & McHugh, 2018; Iivari, 2018). I continued to use the member checking technique by scheduling interviews with the participants until they confirmed that I had interpreted their responses accurately, and no more information was needed.

Population and Sampling

The population of my study was all the eligible senior IT leaders. that have at least 5 years of experience in the strategies used to protect against security violations while adopting IoT in the manufacturing companies, in at least three manufacturers in the eastern United States. In qualitative research, exploring participants with experiences on the phenomenon provides valuable information about the subject of study (Mitchell et al., 2018).

The sample size of the population of my research study consisted of at least two eligible senior IT leaders who have 5 years of involvement in strategies for protecting against security violations during IoT adoption from each of the three manufacturing companies in the eastern United States. In other words, the sample size for this study consisted of at least two individuals in at least three organizations who met the eligibility criteria. Corporate-level IT leaders' positions include corporate-level IT leaders (or the highest-ranking IT employee) (Hickman & Akdere, 2018). I targeted manufacturing industries that have adopted IoT. The sample size in the qualitative study consists of participants who have experience in the phenomenon (Gilpin-Jackson, 2017).

An eligibility criterion was needed in selecting participants from a specific population for this study. In a research study, participants are screened for eligibility before they are recruited based on the number of people approached for the study (MacNeill et al., 2016). The sample comprised of participants who knew about the research topic to ensure appropriate sampling and saturation was reached. The sampling method in qualitative research is often used to look for individuals who know the research topic and can speak about their experiences (Flannery, 2016). Therefore, it is essential to have eligibility criteria in selecting participants to achieve an accurate and meaningful result. Eligibility criteria comprise inclusion and exclusion criteria based on the location, participant homogeneity, and research topic (Young et al., 2019). The eligible participants in this study will be (a) more than 18 years of age, (b) still working with the participating manufacturing industry, (c) willing to share their experiences about strategies for protecting against security violations while adopting IoT, (d) being corporate-level IT leaders within the organization, and (e) have a good experience of IoT and IoT devices.

I identified the people to participate in this study through sampling. In qualitative research, sampling a population tends to be small to provide an in-depth understanding of the phenomenon under investigation and help in the case analysis (Vasileiou et al., 2018). I used a purposive sampling method to recruit participants. Data were collected based on the eligibility criteria of the population that provided an in-depth understanding of the phenomenon of my study on the strategies needed to protect against security violations while adopting IoT in the manufacturing industry. Purposive sampling is suitable when

researchers want to intentionally learn from people who live within the phenomena under study, and they are strategically sampled (Ngozwana, 2018). I used purposive sampling because I needed experts to be selected from the population to participate in the study. Researchers use purposive sampling when they are interested in knowing experts' opinions in a particular field of study (Martínez-Mesa et al., 2016). I used expert purposive sampling because I wanted to access a subset of IT leaders that would provide me the strategies that they use in protecting against security violations while adopting IoT. Reducing the number of participants using purposeful sampling techniques such as intensity sampling, maximum variation sampling, and confirming/disconfirming case sampling helps access the specific members of the population (Benoot et al., 2016).

The sample size for this study consisted of at least two individuals in at least three organizations who met the eligibility criteria, which helped reach data saturation. The minimum size of a purposive sample needed to reach saturation is difficult to estimate but can be achieved by simulating the factors that influence them using different sampling scenarios (van Rijnsoever, 2017). The purposive sample for this multiple case study consisted of two corporate-level IT leaders in at least three manufacturing industries in eastern United States. Researchers use qualitative research by focusing on purposively selected members of a population who know about the topic of study (Pearce et al., 2016). The sample size needed to reach data saturation can be easily achieved by interviewing participants who are knowledgeable and experienced in the phenomenon under study (Malterud et al., 2016). The interviews that I used for this study included all the estimated samples of at least two corporate-level IT leaders in at least three

manufacturing industries in the eastern United States. based on the eligibility criteria of the population. I interviewed all the eligible participants in this population until there was no latest information needed to reach saturation.

A convenient and appropriate interview setting was necessary so that the participants would be encouraged to provide detailed responses to the questions. The interview setting should be such that the interviewee always feels comfortable during the interview to respond to the questions. The interviewer should actively track all aspects of the in-depth interview to ensure success (Rosenthal, 2016). An interview setting should be where there is no distraction, quiet, without connection lags, and in one fixed location, as opposed to walking around (Seitz, 2016). The interview setting should be where the interviewer and interviewee are safe because of their safety, such as sexual harassment or impropriety (Oltmann, 2016). I conducted Skype/Zoom or telephone interviews in a quiet secluded location and suggested that the participant have a similar quiet environment. I suggested to the participant to reserve a room without background noise to avoid distractions. Before the interviews began, I closed the door.

Ethical Research

I observed all ethical rules for this research during the interview and data collection processes to protect participants. One of Walden University's requirements is for researchers to get approval from the IRB before commencing the research study. Researchers should consider ethical issues related to the topic of study during the design, data collection, and detailed description of potential participants' experiences to protect their overall interests (O'Hara & Higgins, 2019). I obtained approval from the IRB and

included the approval number before data collection at the participating manufacturing organizations. The IRB approval number for this study is 07-14-20-0751729. Researchers should get approval from the IRB before commencing on data collection from the participants of the participating organizations to ensure that they adhere to ethical principles (Slovin, & Semenec, 2019). Before I commenced collecting data, each potential participant received an email invitation (see Appendix D) asking for their participation in the study and an informed consent form containing how their confidential information and privacy will be protected. I used an informed consent form to ensure that my study adhered to the Belmont Report principles. The informed consent form aims to protect research participants based on the Belmont Report principles, and the participant signed it. The informed consent form included a detailed description of the research procedure and stating that participation is voluntary without fear of reprisal if the participant refuses to participate (Weissinger & Ulrich, 2019). The Belmont Report has three basic ethical principles and guidelines that should help resolve the ethical problems encountered during the conduct of research with human subjects (U.S. Department of Health & Human Services, 1979). As a researcher, I adhered to those ethical principles during the data collection process from participants. Researchers need various ethical principles: respect for persons that are based on allowing people to make their own decisions and accommodating vulnerable persons who need more protection, ensuring people are not harmed, and they are treated equally and fairly (DiGiacinto, 2019). I completed the National Institutes of Health Office of Extramural Research training course (certification number: 2822658) to protect human research participants and

included the certificate in Appendix B.

I sent the consent form to the participants by email for their review and understanding; they signed by responding to my email with the phrase “I Consent.” Then each of us had a copy of the “I consent” email. Those actions ensured that they acknowledged my responsibility as a researcher to protect their privacy. Participation in the study is voluntary, and participants can withdraw from the research process anytime, even if they have signed the consent form. Participants have the right to withdraw from the study even when consent is obtained or decide not to participate in some aspects of the research study (Mamotte & Wassenaar, 2017). Participant's withdrawal from the research study could be verbally or in writing. Once a participant withdraws from the research study, the data collected from that participant will be destroyed immediately. I used a purposive sampling method to replace participant(s) who withdrew from my study since I interviewed other participants in the population.

There were no incentives to participate in this study, to prevent any sort of pressure, prejudice, or bias in the data to be collected to maintain the integrity of the research outcome. Researchers giving incentives to participants might affect the study's outcome and result in oversampling populations coming from socioeconomic backgrounds (Brown et al., 2018). Not providing incentives enabled participants to withdraw from the study without fear of any penalty.

To ensure that there was adequate ethical protection of participants, I disguised the research participant and organization names using fictional names and codes so that there was no violation of their privacy and confidential information. To maintain the

confidentiality and anonymity of the participants, their identities can be masked using codes or numbers when transcribing and translating the data (Ngozwana, 2018). The participants' real names corresponded to the participant code and fictional names and were stored in an encrypted format that was accessible to only me. My assignment of the codes and names were Participant 1, Participant 2, and Participant 3, respectively, to avoid the privacy and confidentiality of the participants being violated. Researchers' anonymization of the identity of study participants is essential in research to protect vulnerable participants (Surmiak, 2018). To further protect the participants' confidentiality, I made sure that all private and confidential information collected during the interview that bears the organization's name or participants' identity was kept on an encrypted USB drive that was password-protected until 5 years after the approval of the Chief Academic Officer (CAO). USB drive and any other confidential information that I collected were kept in a locked safe. These data would be retained for 5 years and would be destroyed by shredding all paper documents and deleting the USB drive's entire content. I ensured that the interviews were conducted securely without disclosing any information related to the participants to anyone that was not within the participants' organizations.

Data Collection

Instruments

I was the primary data collection instrument for this qualitative research study. The researchers are usually the instrument for the data collection process in the qualitative study because they are responsible for gathering data through interviews and

interactions with the participants (Hammarberg et al., 2016). Researchers often explore participants' experiences to address the research question (Moser & Korstjens, 2018). As the primary data collection instrument for this research study, I collected, organized, analyzed data to ensure that they addressed my research question. Researchers in the qualitative study collect, organize, and analyze data collected (Gallo, 2017).

In this research study, semistructured interviews were my primary data collection method, and the organization's documents related to the research topic were the secondary collection method. In a qualitative research study, primary data can be collected from semistructured interviews (Brown & Danaher, 2019).

I used secondary data from other sources related to the strategies to protect against security violations while adopting IoT for this study. Secondary data can be collected from other sources, including documents that can be of value in answering research questions (Helmich et al., 2018). Organization documents were my secondary data collection method to validate the accuracy of the primarily collected data. Secondary data can be used to verify the accuracy of the primary data. It is a development in data management and analysis that addresses data entry errors and missing data (Goode et al., 2017). I used secondary data from multiple sources to confirm that the primary data relates to my research study. Multiple data sources can help understand data related to the phenomenon under study (Percival et al., 2017).

I reviewed the company documents that I collected from participating manufacturing organizations. In a qualitative study, researchers, while conducting multiple case studies, ensure that data collected from multiple participants, such as

documents, are reviewed and interpreted for authenticity and consistency (Amankwaa, 2016). The document review technique is one of the qualitative research methods (Haçat, 2018). Qualitative multiple case study explores the research topic through in-depth interviews, observations, and document reviews, and document reviews are used as tools for data collection (Waheed et al., 2018). Organization's documents may include but not limited to relevant documentation on policies and procedures, organizational and operational regulations, emergency plans, safety and security recommendations, handwritten notes about organizational documents, email communication, audit data, project proposals, reports, and presentations (Díaz-Vicario & Gairín-Sallán, 2017). The organization's document that was relevant to this study included documentation on security policies and procedures, organizational and operational regulations, emergency plans, safety and security recommendations, handwritten notes about organizational documents, email communication, audit data, project proposals, reports, and presentations, security plans, architecture plans and other documents that I could get information that was useful to my study.

I used member checking to ensure that data collected from interviews and documents were accurate and valid. Researchers can present data transcripts or data interpretations to participants for comments using a member checking approach to ensure that data are valid and accurate (Varpio et al., 2017). Participants with deep knowledge about the phenomenon under study can provide data based on what they perceived (Jin & Bridges, 2016). I ensured that I built a rapport with the participants to make them feel comfortable to answer my interview questions so that enough data could be collected.

Researchers in the qualitative study need to establish rapport with the interviewee to answer the interview questions willingly (Pang et al., 2018). Participants' experiences on the phenomenon under study help in the data collection process (Keedle et al., 2018). I sought to clarify any responses that I didn't understand during the interview with the participants. In semistructured interviews, researchers ask participants follow-up questions so that they can provide in-depth information about the research topic (Overmars-Marx et al., 2018). I was flexible before the interview and refined the interview protocol so that it would be easily understood and to avoid any complexity. Interview protocols in the semistructured interview will be an effective way of gathering data if they are designed to be flexible and refined, thereby ensuring the interview is more structured, systematic, and organized (Cheah et al., 2019).

The audio of the interview with each participant was recorded so that it could be transcribed and referenced. Researchers use audio-recorded semistructured interviews for data collection and ensure the semistructured interview's credibility (Quek et al., 2019). I used two recording devices for failsafe backup. It is essential to keep a backup of the audio-recorded semistructured interviews if one of them crashes (Farooq & Villiers, 2017).

The interview protocol that I used for this study (see Appendix B) lists the activities and interview questions (see Appendix C) that I asked participants. Researchers use interview protocols to build rapport with participants to ease the establishment of trust and make them feel comfortable during the interview, helps participants to be neutral or positive when responding to open-ended questions, and provide purpose and

conversational rules (Hamilton et al., 2017). Interview protocol is a qualitative data analysis procedure that consists of questions to get participants' opinions and ensure good qualitative data (Yeong et al., 2018). I used an interview protocol to ensure consistency during my interviews, thereby increasing its reliability and accuracy. The qualitative research study's interview protocol is based on the study's research question and is used well in each interview to maintain consistency (Atif et al., 2016). My interview protocol started with preinterview activities by introducing, checking to ensure that every participant signed the informed consent form and reminded them their privacy and confidential information would be protected. An interview protocol is a set of rules and guidelines used by researchers for the interviews and consists of pre and post interview guidelines and a set of questions being asked during the interview (Dikko, 2016). The interviews that I conducted started by powering the audio recording devices on, mentioning the participant's identifying code name. Next, I stated the interview date and time and then asked the semistructured interview questions, allowing the participants to express relevant information on the research topic. Then, I stopped and powered off the audio recording devices. One of my post-interview activities was to explain the use of member checking; I thanked the participants and gave them my contact details.

Data Collection Technique

The data collection for this study began by conducting semistructured interviews consisting of ten questions as contained in the interview protocol (see Appendix C). Interview protocol helped and guided me when conducting the interview. The interview settings were comfortable for the participants to answer the interview questions on the

strategies use in protecting against security violations while adopting IoT in their organizations. I built a relationship or a rapport with the participants to be comfortable answering my questions. Before each interview with the participant, I sent them an email that contains a concise overview of the research, the research aims and objectives, and some open-ended questions so that they will be familiar with the interview questions and topic of study. Researchers could send the participants some details about the research through email so that they will be familiar with the discussion before the interview, and the interview date, time, and location would have been agreed upon between the participants and the primary researcher (Siew Khoon Khoo, & Saleh, 2017). I began with the interview protocol by introducing and thanking them for being my participants. I reminded the participants about the consent form they signed and reassured them that their privacy and confidential information were not being compromised and asked if they had any concerns.

I explained the interview process, which included audio recording, transcription, and interpretation that I did. My participants were reminded that the audio recording was one way of collecting data, and anything recorded will be confidential. Also, the audio recorded information will be destroyed at the end of my study. I checked the audio recorder to ensure that it was working as expected and turned it on, stating the date of the interview and the identification codes or names of the participant. Using my interview protocol, I asked the participant the first question; gave him enough time to respond before moving to the next question. I asked the participant probing questions to get more information and some clarifications. I adjusted the interview protocol before the

interviews so that they were clear to ensure participants' responses address my primary research question. I continued with the rest of the interview questions until all questions were answered. Researchers should make sure that the interview protocol is flexible by refining the research questions, and it should be easily understood and cover all research questions to gain insights into participants' experiences and increase the effectiveness of an interview process by ensuring comprehensive information is obtained within the allocated time (Yeong et al., 2018).

After exhausting all my interview questions and receiving a response, I asked the participants if they had any additional information that they would like to share. I asked the participants if they had organizational documents that could help me understand the topic more. I explained the concept of member checking to the participants and schedule a follow-up interview to review my interpretations from the transcribed audio recorded information. Finally, I turned off the audio recording devices, thanked them for being my participants, and asked them if they would be okay if I called them for further clarification and a follow-up interview.

After each interview, I transcribed the recorded information into different Microsoft Word documents. To ensure the confidentially of the participants, any identifiable information from the transcription was replaced with their code names. Researchers listen to an audio recording of an interview multiple times during transcription to fully understand the information (Naidoo et al., 2016). I interpreted and transcribed the audio recorded information based on my understanding during the interviews and searched for common themes. Researchers listen and transcribe the audio

recorded interview, and common themes are identified based on their understanding (Campanotta et al., 2018). I continued the transcription process until I was ready for member checking. Audio recording helps participants express themselves better and avoids the painful effects of self-editing in written diaries, and interview transcription issues can be resolved with member checking (Fitt, 2018).

After my interview with the participants, I began member checking by transcribing my recordings. Then summarized the findings in a few brief bullets and asked the interviewee to verify the bullets. Researchers use member checking in diverse ways, such as sending participants a general or coded interview transcript with instructions asking participants to verify the accuracy and clarity in interpreting the data (DeCino, & Waalkes, 2019). Member checking could be done by sending participants an email with a brief bulleted summary to validate themes. If it doesn't result in major changes to themes, some themes could be expanded to clarify meaning (Hagemeier et al., 2018). I sought to clarify any responses that I didn't understand in the initial interview or any latest information they might have. To achieve data saturation, I continued to interview more people from the same firm until no latest information was revealed and participants confirmed the validity of the interpretations. Then I moved to another firm and repeated the same process until no latest information was provided, and participants confirmed the validity of the interpretations. Researchers often continue with member checking with participants until they confirm the interpretations, and there is no latest information to be provided (Caretta, 2016).

I used organizations' documents that contained security policies and procedures to

reconfirm information from other data sources. Documents can be used to corroborate data from other sources to understand the research topic (Eta & Vubo, 2016). The use of the organization's security policies and procedures helped me understand the strategies used in protecting against security violations while adopting IoT. Documents that include policies, strategic plans, legislation, reports, and decisions when analyzed can be used to complement data obtained from audio-recorded interviews to provide a further understanding of the phenomenon under study (Masoumi et al., 2019). I clarified the source of the documents by emailing my interviewees the documents to confirm the authenticity. The primary researcher can use document analysis of specific policy documents as a secondary source for reviewing or evaluating documents and is often used in combination with other qualitative research methods (van den Berg & Struwig, 2017).

A semistructured interview was the data collection technique that I used in this qualitative research data collection process. There are some advantages to using semistructured interviews as a collection technique. First, it helps interviewers to prepare questions ahead of time, thereby doing interviews to be competent while conducting the interview. According to Brown and Danaher (2019), a semistructured interview helps the interviewer prepare a list of questions based on the research question. It initiates a conversation between the interviewer and the interviewee. The second advantage is that a semistructured interview assumes different formats and technologies such as Skype technologies that researchers can use to interview participants even when they are geographically separate (Quartiroli et al., 2017). Third, semistructured interviews allow

participants to express their views the way they understand them, thereby providing an in-depth understanding of the research topic (Overmars-Marx et al., 2018). Fourth, the semistructured interview provides reliable and qualitative data because it allows follow-up interviews to clarify the interviewee's responses (Brown & Danaher, 2019).

However, there are some disadvantages of semistructured interviews as a data collection technique. First, the interviewer's skills and ability when asking questions during the interview determine the quality of data to be collected. For example, Brown and Danaher (2019) stated that the lack of skills and training has made researchers conducting semistructured interviews with limited guidance. Second, semistructured interviews are time-consuming and expensive if it is face-to-face because the researcher must physically meet with the participants (Lekunze & Strom, 2017). Third, open-ended questions in semistructured interviews may be challenging to analyze but using analysis tools such as NVivo can help the researcher conduct the analysis (Kahraman & Kuzu, 2016). Fourth, it may be challenging to compare answers with semistructured interviews, but with member checking, answers could be compared with the company's internal documents (Yeong et al., 2018).

Despite these limitations, the use of a qualitative semistructured interview as a data collection technique is popular among qualitative method researchers. Its effective use depends on the relationship, rapport, and trust between the interviewer and the interviewee.

Data Organization Techniques

Data organization was a vital component of my data analysis and interpretation.

Data analysis typically consists of preparing and organizing the data, reducing the data into themes through coding, condensing the codes, and representing the data in figures, tables, or discussion (Cypress, 2018). I used cataloging/labeling systems to catalog and organize themes from the interview. Researchers in data analysis starts with immersion in the data to obtain a sense of the whole and then cataloging the principal themes that emerged according to the research study framework (Kowalski et al., 2018). With the cataloging/labeling systems, I ordered the field notes and memos chronologically. Data analysis includes organizing data such as documents used in field notes and transcripts recording interviews (Rakhmawati & Nirmalawati, 2017). I cataloged or indexed all documents and artifacts from my study and had a system of designing and implementing labeling and logging interviews to reduce mistakes or errors. An efficient data organization and description can reduce mistakes in data analysis, ensuring the accuracy of the research results (Gorgolewski & Poldrack, 2016). In a qualitative research study, data organization techniques include data sharing, data repositories, archiving, security, and preserving ethics (Glenna et al., 2019). In addition to cataloging/labeling systems, I used a Microsoft Excel spreadsheet that was password protected from organizing all artifacts that included informed consent forms and transcripts from the interviews, emails, and dates of the interviews. I created sub-folders in my password-protected encrypted flash drive for different data from interviews, audio recordings, member checking, and other organization's artifacts and categorized them accordingly.

To ensure the confidentiality of the participants, I masked the organizations' and participants' names with code names so their real identities will not be revealed.

Participant's confidentiality can be kept in a research study by not disclosing what the participants said or did during research unless they consent to do so and only in ways they agreed, and concealing the identity of the participants (Surmiak, 2018). To avoid mixing up the participants based on their responses, I mapped the actual participants' names to the code names in my password-protected Microsoft Excel spreadsheet accessible to only me for reference purposes. Researchers can map the real names of their participants to the pseudonym, which the researcher or the participants may choose to avoid further ethical issues (Brear, 2018). To further protect the participants' confidentiality, I made sure that all private and confidential information collected during the interview that bears the organization's name or participants' identity was kept in an encrypted USB drive that was password-protected and will not be more than 5 years after the approval of Chief Academic Officer (CAO). Maintaining confidentiality means that any information obtained from participants must not be revealed; data must be anonymized as early as possible during the transcription process and stored securely (Farrugia, 2019). USB drive and any other confidential information that I collected were kept in a locked filing cabinet. To ensure confidentiality to participants, data collection should be well-protected to avoid disclosure of information (Lancaster, 2017). These data will be retained for 5 years and destroyed either by shredding the paper documents and deleting the electronic ones. I ensured that the interviews were conducted securely without disclosing any information related to the participants to anyone that was not within the participants' organizations. Researchers are required to plan on how to manage and store the data collected, and the anonymized data should be stored securely, and any

identifiers removed from the data should be stored separately, and the consent form must specify how long the data will be stored (Farrugia, 2019).

Data Analysis Technique

The data analysis for this study began by searching the data that I collected continually until I had enough information that addressed my research question on the strategies that corporate-level IT leaders in at least three manufacturing industries use to protect against security violations while adopting IoT in the manufacturing industry. One of the most critical components in the qualitative research process is data analysis (Raskind et al., 2019). Qualitative research data analysis produces richer, more in-depth, and alternative understandings of the research topic (Jennings et al., 2018). Qualitative research data analysis is used to thoroughly interrogate the data, achieve meaning at a deep, semantic level, and undertake extensive co-revision of themes, codes, and frameworks as findings emerge (Jennings et al., 2018).

I used NVivo version 11 Qualitative Data Analysis Software (NVivo) for my data analysis relating to security violations while adopting IoT in the manufacturing industry. The process for the data analysis in this research study using NVivo as a data analysis tool began by importing data that I collected from various sources into the NVivo software tool. I organized and analyzed the data to have a deeper understanding of the collected data. When conducting data analysis, data are organized, categorized as codes, and themes are created as findings emerge (Jennings et al., 2018). NVivo helped me collect multimedia data from multiple devices to connect them to my transcribed data. That feature of NVivo was important to me because I accessed source data from my

password-protected flash drive and other devices. NVivo helps in qualitative research in data organization, idea management, querying data, and modeling (Guo, 2019). NVivo, through the analysis of multiple codes, helped me identify themes across my data sets because the tool also helped organize and sort data properly. NVivo has a technique called the word tag cloud that helps assess the relevance of the data obtained or gathered based on the research topic (Guo, 2019). NVivo is a tool that extracts new themes and their relationship from the study data (Guo, 2019). Also, NVivo's word count feature helped find the frequency and repetition of the participants' words during the interviews and the organization's documents. When analyzed with the NVivo, collected data could be divided into themes for a presentation showing the duration and frequency of interactions based on the words in the collected data (Kahraman & Kuzu, 2016). I used NVivo to add to my findings in terms of data interpretation and summarization of findings. NVivo provides excellent data management and retrieval facilities that support analysis and write-up and offers a valid and tested analysis method for grounded theory generation (Maher et al., 2018).

I further reviewed the organization's documents to verify the interview transcripts that explained the strategies used to protect against security violations while adopting IoT in the manufacturing industry. Documents are used to corroborate evidence to identify themes and perspectives and serve as a validation strategy for triangulation (Siegner et al., 2018). The internal documents in qualitative research are used to identify emergent themes (Bruce et al., 2016). After my interviews, I analyzed the organization's documents to further clarify data from the interviews based on participants' perspectives

on the strategies they use to protect against security violations while adopting IoT in their organization. Document analysis helps researchers in the interview to gather more facts about a phenomenon (Matlala & Matlala, 2018). I organized and analyzed the data to have a deeper understanding of the collected data. When conducting data analysis, data are organized; categories or codes and themes are created as findings emerge (Jennings et al., 2018).

The data analyzed in this study were from multiple data sources to discover themes that answered my research question. Having multiple types of data analysis in the qualitative study helps diminish researcher bias and thereby supports the credibility and trustworthiness of findings (Peterson, 2019). Methodological triangulation was used in this study by comparing interview data with the organization's documents to understand the strategies used to protect against security violations while adopting IoT in the manufacturing industry. Data collected from the literature review also helped in identifying themes for strategies. In the qualitative research method, methodological triangulation increases the validity of the research and provides a broader perspective of the research question (Osarenkhoe & Byarugaba, 2016). Methodological triangulation was appropriate for my research study because it enabled the search for common themes in different data sources. Researchers use the methodological triangulation approach to ensure that data from multiple sources can complement each other with at least two data collection methods (Sułkowski & Marjański, 2018). Therefore, I used methodological triangulation to address my research question.

I used coding in this research study to search for explanations, patterns, and

relationships of the collected data aligned with security violations and strategies. In a qualitative research study, indexing or breaking down and labeling the data is called coding, and it is a process where the researcher breaks the data into smaller chunks (Raskind et al., 2019). Qualitative research is conducted using semistructured interviews for data collection and coding for data analysis (Hoeber & Shaw, 2017). Some of the actions performed by the researcher in data analysis include preparing and organizing the data, reducing the data into themes through a process of coding (Cypress, 2018). I performed the following activities in a logical and sequential process for the data analysis:

1. Ensured that I familiarize myself with data collected during the interviews and organization documents to generate themes.
2. I listened to the interview audio recordings, read the transcripts, and review all the organization's documents that relate to my research question.
3. I generated a list of codes that relate to data that address my research question.
4. I continued adding to the list of codes as new codes were found from my data.
5. I used codes to search and identify themes, patterns, and relationships in the data.
6. I categorized these codes, discovered, and identified major themes, and ensured that they align with my research question.
7. I repeated the above steps until there were no new themes and codes and I had enough data to address my primary research question.

The next step of the data analysis was to search for major themes in the collected

data for patterns and relationships aligned with security violations and strategies based on the five characteristics of the DOI theory: advantage, compatibility, complexity, and trialability and observability and categorize them. Classification of data help in identifying their characteristics by sorting them into categories based on similarities by providing clarity, support decision-making, or the foundation for theory testing or inductive analysis (Glegg, 2019). My search for patterns and recurring themes produced major themes after a thorough analysis of the data. In a qualitative study, generating themes means that the researcher collates initial codes into potential themes, thereby gathering all data relevant to the theme. Many themes that emerge in qualitative data should answer the research question in each analysis (Scharp & Sanders, 2019). I included data coming from the review of literature that was relevant to my research question. Researchers include data obtained from the literature review, which helps search and find major themes (Akter et al., 2019). I searched for the latest articles that might have data needed in my research question. I included these new data during the data analysis. I sorted, arranged, and analyzed the data until relevant themes emerge that aligned with my research question.

Reliability and Validity

Reliability and validity strategies were included in this study to ensure that it produces excellent quality. Validity and reliability are essential in ensuring excellent quality research; validity ensures that data collected is accurate, and reliability means reproducing the data coming from the research instruments (Jordan, 2018). Validity can also be trustworthiness, credibility, dependability, confirmability, authenticity, rigor,

plausibility, goodness, soundness, transferability, and quality assessment of research study (FitzPatrick, 2019), while reliability could be considered as the degree of consistency of the measuring instrument (Kennedy et al., 2019). In a qualitative research study, reliability and validity are essential elements because in adopting research methods, they are accepted by the researchers as the right ways of collecting and analyzing data that are free of bias (Collingridge & Gantt, 2019). I ensured that this qualitative research study was conducted with reliability by measuring or testing what was intended. In a qualitative research study, reliability is achieved by repeated measures of a phenomenon. Reliability is based on consistency, care, and visibility in applying research practices, and it shows the analysis, conclusions and eliminates the partiality of the research finding (Cypress, 2018). My study was reliable by ensuring that my findings could be confirmed by having some solid evidence. Reliability is essential, and it is a repeated assessment of the consistency of results and means that the researcher does not distort the information and is transparent. Validity means that there are no hidden intentions, beliefs, concepts, and values of the participants (Yardley, 2017).

I used an interview protocol to guide me towards ensuring consistency when interviewing. Reliable and valid interview protocol will not be enough in a research study; adding validation strategies like triangulation and member checking in the data analysis stages will help in ensuring reliability and validity (Yeong et al., 2018). In a qualitative research study, member checking is one way of ensuring the validity and can be reached through triangulation by letting the participants review the interpretations of the study to ensure accuracy (Caretta & Pérez, 2019). Also, due to the subjective nature

of the researchers and participants, it could be challenging to replicate a qualitative study; therefore, I documented my research procedures to overcome that. Reliability could be problematic; however, the more times findings can be replicated, the more stable or reliable the phenomenon under study (Cypress, 2018). Reliability represents consistently repetitive instances using similar participants under the same or different approaches (Cypress, 2018). Therefore, I used interview protocol and member checking to show the reliability and validity of my study and ensure that my findings were consistent and dependable based on the data collected.

This qualitative study ensured that my findings or results were reliable, valid, trustworthy, and accurate. Validity means making sure that the research data is accurate (Cypress, 2018). Morse (2015) broke down criteria to reliability, namely validity and generalizability, and Alsharari and Al-Shboul (2019) further stated that reliability, validity, and generalizability imply that research is trustworthy, credible, confirmable, and transferable. I used some strategies to address these respective criteria in the following subsections.

Dependability

For this qualitative research to be dependable, I used member checking, interview protocol, and methodological triangulation. In qualitative research, dependability can be achieved by having two qualitative researchers review the transcribed information to validate the themes and codes identified (Cypress, 2018). Dependability also requires participants' involvement in evaluating the findings, interpreting, and making recommendations of the study based on data received from participants in the study; it

includes all aspects of consistency (Korstjens & Moser, 2017). Taheri et al. (2019) refer to dependability as the integrity and stability of collected data, findings, and interpretations by allowing the study to be repeated. I included member checking to establish credibility and trustworthiness, which guarantees that interpreted interview data is accurate. After my initial interview, the member checking was used by scheduling Skype, Zoom, or phone interviews with the participants to verify my understanding of their answers. Those activities entailed summarizing their comments into bullet points. Then in the follow-up interview, I covered the bullet points to make sure I understood what the participant had said. Member checking allows the participants to review the transcript, add more information, and ask additional questions to reflect their experiences, meanings, and perspectives (Brear, 2019). If any information was not clear to me initially, I sought to clarify any responses that I didn't understand. Member checking helps eliminate the possibility of the researcher misinterpreting the data in a qualitative method and ensuring that participants' responses are represented accurately by asking follow-up questions (Brear, 2019). Member checking as a quality control technique is used by research to increase the dependability and accuracy of what was recorded during the interview (Iivari, 2018). Member checking technique continued to be used by scheduling interviews with the participants until they all confirmed that I had interpreted their responses accurately, and no more information was needed. Another strategy to ensure credibility and dependability is having a prolonged engagement, persistent observation, triangulation, and member checking (Korstjens & Moser, 2017). I used an interview protocol (see Appendix B) to ensure that there were consistencies when

conducting interviews, thereby increasing the reliability and accuracy of data obtained from participants during the semistructured interviews. To ensure some dependability, qualitative researchers may use documented steps such as detailed drafts of the study protocol, a detailed track record of the data collection process, and measured coding accuracy in the research (Forero et al., 2018).

I used an audit trail to ensure dependability in this research study. An audit trail is a strategy needed to ensure dependability in a qualitative research study (Korstjens & Moser, 2017). I explained every aspect of the study, including the aim, the design of the study, and the participants. The researcher is responsible for providing all the documents and information related to the study to ensure the transparency of the research path (Korstjens & Moser, 2017). I provided an audit trail of this research study by detailing the process of data collection, analysis, how themes were developed, and result interpretation, ensured they were well documented and organized using NVivo data analysis software. Researchers can use NVivo as a data analyst tool for data audit trail and capture informed decisions made by the researcher (Pengfei et al., 2016). NVivo help in qualitative research in data organization, idea management, querying data, and modeling (Guo, 2019).

Credibility

This multiple case study sought to establish credibility by involving manufacturing organizations' corporate-level IT leaders to be the participants for the study. Credibility relates to the trust in the accuracy of the result of the research findings and ensures that it is a true representation of the interpretations drawn from the

participants (Korstjens & Moser, 2017). For this multiple case study, manufacturing organizations' corporate-level IT leaders participated in interviews to answer questions about strategies they use in protecting against security violations while adopting IoT in their organizations. I used member checking to confirm my interpretation from each of the interviewees by setting up a time to review the transcripts with the participants and type out my comments. The transcripts were summarized in bullet points and confirmed with the interviewee, allowing them to add more information to verify my understanding of their answers that accurately reflect their experiences, meanings, and perspectives. Member checking is the most crucial strategy that can be used to achieve credibility (Korstjens & Moser, 2017). Researchers use member checking as a method to present transcribed data to participants for feedback to ensure the validity and accuracy of the data (Varpio et al., 2017). The credibility in this research study was further achieved when the result of the findings of the phenomena came from participants who participated in the decisions made to protect against security violations while adopting IoT in their organizations.

I used methodological triangulation by comparing collected semistructured interview data with organizations' relevant documents and my findings in the literature review. That activity helped me understand strategies used to protect against security violations while adopting IoT in the manufacturing industry, and the literature exposed themes for strategies. Documents are used as corroborating evidence for identifying themes and perspectives and serves as a validation strategy for triangulation (Siegner et al., 2018). I used methodological triangulation to confirm my findings, improve the

dependability in this research study, and bridge the gaps associated with the sole source. Having multiple sources interpreted provided more trust in the findings. Researchers use the methodological triangulation approach to ensure that data from multiple sources can complement each other with at least two data collection methods (Sułkowski & Marjański, 2018). In the qualitative research method, methodological triangulation increases the validity and accuracy of the research and provides a broader perspective of the research question (Osarenkhoe & Byarugaba, 2016).

Transferability

In this research study, I described the research context and the assumptions central to the study to ensure that research can be transferred. Transferability means the level at which the results can be transferred to other contexts or settings with other respondents, and the researcher's transferability judgment facilitates it through the thick description (Korstjens & Moser, 2017). Since this was a multiple case study, my findings were based on specific manufacturing IT organizations and may not be ideal for other contexts or settings. Transferability does not include a wide range of claims (O'Sullivan & Conway, 2016). Transferability provides a thick description of the phenomenon, and it is a technique that provides qualitative researchers with a reliable and detailed account of their experiences during data collection. In a qualitative research study, one of the researcher's responsibilities is to provide a complete description of the participants and the research process (Korstjens & Moser, 2017). Transferability deals with external validity, and it is the ability of the study to be replicated. It supports the research study's detailed description of the context, location, and people studied, thereby ensuring

transparency about the analysis and trustworthiness of the resulting outcome (Connelly, 2016). Transferability also provides the background data to establish similarities in context and describes the phenomenon under study by allowing comparisons. Researchers can use the transferability technique to transfer the study's findings to individuals in contexts that may have some similarities to the context where the study was carried out (Caeiro et al., 2019).

Confirmability

In this research study, I presented credible findings to achieve confirmability by documenting the procedures for checking and rechecking the data throughout the study. Confirmability refers to the extent to which researchers confirm the study of others, and it is achieved by ensuring interpretation data are derived from the collected data (Korstjens & Moser, 2017). I used methodological triangulation by comparing semistructured interview data with the organization's documents and my findings in the literature review to confirm the data being interpreted for accuracy. Researchers in the qualitative study uses a methodological triangulation approach to ensure that data from multiple sources can complement each other with at least two data collection methods to address confirmability (Sułkowski & Marjański, 2018). I used an audit trail to confirm my research findings by establishing that the findings were from participants' responses in the interviews and not my preconceptions and biases to ensure accuracy. Again, confirmability includes recording interviews, interview protocol, and member checking (Connelly, 2016). Qualitative study researchers can conduct member-checking with study participants or similar individuals to address confirmability (Connelly, 2016).

Furthermore, NVivo software can help in addressing confirmability based on the collected data. NVivo helps researchers conducting data analysis to search patterns for words, codes, or themes and their relationships to confirm their findings (Yelpaze & Ceyhan, 2019). I used NVivo to ensure that my research addresses confirmability based on the collected data.

Data Saturation

To achieve data saturation, I continued to interview more people from the same firm until no latest information was revealed. I also compared the data from one organization to the others to ensure I reached interorganizational saturation. In qualitative research, researchers will achieve data saturation if no new perspectives and explanations come from participants (Tran et al., 2016). Also, using triangulation by collecting data from at least two data sources, researchers may be able to reach data saturation, and that helps in enhancing the credibility and validity of the result (Varpio et al., 2017). Another way of reaching data saturation was to collect data from organizations' documents and other relevant artifacts on strategies used to protect against security violations while adopting IoT. Qualitative research always relies on data collected from interviews, focus groups, observations or documents, and other written materials (Carr et al., 2019). Researchers use iterative sampling to reach saturation and interpret the finding (Forero et al., 2018). I continued collecting data from semistructured interviews and organizations' documents pending when no new themes were being generated, which indicated that I had reached data saturation. Data is saturated when a dataset does not provide more information or themes related to the research question, and saturation means in-depth

information has been provided to the researcher (Constantinou et al., 2017). To reach saturation, participants are continuously recruited until no new themes are emerging from the collected data (Pang et al., 2018). If there was a repetition of data, and there were no new themes identified, that meant that data saturation had been reached.

Transition and Summary

Section 2 included the researcher's role that described the researcher's expectations in this study, the participants, the research method and design, population and sampling, ethical research related to this study about security violation strategies while adopting IoT in the manufacturing industry. For the data collection and analysis techniques used in this study on security violation strategies while adopting IoT, I used qualitative multiple case studies. Data were gathered from semistructured interviews and organization documents. The data from semistructured interviews and organization documents helped me understand the strategies corporate-level IT leaders use to protect against security violations while adopting IoT in the manufacturing industry. The reliability and validity of the collected data were ensured using member checking and triangulation.

Section 3 included the discussion on application to professional practice and implications for change. Topics discussed here were an overview of this study, presentation of the findings, applications to professional practice, implications for social change, recommendations for action, recommendations for further study, reflections, and summary, and the conclusions of this study.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative multiple case study was to explore the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry. I gathered data from corporate-level IT leaders who had been involved in strategies to protect against security violations while adopting IoT in three manufacturers in the eastern United States by interviewing six corporate-level IT leaders. I performed member checking by conducting follow-up interviews so that the participants could review the summary of my transcripts. I used 10 company documents that I collected for methodological triangulation.

The findings showed that corporate-level IT leaders used different strategies to protect against security violations while adopting IoT. Findings from data collection included the case organization's security violation strategies and how DOI theory contributed to those strategies. During my analysis, four major themes emerged: relevance of securing IoT devices in IoT adoption, identifying and separating personal and confidential data from analytical data, adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption, and risk mitigation policy relevant to securing IoT devices (see Table 1).

Table 1

Frequency of Major Themes

Major theme	Participants		Documents	
	Count	References	Count	References
Relevance of securing IoT devices in IoT adoption	6	70	8	51
Identifying personal and confidential data from analytical data	6	52	6	41
Adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption	6	71	9	52
Risk mitigation policy relevant to securing IoT devices.	6	72	9	49

These themes essentially describe potential strategies related to protecting against security violations such as sensitive data by properly identifying confidential data for privacy and ensuring that customers' and employees' data are not compromised because of adopting IoT in manufacturing industries.

Presentation of the Findings

The research question used for this study was as follows: What are the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry? I analyzed data obtained from semistructured interviews and followed up with participants to member check the summarized transcripts from interviews, applied an audit trail, and used methodological triangulation

for collected company documents on information related to IoT security violation strategies.

I interviewed members of the management team with direct reports who provided strategies to protect against security violations while adopting IoT. I used DOI theory as the conceptual framework in this study to explore strategies used by manufacturing organizations to protect against security violations while adopting IoT and bridge the knowledge gap in the literature. The data collection method included semistructured interviews with two participants from three manufacturing companies and collected company documents about security violations in IoT. I used semistructured interviews to understand details; this approach enabled me to seek clarification from each participant. I used company documents from the organizations to ensure methodological triangulation of the data. The collected company documents included PowerPoint presentations, policy documents, downloaded documents, and videos from the company's websites addressing IoT security violation concerns. I loaded responses from interviews, transcribed scripts, and company documents into NVivo software for analysis, which helped in categorizing and creating themes based on the responses from participants. The remainder of this section consists of discussion of the four main themes that I identified in the research study.

Theme 1: Relevance of Securing Internet of Things Devices in Internet of Things Adoption

Results of Data Analysis

The relevance of securing IoT devices while adopting IoT was the first theme to emerge from data collection. Security violations have been a huge hindrance for some manufacturing industries in adopting IoT due to several security vulnerabilities that IoT presents. The participants in the case organization recognized the need to consider compliance with standards and requirements as a sine qua non while adding IoT devices to their IoT networks. Study findings revealed that security violations were key factors considered in IoT device acquisition and an integral part of the case organization, irrespective of the existing technology. All six participants at the case organization indicated that protecting against security violations was a critical factor for IoT adoption, and eight of 10 company documents supported the theme (see Table 2).

Table 2

Frequency of First Major Theme

	Participants		Documents	
Major theme	Count	References	Count	References
Relevance of securing IoT devices in IoT adoption	6	70	8	51

Six participants clearly expressed that securing IoT devices is essential, especially in gaining a relative advantage over their competitors and earning customers' trust in their products. An IoT security violations strategy is also necessary because of the

reputational loss that the manufacturing company could face if there were a security breach. Participant 1 stated,

> IoT devices can be helpful in many cases because they can collect data, but IoT devices and network devices like every other IT device need to be protected, and there are so many strategies that can be put in place to ensure that IoT devices are well secured.

The security strategies included having several firewalls at several levels to ensure that intruders cannot connect to IoT devices, having regular updates of operating systems of all applications, and using encryption. All participants mentioned the need for security strategies to protect IoT devices, which would help their customers build trust in their products so the organization could focus more on the day-to-day running of manufacturing plants to increase productivity and efficiency without worrying about managing access controls or preventing adversaries from accessing IoT devices. Four interviewed participants mentioned that existing standards and regulations in information security were the guiding principles for IoT adoption strategies. Five of the six participants stated that lack of security strategy violations in IoT led to some security breaches in other industries that were not manufacturing, resulting in some negative perception of those industries' products and negative images of those industries. Participants from the case organizations mentioned that security violation strategies that they had in place gave them the confidence to use the phrase "Internet of Things" when marketing their products to their clients. Two of six participants indicated that some of their clients did not know what IoT meant; instead, they were more concerned about the

products and how their personal information would not be compromised. Participant 2 stated, “Our security violation strategies are often determined during employees’ security, threat, and vulnerability awareness sessions, and employees are encouraged to attend and speak freely.” Participant 6 also stated, ”They constantly review their security policies to ensure that their products meet security requirements.” Participant 4 mentioned that they had a checklist of security action items that must be met before their products are made available to their clients.

All eight documents of the case organizations revealed that securing IoT devices is relevant in IoT adoption. Documents 3, 4, 7, and 8 revealed that applying network segmentation by dividing the network into different segments helps to control the traffic between devices. If an IoT network is not segmented, any malicious entry can easily spread throughout the entire network’s endpoints communicating directly. Document 2 of one of the case organizations stated, ”Our organization uses VLAN configurations and next-generation firewall policies to implement network segmentation, and that approach keeps IoT devices separate from other IT assets.” Document 1 of another case organization stated, “When we integrate IoT security solution and next-generation firewall, it adds value to our IoT networks and reduces time and effort in creating a security policy.’

Six documents of the case organizations revealed the need to enforce and maintain strong password security practices to secure IoT endpoints. Document 3 of one of the case organizations stated, “We need to reset the passwords that IoT devices come with before they are connected to the network because they are easy to find online.”

Additionally, Documents 2, 6, and 7 mentioned that the new IoT device password should be difficult to guess and in line with the information security team's password policies.

Comparison to the Literature

The strategy to protect against security violations described by the case organizations is in line with various studies found in the literature in which IoT adopters have been skeptical in adopting the solution due to security concerns. A survey conducted by Al-Garadi et al. (2020) indicated that despite the huge benefits of IoT adoption, security is still a big challenge because implementing security measures such as encryption and access control on IoT devices is still ineffective in protecting against their vulnerabilities. Khanam et al. (2020) indicated that security attacks on IoT devices occur at different architectural layouts of IoT networks such as application, network and physical. Khanam et al. (2020) further noted the need to have some security strategies such as security patches and porting of memory-efficient security schemes to ensure that IoT devices do not run out of memory after booting up the operating system. The responses from Participants 2, 5, and 6 indicated that their IoT devices were secured at those various layers when connecting to the cloud. Besides securing the layers above at their endpoints, the case organizations had existing security measures such as defense in depth, encryption, firewall, network, and device separation, network monitoring, password change or rules, physical security, software or patches updates, and standards that were implemented. Besides, a malicious attack could occur at the topology of the IoT, degrading its performance. Malicious attacks are major challenges in IoT adoption because they cause some damage to the network parameters (Boudouaia et al., 2020).

Participant 1's feedback aligned with this idea, as Participant 1 stated, "Having industrial firewall before the IoT networks will protect it from a malicious attacker who tries to change the network parameter."

Furthermore, attacks could come from manufacturers of IoT devices not patching these devices before they were produced and deployed to the market, thereby creating security issues (Cruz et al., 2019). Six participants agreed that devices might not be patched and indicated that they performed regular updates of IoT devices' operating system. If devices were unpatched by their manufacturers, it causes them some security violations. Meanwhile, Rizvi et al. (2020) suggested that vulnerabilities could come from a weak link in a network that exposes IoT devices to external attacks. They recommended using a device-level strategy to analyze the vulnerabilities of the devices to eliminate the weak link (Rizvi et al., 2020). Participants 2, 3, 4, and 5 stated that a strategy such as weak link elimination ensures that devices communicate to known IP addresses or domain names and block all unknown inbound traffic so that the external network cannot reach their devices. The case organization's strategies aligned with the literature on the relevance of securing IoT devices in adopting IoT to protect against security violations.

Ties to the Conceptual Framework

DOI theory was the conceptual framework for this study. DOI's five characteristics align with the case organizations' IoT security strategy. Nikou (2019) stated that applying five characteristics of DOI theory helped in adopting smart home technology, which is an application of IoT. Still, privacy and security issues were factors identified that hindered the adoption of the technology. Additionally, the study's findings

revealed that three attributes of DOI, namely compatibility, trialability, and observability, influenced the usage intention of the technology (Nikou, 2019). Within each organization, the IT staff seemed to apply DOI theory to guide the adoption and implementation of security violation strategies for IoT.

Within each organization, the IT staff seemed to apply complexity and compatibility characteristics of DOI by conforming to existing security standards to secure IoT and making configuration changes. In their study, Waheed et al. (2020) asserted that as IoT devices are from different vendors with different standards and protocols, communications between these devices are often challenging, leading to malicious attacks. Therefore, there is a need for additional security measures. Participants 3, 4, and 5 indicated that they used security guidelines that best fit each unique case for different IoT devices and controls to address the compatibility and complexity of IoT devices. Management in each organization seemed to recognize the need to have an IoT solution with a robust framework that protected against security violations despite the complexity and incompatibility of the IoT devices.

The trialability characteristic of DOI theory is essential for organizations to test IoT devices' compatibility and security standards before integrating them into IoT networks. Testing is critical in developing a solution, especially in standardization (Zhang et al., 2019). The trialability characteristic of DOI theory aligned with Participant 1's feedback that as a normal standard, IoT devices that are brought to the IoT network are first connected to the test center to determine whether those devices are capable of running the software application. Participant 3 agreed that trialability is significant in

securing IoT devices. The strategy involves conducting testing in a sandbox or development environment that has no outside access to some of the other systems or other parts of the network, so that one can easily discover security flaws or vulnerabilities within the system ahead of time to avoid spreading them to other parts of the network. Participant 5 added, "This strategy proved to be effective because it provided an opportunity to carry a full security assessment of the new device so that IoT adopters could verify if those devices met policies and procedures."

Within each organization, the IT staff seemed to apply observability characteristics of DOI by monitoring how the existing security procedures such as access control and password authentication were enforced and a robust monitoring platform that could identify any malicious IP address. An aspect of observing a solution could be monitoring system performance and how efficiently resources are being utilized (Syed et al., 2017). Participant 4's feedback aligned with monitoring the system performance because one of the organization's strategies was to observe the security measures to monitor any security violations or have software that could detect any kind of breach in a network so that action could easily be taken to mitigate and remediate it. Participants 3 and 5 mentioned that their organizations' observation and monitoring strategy was continuous monitoring of the network to ensure that IoT devices securely communicated on the Internet and had strong and robust mitigation and remediation policies. Participants 1, 2, and 6 reinforced the point that the principle of defense and depth helps to ensure that there are many security measures in place. These participants further indicated that regularly monitoring whether best practices are being followed is

extremely important. Participants indicated that observability of IoT as a strategy is carried out to detect noncompliant devices, along with using security scans to check whether devices are hardened.

Within each organization, the IT staff seemed to apply relative advantage characteristics of DOI by having their products trusted more because customers have the confidence that their personal information is not compromised. Organizations protecting their IoT devices from security violations gives them a relative advantage over their competitors. Organizations adopt an IT solution to have a relative advantage over competitors, but that solution must be secured against outside threats (Naushad & Sulphey, 2020). Participants indicated that protecting their IoT devices against security violations gives them a relative advantage over their competitors because customers trust their products more. Participants 3, 4, and 5 pointed out that having a strategy to protect against security violations from IoT devices could ensure that employees' data are protected, giving their organizations wins in the industry. Participant 6's feedback was that security is being viewed as part of the quality of service. Participant 4 aligned with that strategy by stating, "Competitive advantage could mean having very strong security built into whatever kind of IoT devices we are using." Participant 2's feedback was that security creates a competitive advantage because they could talk about how they meet their business goals, such as reducing costs, optimize the process, and creating new business models. According to Mombeuil (2020), relative advantage and the envisaged security issues influence the adoption of an IT solution because of consumers' concerns regarding how their personal information could be collected and disseminated.

Participant 1's feedback aligned with that issue of personal information that could be collected and disseminated, by indicating that a big data breach will cost a lot of money, including paying some fines and losing reputation. Also, their competitor may have a relative advantage over them because of security breaches. Thus, the relative advantage of IoT required the case organization to have some strategies in place while adopting IoT to protect IoT devices from security violations.

Generally, the complexity of IoT devices required case organizations to have security standards to ensure that security violations are protected. Observability and relative advantage characteristics of DOI theory did not influence the security strategy; instead, they were significant in IoT adoption. If addressed, the problem of interoperability and security could make IoT devices' communication standard and an end-to-end security solution adaptable (Bujari et al., 2018). According to Bicaku et al. (2020), for organizations to be competitive and remain in business, their IoT devices need to comply with multiple standards as that supports interoperability among them. Observability and relative advantage were also not essential to security violations because of the lack of standards in securing IoT devices.

Theme 2: Identifying and Separating Personal and Confidential Data From Analytical Data

Results of Data Analysis

Identifying personal and confidential data from analytical data on IoT devices was the second theme that emerged from data collection and analysis. Ensuring that personal information is not compromised is vital for organizations to gain their customers' trust

and keep their reputation. Management in each organization seemed to recognize the importance of protecting personal and confidential data and tried to address the security violation component during the security breach discussions. All six participants at the case organizations indicated that personal data protection was a critical factor for IoT adoption. Six of 10 company documents supported the theme (see Table 3).

Table 3

Frequency of Second Major Theme

Major theme	Participants		Documents	
	Count	References	Count	References
Identifying personal and confidential data from analytical data	6	52	6	41

All six participants indicated the need for a strategy to protect data to ensure there are no security violations. Participants 2 and 5 indicated that data protection includes securing communication with the IoT device, ensuring proper encryption of data going to external customers, having password tokens and passwords changed periodically. Participants 1 and 6 mentioned encryption to ensure that data transmitted to external companies are protected from malicious attackers, and protocols are encrypted as well. Four of six participants also explained that their case organizations protect data against security violations whether they are sensitive or not. Participant 1 stated, “Securing personal and confidential data is very important to any organization because it could lead to violations of security regulations and security breach.” Management in each organization seemed to recognize the importance of data protection strategy to address

industry regulatory requirements. Participants 3, 4, 5, and 6 indicated that a data protection strategy is necessary for IoT because of the data generated from connected IoT devices. Participant 2 stated, “Data protection strategy includes ensuring that our organization mobile phones get regular updates using encryption to avoid eavesdropping and disclosure of sensitive and nonsensitive data sent over the Internet.” Also, Participant 5’s feedback was their organization has rules surrounding data protection, especially with cloud storage, to ensure that all sensitive data are encrypted and passwords changed periodically. All the participants indicated that protecting data from security violations is challenging because IoT aims at making data available for organizations to make informed decisions.

All the six documents of the case organizations revealed that identifying personal and confidential data from analytical data is a strategy to protect data to ensure there are no security violations. Documents 2 and 5 revealed that case organizations classify data to help mitigate risk and manage data governance policies related to IoT. Document 3 of one of the case organizations stated, ”We store most essential data or sensitive data of our customers separately from analytical data.” Also, Document 8 noted, “Our data classification method helps us to adhere to modern data privacy regulations.”

All the six documents of the case organizations revealed that they identify which compliance regulations or privacy laws apply to their organization and classify them accordingly. Document 5 of one of the case organizations clearly stated, “Data classification is one of the organization’s data protection strategy to identify sensitive

data." Document 4 further indicated "Identifying and classifying data helps our organization to protect sensitive data from adversaries and security breach."

Comparison to the Literature

An effective data protection strategy is necessary so that customers can trust products manufactured in an IoT environment. Multiple studies found in the literature support the data protection strategy described by the case organizations where IoT has been adopted. They expressed protecting against security violations as an essential factor in doing business. Khan et al. (2019) recognized the need for IoT adoption, but consumers are not aware of the extent to which their personal information is being collected and shared with third parties. In a study conducted by Hsu and Lin (2018) about factors affecting IoT adoption, they observed that perceived private information risks affect users from adopting IoT and IoT services. All the participants had the same notion about perceived private information risks. Participant 1's feedback was that encrypting data going to external clients is vital to their organization. Participant 3 added, "Our organization has encrypted protocols for IoT devices, for example, using HTTPS instead of HTTP for Web services."

The case organization's clients have some technology in place to ensure that data are protected. Participant 3 stated, "These data protection strategies enhanced trustworthy relationship between our organization and clients." Jiang et al. (2020) studied the data security protection method for power IoT proposed using a multilevel hidden authentication approach and encryption method to protect intruders from accessing personal data transmitted through the smart meter and other IoT devices on the network.

That statement aligned with Participant 1, “We have ‘managed’ PCs and IPCs that are scanned for virus and use encryption software to encrypt data going to third parties to protect personal data.” Besides, Participant 3 noted, “We employ the principle of least privilege so that only specific devices can talk to other specific devices as a strategy to protect personal data from exfiltration.” Veleva (2019) suggested that applying cryptographic techniques will allow protected data to be processed and stored without personal information being made available to external people for users accessing IoT remotely.

Further, Owoh and Singh (2018) proposed a security strategy that ensures mobile phone data are encrypted and authenticated using “Advanced Encryption Standard 256-Galois Counter Mode” so that users’ personal information is not compromised during data transfer. Participant 3’s feedback aligned with the issue of compromising personal information because the case organization uses cryptographic techniques for their employees who access their IoT network remotely. However, other studies in the literature mentioned alternative ways to protect sensitive data, such as anonymizing data but could be considered less effective. Bordel et al. (2021) indicated that data anonymization and authentication in IoT solutions have been challenging and require future work as they do not wholly protect private customer information. Adhering to regulatory standards on data protection has been an effective means of protecting customers’ personal information (Terry, 2017). Again, according to Nekit et al. (2020), regulatory bodies such as the European Commission and US Congress faction that was formed on issues of the IoT devices recommended that IoT companies should design

devices based on data security so that users will have the opportunity to choose the kind of information they want disseminated, to avoid data protection violations. The participants indicated they have all the mechanisms to protect personal and confidential data and strictly adhere to regulatory requirements. Participant 2 explained that their data protection strategy was simple and conformed to the regulatory requirements, and well-segmented to avoid exposing sensitive data. Participant 5 indicated that private data should not be allowed to make its way to the IoT devices. The case organizations' strategies align with the literature on data protection strategy for identifying personal and confidential data from analytical data in adopting IoT to protect against security violations.

Ties to the Conceptual Framework

The five characteristics of the DOI theory provide a detailed explanation of the case organization's data protection strategy. A study about IoT adoption in the manufacturing and usage of implanted devices indicated that the use of DOI theory helped develop a data protection strategy for the manufacturers and the end-users (Breese & Zwerling, 2020). Within each organization, the IT staff seemed to apply that theory in identifying and protecting private and confidential data during the analysis of IoT data and requirements gathering before the adoption.

Compatibility and complexity DOI characteristics played essential roles in their data protection strategy. The IT staff seemed to apply that strategy within each organization by separating confidential data from the analytical data. That data separation technique enabled the case organization to adopt IoT without worrying that sensitive data

would make it to the IoT device. Participant 2 stated, “We do not have any need to collect personal information of our customers, but when it did happen, they were segmented.” Participant 6 mentioned that data protection is an area that their organization takes seriously because of its risk. Participant 3 added, “We strive to provide customers with the best products and cannot afford to expose their personal information, hence the need for segmenting personal data from analytical data.” The complexity characteristic of DOI seemed to be applied within each organization because the heterogenous IoT devices created the need for having a data protection strategy of using segmentation of data to address the privacy violations associated with security violations while adopting IoT. Schneider et al. (2017) supported and applied the same strategy in their study on protecting customers' privacy when marketing with second-party data by indicating that data protection can be achieved by allowing data providers to protect all customer segmented data at the individual customer level instead of only at the aggregate level. A similar study about sensitive data segmentation technology for privacy included the use of Consent2Share software to segment health-sensitive data and other health data coming from electronic health records (EHRs) (Grando et al., 2020). Management in each organization seemed to recognize the need to have an IoT solution with a robust framework that protects the data of their employees and clients against security violations despite the complexity and compatibility issues of the IoT devices.

When analyzing the case organization’s data protection strategy, the trialability characteristic of DOI theory seemed to have played a significant role. Organizations use trialability to try an innovation before committing and can help customers accept a

product to be comfortable that their privacy is protected (Johnson et al., 2018). The trialability characteristic of DOI theory aligned with Participant 5's feedback that their case organization tests its data segmentation process to ensure that personal information is identified and separated from analytical data during IoT devices data processing. Participant 4 agreed that trialability is significant in securing IoT devices. The strategy for the case organization is testing the effectiveness of their access controls so that unauthorized users do not have access to their sensitive data. Participant 3 added, "This strategy proved to be effective because it provided an opportunity to review our security policy as it relates to IoT devices and data collection process." Four participants indicated that one of the strategies in testing data protection strategy is conducting periodic audit trail of the security and access control mechanisms to ensure there are no security violations. Participant 1's feedback was the case organization enforcement of periodic password change of IoT devices has been significant in protecting data from security violations. Management in each organization seemed to recognize the need to have an IoT solution with a robust framework that protects the data of their employees and clients against security violations by testing to ensure IoT devices meet standards and procedures for data protection.

Within each organization, the IT staff seemed to apply the observability characteristic of DOI by monitoring how the existing security procedures such as access control and password authentication are enforced and monitoring platform for data protection violations. The observability characteristic of DOI theory helps monitor the results of a solution or a mechanism put in place (Nikou, 2019). Participant 1's feedback

aligned with the observability characteristic of DOI theory because one of the case organization's strategies is observing the effectiveness of access control measures to protect against security violations because of a data breach. Participants 4 and 6 indicated that the case organization's observation and monitoring strategies monitor the IoT network to ensure that personal information is not being exposed and violated. The six participants reemphasized that their case organizations constantly review their security policy to ensure that new access control measures are implemented with the latest IT solutions. Within each organization, there was a recognition that observability of IoT as a strategy is carried out to detect data violations and other aspects of security violations within their IoT network.

Within each organization, the IT staff seemed to apply relative advantage characteristics of DOI by having their products trusted more because customers have the confidence that their personal information is not compromised based on the data protection strategy they have in place. Organizations protecting their IoT devices from data protection violations give them a relative advantage over their competitors. Organizations have a relative advantage over competitors by adopting IoT. Still, they should have a good understanding of the kind of data they would like their IoT devices to transmit to not expose data to cyber-attacks that could adversely affect the same organization (Rutherford, 2019). Each organization aligned with that concept and indicated that protecting data transmitted to IoT devices gives them a relative advantage over their competitors because customers trust their products more. Participants 1, 3, and 5 pointed out that having a strategy to protect their data against privacy violations ensures

that employees' data are protected. That strategy gives their case organizations a relative advantage over their competitors in the market. Participant 6's feedback was that data protection is being viewed as part of the quality of service for the case organization. Participant 2 aligned with that strategy by stating, "Competitive advantage could mean having very strong data protection mechanism built into whatever kind of IoT devices we are using." Relative advantage and the envisaged data protection issues influence the adoption of an IT solution because of consumers' concerns regarding how their personal information could be collected and disseminated (Mombeuil, 2020). In line with the envisaged data protection issues, Participant 3's stated, "Big data breach will cost a lot of money including paying some fines and losing reputation, and our competitor may have a relative advantage, and that is why we take data protection seriously." Thus, the relative advantage of IoT required the case organization to have some data-preserving and protection strategies in place while adopting IoT to protect IoT devices from security violations.

The complexity and compatibility characteristics of DOI theory as seemed to apply within each organization by the IT staff necessitated the need to adhere to regulatory standards to ensure that the privacy of individuals is protected. Observability and relative advantage characteristics of DOI theory seemed to have been applied within each organization by the IT staff had to influence their data protection strategy approach and were significant in IoT adoption. The trialability characteristic of DOI theory seemed to influence the constant review of the case organization security policy related to IoT adoption.

Theme 3: Adequate Budget for Securing Internet of Things Network Devices and Infrastructure as Key Factors in Internet of Things Adoption

Results of Data Analysis

Adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption was the third theme to emerge from data collection. Lack of budget for securing IoT devices and infrastructure has been a huge hindrance for some manufacturing industries in adopting IoT. The six participants seemed to recognize the need for management to have enough budget to purchase all the tools needed to prevent IoT devices and IoT infrastructure from being invaded by malicious attackers. Study findings revealed that the budget to secure IoT devices and infrastructure was one of the key factors considered in IoT device acquisition and adoption. That factor applies to other existing technology as well. All six participants in the case organizations indicated that securing IoT network devices and infrastructure is a key factor in protecting against security violations while adopting IoT, and 9 of 10 company documents supported the theme (see Table 4).

Table 4

Frequency of Third Major Theme

Major theme	Participants		Documents	
	Count	References	Count	References
Adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption	6	71	9	52

Six participants clearly expressed that enough budget to purchase all the tools is needed to prevent IoT devices and IoT infrastructure from being invaded by malicious attackers to protect against security violations in IoT networks. Having enough budget to purchase all the tools needed to protect IoT devices and IoT infrastructure is vital because it promotes customers' confidence in the manufacturer's products and prevents reputational loss because of a security breach. Participant 2 stated, "Having enough budget ensures the security of IoT devices, but this approach should occur at the planning stage of the project." Besides, Participant 6's feedback was that the case organization has enough budget to secure several firewalls at several IoT layers and implementation of DMZ to prevent DoS and ensure that intruders cannot connect to IoT devices. All participants mentioned having security strategies to protect the IoT devices could be achieved if management approves enough money to buy all the tools to protect the IoT devices and infrastructure from external attacks. Participant 4 aligned with that method of management approving enough money by stating, "We are a cost-driven organization and always looking at every cent, but still have adequate budget to protect our infrastructure from external attacks." Participant 3 added,

> When we experience a security violation or security breach, the information security team write it down and raise awareness, so at the end of the year we request for budget based on how the information security team presents it to management, for example, what happened, and necessary actions to be taken to prevent it from reoccurring.

Further, Participant 5 mentioned that their case organization often has enough budget to ensure that whatever IoT devices are added to the legacy network is protected to avoid security violations. Participant 1 added,

> Senior management must approve the necessary budget for IoT security, but the information security team needs to communicate the benefits and the risks of IoT in a way that they will understand, once senior management understands the value, and sees the total cost of ownership (including security) is outweighed by the value, then they will approve.

Five interviewed participants mentioned that the budget should include the cost of the IoT, infrastructure, and sometimes the wages of the employees maintaining the IoT environment, but such costs should be done at the planning stages. Two interviewed participants mentioned that an adequate budget should be set aside if something goes wrong, like a security breach that requires immediate mitigation.

All the nine documents of the case organizations revealed that adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption. Seven out of nine documents revealed that case organizations budget so much money to solve IoT security issues and protect IT infrastructure. Document 5 of one of the case organizations stated," If we don't provide an adequate budget to protect our IoT network and infrastructure, we are putting ourselves into security risk that can affect our market share." Also, Document 8 stated, "IoT budget covers storage capacity, network edge equipment, server infrastructure, and device maintenance."

All the nine documents of the case organizations revealed that as IoT devices are continuously transmitting data, hence the need to have enough budget to provide additional bandwidth for infrastructure and securing IoT devices. Document 8 supported that and stated, “Our organization’s IoT will expand demand and introduce additional information sources and access points that don’t come with own security protocols; hence we need enough money to protect the devices.”

Comparison to the Literature

Adequate budget for securing IoT network devices and infrastructure as a strategy for IoT adoption described by the case organization is in line with different studies found in the literature. Maintenance, business processes, and services cost of IoT devices such as IoT and radio frequency identification (RFID) devices influence IoT adoption (Yan et al., 2018). Having a device to act as a gateway for another device to protect devices against security vulnerabilities increases costs in an IoT platform (Martín-Lopo et al., 2020). The responses from six participants showed that their case organizations have an adequate budget to implement firewall so that IoT devices could be monitored and controlled to avoid external and malicious attacks. Zhou et al. (2019) study in financial risk management of IoT stated that due to data generated by IoT deployment, there is a need to have enough budget to manage any security breach's financial risk. Participant 1 stated, “We have a financial plan to mitigate any security breach that IoT device vulnerability might present, even as we strive to implement mechanisms to protect against security violations.” Also, Participant 3 mentioned that their case organization has a budget plan for software security updates or patches for their IoT devices. Danubianu et

al. (2019), in their study, used SWOT (Strength, Weakness, Opportunities, and Traits) method to analyze the strength and opportunities of IoT and suggested the need to have enough means to sustain the implementation of the solution in industries specifically to protect it against security violations. Yang et al. (2020) studied implementing an IoT solution called an intelligent building management system, suggested budgeting for the installation cost of devices, IoT infrastructure, and disaster prevention. Participant 2 stated, "The accounting department handles IoT budget planning because it is part of entire asset cost and enough budget is often made for any disaster recovery." The case organizations' strategies align with the literature on having an adequate budget for securing IoT network devices and infrastructure as a strategy for IoT adoption to protect against security violations.

Ties to the Conceptual Framework

DOI theory is the conceptual framework of this study, and the five characteristics align with the case organizations' strategy of having an adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption. Habiyaremye (2020) studied using DOI to explain the pace of innovation diffusion in the South African water sector and suggested that adoption costs and not having an adequate budget affect the adoption of water innovations. The study's findings also revealed that applying the five characteristics of DOI played essential roles in achieving balanced and sustainable water resources management along the entire value chain (Habiyaremye, 2020). Within each organization, the IT staff seemed to apply DOI theory as a guide when considering how

adequate budget influences adopting and implementing security violation strategies for IoT.

Within each organization, the IT staff seemed to apply compatibility characteristics of DOI by purchasing IoT devices that conform to the standards and procedures they apply to protect IoT devices from security violations. Rice and Hoffmann (2018) referred to the compatibility of DOI as having an IT solution that is easy to integrate, migrate and implement with existing systems. IoT devices from different vendors require extra security measures to manage their heterogeneous nature (Waheed et al., 2020). All six participants indicated that the heterogeneous nature of the IoT devices necessitated the need to have the budget for managing their configuration changes. Participants 2, 4, and 6 mentioned that their case organizations considered the security of IoT devices that could come from its incompatibility characteristic and made an additional budget for adding them to their legacy network at the beginning of the IoT project. Participant 6 stated, "Our organization does a risk assessment or security risks of the IoT devices ahead of time to ensure that enough budget is provided for managing them." Participant 3 also stated," The concept of bringing your device poses compatibility issues, hence the need for an adequate budget to manage their vulnerabilities." The management in each organization seemed to recognize the need to have an adequate budget to manage the compatibility issues with IoT devices to protect them against security violations.

Within each organization, the IT staff seemed to apply the complexity characteristic of DOI theory by having an adequate budget to protect IoT devices from

malicious attacks due to the complexity of the IoT devices. In their study, Jacob et al. (2020) indicated that the complex nature of IT solutions coupled with budget deficit could affect adopting those solutions. Management in each organization seemed to recognize that approach, and their strategy is having enough budget to purchase IoT devices that are interoperable with the existing technologies. Participant 3 stated,

> The right thing our organization does is building this complex nature of IoT devices in the planning stages of IoT adoption, this helps us not to be scrambling for money if there is a security breach as a result of this complexity.

Yoo et al. (2020), in their study on a user acceptance model of bitcoin transaction services, considered perceived risk, budget, and complexity as factors that could influence user's adoption of the solution. Participant 2's feedback aligned with that factor because their case organization ensures enough budget to have IoT devices patched regularly due to their heterogeneous nature to protect them from security violations. Participant 5 stated, "Part of our organization's budget for IoT devices covers headcount of the number of employees that will maintain them due to the complex nature of these IoT devices to ensure security." Participant 1 further added, "Our organization has the budget to cover service level agreement (SLA) costs from external companies maintaining their complex IoT devices." The participants recognized the need to have an adequate budget to manage the complexity characteristic of IoT devices to protect them against security violations.

The trialability characteristic of DOI theory is essential for organizations to test IoT devices' compatibility and security standards before they are integrated into IoT

networks, and requires an adequate budget to be set aside. Testing an IoT solution can be done in a real live Testbed or any test environment (Sheikh & Halima, 2017). The trialability characteristic of DOI theory aligned with Participant 1's feedback that their case organization has an adequate budget to maintain their test center because IoT devices that are being brought to the IoT network are first connected to the test center to see if those devices can run the software application. Participant 2 agreed that trialability is considered a factor in the operational budget because enough money is needed for securing IoT devices. Their case organization strategy is conducting the testing in a sandbox or development environment that has no outside access to some of the other systems or other parts of their network so that they quickly discover security flaw or vulnerability with the system ahead of time to avoid spreading to other parts of the network. Participant 4 added, "Having adequate budget as a strategy proved to be effective because it provides enough money to carry a full security assessment of the new device so that our organization could verify if those devices met policies and procedures." The six participants indicated that an adequate budget to carry out full testing of the IoT devices before they are connected to their case organizations' IoT network is significant in protecting against security violations while adopting IoT.

Within each organization, the IT staff seemed to apply the observability characteristic of DOI by monitoring how the budget for maintaining IoT and infrastructure is used to protect against security violations. In their study, Yu et al. (2020) indicated that if the maintenance costs of IoT solution, if not monitored while ensuring tolerable sensing quality and complete connectivity, could affect the overall adoption.

Participant 3's feedback aligned with Yu et al.'s study because one of the case organization's strategies is observing how the money budgeted for IoT device maintenance is spent to ensure that security breaches are prevented. Participants 2 and 4 mentioned that their case organizations' budget monitoring strategy helps them know when certain IoT devices should be retired from the network because they could be obsolete and vulnerable to security attacks and violations. Participants 1, 5, and 6 reemphasized that an adequate budget is necessary for their case organizations to implement some security framework such as the principle of defense and depth that helps make sure that there are many security measures in place. The six participants further indicated that regularly monitoring with an adequate budget is a strategy that allows their case organizations to react immediately if a security breach occurs, such as having resources to implement network segmentation. Also, participants emphasized that observability of IoT as a strategy is applied to know the areas to channel their budgeted money in their IoT networks.

Within each organization, the IT staff seemed to apply relative advantage characteristics of DOI by having an adequate budget to protect their IoT devices and infrastructure from security violations. Their products could be trusted more, and customers have the confidence that their personal information is not compromised. Organizations knowing the cost associated with the implementation of IoT and the cost of making IoT devices secure gives them a relative advantage over their competitors (Tedeschi et al., 2018). Participants indicated an adequate budget for protecting their IoT devices and infrastructure against security violations gives them a relative advantage over

their competitors because it builds more trust from their customers. Six participants pointed out that having enough budget for protecting IoT devices and infrastructure is a strategy that helps their case organization to protect against security violations from IoT networks. Participant 5's feedback was that having enough budget has helped their case organization implement firewalls and DMZ that protect customers' data from security violations. Participant 2 aligned with that strategy by stating, "Our organization having an adequate budget to protect our IoT devices makes us have a competitive advantage because our products are trusted more, and the information security team has little to worry about." Participant 4's feedback was that an adequate budget creates a competitive advantage because they could improve the business to be more competitive in the market instead of worrying about a limited budget to protect their IoT devices and infrastructure. Cost and insecurity can affect the adoption of an IT solution, but when managed can give adopters a relative advantage over their competitors because the customer will trust their products and services (Mombeuil, 2020). Participant 3's feedback aligned with Mombeuil's study by indicating that a security breach could cost a lot of money, including paying some fines and losing reputation, and their competitor may have a relative advantage over them; that is why their case organization ensures that they have adequate budget to protect their IoT devices and infrastructure. Thus, the relative advantage of IoT required the case organization to have some strategies in place while adopting IoT to protect IoT devices from security violations. Participants 4 and 6 indicated that regular software patch of their IoT devices and proper maintenance of IT infrastructure gives their case organization relative advantage over their competitors, so

they have adequate budget to cover the cost associated with it. Participant 2 stated, “Our management usually approves enough money for the maintenance of IoT devices and infrastructure once they understand the return-on-investment IoT provides.”

The complexity and compatibility characteristics of DOI required case organizations to have an adequate budget to protect the heterogeneous IoT devices to ensure that security violations are protected. Observability and relative advantage characteristics of DOI theory did not explicitly play any role in the security strategy. Instead, they were significant in monitoring how the budget allocated for IoT devices' protection was disbursed in IoT adoption.

Theme 4: Risk Mitigation Policy Relevant to Securing Internet of Things Devices

Results of Data Analysis

Risk mitigation policy is relevant to securing IoT devices was the final theme to emerge from data collection. The confidentiality, integrity, and availability (CIA) triad concerns have been a considerable hindrance for some manufacturing industries in adopting IoT. Management in each organization seemed to recognize the need to ensure IoT devices are prevented from attacks such as distributed denial of service (DDoS) and eavesdropping on their network traffic or other devices on the same network segment. One of the risk mitigation strategies employed by case organizations is having a vulnerability management framework that identifies and eliminates known vulnerabilities in IoT device software and firmware to ensure that their devices are not compromised or exploited. All six participants in the case organization recognized the need to have an effective risk mitigation policy to ensure that IoT devices are proactively managed. Any

vulnerabilities or unauthorized and improper physical and logical access to IoT devices are eliminated to protect against security violations. Study findings revealed that risk mitigation is a strategy to protect devices, individuals' privacy, and data from security violations while adopting IoT. All six participants at the case organization indicated that new vulnerabilities are being constantly discovered, which means there is a need to monitor, maintain and review risk mitigation policy regularly as a strategy to protect IoT devices against security violations, and 9 of 10 company documents supported the theme (see Table 5).

Table 5

Frequency of Fourth Major Theme

Major theme	Participants		Documents	
	Count	References	Count	References
Risk mitigation policy relevant to securing IoT devices.	6	72	9	49

Six participants clearly expressed that risk mitigation policy ensures that their case organizations protect customers' and employees' privacy by being exposed by personally identifiable information (PII) processing from IoT devices by applying data classification. Participant 1 stated, "Risk mitigation and remediation policies help to monitor and analyze the IoT devices' activities to ensure that personal information is not compromised." Also, Participant 3 stated, "To ensure the reliability of IoT, we need to protect the confidentiality, integrity, and availability of data transmitted through IoT devices." That strategy from the case organization includes preventing access to sensitive

information and not allowing manipulation and disruption of IoT device operations. All six participants mentioned the need to have regular monitoring and analysis of IoT devices to protect against security violations. Three interviewed participants mentioned that their case organizations have measures that detect when IoT devices have tampered with to not be decoded. Participant 1 stated, “We have a mechanism called remote wiping that ensures that data related to personal information is erased from a device that is compromised to prevent them from being used maliciously.” Participant 5 further stated, “Part of risk mitigation strategies employed is having a unique identity for the IoT devices in our IoT network, to ensure the authenticity of the device.” In line with that strategy, five participants mentioned that their case organizations ensure that their device’s UDID is not copied, monitored, or captured. Their devices, when registering online, are not vulnerable to interception, surveillance, or unlawful monitoring by adversaries. Participant 6 also stated, ”Our constant reviews of the risk mitigation IoT security policies ensure that our products meet security requirements.”

All the nine documents of the case organizations revealed that risk mitigation policy is relevant to securing IoT devices. Eight documents revealed that case organizations use strong passwords and security keys, and regular updates as a part of the risk mitigation strategies. Document 6 of one of the case organizations stated,” Risk mitigation is essential for our IoT and includes monitoring the devices and systems to detect and respond to security events, and continuously updating the security of devices with the download of software patches from the manufacturers.” Document 9 stated, “We upgrade our devices and apply security patches, something like firmware updates.”

Furthermore, Document 7 stated, “Educating employees on the effects of PII processing by IoT devices could be seen as a risk mitigation strategy.”

Six documents of the case organizations revealed that part of the risk management strategy is applying network segmentation by categorizing devices. Based on the connectivity requirements of each IoT endpoint, they can isolate or block network access to endpoints that do not need it. Document 6 clearly stated, “Our network segmentation strategy prevents attackers or malicious insiders from connecting to IoT devices or can prevent compromised devices from infecting other parts of the network.” Besides, Document 9 stated,

> Part of our segmentation strategy is having a list of IoT devices we are currently using and the connection methods, how and what type of data they transmit, and which other devices on the network each device needs to connect to.

Comparison to the Literature

The risk mitigation policy to secure IoT devices described by the case organizations is in line with different studies found in the literature where IoT adopters have been skeptical in adopting the solution due to security concerns. Bhattarai and Wang (2018) studied the security and privacy challenges of IoT, including several ways to mitigate risks. They found that layering and limiting, identifying, and tracking the location of all IoT devices in a network, adopting a fog computing architecture, and IoT application developers leveraging a defense-in-depth strategy are some of the different methods to mitigate risks. Participant 2 aligned with that strategy and stated, “Defense in depth concept is about physical security, something as simple as locking the control

cabinet or locking the server room, blocking unused ports and use specific security devices." Having a unique identifier and proper characterization of vulnerabilities helps in risk assessment and designing risk mitigation strategies (George & Thampi, 2019). Participant 4's feedback aligned with that strategy because their case organization has a unique identity for their different IoT devices connected to their management consoles. The need for some IoT adopters to work on a limited budget while ensuring that IoT devices are protected from security violations necessitated the need for risk assessment and mitigation strategies (Stergiopoulos et al., 2020).

Seliem et al. (2018), in their survey on solutions to rising privacy concerns from a multipoint of view to identify the risks and mitigations, proposed **c**ryptography technology as one of the risk mitigation strategies for privacy protection, confidentiality, integrity, and authenticity of an individual's data. Participants 3, 5, and 6 indicated that their case organizations use encryption to ensure that no one can eavesdrop on the data they are sending over the internet from their mobile devices or other devices on the IoT network as a risk mitigation strategy. In their study on risk assessment methodologies for the internet of medical things, Malamas et al. (2021) indicated that risk mitigation in IoT involves assessing potential security risks because it is easier to mitigate threats, identify vulnerabilities, and reduce the exposure and impact of security breaches. Participant 4's feedback aligned with that strategy because their case organization uses a secure software development platform to reduce the vulnerabilities, identify vulnerabilities by coding or classifying them. Also, Participant 2 stated, "The IoT devices are updated regularly, and these software patch updates are transparent to users to avoid anyone obstructing the

patching process." According to Alvarez et al. (2021), one of the risk mitigation strategies is having security policies that will manage security risks associated with IoT and Big Data, including cryptography, credential management, and password management. Participant 3's feedback aligned with that strategy and indicated that their case organization has security policies in place on how to protect their IoT networks, implementing firewalls or endpoint protection, and network segmentation.

Furthermore, an IoT framework risks should be prioritized, and IoT threat modeling used so that necessary actions for mitigation of those risks could be taken (Kandasamy et al., 2020). Six participants agreed with that strategy and indicated that their risk mitigation processes involve de-identification and classification of data to understand their threat or security level to enhance privacy controls in terms of data protection. The case organizations' strategies align with the literature on risk mitigation policy as being relevant to securing IoT devices and protecting against security violations while adopting IoT.

Ties to the Conceptual Framework

DOI theory is the conceptual framework of this study. The five characteristics align with the case organizations' risk mitigation policy to secure IoT devices and protect against security violations while adopting IoT. The Liu et al. (2017) study indicated that applying the five characteristics of DOI theory helped understand the impact risk mitigation efforts have in adopting a solution. Within each organization, the IT staff seemed to apply DOI theory to apply risk mitigation policy as a strategy for securing IoT devices and protecting against security violations while adopting IoT.

Within each organization, the IT staff seemed to apply compatibility characteristics of DOI by using risk mitigation strategy to ensure that IoT devices being incompatible with the existing technology does not constitute security vulnerabilities. IoT devices are from different vendors with different standards and protocols; communications between these devices are often challenging, leading to perceived vulnerabilities, threats, and security risks (Waheed et al., 2020). Participants 2, 4, and 6 indicated that their case organizations embed cryptographic key pairs into IoT devices to enhance encrypted communications with the existing technology because these devices come from different vendors. Also, Participant 1 stated, "There are some IoT devices we don't use because they do not support encrypt communications." All six participants indicated that they implement different protocols for heterogeneous IoT devices within the same system as a risk mitigation strategy to ensure security and interoperability between protocols that occur because of incompatibility. Management in each organization seemed to recognize the need to have an IoT solution with a risk mitigation policy to protect IoT devices against security violations despite the compatibility issues with existing technology.

Within each organization, the IT staff seemed to apply the complexity characteristic of DOI by using a risk mitigation strategy to ensure that the complex nature of IoT devices does not pose some security risks when connected to the existing IoT network. Malamas et al. (2021) noted that the classification of medical devices helped to synthesize the risks involved during the adoption of the Internet of Medical Things to ensure security requirements are met. All six participants indicated that their case

organizations use a unique identifier for their IoT devices as one of the risk mitigation strategies for reducing the impact of vulnerabilities associated with the complexity of IoT adoption. Besides, Participant 6 stated, "We register IoT devices in our database and have a standard operating procedure that ensures new IoT devices are registered and assigned unique identity." Furthermore, Participants 3, 4, and 5 indicated that part of their case organizations' effort in mitigating risk is to maintain an inventory of the devices they have in their IoT network because the more knowledge they have about these devices, the more they can respond effectively to security breaches. The participants recognized the need to have an IoT solution with a risk mitigation policy to protect IoT devices against security violations despite the complexity of IoT adoption.

Within each organization, the IT staff seemed to apply the trialability characteristic of DOI theory in testing their risk mitigation and policies for securing their IoT network from security violations. Hirman et al. (2020) studied design, fabrication, and risk assessment of IoT unit-to-reliability improvement of products manufactured in the Industry 4.0 factory, applied risk analysis, risk assessment, and recommended high-risk mitigation strategy to the whole approach should be tested. Participant 2 stated, "Testing of their risk mitigation strategy is essential to our organization because so many distributed denial-of-service botnet attacks can manipulate their IoT security policy to gain access to our data or even shut down operations entirely." Also, Participant 6 stated, "We use quality risk analysis which includes test plans to cover the risks as a way of testing our risk mitigation policy."

Meanwhile, Participants 1 and 4 indicated that testing the risk mitigation policy by their case organization is carried out by their information security team or incident response team. If risks are identified, the information security team can update the policy with the identified risks during their reviews as mitigating action. Participant 1 added, "This strategy proved to be effective because it provides our organization the opportunity to identify and evaluate security risks to ensure that IoT networks are protected from security violations." The participants recognized the need to test and review the risk mitigation policy as a strategy to protect IoT devices against security violations.

Within each organization, the IT staff seemed to apply observability characteristics of DOI by monitoring the effectiveness of their risk mitigation policy in executing the existing security procedures such as access control, password authentication, and having a robust monitoring platform that can identify and classify different kinds of threats and vulnerabilities. A risk mitigation strategy is essential for observing when errors are present in the algorithms of an IoT solution, such as a smart grid, which helps identify devices that have been compromised (Ding et al., 2020). All six participants indicated that when devices are unmonitored, it opens their case organizations to unwarranted access, thereby allowing other IoT devices to access their network, leading to security breaches: thus, the need for a risk mitigation strategy. Participant 5 stated, "The result obtained from risk assessment and analysis is one of the ways we monitor the effectiveness of our risk mitigation policy." Participant 2's feedback aligned with that strategy because one of the case organization's strategies is observing the effectiveness of risk mitigation policy using software that can detect any breaches in a

network to easily mitigate it. Participants 5 and 6 mentioned that observation and monitoring applying to their case organizations are continuous monitoring of the network to ensure that IoT devices securely communicate on the Internet as contained in the mitigation policy. Participants 3, 4, and 6 indicated that their case organizations monitor risks so that management can act quickly when there is a potential threat or when security risk goes outside tolerance levels. Participants emphasized that observability of IoT as a strategy is carried out to determine the effectiveness of the risk mitigation policy.

Within each organization, the IT staff seemed to apply relative advantage characteristics of DOI by having their products trusted more because risks are assessed and mitigated. Hence, customers have the confidence that their personal information is not compromised. Organizations protecting their IoT devices from security violations give them a relative advantage over their competitors, which may be achieved by having a strong risk mitigation policy. Kropp and Totzek (2020), in their study on how system characteristics influence business-to-business (B2B) customer acceptance of smart product-service systems (PSSs), indicated that IT solutions have a relative advantage over the other if the risks are identified and mitigated. Participants indicated that having a risk mitigation policy gives them a relative advantage over their competitors because vulnerabilities and threats are detected ahead of time, ensuring that their devices are protected against security violations. All six participants indicated that having a risk mitigation strategy ensures that the customer's personal information and employees' data are proactively protected, thereby making their products more trusted. Participant 6's feedback was their case organization, first identifies the risk, followed by observed

strategies. A contingency plan is put in place to lower the risk's impact, ensuring that they have products devoid of security violations. Participant 3 aligned with that strategy by stating, “Risk mitigation policy strategy for our organization could mean having strong security built into whatever kind of IoT devices we are using.” Participant 3’s feedback was that their constant review of the risk mitigation policy gives them a competitive advantage over their competitors. Their case organization identifies new vulnerabilities or threats and implements actions to minimize the impact or likelihood of the risk.

Furthermore, the Sivathanu (2018) study in applying the behavioral reasoning theory (BRT) to examine the adoption of IoT-based wearables for the healthcare of older adults suggested that risk barrier influences the relative advantage and adoption of an IoT solution. Participant 4’s feedback aligned with that suggestion by indicating that they adjust risk mitigation policy from time to time to eliminate or reduce the risk for their case organization to remain competitive. Therefore, the relative advantage characteristics of DOI as seemed to apply within each organization by the IT staff was assessing the vulnerability of IoT network and infrastructure to specific threats and identify ways to reduce those risks to have a competitive advantage over others.

In a nutshell, DOI's complexity and compatibility characteristics required case organizations to have a risk mitigation policy strategy to identify, characterize, and assess threats to ensure that IoT devices are protected against security violations. Observability and relative advantage characteristics of DOI theory influenced the risk mitigation strategy and were significant in IoT adoption.

Applications to Professional Practice

The specific IT problem that formed this research study was that corporate-level IT leaders lack strategies to protect against security violations while adopting IoT in the manufacturing industry. Participants in this study discussed their strategies that corporate-level IT leaders might use to protect against security violations while adopting IoT in the manufacturing industry. All the participants stated that they relied on standards and regulations to guide when adopting the best strategy. After analyzing collected data, four major themes emerged: the relevance of securing IoT devices in IoT adoption, identifying and separating personal and confidential data from analytical data, adequate budget for securing IoT network devices and infrastructure as key factors in IoT adoption, and risk mitigation policy relevant to securing IoT devices. Corporate-level IT leaders may use these results as a guide to developing security violation strategies before IoT adoption.

New vulnerabilities are being constantly discovered, which means there is a need for corporate-level IT leaders to monitor, maintain, and review risk mitigation policy regularly as a strategy to protect IoT devices against security violations. A complex system like IoT still lacks risk analysis and mitigation strategies. Therefore, there should be a framework for mitigation decisions such as the risk analysis process (Kieras et al., 2021)

Also, the findings on risk mitigation strategy may help corporate-level IT leaders to prepare for new threats proactively and nip them in the bud; this strategy could be achieved by assessing the security risks. George and Thampi (2019) recognized the need

to have risk mitigation strategies to secure the industrial devices and controls from the vulnerability-based threats and discussed having unique identification and characterization of vulnerabilities as essential in designing risk mitigation strategies. Some of the risk mitigation strategies revealed in this study include applying network segmentation by categorizing devices. Based on the connectivity requirements of each IoT endpoint, IT staff can isolate or block unwanted network access to endpoints to protect IoT devices from security violations such as compromising individuals' privacy and data because of IoT adoption. According to Mhaskar et al. (2021), network segmentation means having resources of different security levels being placed in different zones protected by firewalls and putting resources with similar policies under the same firewall.

In IoT adoption, maintenance cost plays an increasingly significant role. Without careful management, costs can reach up to 80% of the total expenses in deploying IoT and will gradually replace installation cost as the dominant role in expenditure (Yu et al., 2020). Yu et al.'s research study provided the security challenges in adopting IoT. The management in each organization seemed to recognize that having enough budget for securing IoT devices and maintaining infrastructure is vital to IoT adoption. Therefore, corporate-level IT leaders need to have enough budget for securing and maintaining IoT devices and infrastructure as a strategy to protect IoT devices against security violations.

The findings further revealed that data-preserving, identification, and classification might help IT staff ensure that sensitive data are not exposed and compromised because of IoT adoption. Cano and Cañavate-Sanchez (2020) stated that

disclosure of personal and private information is one of the main challenges of the Internet of Medical Things (IoMT) and proposed a method that preserves the privacy of data sent by IoMT devices to the cloud. Also, Amin and Hossain (2021) analyzed the existing and evolving edge computing architectures and techniques for smart healthcare, applied data identification techniques in classifying vital signs using state-of-the-art deep learning techniques. Besides, IoT has broader characterization, where diverse data or information could come from ubiquitous and persistent sources, hence the need for their classification and protecting them from security violations (Huang et al., 2018).

A lot of industry standards and frameworks such as Industrial Internet Consortium (IIC) and OpenFog Consortium for manufacturing IoT device, communication protocols, and security violations guidelines and requirements have been proposed which detail mechanisms on how to best integrate IoT devices into IoT networks (Gebremichael et al., 2020). The findings from the Gebremichael et al. study may help corporate-level IT leaders seeking to adopt IoT to ensure that they comply with standards and requirements while adding IoT devices to their IoT networks as one of the ways to secure IoT devices against malicious attacks.

Furthermore, the findings revealed that corporate-level IT leaders should consider having the following strategies for protecting IoT devices against security violations. The strategies include weak link elimination by making sure that devices communicate to known IP addresses or domain names and block all unknown inbound traffic so that external network is unable to reach their devices, constantly review their security policies to ensure that their products meet security requirements, have industrial firewall before

the IoT networks that will protect it from a malicious attacker who tries to change the network parameter and ensuring IoT devices are patched regularly. According to Cangea (2019), security strategies could mean the protection of information and informatics systems from unauthorized access from using, exposing data, interception, modification, or destruction of information; an example is protecting the network that connects IoT devices and their data to back-end systems; antivirus and antimalware, firewalls and systems used for preventing and detecting the intrusions. Application of these findings would be significant to IT practitioners and may aid in solving the specific IT problem in several ways.

The five characteristics of the DOI theory helped in describing the findings of this research study. The trialability characteristic of the DOI theory refers to how innovation could be tested on a limited basis (Karahoca et al., 2018). Trialability stood out for the participating organizations due to the need to test IoT devices before connecting to the existing IoT networks. Participants seemed to test all themes identified in the Karahoca et al. study by conducting pilots and system integration tests. These tests put so much confidence on the corporate-level IT leaders on products coming from IoT adoption because of various strategies to protect IoT devices against security violations. Therefore, corporate-level IT leaders in the manufacturing industry seeking to adopt IoT should test their devices for vulnerabilities before added to the IoT network.

The complexity characteristic of the DOI theory refers to the extent to which an innovation is perceived as relatively difficult to understand and use (Yoon et al., 2020). Management in each organization seemed to recognize the heterogeneous nature of IoT

devices, the threats, and vulnerabilities it presents. The complexity characteristic of DOI theory as seemed to apply within each organization by the IT staff necessitated the need to have strategies such as inventory of IoT devices and assignment of unique identifiers to manage the security violations such could present. Therefore, corporate-level IT leaders in the manufacturing industry seeking to adopt IoT may have strategies such as network segmentation, defense in depth, inventory of IoT devices, and assignment of unique identifiers to manage the security violations because of the heterogeneous nature of IoT devices.

Compatibility characteristic of the DOI theory refers to how innovation is perceived to integrate with the existing technology or practices (Yoon et al., 2020). The compatibility characteristic of DOI theory as seemed to apply within each organization by the IT staff necessitated the need to have strategies such as network segmentation and defense in depth to manage the security violations such could present. Therefore, corporate-level IT leaders in the manufacturing industry seeking to adopt IoT may have strategies such as network segmentation and defense in depth to manage the security violations because of the heterogeneous nature of IoT devices.

Observability characteristic of the DOI theory could mean how available and visible an innovation is to adopters (Mamun, 2018). The observability characteristic of DOI theory as seemed to apply within each organization by the IT staff helped in the constant monitoring of the strategies to ensure their effectiveness. The observability characteristic of the DOI theory includes the identification and classification of risk and having a risk mitigation strategy to prepare for new vulnerabilities and threats and

monitor their effectiveness. The corporate-level IT leaders were well prepared to answer questions from customers and external clients relating to security and privacy violations, having observed that their strategies were working. Therefore, corporate-level IT leaders in the manufacturing industry seeking to adopt IoT may have strategies such as identification and classification of risks and having a risk mitigation strategy to prepare for new vulnerabilities and threats and monitor their effectiveness.

The relative advantage characteristic of the DOI theory refers to how an invocation is perceived to be better than its competitors (Mamun, 2018). The relative advantage characteristic of DOI theory as seemed to apply within each organization by the IT staff helped corporate-level IT leaders to recognize that protecting IoT devices against security violations gives them a competitive advantage over their competitors. Customers are attracted to products that guarantee that their personal information is not compromised. Therefore, corporate-level IT leaders in the manufacturing industry seeking to adopt IoT should observe the security and privacy violations strategies they have to have a relative advantage over their competitors in the market.

Corporate-level IT leaders in the manufacturing industries should ensure a robust framework with the five characteristics of DOI theory as a model for building security violations. The application of these five characteristics of DOI theory may help adopt IoT with proper protection against security violations.

Corporate-level IT leaders should see the need to secure IoT devices as a priority. Securing IoT device as a priority includes, among others, having a regular review process where security violation strategies are deliberated. The review process should be all-

encompassing, and employees have opportunities to speak freely.

The product consumers should have a trial period to test the effectiveness of these strategies to ensure that meeting these security violations is met. Corporate-level IT leaders should encourage feedback from product customers and incorporate them in the overall strategies to protect IoT devices against security violations.

Implications for Social Change

The findings from this research study may add to the existing body of knowledge on the security violation strategies necessary to protect against IoT devices while adopting IoT in the manufacturing industry. The implication for social change may include the need for IT organizations to develop tools that will detect threats, prevent malicious attacks, and monitor IoT networks for any IoT device vulnerabilities. This study's findings and recommendations may serve as a basis for positive social change for the manufacturing industry because they may provide opportunities to prevent any big data breach that could cost them a lot of money, including paying some fines and losing reputation; that could lead to a competitor having a relative advantage over them.

The study data and findings revealed that another social implication is that it may help industrial manufacturing by efficiently utilizing natural resources. For example, remote-control thermostats in industrial manufacturing might help in better utilization of natural resources. Another natural resource benefit of IoT is that it may provide an efficient way of conserving water supply. For example, intelligent water management has become a viable option to preserve water resources, and IoT is making it possible. Another example is that the introduction of IoT-based smart water meters may help

consumers understand what they use and help them downsize their consumption to be more conservative, especially in areas where droughts are the norm. Besides, in terms of electricity usage, it may provide a more efficient resource consumption through increased use of smart meters by consumers to get rid of estimated bills, control, and reduce energy consumption.

The positive societal implication is that the findings may lead to increased trust by the public that personal data will not be compromised, potentially leading to greater IoT use. The greater use of IoT may have myriad societal benefits such as fuel and cost savings from the greater use of smart cars. Furthermore, the application of the findings may lead to better ways of protecting IoT devices that may provide efficient parking systems by helping people working in the cities with an easier way of parking by detecting available parking spaces and having smart cars that take small parking spaces.

Also, the social implication in having security strategies for protecting IoT devices is that it may help organizations' employees use smartphones to share information about their products and promote social media and other forms of social networking. Another example is that the use of smartphones connected to IoT may simplify people's lives because it may be possible to interlink many gadgets and exchange information like Bluetooth and Wi-Fi connected to wearables, wristwatches, eyeglasses, and smartphones.

Moreover, the findings may help in family relationships, and customers may trust IoT products because they will understand that their personal information is not being compromised by using IoT devices. For example, such trust may help healthcare reduce

hospital visits, and the IoT used for medical device sensors to obtain health data from the patient, transferred to the mobile app. The data can be transferred remotely to the doctor or family members in case of an emergency.

Recommendations for Action

This research study explored strategies that corporate-level IT leaders in the manufacturing industry use in protecting against security violations while adopting IoT. The findings revealed that having strategies to protect against security violations while adopting IoT in the manufacturing industry is essential and will provide value to the business and ensures that internal and external customers trust IoT products.

Corporate-level IT leaders in the manufacturing industry should build a culture where protecting against security violations is a priority for IoT adoption. The management of the manufacturing industry should have a formal review process with cross-functional teams where they discuss security violation strategies with an emphasis on risk mitigation. Employees should be encouraged to attend and speak freely. The result of the review processes should lead to well established IoT implementation strategy.

Corporate-level IT leaders in the manufacturing industry should secure their IoT devices so that their customers would build trust in their products and organizations can focus more on the day to day running of their manufacturing plants to increase productivity and efficiency without worrying about managing access controls or preventing adversaries from accessing their IoT devices. Corporate-level IT leaders should secure IoT devices by applying network segmentation by dividing the network

into different segments that help control traffic between devices. If they are not segmented, any malicious entry can easily spread the entire IoT network endpoints when communicating directly. Manufacturing organizations should use VLAN configurations and next-generation firewall policies to implement network segmentation, keeping IoT devices separate from other IT assets.

Manufacturing industry corporate-level IT leaders should identify and separate all IoT sensitive data from the analytical data to protect user privacy, thereby ensuring that sensitive data do not make it to IoT device processing. Also, as part of data protection and preserving strategies, corporate-level IT leaders should use encryption to keep all IoT private data secured and maintain their integrity when employees and customers are sharing confidential data. Corporate-level IT leaders should avoid using PII or sensitive information to protect IoT users from exposing personal and confidential information. Identifying and classifying these data is one way of achieving the protection of personal and confidential information.

Manufacturing organization corporate-level IT leaders should limit physical access or connection to the network where the IoT device is located, and that approach will reduce vulnerabilities. Lack of physical security can make it easy for hackers to gain access to IoT networks through IoT devices and expose IoT infrastructure to exploits. Corporate-level IT leaders should ensure that they have strategies to mitigate against two types of physical security attacks: noninvasive and invasive attacks.

Corporate-level IT leaders in the manufacturing industry should provide enough budget for securing IoT devices and maintain IoT infrastructure. Lack of a budget for

securing IoT devices and infrastructure has been a huge hindrance for some manufacturing industries in adopting IoT. The management team of the manufacturing industry should recognize the need to have enough budget to purchase all the tools needed to prevent IoT devices and IoT infrastructure from being invaded by malicious attackers. Also, corporate-level IT leaders should have enough budget to secure several firewalls at different IoT layers and implement DMZ to prevent DoS and ensure that intruders cannot connect to IoT devices.

Manufacturing industry corporate-level IT leaders should include high availability and data preservation as an overall IoT security violation protection to prevent downtime of IoT networks and make them reliable. Manufacturing industry corporate-level IT leaders should include getting feedback from customers on their impression of IoT products related to data privacy and the best way to protect against security violations in the IoT environment.

Corporate-level IT leaders should apply existing IoT best practices and those found in this research study since IoT lacks standards. Manufacturing industry corporate-level IT leaders should collaborate with their external clients to deliver an IoT solution to agree on effective strategies to reduce vulnerabilities. Such collaboration will enhance a robust framework for security strategies that will add value for all parties. Corporate-level IT leaders in the manufacturing industry who seek to adopt IoT should understand the current information on security violations because new threats constantly emerge. The manufacturing industry must understand the security violations and the benefits of IoT adoption.

I will disseminate a high-level summary of the results of this study to the research participants via email. I will share a high-level summary of the results of this study with the interested organizations, stakeholders via email. Last, I will share a high-level summary of the results of this study, possibly using conferences, trade journals, and training seminars.

Recommendations for Further Study

My research study provides various recommendations for further research, some coming from the limitations stated in this research and others being obtained from the findings of this study. The limitations of this research included that participants may not fully provide the data necessary to answer the research question. That limitation could be because of the interviewees' bias towards IoT or IoT security strategies. I recommend researchers to continue that topic with more case organizations in the manufacturing industry in other regions in the U.S. to compare with the results of this study. Also, the researchers who conduct additional qualitative studies on that topic should structure the interview protocol to eliminate interviewees' bias towards the phenomenon under study. Also, the inclusion of other industries such as healthcare, logistics, and agriculture would add more insight into how other organizations have protected against security violations while adopting IoT. Inclusion will provide researchers cross-industry comparisons between industries and the role that regulations may play for each industry. Inclusion may provide researchers conducting such a study topic knowledge on standardization related to IoT devices and a starting point for corporate-level IT leaders to develop strategies for protecting against security violations for IoT adoption.

Furthermore, my focus was on corporate-level IT leaders' perceptions of my research; I recommend performing similar research and including software application developers, enterprise architects, and business users to allow for end-users and IT technical perspectives. The contributions of end-users and IT technical resources involved in developing and integrating IoT solutions would add more insights on the strategies that corporate-level IT leaders may need to protect against security while adopting IoT.

The acceptance of IoT was a concern for the case organization due to security violations, especially external clients. Many participants commented on that point because of recent security breaches coming from IoT devices. I recommend further research on the use of blockchain and artificial intelligence (AI) to add more protection to IoT devices. For example, using blockchain to store IoT data would add another layer of security that hackers would need to bypass to access the IoT network and provide a much more robust level of encryption that makes it virtually impossible to overwrite existing data records. Moreover, combining AI and IoT while adopting IoT for industries may provide an extra layer of security violation protection.

This study analyzed organizational documents that were publicly available. It would have been ideal to examine and analyze all organizations' documents that relate to the research question, but the partner organizations were hesitant to provide internal confidential documents that pertain to privacy and security violations. Therefore, not examining those documents is a limitation of the study as it might have constrained the number of themes that emerged from the study. I recommend further research on

security strategies intending to find a method of obtaining internal confidential documents from partner organizations that pertain to privacy and security strategies.

Reflections

This doctoral study has offered me a lot of experience both academically and in other areas of life. I have always wanted to obtain a doctorate, but one of my greatest challenges was combining this study with my full-time job. I was so determined to manage my time and family life to attain this goal. I learned a lot from this qualitative research study on strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT specifically how to conduct research, analyze data, and present the results in a way that will be understandable to my audience. I was exposed to the context of DOI theory as it relates to the IT practice. Moreover, interviewing participants expanded my IT social network. Furthermore, the literature review expanded my knowledge on the topic of study.

Starting with writing the proposal, getting it approved, and data collection was never an easy road. COVID-19 worsened the whole case because data collection took a long time. Most offices were closed or working from home because of the pandemic. However, I was able to get the participants that I needed, and they were highly professional and not bias towards the phenomenon under study. Although, my interview protocol was structured to eliminate any bias if it ever happened.

As an IT professional who has worked as a software programmer and currently delivering software solutions, this research study added to my knowledge. I have been interested in exploring IT solutions, especially their impact on IT practice and society.

IoT became one of those solutions that I have heard about but not knowing more about it. During this research study, I can assure myself that I have more information on the topic, especially security violations.

In this research, I was determined to remain objective during my data collection and analysis process, and my interview protocol helped me achieve that objectivity. I eliminated any personal bias on the phenomenon under study, instead of interpreted data based on the responses from the participants.

When presented to the executives, I learned that innovation should indicate the return on investment it would provide for management buy-in. Last, the success of a research study is determined by the academic relationship between the mentor and mentee. I learned a lot from my mentor based on his thorough review and encouraging approach.

Overall, this research study has been extremely valuable to me and maybe valuable to the manufacturing industry seeking to adopt IoT. I now feel prepared to move up to the next level of my career.

Conclusions

IoT adoption is complex and could be subjective due to overwhelming challenges. Security violations remain one of the challenges and concerns for many manufacturing organizations, and this study proved that to be accurate based on the data collected at the case organization. Although security violations may still be a big concern preventing manufacturing organizations from adopting IoT, increase awareness on risk mitigation strategies on infrastructure, policies, and processes, testing of IoT devices before they are

connected to IoT networks, and pilot adoption may not only protect against security but may positively change the perception of corporate-level IT leaders. IoT requires corporate-level IT leaders to seek out support actively and prioritize early IoT projects with the goals of learning, experimenting, and uncovering challenges. Having enough money for IoT project implementation should include a post-implementation budget for maintaining the infrastructure and securing IoT devices. If these strategies were put in place to protect against security violations, the manufacturing industry on the fence about IoT adoption might be swayed to invest in the solution. Corporate-level IT leaders are not concerned about whether IoT can benefit their organization because their interest in IoT proves that fact. Instead, they are skeptical and apprehensive about the vulnerabilities IoT devices may present to the organization. Adequate strategies must be planned and tested to ensure that these vulnerabilities don't impact the security and privacy of data in the organization to have their return on investment.

References

Abbott, P., DiGiacomo, M., Magin, P., & Hu, W. (2018). A scoping review of qualitative research methods used with people in prison. *International Journal of Qualitative Methods*, *17*(1). https://doi.org/10.1177/1609406918803824

Abdullah, A. M. (2018). Diffusion of innovation among Malaysian manufacturing SMEs. *European Journal of Innovation Management*, *21*(1), 113–141. https://doi.org/10.1108/EJIM-02-2017-0017

Abualsaud, K., Elfouly, T. M., Khattab, T., Yaacoub, E., Ismail, L. S., Ahmed, M. H., & Guizani, M. (2019). A survey on mobile crowd-sensing and its applications in the IoT era. *IEEE Access, 7*, 3855-3881. https://doi.org/10.1109/ACCESS.2018.2885918

Aekarat, S., Watcharasuda, H., Supattra, P., & Kanit, K. (2019). Smart car parking mobile application based on RFID and IoT. *International Journal of Interactive Mobile Technologies, 13*(5), 4–14. https://doi.org/10.3991/ijim.v13i05.10096

Aftab, H., Gilani, K., Lee, J., Nkenyereye, L., Jeong, S., & Song, J. (2019). Analysis of identifiers on IoT platforms. *Digital Communications and Networks*, *6*(3), 333–340. https://doi.org/10.1016/j.dcan.2019.05.003

Ahanger, T. A., & Aljumah, A. (2019). Internet of Things: A comprehensive study of security issues and defense mechanisms. *IEEE Access, 7*, 11020-11028. https://doi.org/10.1109/ACCESS.2018.2876939

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. doi:10.1016/0749-5978(91)90020-T

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*.

Prentice-Hall.

Akter, S., Bandara, R., Hani, U., Fosso Wamba, S., Foropon, C., & Papadopoulos, T. (2019). Analytics-based decision-making for service systems: A qualitative study and agenda for future research. *International Journal of Information Management*, *48*, 85–95. https://doi.org/10.1016/j.ijinfomgt.2019.01.020

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. https://doi.org/10.7575/aiac.ijels.v.5n.2p.9

Aldosari, H. M., Snasel, V., & Abraham, A. (2016). A novel security layer for Internet of Things. *Journal of Information Assurance & Security*, *11*(2), 58–66.

Al-Garadi, M. A., Mohamed, A., Al-Ali, A. K., Du, X., Ali, I., & Guizani, M. (2020). A survey of machine and deep learning methods for Internet of Things (IoT) security. *IEEE Communications Surveys & Tutorials, 22*(3), 1646–1685. https://doi.org/10.1109/COMST.2020.2988293

Al-Habaibeh, A., Shakmak, B., & Fanshawe, S. (2017). The development of an experimental test rig to evaluate the performance of a new technology for stratified hot water storage—The water snake. *Energy Procedia, 142,* 3644–3653. https://doi.org/10.1016/j.egypro.2017.12.257

Allen, J. D., Towne, S. D., Maxwell, A. E., DiMartino, L., Leyva, B., Bowen, D. J., Linnan, L., & Weiner, B. J. (2017). Measures of organizational characteristics associated with adoption and/or implementation of innovations: A systematic review. *BMC Health Services Research, 17*(1), Article 591. https://doi.org/10.1186/s12913-017-2459-x

Almalki, S. (2016). Integrating quantitative and qualitative data in mixed methods research—Challenges and benefits. *Journal of Education and Learning, 5*(3), 288–296.

Alotaibi, B. (2019). Utilizing blockchain to overcome cyber security concerns in the Internet of Things: A review. *IEEE Sensors Journal, 19*(23), 10953–10971.

Alpi, K. M., & Evans, J. J. (2019). Distinguishing case study as a research method from case reports as a publication type. *Journal of the Medical Library Association*, *107*(1), 1–5. https://doi.org/10.5195/jmla.2019.615

Al-Rahmi, W. M., Yahaya, N., Aldraiweesh, A. A., Alamri, M. M., Aljarboa, N. A., Alturki, U., & Aljeraiwi, A. A. (2019). Integrating technology acceptance model with innovation diffusion theory: An empirical investigation on students' intention to use e-learning systems. *IEEE Access, 7*, 26797–26809. https://doi.org/10.1109/ACCESS.2019.2899368

Alsharari, M. N., & Al-Shboul, M. (2019). Evaluating qualitative research in management accounting using the criteria of "convincingness." *Pacific Accounting Review, 31*(1), 43-62. https://doi.org/10.1108/PAR-03-2016-0031

Alshehry, A. (2018). Case study of science teachers' professional development in Saudi Arabia: Challenges and improvements. *International Education Studies, 11*(3), 70–76.

Al-Shura, S. M., Zabadi, M. A., Abughazaleh, M., & Alhadi, A. M. (2018). Critical success factors for adopting cloud computing in the pharmaceutical manufacturing companies. *Management and Economics Review*, *3*(2), 2798–2803. https://doi.org/10.24818/mer/2018.12-01

Al-Turjman, F., Mostarda, L., Ever, E., Darwish, A., & Shekh, K. N. (2019). Network experience scheduling and routing approach for big data transmission in the Internet of

Things. *IEEE Access, 7,* 14501-14512. https://doi.org/10.1109/ACCESS.2019.2893501

Alvarez, Y., Leguizamón-Páez, M. A., & Londoño, T. J. (2021). Risks and security solutions existing in the Internet of things (IoT) in relation to Big Data. *Ingeniería y Competitividad, 23*(1), 1–13.

Amankwa, E., Loock, M., & Kritzinger, E. (2018). Establishing information security policy compliance culture in organizations. *Information & Computer Security*, *26*(4), 420–436. https://doi.org/10.1108/ICS-09-2017-0063

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121–127.

Amin, U. S., & Hossain, M. S. (2021). Edge intelligence and Internet of Things in healthcare: A survey. *IEEE Access, 9*, 45–59. https://doi.org/10.1109/ACCESS.2020.3045115

Ammar, M., Russello, G., & Crispo, B. (2018). Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications*, *38*, 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

Andriole, S. J. (2019). Social media analytics, wearable technology, and the Internet of Things. *IT Professional, 21*(5), 11-15. https://doi.org/10.1109/MITP.2019.2907378

Antoniou, J., & Andreou, A. (2019). Case study: The Internet of Things and ethics. *ORBIT Journal*, *2*(2). https://doi.org/10.29297/orbit.v2i2.111

Arwa, A., Al-Rodhaan, M., & Tian, Y. (2018). A randomized watermarking technique for detecting malicious data injection attacks in heterogeneous wireless sensor networks for Internet of Things applications. *Sensors*, *18*(12), Article 4346. https://doi.org/10.3390/s18124346

Atif, M., Javaid, S., Farooqui, M., & Sarwar, M. R. (2016). Rights and responsibilities of tuberculosis patients, and the global fund: A qualitative study. *Plos One*, *11*(3), Article e0151321. https://doi.org/10.1371/journal.pone.0151321

Atout, M., Hemingway, P., & Seymour, J. (2019). The practice of mutual protection in the care of children with palliative care needs: a multiple qualitative case study approach from Jordan. *Journal of Pediatric Nursing, 45*, 9–18. https://doi.org/10.1016/j.pedn.2018.12.004

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. https://doi.org/10.1016/j.adhoc.2016.12.004

Ayoub, W., Samhat, A. E., Nouvel, F., Mroue, M., & Prevotet, J. (2019). Internet of mobile things: Overview of LoRaWAN, DASH7, and NB-IoT in LPWANs standards and supported mobility. *IEEE Communications Surveys & Tutorials, 21*(2), 1561-1581. https://doi.org/10.1109/COMST.2018.2877382

Babaei, A., & Schiele, G. (2019). Physical unclonable functions in the Internet of Things: State of the art and open challenges. *Sensors*, *19*(14), 3208. https://doi.org/10.3390/s19143208

Bendavid, Y., Bagheri, N., Safkhani, M., & Rostampour, S. (2018). IoT device security: Challenging "a lightweight RFID mutual authentication protocol based on physical unclonable function." *Sensors, 18*(12). https://doi.org/10.3390/s18124444

Bendixen, R. M., Morgenroth, L. P., & Clinard, K. L. (2016). Engaging participants in rare disease research: A qualitative study of duchenne muscular dystrophy. *Clinical Therapeutics*, *38*(6), 1474–1484. https://doi.org/10.1016/j.clinthera.2016.04.001

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open, 2*, 8–14. https://doi.org/10.1016/j.npls.2016.01.001

Benoot, C., Hannes, K., & Bilsen, J. (2016). The use of purposeful sampling in a qualitative evidence synthesis: A worked example on sexual adjustment to a cancer trajectory. *BMC Medical Research Methodology, 16*(1), 1-13. https://doi.org/10.1186/s12874-016-0114-6

Berg, S. E. (2016). (Re)Telling lived experiences in different tales: A potential pathway in working towards an inclusive PE. *Sport, Education & Society, 21*(1), 62–81. https://doi.org/10.1080/13573322.2015.1113166

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

Bicaku, A., Tauber, M., & Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things. *International Journal of Distributed Sensor Networks, 16*. https://doi.org/10.1177/1550147720922731

Birt, L., Scott, S., Cavers, D., Campbell, C., & Walter, F. (2016). Member checking: A tool to enhance trustworthiness or merely a nod to validation? *Qualitative Health Research, 26*(13), 1802–1811. https://doi.org/10.1177/1049732316654870

Blind, K., Petersen, S. S., & Riillo, C. A. F. (2017). The impact of standards and regulation on innovation in uncertain markets. *Research Policy, 46*(1), 249–264. https://doi.org/10.1016/j.respol.2016.11.003

Blut, M., Wang, C., & Schoefer, K. (2016). Factors influencing the acceptance of self-service technologies: A meta-analysis. *Journal of Service Research*, *19*(4), 396–416. https://doi.org/10.1177/1094670516662352

Boamah, E. (2018). Relative advantages of digital preservation management in developing countries. *New Review of Information Networking*, *23*(1/2), 83–98. https://doi.org/10.1080/13614576.2018.1544088

Bordel, B., Alcarria, R., Robles, T., & Iglesias, M. S. (2021). Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking. *IEEE Access, 9*, 22378–22398. https://doi.org/10.1109/ACCESS.2021.3055771

Boudouaia, M. A., Ali-Pacha, A., Abouaissa, A., & Lorenz, P. (2020). Security against rank attack in RPL protocol. *IEEE Network, 34*(4), 133–139. https://doi.org/10.1109/MNET.011.1900651

Brear, M. (2018). Swazi co-researcher participants' dynamic preferences and motivations for, representation with real names and (English-language) pseudonyms—An ethnography. *Qualitative Research*, *18*(6), 722–740. https://doi.org/10.1177/1468794117743467

Brear, M. (2019). Process and outcomes of a recursive, dialogic member checking approach: A project ethnography. *Qualitative Health Research, 29*(7), 944–957. https://doi.org/10.1177/1049732318812448

Breese, J. L., & Zwerling, T. (2020). IoT a gateway for acceptance: The potential for broad purpose implant devices. *Issues in Information Systems, 21*(4), 114–122.

Bressanelli, G., Perona, M., & Saccani, N. (2019). Challenges in supply chain redesign for the Circular Economy: A literature review and a multiple case study. *International Journal of Production Research*, *57*(23), 7395–7422.

https://doi.org/10.1080/00207543.2018.1542176

Brous, P., Janssen, M., & Herder, P. (2019). Internet of Things adoption for reconfiguring decision-making processes in asset management. *Business Process Management Journal*, *25*(3), 495–511. https://doi.org/10.1108/BPMJ-11-2017-0328

Brown, A., & Danaher, P. A. (2019). CHE Principles: Facilitating authentic and dialogical semistructured interviews in educational research. *International Journal of Research & Method in Education, 42*(1), 76–90. https://doi.org/10.1080/1743727X.2017.1379987

Brown, B., Galea, J. T., Dubé, K., Davidson, P., Khoshnood, K., Holtzman, L., Marg, L., & Taylor, J. (2018). The need to track payment incentives to participate in HIV research. *Ethics & Human Research*, *40*(4), 8–12.

Bruce, C. R., Bibler, T. M., Pena, A. M., & Kusin, B. (2016). A qualitative exploration of a clinical ethicist's role and contributions during family meetings. *HEC Forum, 28(4),* 283-299. https://doi.org/10.1007/s10730-015-9300-x

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, 11*(2), 178–191. https://doi.org/10.1108/JRIT-03-2017-0004

Buetow, S. (2019). Apophenia, unconscious bias and reflexivity in nursing qualitative research. *International Journal of Nursing Studies*, *89*, 8–13. https://doi.org/10.1016/j.ijnurstu.2018.09.013

Bujari, A., Furini, M., Mandreoli, F., Martoglia, R., Montangero, M., & Ronzani, D. (2018). Standards, security, and business models: key challenges for the IoT scenario. *Mobile*

Networks & Applications, *23*(1), 147–154. https://doi.org/10.1007/s11036-017-0835-8

Burg, A., Chattopadhyay, A., & Lam, K. (2018). Wireless communication and security issues for cyber–physical systems and the Internet-of-Things. *IEEE Proceedings, 106*(1), 38-60. https://doi.org/10.1109/JPROC.2017.2780172

Burrows, C., Usher, L., Schwartz, C., Mundy, P., & Henderson, H. (2016). Supporting the spectrum hypothesis: Self-Reported temperament in children and adolescents with high functioning autism. *Journal of Autism & Developmental Disorders, 46*(4), 1184–1195. https://doi.org/10.1007/s10803-015-2653-9

Bustard, T. R. J., Bolan, P., Devine, A., & Hutchinson, K. (2019). The emerging smart event experience: An interpretative phenomenological analysis. *Tourism Review, 74*(1), 116-128. https://doi.org/10.1108/TR-10-2017-0156

Caeiro, C., Canhão, H., Paiva, S., Gomes, L. A., Fernandes, R., Rodrigues, A. M., Sousa, R., Pimentel-Santos, F., Branco, J., Fryxell, C. A., Vicente, L., & Cruz, E. B. (2019). Interdisciplinary stratified care for low back pain: A qualitative study on the acceptability, potential facilitators and barriers to implementation. *PLoS ONE, 14*(11), 1–18. https://doi.org/10.1371/journal.pone.0225336

Campanotta, L., Simpson, P., & Newton, J. (2018). Program quality in leadership preparation programs: An assessment tool. *Education*, *138*(3), 219–228

Cangea, O. (2019). A Comparative Analysis of Internet of Things Security Strategies. *Petroleum - Gas University of Ploiesti Bulletin, Technical Series*, *71*(1), 1–10.

Cano, M.-D., & Cañavate-Sanchez, A. (2020). Preserving data privacy in the Internet of Medical Things using dual signature ECDSA. *Security & Communication Networks*, 1–9.

https://doi.org/10.1155/2020/4960964

Caputo, A., Marzi, G., & Pellegrini, M. M. (2016). The Internet of Things in manufacturing innovation processes development and application of a conceptual framework. *Business Process Management Journal, 22*(2), 383–402. https://doi.org/10.1108/BPMJ-05-2015-0072

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

Caretta, M. A., & Pérez, M. A. (2019). When participants do not agree: member checking and challenges to epistemic authority in participatory research. *Field Methods*, *31*(4), 359–374. https://doi.org/10.1177/1525822X19866578

Carr, E. M., Zhang, G. D., Ming, J. Y., & Siddiqui, Z. S. (2019). Qualitative research: An overview of emerging approaches for data collection. *Australasian Psychiatry, 27*(3), 307–309. https://doi.org/10.1177/1039856219828164

Castillo-Montoya, M. (2016). Preparing for interview research: the interview protocol refinement framework. *Qualitative Report, 21*(5), 811–831.

Celic, L., & Magjarevic, R. (2020). Seamless connectivity architecture and methods for IoT and wearable devices. *Automatika: Journal for Control, Measurement, Electronics, Computing & Communications*, *61*(1), 21–34. https://doi.org/10.1080/00051144.2019.1660036

Cheah, P. K., Unnithan, N. P., & Raran, A. M. S. (2019). Interviewing criminal justice populations without electronic recording devices: A guide. *Qualitative Report*, *24*(4),

705-716.

Chen, C. H., & Lo, K. R. (2018). Applications of Internet of Things. *International Journal of Geo-Information, 7*(9). https://doi.org/10.3390/ijgi7090334

Chen, H., Rong, W., Ma, X., Qu, Y., & Xiong, Z. (2017). An extended technology acceptance model for mobile social gaming service popularity analysis. *Mobile Information Systems, 2017.* https://doi.org/10.1155/2017/3906953

Chen, J., & Yang, A. (2019). Intelligent agriculture and its key technologies based on Internet of Things architecture. *IEEE Access, 7,* 77134- 77141. https://doi.org/10.1109/ACCESS.2019.2921391

Chen, X., & Zhang, X. (2016). How environmental uncertainty moderates the effect of relative advantage and perceived credibility on the adoption of mobile health services by Chinese organizations in the big data era. *International Journal of Telemedicine and Applications*, *2016*. https://doi.org/10.1155/2016/3618402

Chen, Y., Li, M., Chen, P., & Xia, S. (2019). Survey of cross-technology communication for IoT heterogeneous devices. *IET Communications*, *13*(12), 1709–1720. https://doi.org/10.1049/iet-com.2018.6069

Cheng, E. W. L. (2019). Choosing between the theory of planned behavior (TPB) and the technology acceptance model (TAM). *Educational Technology Research & Development*, 67(1), 21–37. https://doi.org/10.1007/s11423-018-9598-6

Chi, Z., Li, Y., Sun, H., Yao, Y., & Zhu, T. (2019). Concurrent cross-technology communication among heterogeneous IoT devices. *IEEE/ACM Transactions on Networking, 27*(3), 932-947. https://doi.org/10.1109/TNET.2019.2908754

Choi, J., Nazareth, D. L., & Ngo-Ye, T. L. (2018). The effect of innovation characteristics on cloud computing diffusion. *Journal of Computer Information Systems*, *58*(4), 325–333. https://doi.org/10.1080/08874417.2016.1261377

Chrismas, R. (2018). Gaining a fuller picture of sex trafficking in Manitoba: a case study of narrative-based research utilizing "low tech" thematic analysis. *Journal of Research Practice, 14*(1). https://search-ebscohost-com.

Clapp, J. T., Gleason, K. A., & Joffe, S. (2017). Justification and authority in institutional review board decision letters. *Social Science & Medicine, 194*, 25–33. https://doi.org/10.1016/j.socscimed.2017.10.013

Cocosila, M., & Turel, O. (2019). Adoption and non-adoption motivational risk beliefs in the use of mobile services for health promotion. *Internet Research*, *29*(4), 846–869. https://doi.org/10.1108/IntR-04-2018-0174

Čolaković, A., & Hadžialić, M. (2018). Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. *Computer Networks, 144*, 17–39. https://doi.org/10.1016/j.comnet.2018.07.017

Collingridge, D. S., & Gantt, E. E. (2019). The quality of qualitative research. *American Journal of Medical Quality*, *34*(5), 439-445.

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *Medsurg Nursing*, *25*(6), 435–436.

Constantinou, C. S., Georgiou, M., & Perdikogianni, M. (2017). A comparative method for themes saturation (CoMeTS) in qualitative interviews. *Qualitative Research, 17*(5), 571–588. https://doi.org/10.1177/1468794116686650

Coskun, A., Kaner, G., & Bostan, İ. (2018). Is smart home a necessity or a fantasy for the mainstream user? A study on users' expectations of smart household Appliances. *International Journal of Design*, *12*(1), 7–20.

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. https://doi.org/10.1155/2019/9067512

Currie, G., & Spyridonidis, D. (2019). Sharing leadership for diffusion of innovation in professionalized settings. *Human Relations*, *72*(7), 1209–1233. https://doi.org/10.1177/0018726718796175

Cybersecurity and Infrastructure Security Agency. (2019). *Securing Wireless Networks.* https://www.us-cert.gov/ncas/tips/ST05-003

Cypress, B. (2018). Qualitative research methods: A phenomenological focus. *Dimensions of Critical Care Nursing: DCCN*, *37*(6), 302–309. https://doi.org/10.1097/DCC.0000000000000322

Danubianu, M., Teodorescu, C., & Corneanu, I. (2019). Internet of Things and the environment. *Present Environment & Sustainable Development*, *13*(1), 181–190. https://doi.org/10.2478/pesd-2019-0014

Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer Systems-The International Journal of Escience, 89,* 110–125. https://doi.org/10.1016/j.future.2018.06.027

David, H. (2017). Ethical considerations in qualitative case study research recruiting participants with profound intellectual disabilities. *Research Ethics 13* (3-4), 219–232.

https://doi.org/10.1177/1747016117711971

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

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

DeCino, D. A., & Waalkes, P. L. (2019). Aligning epistemology with member checks. *International Journal of Research & Method in Education*, *42*(4), 374–384. https://doi.org/10.1080/1743727X.2018.1492535

De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): On understanding its dark side. *Journal of Marketing Management*, *33*(1/2), 145–158. https://doi.org/10.1080/0267257X.2016.1247517

Dellinger, M. J., Olson, J., Clark, R., Pingatore, N., & Ripley, M. P. (2018). Development and pilot testing of a model to translate risk assessment data for Great Lakes Native American communities using mobile technology. *Human and Ecological Risk Assessment*, *24*(1), 242–255. https://doi.org/10.1080/10807039.2017.1377596

Dewilde, J., Kjørven, O. K., Skaret, A., & Skrefsrud, T. (2018). International week in a Norwegian school. A qualitative study of the participant perspective. *Scandinavian Journal of Educational Research, 62*(3), 474–486.

Díaz-Vicario, A., & Gairín-Sallán, J. (2017). A comprehensive approach to managing school safety: Case studies in Catalonia, Spain. *Educational Research*, *59*(1), 89–106.

Dibra, M. (2015). Rogers theory on diffusion of innovation-the most appropriate theoretical model in the study of factors influencing the integration of sustainability in tourism

businesses. *Procedia - Social and Behavioral Sciences*, *195*, 1453–1462. https://doi.org/10.1016/j.sbspro.2015.06.443

DiGiacinto, D. (2019). The importance of the internal review board for approving proposed research. *Journal of Diagnostic Medical Sonography*, *35*(2), 85–86. https://doi.org/10.1177/8756479318817220

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *Qualitative Report*, *21*(3), 521–528.

Ding, W., Jing, X., Yan, Z., & Yang, L. T. (2019). A survey on data fusion in internet of things: Towards secure and privacy-preserving fusion. *Information Fusion*, *51*, 129–144. https://doi.org/10.1016/j.inffus.2018.12.001

Ding, W., Xu, M., Huang, Y., & Zhao, P. (2020). Cyber risks of PMU networks with observation errors: Assessment and mitigation. *Reliability Engineering and System Safety*, 198. https://doi.org/10.1016/j.ress.2020.106873

Dobson-Lohman, E. (2019). Wearable sensors, remote patient monitoring, and cloud computing. *American Journal of Medical Research*, *6*(1), 7–12. https://doi.org/10.22381/AJMR6120191

Dohmen, A. E., & Raman, D. R. (2018). Healthy food as a new technology—The implications of technological diffusion and food price for changes in eating habits. *Frontiers in Nutrition 5*. https://doi.org/10.3389/fnut.2018.00109

do Rosário Cabrita, M., Machado, V. H., Barroso, A. P., & Cruz-Machado, V. (2015). Diffusion of innovation concepts in Portuguese manufacturing companies. *International Journal of Management Science and Engineering Management, 10*(2), 126-136.

https://doi.org/10.1080/17509653.2014.943316

Dong, Y., Zhao, X., Tong, Y., & Li, D. (2018). Service optimization of internet of manufacturing things based on mixed information axioms. *IEEE Access*, *6*, 3254–3264. https://doi.org/10.1109/ACCESS.2018.2871252

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., & Williams, D. M. (2019). Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers, 21*(3), 719-734. https://doi.org/10.1007/s10796-017-9774-y

Ehret, M., & Wirtz, J. (2017). Unlocking value from machines: business models and the industrial internet of things. *Journal of Marketing Management*, *33*(1/2), 111–130. https://doi.org/10.1080/0267257X.2016.1248041

El-hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019). A Survey of Internet of Things (IoT) authentication Schemes. *Sensors*, (5), Article 1141. https://doi.org/10.3390/s19051141

Elizabeth, M. J., Busisiwe, P. N., & Omolola, I. (2019). Developing and pilot testing an integrated technology–moderated institutional health promotion model using operational research approach. *CIN: Computers, Informatics, Nursing*, *37*(10), 532-540. https://doi.org/10.1097/CIN.0000000000000556

Erhan, L., Ndubuaku, M., Ferrara, E., Richardson, M., Sheffield, D., Ferguson, F. J., Brindley, P., & .Liotta, A. (2019). Analyzing objective and subjective data in social sciences: Implications for smart cities. *IEEE Access, 7,* 19890-19906. https://doi.org/10.1109/ACCESS.2019.2897217

Eskridge, M. (2019). Privacy and security data governance: Surveillance mechanisms and resilience risks of smart city technologies. *Contemporary Readings in Law and Social Justice*, *11*(2), Article 63.

Eta, E. A., & Vubo, E. Y. (2016). Global references, local translation: Adaptation of the bologna process degree structure and credit system at universities in Cameroon. *Globalisation, Societies and Education*, *14*(4), 492–512.

Farooq, M. B., & Villiers, C. (2017). Telephonic qualitative research interviews: When to consider them and how to do them. *Meditari Accountancy Research*, *25*(2), 291-316. https://doi.org/10.1108/MEDAR-10-2016-0083

Farrugia, L. (2019). WASP (write a scientific paper): The ongoing process of ethical decision-making in qualitative research: Ethical principles and their application to the research process. *Early Human Development*, *133*, 48–51. https://doi.org/10.1016/j.earlhumdev.2019.03.011

Feit, J. (2017). Do your IoT devices risk a security breach? The Internet of Things can open you up to cyber-attacks; stop them with proper security practices. *Buildings, 111*(7), 18–22.

Feldner, B., & Herber, P. (2018). A qualitative evaluation of IPv6 for the industrial Internet of Things. *Procedia Computer Science*, *134*, 377–384. https://doi.org/10.1016/j.procs.2018.07.195

Ficco, M., & Palmieri, F. (2019). Leaf: An open-source cybersecurity training platform for realistic edge-IoT scenarios. *Journal of Systems Architecture*, *97*, 107–129. https://doi.org/10.1016/j.sysarc.2019.04.004

Fitt, H. (2018). Researching mobile practices: Participant reflection and audio-recording in

repeat question diaries. *Qualitative Research*, *18*(6), 654-670.

FitzPatrick, B. (2019). Validity in qualitative health education research. *Currents in Pharmacy Teaching & Learning, 11*(2), 211–217. https://doi.org/10.1016/j.cptl.2018.11.014

Flannery, M. (2016). Common perspectives in qualitative research. *Oncology Nursing Forum*, 43(4), 517–518. https://doi.org/10.1188/16.ONF.517-518

Forero, R., Nahidi, S., De Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarthy, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research*, *18*(1), Article 120. https://doi.org/10.1186/s12913-018-2915-2

Fuller, S. S., Pacho, A., Broad, C. E., Nori, A. V., Harding-Esch, E. M., & Sadiq, S. T. (2019). "It's not a time spent issue; it's a 'what have you spent your time doing?' issue…" A qualitative study of UK patient opinions and expectations for implementation of Point of Care Tests for sexually transmitted infections and antimicrobial resistance. *PLoS ONE, 14*(4), 1–16. https://doi.org/10.1371/journal.pone.0215380

Gallo, L. L. (2017). Professional issues in school counseling and suicide prevention. *Journal of School Counseling, 15*(11). https://search-ebscohost-com.

Gazis, V. (2017). A survey of standards for machine-to-machine and the Internet of Things. *IEEE Communications Surveys & Tutorials, 19*(1), 482-511. https://doi.org/10.1109/COMST.2016.2592948

Gebremichael, T., Ledwaba, L. P. I., Eldefrawy, M. H., Hancke, G. P., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and privacy in the Industrial Internet of Things: Current standards and future challenges. *IEEE Access, 8*, 152351–152366.

https://doi.org/10.1109/ACCESS.2020.3016937

Georgakopoulos, D., & Jayaraman, P. (2016). Internet of Things: From internet scale sensing to smart services. *Computing*, *98*(10), 1041–1058. https://doi.org/10.1007/s00607-016-0510-0

George, G., & Thampi, S. M. (2019). Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things. *Pervasive and Mobile Computing*, 59. https://doi.org/10.1016/j.pmcj.2019.101068

Gessl, A. S., Schlögl, S., & Mevenkamp, N. (2019). On the perceptions and acceptance of artificially intelligent robotics and the psychology of the future elderly. *Behaviour & Information Technology*, *38*(11), 1068–1087. https://doi.org/10.1080/0144929X.2019.1566499

Gibson, S., & Sullivan, C. (2018). A changing culture? Qualitative methods teaching in UK psychology. *Qualitative Psychology*, *5*(2), 197–206. https://doi.org/10.1037/qup0000100

Gilpin-Jackson, Y. (2017). Participant experiences of transformational change in large-scale organization development interventions (LODIs). *Leadership & Organization Development Journal, 38*(3), 419-432. https://doi.org/10.1108/LODJ-12-2015-0284

Glegg, S. M. N. (2019). Facilitating interviews in qualitative research with visual tools: A typology. *Qualitative Health Research*, *29*(2), 301–310. https://doi.org/10.1177/1049732318786485

Glenna, L., Hesse, A., Hinrichs, C., Chiles, R., & Sachs, C. (2019). Qualitative research ethics in the big data era. *American Behavioral Scientist*, *63*(5), 560–583. https://doi.org/10.1177/0002764219826282

Gonzalo, J. D., Graaf, D., Ahluwalia, A., Wolpaw, D. R., & Thompson, B. M. (2018). A practical guide for implementing and maintaining value-added clinical systems learning roles for medical students using a diffusion of innovations framework. *Advances in Health Sciences Education: Theory and Practice*, *23*(4), 699–720. https://doi.org/10.1007/s10459-018-9822-5

Goode, V., Crego, N., Cary, M. P., Thornlow, D., & Merwin, E. (2017). Improving quality and safety through use of secondary data: Methods case study. *Western Journal of Nursing Research*, *39*(11), 1477–1501. https://doi.org/10.1177/0193945916672449

Gorgolewski, K. J., & Poldrack, R. A. (2016). A practical guide for improving transparency and reproducibility in neuroimaging research. *PLoS Biology, 14*(7). Article e1002506. https://doi.org/10.1371/journal.pbio.1002506

Grando, A., Sottara, D., Singh, R., Murcko, A., Soni, H., Tang, T., Idouraine, N., Todd, M., Mote, M., Chern, D., Dye, C., & Whitfield, M. J. (2020). Pilot evaluation of sensitive data segmentation technology for privacy. *International Journal of Medical Informatics*, *138*. https://doi.org/10.1016/j.ijmedinf.2020.104121

Groenewald, T. (2018). Reflection/commentary on a past article: "a phenomenological research design illustrated." *International Journal of Qualitative Methods*, *17*. https://doi.org/10.1177/1609406918774662

Grysman, A., & Lodi-Smith, J. (2019). Methods for conducting and publishing narrative research with undergraduates. *Frontiers in Psychology, 9*. https://doi.org/10.3389/fpsyg.2018.02771

Guetterman, T. C., & Fetters, M. D. (2018). Two methodological approaches to the integration of

mixed methods and case study designs: A systematic review. *American Behavioral Scientist, 62*(7), 900–918. https://doi.org/10.1177/0002764218772641

Guo, L., Wang, J., & Yau, W. (2019). Efficient hierarchical identity-based Encryption system for Internet of Things infrastructure. *Symmetry, 11*(7), Article 913. https://doi.org/10.3390/sym11070913

Guo, X. J. (2019). Measuring information system project success through a software-assisted qualitative content analysis. *Information Technology & Libraries*, *38*(1), 53–70. https://doi.org/10.6017/ital.v38i1.10603

Gutschow, E. (2019). Big data-driven smart cities: Computationally networked urbanism, real-time decision-making, and the cognitive Internet of Things. *Geopolitics, History, and International Relations*, *11*(2), 48–54. https://doi.org/10.22381/GHIR11220197

Habiyaremye, A. (2020). Water innovation in South Africa: Mapping innovation successes and diffusion constraints. *Environmental Science & Policy*, 114, 217–229. https://doi.org/10.1016/j.envsci.2020.08.011

Haçat, S. O. (2018). Opinions of middle school students on the justice concept within the framework of social studies education. *International Journal of Higher Education*, *7*(2), 210–215.

Hadadgar, A., Changiz, T., Masiello, I., Dehghani, Z., Mirshahzadeh, N., & Zary, N. (2016). Applicability of the theory of planned behavior in explaining the general practitioners eLearning use in continuing medical education. *BMC Medical Education*, *16*(1), 215. https://doi.org/10.1186/s12909-016-0738-6

Hagemeier, N. E., Tudiver, F., Brewster, S., Hagy, E. J., Ratliff, B., Hagaman, A., & Pack, R. P.

(2018). Interprofessional prescription opioid abuse communication among prescribers and pharmacists: A qualitative analysis. *Substance Abuse*, *39*(1), 89–94. https://doi.org/10.1080/08897077.2017.1365803

Haines-Saah, R. J., Mitchell, S., Slemon, A., & Jenkins, E. K. (2019). 'Parents are the best prevention'? Troubling assumptions in cannabis policy and prevention discourses in the context of legalization in Canada. *International Journal of Drug Policy, 68*, 132–138. https://doi.org/10.1016/j.drugpo.2018.06.008

Hamilton, G., Powell, M. B., & Brubacher, S. P. (2017). Professionals' perceptions regarding the suitability of investigative interview protocols with aboriginal children. *Australian Psychologist*, *52*(3), 174–183. https://doi.org/10.1111/ap.12196

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

Harbi, Y., Aliouat, Z., Refoufi, A., Harous, S., & Bentaleb, A. (2019). Enhanced authentication and key management scheme for securing data transmission in the Internet of Things. *Ad Hoc Networks, 94*. https://doi.org/10.1016/j.adhoc.2019.101948

Hassan, A. M., & Awad, A. I. (2018). Urban transition in the era of the internet of things: Social implications challenges. *IEEE Access, 6,* 36428-36440. https://doi.org/10.1109/ACCESS.2018.2838339

Hassan, H., Tretiakov, A., & Whiddett, D. (2017). Factors affecting the breadth and depth of e-procurement use in small and medium enterprises. *Journal of Organizational Computing & Electronic Commerce*, *27*(4), 304–324.

https://doi.org/10.1080/10919392.2017.1363584

He, Y., Han, G., Wang, H., Adu Ansere, J., & Zhang, W. (2019). A sector-based random routing scheme for protecting the source location privacy in WSNs for the Internet of Things. *Future Generation Computer Systems*, *96*, 438–448. https://doi.org/10.1016/j.future.2019.02.049

Heilmann, S. (2018). A scaffolding approach using interviews and narrative inquiry. *Networks*: *An Online Journal for Teacher Research, 20*(2). Article 3.

Helmich, E., Stenfors, T., & Barrett, A. (2018). How to…choose between different types of data. *The Clinical Teacher*, *15*(5), 366–369. https://doi.org/10.1111/tct.12925

Henk-Jan van Roekel, & Martijn van der Steen. (2019). Integration as unrealised ideal of ERP systems: An exploration of complexity resulting from multiple variations of integration. *Qualitative Research in Accounting & Management, 16*(1), 2–34. https://doi.org/10.1108/QRAM-08-2014-0052

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. https://doi.org/10.1016/j.comcom.2018.08.010

Hickman, L., & Akdere, M. (2018). Effective leadership development in information technology: Building transformational and emergent leaders. *Industrial & Commercial Training*, *50*(1), 1–9. https://doi.org/10.1108/ICT-06-2017-0039

Hirman, M., Benesova, A., Sima, K., Steiner, F., & Tupa, J. (2020). Design, fabrication, and risk assessment of IoT unit for products manufactured in industry 4.0 factory. *Procedia*

Manufacturing, *51*, 1178–1183. https://doi.org/10.1016/j.promfg.2020.10.165

Hoeber, L., & Shaw, S. (2017). Contemporary qualitative research methods in sport management. *Sport Management Review, 20*(1), 4–7. https://doi.org/10.1016/j.smr.2016.11.005

Hoffman, D. L., & Novak, T. P. (2018). Consumer and object experience in the Internet of Things: An assemblage theory approach. *Journal of Consumer Research*, *44*(6), 1178–1204. https://doi.org/10.1093/jcr/ucx105

Hoffman, F. (2019). Industrial Internet of Things vulnerabilities and threats: what stakeholders need to consider. *Issues in Information Systems*, *20*(1), 119-133.

Holt, N. L., & McHugh, T.-L. (2018). A critical evaluation of three member-checking procedures. *International Journal of Qualitative Methods, 17*(1).

Hsu, C.-L., & Lin, J. C.-C. (2018). Exploring factors affecting the adoption of Internet of Things services. *Journal of Computer Information Systems, 58*(1), 49–57. https://doi.org/10.1080/08874417.2016.1186524

Huang, J., Zhu, L., Liang, Q., Fan, B., & Li, S. (2018). Efficient classification of distribution-based data for Internet of Things. *IEEE Access, 6,* 69279–69287. https://doi.org/10.1109/ACCESS.2018.2879652

Hubert, M., Blut, M., Brock, C., Zhang, R. W., Koch, V., & Riedl, R. (2019). The influence of acceptance and adoption drivers on smart home usage. *European Journal of Marketing, 53*(6), 1073-1098. https://doi.org/10.1108/EJM-12-2016-0794

Hwang, Y., Al-Arabiat, M., & Shin, D. H. (2016). Understanding technology acceptance in a mandatory environment. *Information Development, 32*(4), 1266–1283.

https://doi.org/10.1177/0266666915593621

Ifinedo, P. (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, *33*(1), 30–41. https://doi.org/10.1080/10580530.2015.1117868

Iivari, N. (2018). Using member checking in interpretive research practice: A hermeneutic analysis of informants' interpretation of their organizational realities. *Information Technology & People*, *31*(1), 111-133. https://doi.org/10.1108/ITP-07-2016-0168

Indrianto, I., Susanti, M. N. I., Siregar, R. R. A., Putri, P. J., & Purwanto, Y. (2019). Smart taxi security system design with internet of things (IoT). *Telkomnika*, *17*(3), 1250–1255. https://doi.org/10.12928/TELKOMNIKA.v17i3.10167

Ioannou, C., & Vassiliou, V. (2019). Security agent location in the Internet of Things. *IEEE Access, 7*, 95844–95856. https://doi.org/10.1109/ACCESS.2019.2928414

Iskandar, M., Hartoyo, H., & Hermadi, I. (2020). Analysis of factors affecting behavioral intention and use of behavioral of mobile banking using unified theory of acceptance and use of technology 2 model approach. *International Review of Management and Marketing, 10*(2), 41-49.

Jacob, C., Sanchez-Vazquez, A., & Ivory, C. (2020). Understanding clinicians' adoption of mobile health tools: A qualitative review of the most used frameworks. *JMIR MHealth and UHealth*, *8*(7), Article e18072. https://doi.org/10.2196/18072

Jamshidi, D., & Hussin, N. (2018). An integrated adoption model for Islamic credit card: PLS-SEM based approach. *Journal of Islamic Accounting & Business Research*, *9*(3), 308 - 335. https://doi.org/10.1108/JIABR-07-2015-0032

Jang, S., Lim, D., Kang, J., & Joe, I. (2016). An efficient device authentication protocol without certification authority for Internet of Things. *Wireless Personal Communications*, *91*(4), 1681–1695. https://doi.org/10.1007/s11277-016-3355-0

Jennings, H., Slade, M., Bates, P., Munday, E., & Toney, R. (2018). Best practice framework for Patient and Public Involvement (PPI) in collaborative data analysis of qualitative mental health research: methodology development and refinement. *BMC Psychiatry, 18*(1), 1-11. https://doi.org/10.1186/s12888-018-1794-8

Jiang, W., Yang, Z., Zhou, Z., & Chen, J. (2020). Lightweight data security protection method for AMI in power Internet of Things. *Mathematical Problems in Engineering*, 1–9. https://doi.org/10.1155/2020/8896783

Jiang, W., Yin, Z., Liu, R., Li, Z., Kim, S. M., & He, T. (2019). Boosting the bitrate of cross-technology communication on commodity IoT devices. *IEEE/ACM Transactions on Networking*, *27*(3), 1069 -1083. https://doi.org/10.1109/TNET.2019.2913980

Jin, J., & Bridges, S. (2016). Qualitative research in PBL in health sciences education: A review. *Interdisciplinary Journal of Problem-Based Learning, 10*(2). 156-182. https://doi.org/10.7771/1541-5015.1605

Johansson, C. B. (2019). Introduction to qualitative research and grounded theory. *International Body Psychotherapy Journal, 18*(1), 94-99.

Johnson, V. L., Kiser, A., Washington, R., & Torres, R. (2018). Limitations to the rapid adoption of M-payment services: Understanding the impact of privacy risk on M-Payment services. *Computers in Human Behavior*, *79*, 111–122. https://doi.org/10.1016/j.chb.2017.10.035

Jordan, K. (2018). Validity, reliability, and the case for participant-centered research: Reflections on a multi-platform social media study. *International Journal of Human-Computer Interaction*, *34*(10), 913–921. https://doi.org/10.1080/10447318.2018.1471570

Kahraman, M., & Kuzu, A. (2016). E-Mentoring for professional development of pre-service teachers: A case study. *Turkish Online Journal of Distance Education*, *17*(3), 76–89.

Kallio, H., Pietila, A., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semistructured interview guide. *Journal of Advanced Nursing, 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. P. (2020). IoT cyber risk: a holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security, 2020*(1), 1–18. https://doi.org/10.1186/s13635-020-00111-0

Kang, H., Chen, G., & Luna-Reyes, L. F. (2019). Key determinants of online fiscal transparency: A technology-organization-environment framework. *Public Performance & Management Review*, *42*(3), 606–631. https://doi.org/10.1080/15309576.2018.1486213

Kaňovská, L., & Tomášková, E. (2018). Drivers for smart servitization in manufacturing companies. *Agris On-Line Papers in Economics & Informatics, 10*(3), 57–68. https://doi.org/10.7160/aol.2018.100305

Karagiozis, N. (2018). The complexities of the researcher's role in qualitative research: the power of reflexivity. *International Journal of Interdisciplinary Educational Studies*, *13*(1), 19–31. https://doi.org/10.18848/2327-011X/CGP/v13i01/19-31

Karahoca, A., Karahoca, D., & Aksöz, M. (2018). Examining intention to adopt to internet of

things in healthcare technology products. *Kybernetes*, *47*(4), 742–770. https://doi.org/10.1108/K-02-2017-0045

Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). A reversible and secure patient information hiding system for IoT driven e-health. *International Journal of Information Management, 45*, 262–275. https://doi.org/10.1016/j.ijinfomgt.2018.09.008

Keedle, H., Schmied, V., Burns, E., & Dahlen, H. (2018). The design, development, and evaluation of a qualitative data collection application for pregnant women. *Journal of Nursing Scholarship*, *50*(1), 47–55. https://doi.org/10.1111/jnu.12344

Kennedy, K. M. (2019). Promoting the qualitative research approach in the discipline of forensic and legal medicine: Why more qualitative work should be promoted and how that can be achieved. *Journal of Forensic and Legal Medicine, 62*, 72–76. https://doi.org/10.1016/j.jflm.2019.01.009

Kennedy, L. G., Kichler, E. J., Seabrook, J. A., Matthews, J. I., & Dworatzek, P. D. N. (2019). Validity and reliability of a food skills questionnaire. *Journal of Nutrition Education & Behavior*, *51*(7), 857–864. https://doi.org/10.1016/j.jneb.2019.02.003

Khan, W. Z., Aalsalem, M. Y., & Khan, M. K. (2019). Communal acts of IoT Consumers: A potential threat to security and privacy. *IEEE Transactions on Consumer Electronics*, *65*(1), 64–72. https://doi.org/10.1109/TCE.2018.2880338

Khanam, S., Ahmedy, I. B., Idna Idris, M. Y., Jaward, M. H., & Bin Md Sabri, A. Q. (2020). A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things. *IEEE Access*, 8, 219709–219743.

https://doi.org/10.1109/ACCESS.2020.3037359

Kieras, T., Farooq, J., & Zhu, Q. (2021). I-SCRAM: A framework for IoT supply chain risk analysis and mitigation decisions. *IEEE Access*, *9*, 29827–29840. https://doi.org/10.1109/ACCESS.2021.3058338

Kim, D., Park, K., Park, Y., & Ahn, J.-H. (2019). Willingness to provide personal information: Perspective of privacy calculus in IoT services. *Computers in Human Behavior*, *92*, 273–281. https://doi.org/10.1016/j.chb.2018.11.022

Kim, H., & Lee, E. A. (2017). Authentication and authorization for the Internet of Things. *IT Professional, 19*(5), 27–33. https://doi.org/10.1109/MITP.2017.3680960

Kim, M., & Chai, S. (2017). The impact of supplier innovativeness, information sharing and strategic sourcing on improving supply chain agility: Global supply chain perspective. *International Journal of Production Economics*, *187*, 42–52. https://doi.org/10.1016/j.ijpe.2017.02.007

Kirkegaard, P., Edwards, A., Larsen, M. B., & Andersen, B. (2018). Waiting for diagnostic colonoscopy: a qualitative exploration of screening participants' experiences in a FIT-based colorectal cancer screening program. *Patient Preference and Adherence*, *12*, 845-852.

Kobrakov, K. I., Zakuskin, S. G., Zolina, L. I., Stankevich, G. S., Kuznetsov, D. N., & Rodionov, V. I. (2017). Nanomodified textile materials with biocidal properties: Development and pilot testing of manufacturing technology. *Theoretical Foundations of Chemical Engineering*, *51*(5), 815–819. https://doi.org/1134/S004057951705013X

Kokila, J., Ramasubramanian, N., & Naganathan, N. (2019). Resource efficient metering scheme

for protecting SoC FPGA device and IPs in IoT applications. *IEEE Transactions, 27*(10), 2284-2295. https://doi.org/10.1109/TVLSI.2019.2926788

Korstjens, I., & Moser, A. (2017). Series: Practical guidance to qualitative research. Part 2: Context, research questions and designs. *European Journal of General Practice, 23*(1), 274-279. https://doi.org/10.1080/13814788.2017.1375090

Koskey, K. L. K. (2016). Using the cognitive pretesting method to gain insight into participants' experiences: an illustration and methodological reflection. *International Journal of Qualitative Methods*, *15*(1), 1-13. https://doi.org/10.1177/1609406915624577

Kouicem, D. E., Bouabdallah, A., & Lakhlef, H. (2018). Internet of things security: A top-down survey. *Computer Networks, 141*, 199–221. https://doi.org/10.1016/j.comnet.2018.03.012

Kowalski, C. P., Veeser, M., & Heisler, M. (2018). Formative evaluation and adaptation of pre- and early implementation of diabetes shared medical appointments to maximize sustainability and adoption. *BMC Family Practice*, *19*. https://doi.org/10.1186/s12875-018-0797-3

Kropp, E., & Totzek, D. (2020). How institutional pressures and systems characteristics shape customer acceptance of smart product-service systems. *Industrial Marketing Management*, *91*, 468–482. https://doi.org/10.1016/j.indmarman.2020.10.008

Kshetri, N. (2017). The economics of the Internet of Things in the global south. *Third World Quarterly*, *38*(2), 311–339. https://doi.org/10.1080/01436597.2016.1191942

Lade, P., Ghosh, R., & Srinivasan, S. (2017). Manufacturing analytics and industrial Internet of Things. *IEEE Intelligent Systems, 32*(3), 74-79. https://doi.org/10.1109/MIS.2017.49

Lampropoulos, G., Siakas, K., & Anastasiadis, T. (2019). Internet of Things in the context of

industry 4.0: An overview. *International Journal of Entrepreneurial Knowledge*, *7*(1), 4–19. https://doi.org/10.2478/IJEK-2019-0001

Lancaster, K. (2017). Confidentiality, anonymity and power relations in elite interviewing: Conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology, 20*(1), 93–103. https://doi.org/10.1080/13645579.2015.1123555

Lee, B. M., Patil, M., Hunt, P., & Khan, I. (2019). An easy network onboarding scheme for Internet of Things networks. *IEEE Access, 7,* 8763-8772. https://doi.org/10.1109/ACCESS.2018.2890072

Lekunze, L. M. G., & Strom, B. I. (2017). Bullying and victimisation dynamics in high school: an exploratory case study. *Journal of Teacher Education for Sustainability, 19*(1), 147–163.

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

Lim, R. B. T., Cheung, O. N. Y., Tham, D. K. T., La, H. H., Win, T. T., Chan, R., & Wong, M. L. (2018). Using qualitative and community-based engagement approaches to gain access and to develop a culturally appropriate STI prevention intervention for foreign female entertainment workers in Singapore. *Globalization and Health*, *14*. https://doi.org/10.1186/s12992-018-0358-5

Liu, B. F., Roberts, H., Petrun Sayers, E. L., Ackerman, G., Smith, D., & Iles, I. (2017). Preparing for the worst: public perceptions of risk management innovations. *Journal of Risk Research*, *20*(11), 1394–1417. https://doi.org/10.1080/13669877.2016.1153508

Liu, S., Guo, L., Webb, H., Ya, X., & Chang, X. (2019). Internet of Things monitoring system of modern eco-agriculture based on cloud computing. *IEEE Access, 7,* 37050-37058. https://doi.org/10.1109/ACCESS.2019.2903720

Lo, S. B., Ryba, M. M., Brothers, B. M., & Andersen, B. L. (2019). Predicting implementation of an empirically supported treatment for cancer patients using the theory of planned behavior. *Health Psychology*, *38*(12), 1075–1082. https://doi.org/10.1037/hea0000794

Lodge, L., & Crabtree, A. (2019). Privacy engineering for domestic IoT: Enabling due diligence. *Sensors*, *19*(20), Article 4380. https://doi.org/10.3390/s19204380

Lu, C. (2018). IoT-enabled adaptive context-aware and playful cyber-physical system for everyday energy savings. *IEEE Transactions on Human-Machine Systems,* 48(4), 380-391. https://doi.org/10.1109/THMS.2018.2844119

Lundgren, J., Johansson, P., Jaarsma, T., Andersson, G., & Kohler, A. K. (2018). Patient experiences of web-based cognitive behavioral therapy for heart failure and depression: qualitative study. *Journal of Medical Internet Research, 20*(9). Article e10302. https://doi.org/10.2196/10302

MacNeill, V., Foley, M., Quirk, A., & McCambridge, J. (2016). Shedding light on research participation effects in behaviour change trials: a qualitative study examining research participant experiences. *BMC Public Health, 16*(1), 1-8. https://doi.org/10.1186/s12889-016-2741-6

Madill, A., & Sullivan, P. (2018). Mirrors, portraits, and member managing difficult moments of knowledge exchange in the social sciences checking. *Qualitative Psychology, 5*(3), 321-339. https://doi.org/10.1037/qup0000089

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). https://doi.org/10.1177/1609406918786362

Majid, M. A. A., Othman, M., Mohamad, F. S., Lim, S. A. H., & Yusof, A. (2017). Piloting for interviews in qualitative research: operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences 7*(4), 1073-1080. https://doi.org/10.6007/IJARBSS/v7-i4/2916

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P., & Ni, W. (2019). Anatomy of threats to the Internet of Things. *IEEE Communications Surveys & Tutorials, 21*(2), 1636–1675. https://doi.org/10.1109/COMST.2018.2874978

Malamas, V., Chantzis, F., Dasaklis, T. K., Stergiopoulos, G., Kotzanikolaou, P., & Douligeris, C. (2021). Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal. *IEEE Access*, *9*, 40049–40075. https://doi.org/10.1109/ACCESS.2021.3064682

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

Mamotte, N., & Wassenaar, D. (2017). Voluntariness of consent to HIV clinical research: A conceptual and empirical pilot study. *Journal of Health Psychology, 22*(11), 1387–1404. https://doi.org/10.1177/1359105316628737

Mamun, A. A. (2018). Diffusion of innovation among Malaysian manufacturing SMEs.

European Journal of Innovation Management, *21*(1), 113–141. https://doi.org/10.1108/EJIM-02-2017-0017

Marks, A., Wilkes, L., Blythe, S., & Griffiths, R. (2017). A novice researcher's reflection on recruiting participants for qualitative research. *Nurse Researcher*, *25*(2), 34-38. https://doi.org/10.7748/nr.2017.e1510

Martínez-Mesa, J., González-Chica, D. A., Duquia, R. P., Bonamigo, R. R., & Bastos, J. L. (2016). Sampling: how to select participants in my research study? *Anais Brasileiros De Dermatologia, 91*(3), 326–330. https://doi.org/10.1590/abd1806-4841.20165254

Martín-Lopo, M. M., Boal, J., & Sánchez-Miralles, Á. (2020). A literature review of IoT energy platforms aimed at end users. *Computer Networks*, *171*. https://doi.org/10.1016/j.comnet.2020.107101

Martín-Ruíz, M. L., Fernández-Aller, C., Portillo, E., Malagón, J., & Del Barrio, C. (2018). Developing a system for processing health data of children using digitalized toys: Ethical and privacy concerns for the Internet of Things paradigm. *Science and Engineering Ethics*, *24*(4), 1057–1076. https://doi.org/10.1007/s11948-017-9951-x

Masoumi, D., Hatami, J., & Pourkaremi, J. (2019). Continuing professional development: policies, practices and future directions. *International Journal of Educational Management*, *33*(1), 98-111. https://doi.org/10.1108/IJEM-03-2018-0109

Matlala, S. F., & Matlala, M. N. (2018). The use of a smartphone to facilitate qualitative research in South Africa. *Qualitative Report*, *23*(10), 2264–2275. https://doi.org/10.46743/2160-3715/2018.3409

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative, or mixed

methods and choice based on the research. *Perfusion, 30*(7), 537-542. https://doi.org/10.1177/0267659114559116

Mhaskar, N., Alabbad, M., & Khedri, R. (2021). A formal approach to network segmentation. *Computers & Security*, *103*. https://doi.org/10.1016/j.cose.2020.102162

Miller, D. (2018). Blockchain and the Internet of Things in the industrial sector. *IT Professional, 20* (3), 15-18. https://doi.org/10.1109/MITP.2018.032501742

Miracle, V. A. (2016). The Belmont Report: The triple crown of research ethics. *Dimensions of Critical Care Nursing, 35*(4), 223–228. https://doi.org/10.1097/DCC.0000000000000186

Mitchell, F., Stalker, K., Matthews, L., Mutrie, N., Melling, C., McConnachie, A., Murray, H., & Melville, C. A. (2018). A qualitative exploration of participants' experiences of taking part in a walking programme: Perceived benefits, barriers, choices and use of intervention resources. *Journal of Applied Research in Intellectual Disabilities, 31*, 110–121. https://doi.org/10.1111/jar.12326

Mombeuil, C. (2020). An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets. *Journal of Retailing and Consumer Services*, *55*. https://doi.org/10.1016/j.jretconser.2020.102127

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

Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. *IEEE Transactions, 5*(4), 586–602. https://doi.org/10.1109/TETC.2016.2606384

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. https://doi.org/10.1080/13814788.2017.1375091

Munthe-Kaas, M. H., Glenton, C., Booth, A., Noyes, J., & Lewin, S. (2019). Systematic mapping of existing tools to appraise methodological strengths and limitations of qualitative research: first stage in the development of the CAMELOT tool. *BMC Medical Research Methodology*, *19*(1), 1-13. https://doi.org/10.1186/s12874-019-0728-6

Murray, L. C. (2016). Review of the problem-centred interview. *Journal of Mixed Methods Research*, *10*(1), 112–113. https://doi.org/10.1177/1558689815577032

Naidoo, D., Van Wyk, J., & Joubert, R. W. E. (2016). Exploring the occupational therapist's role in primary health care: Listening to voices of stakeholders. *African Journal of Primary Health Care & Family Medicine*, *8*(1), e1–e9. https://doi.org/10.4102/phcfm.v8i1.1139

Natarajan, T., Balasubramanian, S. A., & Kasilingam, D. L. (2018). The moderating role of device type and age of users on the intention to use mobile shopping applications. *Technology in Society*, *53*, 79–90. https://doi.org/10.1016/j.techsoc.2018.01.003

Nath, N., Hu, Y., & Budge, C. (2016). Information technology and diffusion in the New Zealand public health sector. *Qualitative Research in Accounting & Management*, *13*(2), 216–251. https://doi.org/10.1108/QRAM-02-2015-0026

Naushad, M., & Sulphey, M. M. (2020). Prioritizing technology adoption dynamics among SMEs. *TEM Journal, 9*(3), 983–991. https://doi.org/10.18421/TEM93-21

Nehme, E. K., Pérez, A., Ranjit, N., Amick, I. B. C., & Kohl, I. H. W. (2016). Behavioral theory and transportation cycling research: Application of Diffusion of Innovations. *Journal of*

Transport & Health, *3*(3), 346–356. https://doi.org/10.1016/j.jth.2016.05.127

Nekit, K., Kolodin, D., & Fedorov, V. (2020). Personal data protection and liability for damage in the field of the internet of things. *Juridical Tribune, 10*(1), 80–93.

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

Nikou, S. (2019). Factors driving the adoption of smart home technology: An empirical assessment. *Telematics & Informatics*, 45, N.PAG. https://doi.org/10.1016/j.tele.2019.101283

Nikoukar, A., Raza, S., Poole, A., Gunes, M., & Dezfouli, B. (2018). Low-power wireless for the Internet of Things: standards and applications. *IEEE Access, 6*, 67893-67926. https://doi.org/10.1109/ACCESS.2018.2879189

Noguchi, H., Kataoka, M., & Yamato, Y. (2019). Device identification based on communication analysis for the Internet of Things. (2019). *IEEE Access, 7,* 52903-52912. https://doi.org/10.1109/ACCESS.2019.2910848

Nurse, J. R. C., Creese, S., & De Roure, D. (2017). Security risk assessment in Internet of Things systems. *IT Professional, 19*(5), 20–26. https://doi.org/10.1109/MITP.2017.3680959

O'Boyle, A. (2018). Encounters with identity: reflexivity and positioning in an interdisciplinary research project. *International Journal of Research & Method in Education, 41*(3), 353–366.

O'Hara, L., & Higgins, K. (2019). Participant photography as a research tool: Ethical issues and practical implementation. *Sociological Methods & Research*, *48*(2), 369–399.

Oltmann, S. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Forum: Qualitative Social Research, 17*(2).

Oplatka, I. (2018). Understanding emotion in educational and service organizations through semi-structured interviews: some conceptual and practical insights. *Qualitative Report*, *23*(6), 1347–1363.

Osarenkhoe, A., & Byarugaba, J. M. (2016). Service quality perceptions of foreign direct investors. *Journal of Promotion Management*, *22*(5), 684-704. https://doi.org/10.1080/10496491.2016.1185492

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

Overmars-Marx, T., Thomése, F., & Moonen, X. (2018). Photovoice in research involving people with intellectual disabilities: A guided photovoice approach as an alternative. *Journal of Applied Research in Intellectual Disabilities*, *31*(1), e92–e104. https://doi.org/10.1111/jar.12329

Owoh, N. P., & Singh, M. M. (2018). Security analysis of mobile crowd sensing applications. *Applied Computing and Informatics*. https://doi.org/10.1016/j.aci.2018.10.002

Ozturk, A. B., Bilgihan, A., Salehi-Esfahani, S., & Hua, N. (2017). Understanding the mobile payment technology acceptance based on valence theory: A case of restaurant transactions. *International Journal of Contemporary Hospitality Management*, *29*(8), 2027–2049. https://doi.org/10.1108/IJCHM-04-2016-0192

Padyab, A., Habibipour, A., Rizk, A., & Ståhlbröst, A. (2019). Adoption barriers of IoT in large scale pilots. *Information*, *11*(1), Article 23. https://doi.org/10.3390/info11010023

Pagan, V. (2019). Being and becoming a "good" qualitative researcher? Liminality and the risk of limbo. *Qualitative Research in Organizations and Management, 14*(1), 75-90. https://doi.org/10.1108/QROM-04-2017-1523

Pal, D., Funilkul, S., & Papasratorn, B. (2019). Antecedents of trust and the continuance intention in IoT-Based smart products: The case of consumer wearables. *IEEE Access, 7*, 184160–184171. https://doi.org/10.1109/ACCESS.2019.2960467

Paliszkiewicz, J. (2019). Information security policy compliance: Leadership and trust. *Journal of Computer Information Systems*, *59*(3), 211–217. https://doi.org/10.1080/08874417.2019.1571459

Pan, H., & Yang, X. (2019). Application of Internet of Things technology in 3D medical image model. *IEEE Access, 7*, 5508-5518. https://doi.org/10.1109/ACCESS.2018.2886223.

Pang, P. C., Chang, S., Verspoor, K., & Clavisi, O. (2018). The use of web-based technologies in health research participation: Qualitative study of consumer and researcher experiences. *Journal of Medical Internet Research*, *20*(10), Article e12094. https://doi.org/10.2196/12094

Pearce, P. H., Marks, L. D., & Hawkins, A. J. (2016). Why we chose to stay together: Qualitative interviews with separated couples who chose to reconcile. *Journal of Divorce & Remarriage*, *57*(5), 317–337. https://doi.org/10.1080/10502556.2016.118508

Pengfei, Z., Peiwei, L., Karen, R., & Barbara, D. (2016). Methodological tool or methodology? Beyond instrumentality and efficiency with qualitative data analysis software. *Forum:*

Qualitative Social Research, *17*(2).

Percival, J., Donovan, J., Kessler, D., & Turner, K. (2017). "She believed in me". What patients with depression value in their relationship with practitioners. A secondary analysis of multiple qualitative data sets. *Health Expectations, 20*(1), 85–97. https://doi.org/10.1111/hex.12436

Peterson, J. S. l. (2019). Presenting a qualitative study: a reviewer's perspective. *Gifted Child Quarterly, 63*(3), 147–158. https://doi.org/10.1177/0016986219844789

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

Pezalla, A. E., Pettigrew, J., & Miller-Day, M. (2012). Researching the researcher-as-instrument: an exercise in interviewer self-reflexivity. *Qualitative Research*, *12*(2), 165–185. https://doi.org/10.1177/1468794111422107

Pinnegar, E., & Quiles-Fernández, E. (2018). A self-study of researcher relationships with research participants. *Studying Teacher Education*, *14*(3), 284–295. https://doi.org/10.1080/17425964.2018.1541287

Plowman, L. (2017). Revisiting ethnography by proxy. *International Journal of Social Research Methodology, 20*(5), 443-454. https://doi.org/10.1080/13645579.2016.1196902

Preuveneers, D., Joosen, W., & Ilie-Zudor, E. (2017). Trustworthy data-driven networked production for customer-centric plants. *Industrial Management & Data Systems, 117*(10), 2305–2324. https://doi.org/10.1108/IMDS-10-2016-0419

Quartiroli, A., Knight, S. M., Etzel, E. F., & Monaghan, M. (2017). Using Skype to facilitate

team-based qualitative research, including the process of data analysis. *International Journal of Social Research Methodology, 20*(6), 659–666. https://doi.org/10.1080/13645579.2016.1275371

Quek, G. J. H., Ho, G. H. L., Hassan, N. B., Quek, S. E. H., & Shorey, S. (2019). Perceptions of preceptorship among newly graduated nurses and preceptors: A descriptive qualitative study. *Nurse Education in Practice*, *37*, 62–67. https://doi.org/10.1016/j.nepr.2019.05.001

Rakhmawati, F., & Nirmalawati, W. (2017). Grammar teaching at pre-service training program in Kampung Inggris (a case study on mastering system program). *Journal of Applied Studies in Language*, 1(1), *6*-12.

Randall, C. G., Justina, W., Taryn, E., Mark, B., Caitlin, M. R., Laura, J. D., & Amanda, M. M. (2019). Comparison of rapid vs in-depth qualitative analytic methods from a process evaluation of academic detailing in the veterans health administration. *Implementation Science, 14*(1), 1-12. https://doi.org/10.1186/s13012-019-0853-y

Raskind, I. G., Shelton, R. C., Comeau, D. L., Cooper, H. L. F., Griffith, D. M., & Kegler, M. C. (2019). A review of qualitative data analysis practices in health education and health behavior research. *Health Education & Behavior*, *46*(1), 32–39.

Realyvásquez, A., Maldonado-Macías, A. A., García-Alcaraz, J. L., & Blanco-Fernández, J. (2019). Effects of macroergonomic compatibility of information and communication technologies on the performance of manufacturing systems. *Behaviour & Information Technology, 38*(7), 651–663. https://doi.org/10.1080/0144929X.2018.1551422

Rekers, J. V. (2016). What triggers innovation diffusion? Intermediary organizations and

geography in cultural and science-based industries. *Environment and Planning C-Government and Policy*, *34*(6), 1058–1075. https://doi.org/10.1177/0263774X15625226

Riad, K., & Ke, L. (2018). Secure storage and retrieval of IoT data based on private information Retrieval. *Wireless Communications & Mobile Computing*, 1–8. https://doi.org/10.1155/2018/5452463

Rice, R. E., & Hoffmann, Z. T. (2018). Attention in business press to the diffusion of attention technologies, 1990-2017. *International Journal of Communication 12*, 3227–3252.

Riki - Riki. (2019). Acceptance of web-based technology as a harmonious community of citizen with the concept of technology model acceptance. *Jurnal TAM, 1*(1), 8-11.

Rizvi, S., Pipetti, R., McIntyre, N., Todd, J., & Williams, I. (2020). Threat model for securing internet of things (IoT) network at device-level. *Internet of Things*, *11*. https://doi.org/10.1016/j.iot.2020.100240

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

Rogers, E. M. (2003). *Diffusion of innovations*: 3rd ed. New York: Free Press.

Rolfe, E. D., Ramsden, R. V., Banner, D., & Graham, D. I. (2018). Using qualitative health research methods to improve patient and public involvement and engagement in research. *Research Involvement and Engagement*, *4*(1), 1-8. https://doi.org/10.1186/s40900-018-0129-8

Roopa, M. S., Santosh, P., Rajkumar, B., Rajkumar, K. R., Iyengar, S. S., & Patnaik, L. M. (2019). Social Internet of Things (SIoT): foundations, thrust areas, systematic review and future directions. *Computer Communications*, *139*, 32–57. https://doi.org/10.1016/j.comcom.2019.03.009

Rosenthal, M. (2016). Qualitative research methods: Why, when, and how to conduct interviews and focus groups in pharmacy research. *Currents in Pharmacy Teaching & Learning, 8*(4), 509–516. https://doi.org/10.1016/j.cptl.2016.03.021

Roxana, H., & Mircea, G. (2016). Small steps or big changes in actual society: the impact of Internet of Things. *Journal of Public Administration, Finance & Law*, *5*(10). 132-141.

Rutherford, R. (2019). Internet of Things – striking the balance between competition and security. *Network Security*, *2019*(2), 6–8. https://doi.org/10.1016/S1353-4858(19)30020-0

Sabet, M. K., & Minaei, R. (2017). A comparative corpus-based analysis of genre-specific discourse: The quantitative and qualitative academic papers in the field of the TEFL. *Theory & Practice in Language Studies, 7*(4), 294–304. https://doi.org/10.17507/tpls.0704.08

Saez, M., Maturana, F. P., Barton, K., & Tilbury, D. M. (2018). Real-Time manufacturing machine and system performance monitoring using Internet of Things. *IEEE Transactions 15*(4), 1735-1748. https://doi.org/10.1109/TASE.2017.2784826

Salman, S., Ngueng, F. I., & Joly, Y. (2016). Disclosure of insurability risks in research and clinical consent forms. *Global Bioethics*, *27*(1), 38–49. https://doi.org/10.1080/11287462.2016.1183442

Sayar, D., & Er, Ö. (2018). The antecedents of successful IoT service and system design: Cases from the manufacturing industry. *International Journal of Design, 12*(1), 67-78.

Scharp, K. M., & Sanders, M. L. (2019). What is a theme? Teaching thematic analysis in qualitative communication research methods. *Communication Teacher*, *33*(2), 117–121.

Schneider, M. J., Jagpal, S., Gupta, S., Li, S., & Yu, Y. (2017). Protecting customer privacy when marketing with second-party data. *International Journal of Research in Marketing, 34*(3), 593–603. https://doi.org/10.1016/j.ijresmar.2017.02.003

Scott, S., & McGuire, J. (2017). Using diffusion of innovation theory to promote universally designed college instruction. *International Journal of Teaching & Learning in Higher Education, 29*(1), 119–128. Retrieved from https://search-ebscohost-com

Sebetci, Ö. (2018). Enhancing end-user satisfaction through technology compatibility: An assessment on health information system. *Health Policy and Technology, 7*(3), 265–274. https://doi.org/10.1016/j.hlpt.2018.06.001

Seetharaman, A., Patwa, N., Saravanan, A. S., & Sharma, A. (2019). Customer expectation from Industrial Internet of Things (IIOT). *Journal of Manufacturing Technology Management*, *30*(8), 1161–1178. https://doi.org/10.1108/JMTM-08-2018-0278

Segarra, T. I. J., Jammal, A. B., & Chaouchi, H. (2017). New IoT proximity service based heterogeneous RFID readers collision control. *PSU Research Review, 1*(2), 127-149. https://doi.org/10.1108/PRR-03-2017-0019

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

Seliem, M., Elgazzar, K., & Khalil, K. (2018). Towards privacy preserving IoT Environments: A survey. *Wireless Communications & Mobile Computing*, 1–15. https://doi.org/10.1155/2018/1032761

Sethi, P., & Sarangi, R. S. (2017). Internet of Things: Architectures, protocols, and

applications. *Journal of Electrical and Computer Engineering*. 1–25. https://doi.org/10.1155/2017/9324035

Shafiq, S. I., Szczerbicki, E., & Sanin, C. (2018). Manufacturing data analysis in Internet of Things/Internet of data (IoT/IoD) scenario. *Cybernetics and Systems*, *49*(5–6), 280–295. https://doi.org/10.1080/01969722.2017.1418265

Sheikh, S. M., & Halima, N. B. (2017). Design, implementation and testing of a cost function based scheduling mechanism for a water management system. *Procedia Computer Science*, *110*, 54–61. https://doi.org/10.1016/j.procs.2017.06.114

Shoaib, N., & Shamsi, J. A. (2019). Understanding Network Requirements for Smart City Applications: Challenges and Solutions. *IT Professional, 21*(3), 33–40. https://doi.org/10.1109/MITP.2018.2883047

Si, H., Shi, J. G., Tang, D., Wen, S., Miao, W., & Duan, K. (2019). Application of the theory of planned behavior in environmental science: A comprehensive bibliometric analysis. *International Journal of Environmental Research and Public Health*, *16*(15). https://doi.org/10.3390/ijerph16152788

Siegner, M., Hagerman, S., & Kozak, R. (2018). Going deeper with documents: A systematic review of the application of extant texts in social research on forests. *Forest Policy and Economics, 92*, 128–135. https://doi.org/10.1016/j.forpol.2018.05.001

Siew Khoon Khoo, Y., & Saleh, K. (2017). A qualitative study among potential manufacturers on the development of "Made in Malaysia" biological products: challenges and proposed solutions. *Journal of Commercial Biotechnology*, *23*(4), 44–61. https://doi.org/10.5912/jcb814

Silva, J. C., Rodrigues, J. J. P. C., Al-Muhtadi, J., Rabêlo, R. A. L., & Furtado, V. (2019). Management platforms and protocols for Internet of Things: A Survey. *Sensors*, *19*(3), Article 676. https://doi.org/10.3390/s19030676

Simranjeet, S., Bassam, J. M., & Thaier, H. (2019). Hardware security in IoT devices with emphasis on hardware trojans. *Journal of Sensor and Actuator Networks, 8*(3), Article 42. https://doi.org/10.3390/jsan8030042

Singh, G., & Shrimankar, D. (2018). A privacy-preserving authentication protocol with secure handovers for the LTE/LTE-A networks. *Sadhana*, *43*(8), Article 1. https://doi.org/10.1007/s12046-018-0891-1

Sivathanu, B. (2018). Adoption of internet of things (IOT) based wearables for healthcare of older adults – a behavioural reasoning theory (BRT) approach. *Journal of Enabling Technologies, 12*(4), 169–185. https://doi.org/10.1108/JET-12-2017-0048

Slovin, L. J., & Semenec, P. (2019). Thinking/writing within and outside the IRB box: Ethical disruptions of data in qualitative research. *Reconceptualizing Educational Research Methodology, 10*(1), 14–27. https://doi.org/10.7577/rerm.3241

Sohel, S. M., & Quader, M. S. (2017). Transforming IT from a cost centre to a value centre perspective: a case study on the British standards institute. *Journal of Services Research*, *17*(1), 71–105.

Sohrabi, S. N., Von, S. R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/j.cose.2015.10.006

Spano, E., Niccolini, L., Di Pascoli, S., & Iannaccone, G. (2015). Last-Meter smart grid

embedded in an Internet-of-Things platform. *IEEE Transactions 6*(1), 468- 476. https://doi.org/10.1109/TSG.2014.2342796

Springer, S. I., Land, C. W., Moss, L. J., & Cinotti, D. (2018). Collecting school counseling group work data: initiating consensual qualitative research through practitioner-researcher partnerships. *Journal for Specialists in Group Work*, *43*(2), 128–143. https://doi.org/10.1080/01933922.2018.1431346

Stergiopoulos, G., Dedousis, P., & Gritzalis, D. (2020). Automatic network restructuring and risk mitigation through business process asset dependency analysis. *Computers & Security*, *96*. https://doi.org/10.1016/j.cose.2020.101869

Stieninger, M., Nedbal, D., Wetzlinger, W., Wagner, G., & Erskine, A. M. (2018). Factors influencing the organizational adoption of cloud computing: a survey among cloud workers. *International Journal of Information Systems and Project Management*, *6*(1), 5-23. https://doi.org/10.12821/ijispm060101

Stracener, C., Samelson, Q., Mackie, J., Ihaza, M., Laplante, P. A., & Amaba, B. (2019). The Internet of Things grows artificial intelligence and data sciences. *IT Professional, 21* (3), 55-62. https://doi.org/10.1109/MITP.2019.2912729

Sułkowski, Ł., & Marjański, A. (2018). Duo-ethnography as the qualitative inquiry in small family business research. *Management*, *22*(2), 95-109. https://doi.org/10.2478/manment-2018-0025

Sun, J., & Ting, C. (2019). Investigating the adoption of apparel m-commerce in the US market. *International Journal of Clothing Science and Technology*, *31*(4), 544–563. https://doi.org/10.1108/IJCST-03-2018-0038

Sun, Y., Lo, F. P., & Lo, B. (2019). Security and Privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access, 7*, 183339–183355. https://doi.org/10.1109/ACCESS.2019.2960617

Surmiak, A. (2018). Confidentiality in qualitative research involving vulnerable participants: researchers' perspectives. *Forum: Qualitative Social Research*, *19*(3), 393–418. https://doi.org/10.17169/fqs-19.3.3099

Syed, H. J., Gani, A., Ahmad, R. W., Khan, M. K., & Ahmed, A. I. A. (2017). Cloud monitoring: A review, taxonomy, and open research issues. *Journal of Network and Computer Applications*, *98*, 11–26. https://doi.org/10.1016/j.jnc

Taheri, F., Jami Pour, M., & Asarian, M. (2019). An exploratory study of subjective well-being in organizations–A mixed method research approach. *Journal of Human Behavior in the Social Environment*, *29*(4), 435–454. https://doi.org/10.1080/10911359.2018.1547671

Talebian, A., & Mishra, S. (2018). Predicting the adoption of connected autonomous vehicles: A new approach based on the theory of diffusion of innovations. *Transportation Research Part C-Emerging Technologies, 95*, 363–380. https://doi.org/10.1016/j.trc.2018.06.005

Tan, Y. S., Ng, Y. T., & Low, J. S. C. (2017). Internet-of-Things enabled real-time monitoring of energy efficiency on manufacturing shop floors. *Procedia CIRP, 61*, 376–381. https://doi.org/10.1016/j.procir.2016.11.242

Tedeschi, S., Mehnen, J., Tapoglou, N., & Roy, R. (2016). Secure IoT devices for the maintenance of machine tools. *Procedia CIRP*, *59*, 150-155. https://doi.org/10.1016/j.procir.2016.10.002

Tedeschi, S., Rodrigues, D., Emmanouilidis, C., Erkoyuncu, J., Roy, R., & Starr, A. (2018). A

cost estimation approach for IoT modular architectures implementation in legacy systems. *Procedia Manufacturing*, 19, 103–110. https://doi.org/10.1016/j.promfg.2018.01.015

Terry, N. P. (2017). Regulatory disruption and arbitrage in health-care data protection. *Yale Journal of Health Policy, Law & Ethics, 17*(1), 143–207.

Tornatzky, L., & Fleischer, M. (1990). *The process of technology innovations.* MA: Lexington Books.

Totawar, A., & Prasad, M. (2016). Research methodology: A step-by-step guide for beginners. *South Asian Journal of Management, 23*(3), 210–213.

Tran, V. T., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology, 80*, 88–96. https://doi.org/10.1016/j.jclinepi.2016.07.014

Trappey, A. J. C., Trappey, C. V., Hareesh-Govindarajan, U., Chuang, A. C., & Sun, J. J. (2017). A review of essential standards and patent landscapes for the Internet of Things: A key enabler for industry 4.0. *Advanced Engineering Informatics, 33*, 208–229. https://doi.org/10.1016/j.aei.2016.11.007

Tresanchez, M., Pujol, A., Pallejà, T., Martínez, D., Clotet, E., & Palacín, J. (2018). A proposal of low-cost and low-power embedded wireless image sensor node for IoT applications. *Procedia Computer Science*, *134*, 99-106. https://doi.org/10.1016/j.procs.2018.07.149

Uher, J. (2018). Quantitative data from rating scales: An epistemological and methodological enquiry. *Frontiers in Psychology, 9*. https://doi.org/10.3389/fpsyg.2018.02599

Upadhaya, B., Munir, R., Blount, Y., & Su, S. (2018). Diffusion of corporate social responsibility in the airline industry. *International Journal of Operations & Production Management*, *38*(4), 1020–1040. https://doi.org/10.1108/IJOPM-10-2015-0638

Upasani, K., Bakshi, M., Pandhare, V., & Lad, B. K. (2017). Distributed maintenance planning in manufacturing industries. *Computers & Industrial Engineering, 108*, 1–14. https://doi.org/10.1016/j.cie.2017.03.027

U.S. Department of Health & Human Services. (1979). *The Belmont Report*. https://www.hhs.gov/ohrp/regulations-and-policy/belmont-report/read-the-belmont-report/index.html

U.S. Department of Justice. (2017). *Securing Your "Internet of Things" Devices*. https://www.justice.gov/criminal-ccips/page/file/984001/download

Uttaran, D. (2019). Conducting ethnographic research in low literate, economically weak underserved spaces: an introduction to iconic legisigns-guided interviewing (ILGI). *International Journal of Qualitative Methods, 18*. https://doi.org/10.1177/1609406919855279

Vaibhav, S. N., Rakesh, D. R., Bhaskar, G., Mahesh, S. K., & Balkrishna, E. N. (2019). Factors affecting the adoption of cloud of things: The case study of Indian small and medium enterprises. *Journal of Systems and Information Technology*, *21*(4), 397–418. https://doi.org/10.1108/JSIT-10-2018-0137

van den Berg, A., & Struwig, M. (2017). Guidelines for researchers using an adapted consensual qualitative research approach in management research. *Electronic Journal of Business Research Methods*, *15*(2), 109–119.

van Rijnsoever, F. J. (2017). (I can't get no) saturation: A simulation and guidelines for sample sizes in qualitative research. *Plos One, 12*(7), Article e0181689. https://doi.org/10.1371/journal.pone.0181689

Varpio, L., Ajjawi, R., Monrouxe, L. V., O'Brien, B. C., & Rees, C. E. (2017). Shedding the cobra effect: problematising thematic emergence, triangulation, saturation and member checking. *Medical Education, 51*(1), 40–50. https://doi.org/10.1111/medu.13124

Vasileiou, K., Barnett, J., Thorpe, S., & Young, T. (2018). Characterising and justifying sample size sufficiency in interview-based studies: systematic analysis of qualitative health research over a 15-year period. *BMC Medical Research Methodology, 18*(1), 1-18. https://doi.org/10.1186/s12874-018-0594-7

Veleva, P. (2019). Personal data security for smart systems and devises with remote access. *Trakia Journal of Sciences*, *17*(1), 873–882. https://doi.org/10.15547/tjs.2019.s.01.144

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.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, 17(5), 328–376.

Wadams, M., & Park, T. (2018). Qualitative research in correctional settings: Researcher bias, western ideological influences, and social justice. *Journal of Forensic Nursing*, *14*(2), 72–79. https://doi.org/10.1097/JFN.0000000000000199

Waheed, N., Xiangjian, H., Ikram, M., Usman, M., & Hashmi, S. S. (2020). Security and privacy

in IoT using machine learning and blockchain: Threats and countermeasures. *ACM Computing Surveys, 53*(6), 1–37. https://doi.org/10.1145/3417987

Waheed, Z., Hussin, S., & Bin Megat Daud, M. A. K. (2018). The best practices for school transformation: A multiple-case study. *Journal of Educational Administration, 56*(1), 88–103. https://doi.org/10.1108/JEA-11-2016-0136

Walford, G. (2018). The impossibility of anonymity in ethnographic research. *Qualitative Research, 18*(5), 516–525. https://doi.org/10.1177/1468794118778606

Wang, C., Shen, J., Liu, Q., Ren, Y., & Li, T. (2018). A novel security scheme based on instant encrypted transmission for Internet of Things. *Security & Communication Networks*, 1–7. https://doi.org/10.1155/2018/3680851

Wang, W., Deng, Z., & Wang, J. (2019). Enhancing sensor network security with improved internal hardware design. *Sensors*, *19*(8), Article 1752. https://doi.org/10.3390/s19081752

Wang, Y.-Y., Lin, H.-H., Wang, Y.-S., Shih, Y.-W., & Wang, S.-T. (2018). What drives users' intentions to purchase a GPS navigation app. *Internet Research*, *28*(1), 251–274. https://doi.org/10.1108/IntR-11-2016-0348

Wei, W., Zhang, L., & Hua, N. (2019). Error management in service security breaches. *Journal of Services Marketing, 33*(7), 783–797. https://doi.org/10.1108/JSM-04-2018-0114

Weidinger, J., Schlauderer, S., & Overhage, S. (2018). Is the frontier shifting into the right direction? A qualitative analysis of acceptance factors for novel firefighter information technologies. *Information Systems Frontiers*, *20*(4), 669–692. https://doi.org/10.1007/s10796-017-9785-8

Weissinger, G. M., & Ulrich, C. M. (2019). Informed consent and ethical reporting of research in clinical trials involving participants with psychotic disorders. *Contemporary Clinical Trials, 84*. https://doi.org/10.1016/j.cct.2019.06.009

Wong, F. M. F. (2018). A phenomenological research study: Perspectives of student learning through small group work between undergraduate nursing students and educators. *Nurse Education Today, 68*, 153–158. https://doi.org/10.1016/j.nedt.2018.06.013

Wu, X., Tian, S., & Zhang, L. (2019). The Internet of Things enabled shop floor scheduling and process control method based on petri nets. *IEEE Access, 7*, 27432–27442. https://doi.org/10.1109/ACCESS.2019.2900117

Xi, M., Li, J., Zhou, D., & Yang, D. (2016). 5G technology requirements and related test environments for evaluation. *China Communications, 13*(2), 42–51. https://doi.org/10.1109/CC.2016.7833459

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems*, *33*(3), 267–284. https://doi.org/10.2308/isys-52480

Xu, Y., & Chen, M. (2016). Improving just-in-time manufacturing operations by using Internet of Things based solutions. *Procedia CIRP*, *56*, 326–331. https://doi.org/10.1016/j.procir.2016.10.030

Yan, B., Liu, L., Liu, S., & Yang, J. (2018). Influencing factors in the application of RFID technology in the supply chain. *Engineering Economist, 63*(1), 1–19. https://doi.org/10.1080/0013791X.2016.1269269

Yang, C.-H., Lee, K.-C., & Li, S.-E. (2020). A mixed activity-based costing and resource

constraint optimal decision model for IoT-oriented intelligent building management system portfolios. *Sustainable Cities and Society, 60*. https://doi.org/10.1016/j.scs.2020.102142

Yang, H., Kumara, S., Bukkapatnam, S. T. S., & Tsung, F. (2019). The internet of things for smart manufacturing: A review. *IISE Transactions, 51*(11), 1190-1216. https://doi.org/10.1080/24725854.2018.1555383

Yao, C., Wu, S., Liu, Z., & Li, P. (2019). A deep learning model for predicting chemical composition of gallstones with big data in medical Internet of Things. *Future Generation Computer Systems*, *94*, 140–147. https://doi.org/10.1016/j.future.2018.11.011

Yardley, L. (2017). Demonstrating the validity of qualitative research. *The Journal of Positive Psychology*, *12*(3), 295–296. https://doi.org/10.1080/17439760.2016.1262624

Yelpaze, I., & Ceyhan, A. A. (2019). University students' perceptions about psychological help seeking: a qualitative study. *International Online Journal of Educational Sciences*, *11*(1), 123–139. https://doi.org/10.15345/iojes.2019.01.009

Yen Ting, N., Yee Shee, T., & Sze Choong, L. J. (2017). Internet of Things for real-time waste monitoring and benchmarking: Waste reduction in manufacturing shop floor. *Procedia CIRP*, *61*, 382–386. https://doi.org/10.1016/j.procir.2016.11.243

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. *Qualitative Report*, *23*(11), 2700–2713.

Yoo, K., Bae, K., Park, E., & Yang, T. (2020). Understanding the diffusion and adoption of bitcoin transaction services: The integrated approach. *Telematics & Informatics*, *53*,

https://doi.org/10.1016/j.tele.2019.101302

Yoon, C., Lim, D., & Park, C. (2020). Factors affecting adoption of smart farms: The case of Korea. *Computers in Human Behavior*, *108*. https://doi.org/10.1016/j.chb.2020.106309

Young, R. E., Broom, D., Sage, K., Crossland, K., & Smith, C. (2019). Experiences of venue based exercise interventions for people with stroke in the UK: A systematic review and thematic synthesis of qualitative research. *Physiotherapy*. *110*, 5–14. https://doi.org/10.1016/j.physio.2019.06.001

Yousuf, O., & Mir, N. R. (2019). A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures. *Information & Computer Security*, *27*(2), 292-323. https://doi.org/10.1108/ICS-07-2018-0084

Yu, X., Ergun, K., Cherkasova, L., & Rosing, T. S. (2020). Optimizing sensor deployment and maintenance costs for large-scale environmental monitoring. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 39*(11), 3918–3930. https://doi.org/10.1109/TCAD.2020.3012232

Yu, X., Roy, S. K., Quazi, A., Nguyen, B., & Han, Y. (2017). Internet entrepreneurship and "the sharing of information" in an Internet-of-Things context. *Internet Research, 27*(1), 74–96. https://doi.org/10.1108/IntR-02-2015-0060

Yun, J., Ahn, I.-Y., Choi, S.-C., & Kim, J. (2016). TTEO (Things Talk To Each Other): programming smart spaces based on IoT Systems. *Sensors, 16*(4), 1-21. https://doi.org/10.3390/s16040467

Zalewski, J. (2019). IoT safety: State of the art. *IT Professional, 21*(1), 16-20. https://doi.org/10.1109/MITP.2018.2883858

Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications*, *84*, 25–37. https://doi.org/10.1016/j.jnca.2017.02.009

Zhang, P., Yang, X., Chen, J., & Huang, Y. (2019). A survey of testing for 5G: Solutions, opportunities, and challenges. *China Communications, 16*(1), 69–85. https://doi.org/10.12676/j.cc.2019.01.007

Zheng, K., & Jia, S. (2017). Promoting the opportunity identification of industrial symbiosis: agent-based modeling inspired by innovation diffusion theory. *Sustainability, 9*(5). https://doi.org/10.3390/su9050765

Zhou, H., Sun, G., Fu, S., Liu, J., Zhou, X., & Zhou, J. (2019). A big data mining approach of PSO-Based BP neural network for financial risk management with IoT. *IEEE Access*, *7*, 154035–154043. https://doi.org/10.1109/ACCESS.2019.2948949

Appendix A: Health Office of Extramural Research Certificate

Certificate of Completion

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

Date of Completion: 05/19/2018

Certification Number: 2822658

NIH National Institutes of Health
Office of Extramural Research

Appendix B: Interview Protocol

Interview Title: Exploring strategies to protect against security violations while adopting IoT in the manufacturing industry.

1. I will first introduce myself to the participants and thank them for participating.
2. I will confirm that they received the consent form and answer any questions and concerns that the participants might have.
3. I will collect the signed consent form from the participants.
4. I will let the participant know that the interview will be recorded, and all information will remain confidential.
5. I will turn on the recording devices, state the study participant's anonymous code, and state the date and time of the interview.
6. I will ask the interview questions starting with the first, giving the participant time to answer and continue through to the last question:
7. I will end the interview by asking if there is any other information they would like to share.
8. I will let the participants know about member checking, that I will use to verify the accuracy of the initial interview.

Last, I will thank the participant for taking part in the study. I will confirm the participant's contact information and schedule a time for the follow-up interview.

Appendix C: Interview Questions

1) What are your position and job functions?

2) How long have you been on that role?

3) How long have you used IoT?

4) How many security breaches have you had since IoT implementation?

5) How do you protect against security violations of IoT heterogeneous devices and IT infrastructure in adopting IoT?

6) What kind of security policy do you have in place? If you have, can you describe it?

7) How does creating a relative advantage over competitors impact your security activities when adopting IoT?

8) How does compatibility of IoT devices with existing technology impact your security activities when adopting IoT?

9) How does complexity of IoT devices impact your security activities when adopting IoT?

10) What impact will trialability of IoT devices have on your security activities when adopting IoT?

11) How do you observe that protecting against security violations will help in making IoT a viable solution?

12) How do you ensure that there is an adequate budget for protecting against security violations in adopting IoT?

Appendix D: Participant Invitation

Dear [participant]:

My name is Sixtus Ekwo and I am a Doctor of Information Technology (DIT) student at Walden University. The gatekeeper has given me your names and contact information. I am conducting a doctoral study to explore the following question: What are the strategies that corporate-level IT leaders use in protecting against security violations while adopting IoT in the manufacturing industry?

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

Based on your experiences with IoT adoption and protecting against security violations, I would like to interview you to gather information about your perceptions and beliefs on strategies to protect against the security violations while adopting IoT at [organization name]. The interview will take 30-45 minutes of your time and schedule at your convenience within the next two weeks, following completion of the Walden University IRB process. I will conduct this in-person interview at a location that is most convenient for you.

I am also inviting you to share with me any company or public documents such as emails, administrative documents, reports, and/or memoranda that you feel may provide additional information about the strategies used to protect against security violations while adopting IoT. However, please note the provision of any documents on your part is

voluntary. If you do not wish to provide documents, I am still asking that you participate in the study as an interviewee.

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

Sincerely,

Sixtus Ekwo
<Email and phone redacted>