Walden University
ScholarWorks

Walden Dissertations and Doctoral Studies

Walden Dissertations and Doctoral Studies Collection

2019

Exploring Strategies for Implementing Information Security Training and Employee Compliance Practices

Alan Robert Dawson
Walden University

Follow this and additional works at: https://scholarworks.waldenu.edu/dissertations

 Part of the Databases and Information Systems Commons

This Dissertation is brought to you for free and open access by the Walden Dissertations and Doctoral Studies Collection at ScholarWorks. It has been accepted for inclusion in Walden Dissertations and Doctoral Studies by an authorized administrator of ScholarWorks. For more information, please contact ScholarWorks@waldenu.edu.

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Alan Dawson

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. Charlie Shao, Committee Chairperson, Information Technology Faculty
Dr. Donald Carpenter, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

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

Walden University
2019

Abstract

Exploring Strategies for Implementing Information Security Training and Employee Compliance Practices

by

Alan Dawson

MSIT, Walden University, 2017

MSPD, Rochester Institute of Technology, 2010

MSCS, National Technological University, 2000

BSEE, Rochester Institute of Technology, 1992

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Abstract

Humans are the weakest link in any information security (IS) environment. Research has shown that humans account for more than half of all security incidents in organizations. The purpose of this qualitative case study was to explore the strategies IS managers use to provide training and awareness programs that improve compliance with organizational security policies and reduce the number of security incidents. The population for this study was IS security managers from 2 organizations in Western New York. Information theory and institutional isomorphism were the conceptual frameworks for this study. Data collection was performed using face-to-face interviews with IS managers (n = 3) as well as secondary data analysis of documented IS policies and procedures (n = 28). Analysis and coding of the interview data was performed using a qualitative analysis tool called NVivo, that helped identify the primary themes. Developing IS policy, building a strong security culture, and establishing and maintaining a consistent, relevant, and role-based security awareness and training program were a few of the main themes that emerged from analysis. The findings from this study may drive social change by providing IS managers additional information on developing IS policy, building an IS culture and developing role-specific training and awareness programs. Improved IS practices may contribute to social change by reducing IS risk within organizations as well as reducing personal IS risk with improved IS habits.

Exploring Strategies for Implementing Information Security Training and Employee Compliance Practices

by

Alan Dawson

MSIT, Walden University, 2017

MSPD, Rochester Institute of Technology, 2010

MSCS, National Technological University, 2000

BSEE, Rochester Institute of Technology, 1992

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

December 2019

Dedication

I dedicate this paper to my father Jim, who passed away from lung cancer two years after I started down this path. It was a difficult time for our entire family, but one that we got through together. It was a roadblock at the time, and although I never thought of giving up on my pursuit, it did slow me down as I evaluated life without my father. He was always reading and educating himself and he loved the arts and sciences, as he was an accomplished artist himself. His curiosity and desire to never stop learning is something that he instilled in me and although I know he was proud of my pursuit, I truly wish he was still alive to see me walk across the stage. I love you Dad and thank you for being my role model and for being a loving grandfather to my children! I am paying it forward to my kids in how I live my life and I can only hope I live up to your example.

Acknowledgments

I could not have made it to this point in my academic career without the help of my family and friends. My wife Linda, who has never known me when I was not in school. It has been quite a journey over the 30+ years I have been educating myself and she has been patient and supportive through all of it. My children, Leah, Eric and Jim have all been equally supportive and understanding of my academic pursuits. I hope the value I place on education and hard work to achieve your goals is something they will take with them as they begin their own careers. I must thank my mother, Peg, for being my editor-in-chief and reviewing the final draft and spotting numerous errors. My curiosity and work ethic came from my parents and I am so grateful they have been supportive over these years.

I have been fortunate enough to work for an employer that allowed for flexibility in my schedule over the years as I pursued this doctorate. For that, I thank my supervisor Ladan for allowing me the time to take off work as needed. My doctoral committee has been equally supportive, and I thank Dr. Chao, Dr. Carpenter and Dr. Case for all their patience and feedback. The journey from where I began to where I am has been amazing. Frustrating certainly but rewarding as well and my committee has been guiding me all along the way.

Table of Contents

List of Tables

.

List of Figures

Section 1: Foundation of the Study

Background of the Problem

Humans are the weakest link in any information security (IS) environment (Bauer, Chudzikowski, & Bernroider, 2017; Flowerday & Tuyikeze, 2016; Hwang, Kim, Kim & Kim, 2017). Manworren, Letwat, and Daily (2016) found that humans account for 59% of all security incidents in organizations. Developing effective security strategies to improve training and awareness reduced the number of employees involved in security incidents to below 5% (Manworren et al., 2016). Current literature is focused on trying to better understand the impact of the human factor on information security awareness (ISA).

Themes that evolved from the literature review involved ISA training and awareness, behavioral theory, and knowledge-based awareness and compliance with company security policies and/or culture. IS managers who include proper security habits when developing security strategies can help improve employee compliance (Hwang et al., 2017). ISA programs range from a small number of formally trained employees (Amjad, Naeem, Zaffar, Zaffar & Choo, 2016) to large information technology (IT) organizations that have comprehensive security cultures, continuous oversight, and education campaigns for their employees (Bauer et al., 2017). This study explored the strategies that IS managers use to improve employee security compliance with training and awareness programs that result in reducing the impact the human factor has on IS breaches.

Problem Statement

Employee noncompliance with IS training and security policies is a factor in internal and external security breaches (Karlsson, Hedström, & Goldkuhl, 2016). Human factors account for 95% of all security incidents and are part of the internal conditions that should be accounted for as part of an IS strategy (Horne, Maynard, & Ahmad, 2017). The general IT problem is that employee noncompliance with IS training and policies is a primary cause of organizational security failures. The specific IT problem is that some IS managers lack strategies for improving employee IS training and policy compliance within their organization.

Purpose Statement

The purpose of this qualitative multiple case study was to explore what strategies IS managers use to improve employee compliance with security training and policy. The participants of the study were IS managers from two technology firms in Western New York. This study may increase organizational understanding of effective IS strategies that may then be developed into a set of good practices in the area of IS awareness. This study will lead to social change through increased awareness of the strategies IS managers have used to deliver improved security awareness programs, leading to better habits for protecting both company and personal data. By being more cognizant of effective IS strategies outlined through good practices, everyday computer users may be able to take advantage of these practices to help reduce their risks of becoming victims of identity theft.

Nature of the Study

The intention of this qualitative study was to understand organizational strategies used by IS managers to reduce security risks by improving compliance with security policies. A qualitative researcher studies a phenomenon occurring in a natural setting and develops a deeper understanding and interpretation of its meaning (Moser & Korstjens, 2017). The qualitative research design was an appropriate method because this study explored the strategies IS managers use to improve employee compliance and reduce security breaches. A quantitative researcher seeks to predict behavior based on measuring cause and effect (Rutberg & Bouikidis, 2018). The intention of this study was not to predict how someone will react to the strategies but to understand the strategies used by IS managers to improve employee security policy compliance, making the quantitative method an inappropriate methodology for this study. A mixed methods research (MMR) approach combines both quantitative and qualitative methods and requires analysis of data using both methods (Mabila, 2017). As previously stated, there was no desire to predict human behavior based on measurement, and therefore MMR was also not considered as a research methodology.

A multiple case study design was appropriate for this qualitative study because there was a desire to understand what strategies information managers use to develop and implement IS strategies to improve employee compliance within the natural setting of two technology organizations. An advantage that a multiple case study approach provides is that it allows for comparison (Houghton, Casey, Shaw, & Murphy, 2013; Rihoux & Lobe, 2015). Both organizations serve different purposes, so understanding the strategies

security managers use in both companies revealed good practices that can be shared throughout the IS community. In addition to the case study design, there are other designs that can be applied to qualitative analysis such as narrative, phenomenological, and ethnographic designs. Narrative research involves the use of stories to describe the lives of individuals as told through their own stories (Yang & Hsu, 2017). The intention of this research was to explore the strategies IS managers use to improve employee security compliance through training and policy, not the personal stories of each employee. Therefore, the narrative design was not a suitable design choice for this study. Phenomenological research is appropriate when the goal is to understand individuals' lived experiences in a certain setting (Sloan & Bowe, 2015). However, focusing on individuals' lived experiences would not have provided enough understanding of the strategies IS officers use to improve security compliance for organizations and was also not considered as a design choice. Ethnographic studies are used to understand how specific events may impact a specific culture in a real-life setting and typically require extended periods of study in the field through conversations and workshops (Suopajärvi, 2015). Understanding the culture of a population was not the intention of this research, and therefore ethnography was also not an appropriate design choice for this study.

Research Question

What strategies do IT security managers use to improve employee compliance with security training and policy in order to minimize the risk of security breaches?

Demographic Questions

1. What is your current title and role?

2. What role do you play in managing IS policy and strategy?
3. How many years of experience do you have in this type of role?
4. In your experience, what responsibilities do you have in regard to IS?

Interview Questions

Strategy

1. What types of policies and strategies do you manage?
2. What roles within your organization assist in the development and execution of security policy and strategy?
3. What strategies do you use for IS practices?
4. What strategies have you found to be most effective? What strategies have you found to be ineffective?
5. What factors play a role in decisions regarding how to implement IS strategies?
6. What are the benefits of implementing IS strategies?
7. What are some of the challenges of implementing IS strategies?
8. What external factors or entities play a role in deciding which strategies to implement?
9. What other factors or tactics might you consider adding to improve IS strategies?
10. How do you develop a global information security policy or program that does not fall into a one size fits all mentality?

Compliance

11. How does strategy help improve security policy compliance?
12. What prompts the need for IS practices?
13. Is employee compliance with IS policies tracked/audited?
14. How is noncompliance enforced?
15. Have you found that there is a direct correlation between low compliance with policy and increased security breaches?

Training

16. How are employees educated on new threats?
17. How do local cultures/language/slang impact training and policy development?
18. How often are training programs updated?
19. How do you educate yourself on the constantly changing security landscape and use that knowledge to create or update new or existing policies and programs?

Culture

20. What do you believe are the fundamental steps in building an IS culture?

Human Factors

21. What human factors do you believe contribute to poor IS compliance?
22. As an IS manager, how do you guard against the human factor when developing strategies and new training?

Conceptual Framework

Institutional theory was used as the conceptual framework for this study because

it aligned well with how organizations form and develop. Institutional theory was originally developed by Paul J. DiMaggio and Walter W. Powell in 1983. In their study, the authors advanced work by Meyer and Hannan (1979) and Fennell (1980) on competitive and institutional isomorphism as it relates to constraints within organizations. These constraints can force units within organizations to resemble each other due to experiences with similar environmental conditions (DiMaggio & Powell, 1983). Institutional isomorphism can be useful in understanding the formality and function of organizations. DiMaggio and Powell (1983) identified three specific mechanisms relative to institutional isomorphism: coercive, mimetic and normative. Whereas coercive mechanisms are concerned with political influences and legitimizing organizations, mimetic mechanisms are concerned with how organizations respond to uncertainty, and normative mechanisms deal with the role of professionalization within an organization. Figure 1 illustrates the concept.

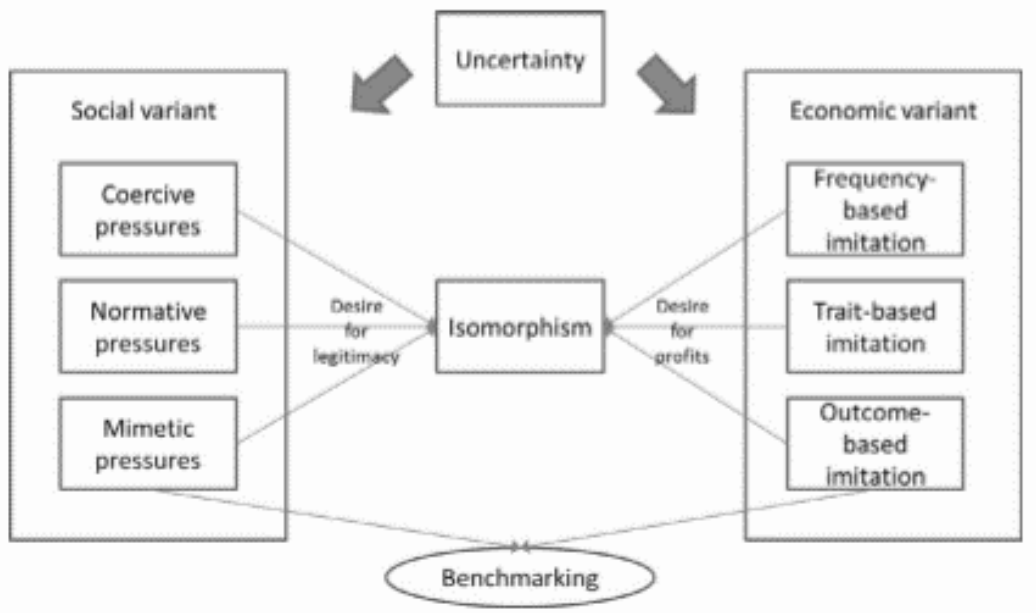

Figure 1. Social and economic variants of institutional theory. Reprinted from "Extending the Use of Institutional Theory in Operations and Supply Chain Management Research: Review and Research Suggestions," by K. Kauppi, 2013, *International Journal of Operations & Production Management*, *33*(10), p. 1322. Copyright 2013 by Emerald Publishing. Reprinted with permission.

Institutional theory can be used to differentiate between symbolic and substantive adoption of activities, or in this context, policies (Angst, Block, D'Arcy, & Kelley, 2017). Symbolic means that form without substance (i.e., only for show to gain legitimacy), and substantive means that there is form (policies) with substance (adopted practices). As DiMaggio and Powell (1983) suggested, when symbolic uncertainty exists, individuals responsible for managing change may attempt to model their organization after processes and policies that have proven successful in other organizations or areas of the company, thereby practicing mimetic isomorphism. Mimetic isomorphism posits that adopted

practices such as procedures and policies which have been used successfully in one part of an organization can be copied, repeated, or imitated in a different part of the organization, benefitting the entire organization (see Figure 1).

Strategies used by IS managers likely originate from institutional environmental conditions such as culture, behavioral frameworks, and regulatory requirements (Sherer, Meyerhoefer, & Peng, 2016). Understanding how IS managers integrate these conditions into the development of IS strategies was helpful in determining the overall strategies they use to improve compliance and reduce security breaches. Security in information systems depends on the actions of the users of the systems (i.e., human actors). The fundamental constructs of this study are IS training, IS policy, and IS compliance. All three constructs depend on human interaction, and IS managers develop strategies to help them implement and enforce security training and policies that ensure compliance. Bjorck (2004) defined institutional theory as a collection of ideas that help form a perspective of the mechanisms that support and restrict social behavior. Bjorck referenced Giddens' duality of social structure, where an actor is institutionalized through a socialization process within the organization. Once this takes place, the process is continuously reproduced throughout the organization, resulting in patterned behavior. Applying institutional theory to this study did help to determine that employees of both organizations were institutionalized with regards to IS training and that institutionalization does play a role in the strategies IS managers use to improve compliance.

Applying the frameworks of institutional theory and isomorphism to the examination of two organizations through a case study also helped determine if IS managers were influenced by social behavior and institutionalization when determining what strategies they use to improve compliance and reduce security breaches. The study shows that IS managers are influenced by the institutional effects of isomorphism of copying behavior (mimetic), learning from others (normative), and forced behavior (coercive), which has a direct impact on the strategies they use to improve employee security compliance. The copied or learned behavior used by IS managers was shown to have a positive impact on reducing security breaches and ensuring compliance.

Definition of Terms

Phishing: a form of web threats that is defined as the art of impersonating a website of an honest enterprise aiming to obtain user's confidential credentials such as usernames, passwords and social security numbers (Mohammad, Thabtah, & McCluskey, 2015).

Social engineering: the science of using social interaction as a means to persuade an individual or an organization to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity (Mouton, Leenen, & Venter, 2016).

Two-factor verification: Sometimes referred to as two-step authentication or 2FA, this is a security process in which the user provides two different authentication factors to verify themselves (Rouse, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

General assumptions are considered perceived facts (Oosterhoff, Shook, & Metzger, 2018), beliefs, or preconceptions accepted as true (Walsh, 2015). For this case study, I assumed that IS managers were available within the organization during the time the study was performed, and they had the proper experiences and backgrounds to develop strategies for implementing IS programs to be able to answer the interview questions. I also assumed that the participants would be representative of the sample population and would understand the interview questions well enough to be able to answer them, and the questions related to the experiences of the participants.

Limitations

Limitations can be unique to the study and in many cases are beyond the control of the researcher (Connelly, 2013). The first limitation was the small number of participants. Small sample sizes can make it difficult to generalize the results for larger populations. The second limitation was lack of availability of participants for follow-up interviews to validate results through member checking, but this did not turn out to be an issue. A potential third limitation was participant bias either in providing only positive responses or limiting their responses due to company policy, but this was also not an issue as all participants spoke candidly and did not attempt to speak “off the record”. As the goal of this proposal was to understand the strategies used to improve security compliance, there was no effort to access statistics relating to percentages of employee compliance with policies, as that was beyond the scope of this study.

Delimitations

Delimitations are boundaries set by the researcher to limit the focus of the study (Svensson & Doumas, 2013). The primary boundary for this study involved experiences of participants. Each participant interviewed for this study was in a role that included developing and implementing IS strategies. Another boundary was that this study was not focused on how IS policies were implemented but rather on identifying strategies for implementing IS practices within an organization. Geographic location was also a boundary for this study as it took place in one region of the country.

Significance of the Study

Contribution to IT Practice

To reduce threats associated with IS awareness and policy noncompliance, IT security managers attempt to implement multiple policies and procedures to achieve compliance. However, employee compliance in this area is still an issue for organizations (Karlsson et al., 2016). The goal of this study was to explore strategies IS managers of two technology firms used to improve employee compliance. The methods and policies used by these companies to improve compliance along with a comprehensive literature review can be used to identify good practices in the area of IS awareness. Organizations and individuals can reference this list to develop or enhance their own IS training policies and procedures, providing value to themselves and the IT practices of organizations.

This study can be used by large and small organizations to provide a positive impact by helping develop standard strategies IT security managers can use to improve employee compliance within their own organizations. These strategies can improve

organizational IT security compliance and positively contribute to an effective IT security awareness practice. Improving compliance within organizations can lead to better internal and external security, reducing costs associated with defending and investigating security threats and building a strong security culture. This study may help organizations in the early stages of developing a security program in terms of executing strategies for implementing IS training policies and procedures.

Implications for Social Change

The implications to positive social change include the ability to educate IS managers and personnel on the risks associated with poor IS awareness compliance. In addition, it can help highlight the different options available to mitigate those risks and protect companies and employees' privacy. Understanding the strategies IS managers use to improve compliance and reduce security breaches can help employees have a better understanding of how to improve their own online security habits.

The study can lead to positive social change by documenting the strategies that have led to improved organizational security compliance. Improved security compliance can lead to better protection of personal identifiable information (PII) for the average computer user by adding to available literature on the subject. Improved protection of PII is fundamental to protecting everyday computer users, increasing their overall awareness of the threats that exist online. Computer threats can include identity theft and exposing personal information by using social media applications.

By being more aware of current threats used by computer criminals and the risks associated with using social media and online commerce, employees can reduce the

likelihood of becoming victims of identity theft in their personal lives. By using information from this study, computer users might reduce the likelihood of becoming targets of security fraud by limiting or eliminating personal information available online, using secure websites and practicing good security habits such as stronger passwords and anti-phishing methods.

A Review of the Professional and Academic Literature

Opening Narrative

This literature review consists of literature from the IS and institutional theory domains. With the IS domain, the focus areas were training, policy, compliance, strategy, and human factors. With the institutional theory, focus was on characteristics of institutional theory, institutional isomorphism, and the constraints these characteristics present to organizations in terms of implementing security strategies. Uncertainty within organizations exists both socially and economically. Social variants consist of coercive, mimetic, and normative behaviors that are used by organizations to legitimize (Kauppi, 2013). Economic variants consist of frequency, trait-based, and outcome-based imitations. Economic variants are primarily used by organizations to achieve efficiency. When organizations have similar processes and structures, it is considered institutional isomorphism. Understanding social and economic factors can be useful in understanding how organizations are formed and how they function.

This literature review is comprised of 157 articles, journals, and seminal books on IS and institutional theory. All literature was obtained from the following research libraries: ACM Digital Library, IEEE, EBSCOHost, Applied Sciences Complete,

ScienceDirect, Google Scholar, and ProQuest, or directly obtained from journal websites. Of the 157 articles, 142 (90%) were peer-reviewed as confirmed by Ulrich's Global Serials database and 133 (85%) were published within 5 years of the anticipated graduation date.

To answer the research question, it was necessary to research and develop an understanding of six key areas: (a) applicability of institutional theory to the study, (b) the impact the human factor has on IS strategy development, (c) challenges IS managers have ensuring IS compliance, (d) challenges IS managers have developing and implementing IS training programs, and (e) the importance of creating and maintaining an IS culture within an organization. Literature revealed that training alone is not always sufficient as employees tend to disregard training. IS managers need to manage this noncompliance as part of their overall strategy. Understanding the impact of the human factor in terms of interactions of humans with systems is crucial for IS managers as they develop strategies. Once IS managers understand why noncompliance exists and the impact of humans on the system, they can begin building a strong security culture within the organization. The applicability of institutional theory, impact of the human factor, and challenges IS managers face ensuring compliance, training, and evolution of a security culture formed the basis of strategies that were explored as part of the literature review.

Application to the Applied IT Problem

The purpose of this qualitative multiple case study was to explore the strategies IS managers use to improve employee compliance with security training and policy that may lead to a lower risk of security breaches. Compliance with policy can be mandatory when

dealing with external regulations and laws. Compliance with internal processes and policies not associated with regulations and laws are generally seen as optional by most employees, even though management may believe full compliance is in the best interest of the organization to minimize the risk of security breaches (Moody, Siponen, & Pahnila, 2018). The primary focus of this study was to answer the research question: What strategies do IT security managers use to improve employee compliance with security training and policy in order to minimize the risk of security breaches? Included in this literature review is a discussion on the conceptual framework selected for this study, which is institutional theory. Understanding institutional isomorphism has helped to better understand both internal and external pressures IS managers face when developing and implementing IS strategies.

Foundations of Institutional Theory

Evolution of institutional theory. Institutional theory is rooted in seminal work by Giddens on the theory of structuration. DiMaggio and Powell advanced Giddens' work in their paper on institutional isomorphism. Giddens (1984) said that under normal circumstances, members of society conform to routine activities that are taken for granted in their daily lives. Influenced by Giddens' work, DiMaggio and Powell also integrated work by Meyer and Hannan (1979) and Fennell (1980) on competitive and institutional isomorphism as it relates to constraints within organizations. These constraints can force units within the organization to resemble each other due to their experience with similar environmental conditions or simply take these conditions as routine as Giddens espoused (DiMaggio & Powell, 1983). Building on theories provided by Giddens, DiMaggio and

Powell made an argument for institutional isomorphism within organizations based on societal tendencies of conformance.

Institutional theory has been a foundation of organizational and social research since the late 1970s and early 1980s. Scott and Amarante (2016) said institutional theory gained acceptance in academia because of the desire to understand the different behavioral forces such as cultural, cognitive, and normative that are naturally present within an organization. Although developed well before the digital age, institutional theory has been successfully applied in practice to help diffuse IS strategies and institutional policies across organizations.

Bjorck (2004) defined institutional theory as a collection of ideas that help form a perspective of the mechanisms that support and restrict social behavior. Bjorck referenced Giddens' duality of social structure, where an actor is institutionalized through a socialization process within the organization. Once this takes place, that socialization process is continuously reproduced throughout the organization, resulting in patterned behavior.

DiMaggio and Powell (1983) theorized that the dependence of one organization on another will result in both organizations becoming similar in terms of structure and culture. Applying the framework of institutional theory and isomorphism has helped determine that IS managers are influenced by social behavior and institutionalization when determining what strategies to use when attempting to improve compliance and reduce security breaches. This study also showed that IS managers are also influenced by the institutional social effects of isomorphism of copying behavior (mimetic), learning

from others (normative), and forced behavior (coercive), which has a direct impact on how they develop strategies to improve employee security compliance. If a copied or learned behavior used by IS managers is enough, the copied or learned behavior may have a positive impact on reducing security breaches and ensuring compliance. However, if the copied or learned behavior is insufficient, it may have a negative impact on compliance. IS managers must understand the different behaviors associated with isomorphism as they develop the foundations for a comprehensive IS strategy.

Institutional theory has also been used to differentiate between symbolic and substantive adoption of activities, or in this context, policies. Whereas symbolic means form without substance (i.e., only for show to gain legitimacy), substantive means form (policies) with substance (adopted practices). As DiMaggio and Powell (1983) suggested, when symbolic uncertainty exists, individuals responsible for managing change may attempt to model their organization after substantive processes and policies that have proven successful in other organizations or areas of the company, thereby practicing mimetic isomorphism. In practicing mimetic isomorphism, successful practices, procedures, and policies are copied, repeated, or imitated in a different part of the organization. The result of mimetic isomorphism coupled with outcome-based imitation leads to benchmarking or studying how successful organizations manage uncertainty and copy or adopt some or all of their processes. This study revealed that IS managers both consciously and unconsciously practice mimetic isomorphism that better helps them develop strategies to ensure compliance.

Fundamentally, the evolution of institutional theory has provided a better understanding of how organizations are constructed and respond to the variety of external pressures to gain legitimacy. Organizations gain legitimacy by responding to external pressures by implementing procedures that are complementary to their organization that have become institutionalized by legitimate external sources. Chandler and Hwang (2015) argued that adopting institutional practices to gain legitimacy or economic benefit, while beneficial to firms, neglects the overall complexity of creating a successful organization. However, examining the social and economic impacts institutional theory may have on how IS managers develop and sustain IS compliance strategies should be sufficient. Therefore, a thorough understanding of the social and economic variants associated with institutional theory is necessary.

Elements of the theory. The social and economic elements of institutional theory provide a solid framework for discussing institutional isomorphism. The leadership of any organization must be able to manage uncertainty as they attempt to gain legitimacy and create a profit for the organization. The three social variants of uncertainty are coercive, normative, and mimetic pressures. The three economic variants of uncertainty are frequency-based, trait-based, and outcome-based imitations. While organizations strive for legitimacy, there is the fundamental need for the organization to yield a profit. Isomorphism is a framework that organizations may take advantage of to manage social and economic pressures associated with uncertainty to gain legitimacy and create profit.

Coercive variants can occur through the need of an organization to comply with regulatory requirements or during periods of assimilation during the merging of two

organizational cultures. DiMaggio and Powell (1983) said that coercive isomorphism can develop from the need for legitimacy for political reasons, government regulations, or partner organizations requiring certain quality or organizational procedures to be followed. Coercive pressures may exist within current IT departments.

A mimetic variant involves how organizations respond to the pressures of uncertainty by modeling themselves after other organizations. DiMaggio and Powell (1983) defined mimetic isomorphism as the need for organizations to become homogenous, or the same throughout. By mimicking behavior proven to be successful and reducing uncertainty within the organization, institutional isomorphism begins to take hold. IS managers do subconsciously practice mimetic isomorphism based on their own experience and desire for legitimacy. Hwang and Choi (2017) suggested organizations can enhance legitimacy by improving their own culture and norms, develop good IS habits, and conform to best practices and standards by mimicking successful organizations.

Normative variants are associated with professional organizations such as education or healthcare. Imitation of processes and policies can be used by organizations to increase efficiency by taking advantage of existing structures to avoid recreating existing processes, thereby saving the organization time and money. Individuals in professional fields are also subject to coercive and mimetic pressures (DiMaggio & Powell, 1983). To increase the legitimacy of a medical organization, these pressures may be applied to increase professional certifications, education, or training. DiMaggio and Powell (1983) said that although these normative pressures may not lead to increased

efficiency within the organization, they can increase legitimacy, resulting in potentially new business. Normative isomorphism exists within IS as industry certifications, education, and training and are used to gain legitimacy. Industry standard certifications are becoming a prerequisite for entry into IS organizations and IS managers may also include them in any cohesive strategy. Understanding the social variants of isomorphism is only part of the analysis.

With frequency-based imitation, organizational leaders may mimic the actions and practices of other organizations simply because these actions and practices have become commonplace and are taken for granted (Kauppi, 2013). An example of frequency-based imitation is achieving industry certifications because they are widely adopted. Where normative pressures exist to help gain legitimacy, adopting industry certifications through frequency-based imitation may occur because the competition is doing it versus there being a strong business need (Kauppi, 2013).

Trait-based imitation is the copying or mimicking of specific traits of an organization, such as size or performance, which can help the imitating firm achieve legitimacy. According to Kauppi (2013), trait-based imitation can often occur in organizations within the same industry or region. Imitation is something IS managers may take advantage of either consciously or unconsciously.

Outcome-based imitation is used by copying an organization or organizations that have successfully demonstrated a behavior that proved beneficial, and therefore the imitating organization can take advantage of the same outcome (Kauppi, 2013). This form of imitation is simply based on the outcome of the copied behavior. If the outcome

of the behavior results in a positive outcome for the firm, the behavior is copied. Toyota and their lean practices are an example of outcome-based imitation. Once lean practices were known to have provided a positive outcome for Toyota, other firms began copying that behavior. If a firm practices good security behavior and has a strong security culture, IS managers may attempt to imitate that behavior for the good of their firm.

When firms successfully couple both social and economic variants into best practices, industry may attempt to imitate that success. When an organization uses outcome-based imitation to respond to mimetic pressures, it can begin to develop benchmarking for successful processes and procedures, allowing for imitation throughout the organization. While economic outcomes are imitated to increase efficiency and improve profits, social outcomes are dependent on the behavior of the actors involved, namely the employees. IS managers should take both economic and social behavioral factors into consideration while developing strategy.

Applications of institutional theory. Institutional theory was developed to help understand how members of societies conform to routine activities in their daily lives. As organizations are now fully immersed in the digital age, IS managers may have developed strategies rooted in institutional environmental conditions such as behavioral frameworks and regulatory requirements. McGovern, Small and Hicks (2017) said that mimetic, coercive, and normative forces play a significant role in driving organizational behavior and providing the foundation of process improvements within organizations.

In addition to isomorphic forces playing a role in process improvement development, Takahashi and Sander (2017) suggested the interpretation of institutional

environmental conditions may be influenced by societal factors such as cultural and social elements. IT departments are no different than any organizational department and may have been organized and institutionalized by conforming to normative organizational pressures symbolic in nature because that is how it has always been done (Kauppi, 2013). Heras-Saizarbitoria and Boiral (2015) found evidence of symbolic adoption of process in their study of small and medium-sized businesses. The authors discovered that coercive forces were applied within organizations to achieve specific industry standard certification. However, while some organizations applied the changes and improved their processes, some organizations only adopted the changes symbolically to achieve certification. In many cases, the authors found that organizations applied the changes as they saw fit within their organization while others were constrained by internal forces or actors that resisted the change.

In a study on low-carbon energy transition, Andrews-Speed (2016) studied how institutionalism and institutional theory applied to the energy industry. The author examined rational choice institutionalism where actors are assumed rationale, historical institutionalism where norms and routines are governed by both formal and informal rules, and sociological institutionalism and the importance of culture. Andrews-Speed (2016) proposes a fourth element of institutionalism he defined as discursive that consider ideas and discourse. The study revealed that bounded rationality of the actors involved with the transition along with the underlying historical elements involved, limited the adoption of new processes and procedures. Similarly, entrenched culture and economic and legal systems were also seen as barriers. However, when applied together

as an integrated concept, the author was able to determine that components of each allowed for change to occur.

A rapidly changing IS environment can add new pressures that may make IT organizational structures insufficient or simply untenable. Conforming to institutional rules and procedures can result in reducing efficiency and legitimacy if those rules and procedures are not properly focused on the work activities (Meyer & Rowan, 1977). Institutional theory is considered a product of the industrial revolution where formal structure was seen as an effective way to control complex work activities (Meyer & Rowan, 1977). Understanding how IS managers integrate these conditions into the development of IS strategies has helped determine that leveraging isomorphism can improve compliance, reduce security breaches, and help gain legitimacy.

Molinillo and Japutra (2017) echoed DiMaggio and Powell's (1983) three characteristics of coercive, mimetic and normative pressures in their study on technology adoption. All organizations face environmental pressures in adopting new technology or complying with processes. Organizations face mimetic pressure from competitors, coercive pressures from suppliers and customers, and potentially normative pressure from professional associations. IS managers may need to consider all three of these pressures as they adopt and integrate new technologies within their organization. Piña and Avellaneda (2018) studied isomorphism in a municipality to understand the impact of institutional theory on organizations. By studying isomorphism in a municipality, the authors were better able to understand the impact of institutionalism on organizations. Piña and Avellaneda's study explained how organizations develop and adapt their

culture, processes and strategies to help gain legitimacy. Applying Molinillo and Japutra's findings on the various external pressures organizations face alongside Piña and Avellaneda's results of institutional isomorphism, may help identify the various factors associated with developing and cultivating culture and processes within an organization. Cultivating a strong security culture can help firms build a reputation and improve legitimacy within the industry.

Legitimacy and reputation are necessary components of IS. IS managers obtain legitimacy and build their reputation by conforming to institutional pressures (institutional isomorphism). Piña and Avellaneda (2018) confirmed that institutional theory, as a theoretical framework, can be used to explain how organizations can work together to form homogenous departments across the company and build internal legitimacy. Achieving internal legitimacy within an organization is a necessary first step for IS managers as it provides them with validation they can then use as leverage to affect change and improve compliance (Piña & Avellaneda, 2018).

Using institutional theory as the conceptual framework, a firm's efficacy in responding to external pressures can help achieve and maintain legitimacy (Bozan, Davey, & Parker, 2015; Hu, Hu, Wei, & Hsu, 2016). External pressures associated with institutional theory; coercive, normative, and mimetic, are all applicable when discussing how a firm adopts a practice such as green IT or an individual adopts to using electronic health records. Using institutional theory as a lens, these articles illustrated the analogies between developing and implementing green IT practices and electronic health records and creating and implementing strategies IS managers can use to improve employee

compliance. Complying with coercive pressures such as the Health Insurance Portability Accountability Act (HIPAA) or Payment Card Industry Data Security Standard (PCI-DSS) are necessary to achieve legitimacy for firms operating in those sectors.

Ensuring organizational compliance to gain legitimacy within the industry and locally within the organization is certainly the goal of decision makers. Environmental pressures previously discussed are all relevant in an organizations' quest for legitimacy. IS managers need to understand the impact of uncertainty when deciding to conform to environmental pressures (Schilke, 2018). Schilke explained why some organizations succumb to environmental pressures and some do not. As much as uncertainty encourages decision makers to adhere to environmental pressures, certainty allows decision makers to resist them. Similar to Bozan et al., Schilke focused on the individual within the organization that exhibits a strong organizational identity. Individuals with a strong identity are certain in their belief that the decisions they make on behalf of the organization are the correct decisions. Individuals of this type are more confident in implementing proper policies to support the regulations within the organization. IS managers are aware of specific regulatory (coercive) pressures that must be adhered to for legal and legitimate reasons regardless of certainty.

Although regulatory pressures require compliance, if an individual has strong organizational identity and certainty in a specific area, the more likely this type of individual will resist complying with other environmental pressures within their organization (Schilke, 2018). Each employee in an organization is an individual contributor with potentially strong organizational identities and certainty in specific

areas. The individual plays a significant role in the adaptation of policy and procedure within an organization. It is these micro-institutional or local conditions that affect how individuals interpret and interact with their environment. IS managers must acknowledge local conditions when creating and implementing IS policies to improve compliance. Institutional isomorphism, as an outcome of institutional theory described by DiMaggio and Powell (1983), is not without criticism as it does not depict the current state of organizational decision making (Schilke, 2018).

Deficiencies of institutional theory. Institutional theory is not without criticism. As influential as the individual is in adapting and complying with policy, critics of institutional theory point to the lack of acknowledgement of the role power plays in organizations (Munir, 2015). Power within organizations is oppressive when it leads to exploitation, inequalities within the workforce or inappropriate influence over external entities such as government or society (Munir, 2015). When power is used in this manner, it may be considered as anti-coercive with pressure applied outward from an organization versus inward. At its core, institutional theory attempts to understand how organizational practices are accepted and taken for granted, including existing power structures (Willmott, 2015) and this is further illustration of a potential weakness with institutional theory.

Understanding the power structure within an organization lends itself more to a study of organizational behavior and not how IS managers develop strategy. Although a perceived weakness of institutional isomorphism, the lack of debate on power structure as part of institutional theory does not prohibit it from consideration as a framework for how

IS managers develop strategy. Consideration of power within institutional theory is not the only criticism. Traditional institutional theory has a long history of studying organizations and institutions as a social structure (Suddaby, 2015). In current neo-institutionalism, there has been more of an attempt to abandon the history of institutional theory in favor of its use in understanding the adoption of institutionalized practices (Suddaby, 2015). While this may be a modern-day weakness of institutional theory, adopting institutional practices was shown to be part of a broader strategy used by IS managers. An additional criticism of neo-institutionalism is that it is more focused on the organization at the macro level, ignoring the impact of the individual on the overall process (Mohamed, 2017).

Institutionalizing common practices requires commitment and action by individuals. The actions of individuals, or actors, within an organization are not only formed by the structure within the organization but also with their own combined internal and external experiences. Individual actions can be constrained by organizational structure as it pertains to functioning within the organizational framework. However, as Cardinale (2018) explained in his study on micro-foundations in institutional theory, working within an organizational structure can also enable actors to function, solve problems, and be productive employees. Employees are not blank slates but bring their experiences and training with them to an organization. The actions of employees are not explicitly defined by the organization or their own reflexivity from working within it (Cardinale, 2018).

Individual actions are a combination of structure, reflexivity, knowledge, training, and the expectation of a future result based on past experiences. Over time, this combination can lead to the development of a strong identity within the organization (Schilke, 2018). Cardinale was more concerned with the interaction between the actor and his or her influence on change and form within the organization. Actors may choose a course of action not because they are constrained by the organization but because they gravitate toward other self-evident actions based on their knowledge and reflexivity of the situation (Cardinale, 2018). These actions are the essence of behavioral theory and is not the direct focus of this discussion on conceptual framework but certainly bares some discussion. Schilke and Cardinale explained the necessity of understanding how the individual reacts and reflects with their environment. Mohamed (2017) echoed the challenges with institutionalism relating to change. Mimicking a successful organization can lead to operational efficiencies and help achieve legitimacy. However, copying an organization can also stifle creation and innovation as the primary work of creating certain aspects of the organization are recreated instead of evolving through knowledge and reflexivity. IS managers need to consider the impact institutionalization has on the individual as they develop IS strategies.

Alternative theories. As humans are the actors in organizations and the users of the technical systems, various social behavioral theories such as Planned Behavior Theory (PBT), Planned Motivation Theory (PMT) and the Theory of Reasoned Action (TRA) may also play a role in developing IS strategies. Security in information systems depends on the actions of the human users of the systems (Bjorck, 2004). In fact, Meyer

and Rowan (1977) observed that although formal organizations exist, there is often a loose coupling of elements where rules are not always followed, decisions go unimplemented, or basic systems are simply ignored. Although not the focus of this framework, these theories also bare some discussion. The theories are directly related to the human element in compliance and may play a role in an employee's decision-making process when deciding to comply with company policy. Exploring alternative theories may be helpful in developing a better understanding the role the human factor plays in IS and may yield information useful to IS managers in the development of strategies for improving training and ultimately improving compliance.

In addition to better understanding how alternative theories may impact the development of IS strategies; IS training, IS policy, and IS compliance are fundamental to understanding the human element. At the institution level, all three constructs depend on how humans interact, socialize, and develop patterned behavior (Bjorck, 2004). Understanding human behavior in this context may help determine how IS managers develop strategies to implement and enforce security training and policies. All three constructs may have a positive impact on employee compliance and help reduce security breaches. Scott and Amarante (2016) explained there is value to understanding how individuals react to their organizational environment through the lens of institutional theory. In doing so, this study may help provide a general framework information security managers (ISMs) can use when developing strategies and policy within organizations.

ISMs must also consider individual behavior when developing strategies and policy as behavior is a component that impacts compliance. ISMs should be knowledgeable with the behavioral theories (PMT, PBT, TRA) when developing strategies to improve security policy compliance. TRA considers an individual's attitude and behavioral intention and can be useful in predicting an individual's action under certain conditions (Paul, Modi, & Patel, 2016). Attitude and intention imply control over conscious behavior and can be argued as a limitation of TRA (Ajzen, 1991).

PBT was introduced by Ajzen to address the limitations of TRA and understand how unconscious behaviors factor into an individual's decision-making process. Perceived behavioral control (PBC), along with attitude and subjective norms, combine to form intention that ultimately leads to a certain behavior (Ajzen, 1991). PBC is an individual's perception of how easy or difficult performing an action is. If the perception that an action is easy helps improve employee IS compliance, it may benefit ISMs to study and apply TRA and PBT as they develop training and awareness programs. An individual's behavior is heavily influenced by their own self-efficacy to perform and control an action, so it would stand to reason that more training and awareness would improve IS compliance.

Madden, Ellen and Ajzen (1992) confirmed that the lack of control in a given situation results in a lower likelihood that someone will perform a given action. Behavior can be changed by providing a mechanism to enable more control over a given situation. Training and awareness is one potential mechanism. In comparing PBT and TRA, when any action or behavior is under an individual's conscious (habit) control, TRA is more

applicable (Madden et al., 1992). However, when actions or behaviors are unconscious in nature and not habitual, PBT is more useful. While either theory may be applied to IS, creating an environment where individual behavior is conscious and ultimately more predictable through training and awareness encourages the examination of TRA by ISMs.

Protection motivation theory (PMT), where fear, danger, or harm is used to help influence decisions, has been shown to produce changes in attitude (Maddux & Rogers, 1983). Severity of the threat and the probability it will occur play a large role in PMT. In the context of IS, PMT may be useful to force compliance when coupled with self-efficacy and threat severity but that it is not effective uniformly across all audiences (Torten, Reaiche, & Boyle, 2018). While the effectiveness of PMT in improving compliance was shown to be effective when combined with other behavioral methods, the authors found that threat awareness was a significant factor in improving compliance when focused on countermeasures that reduce the risks associated with the various threats.

However, although improving compliance through fear of termination may yield positive results; the negative connotations associated with not complying with a procedure or policy may lead to lower employee morale. Maddux & Rogers did not address the long-term effects of fear-based motivation theory other than acknowledging it had a positive impact on stimulating change. Safa et al. (2015) applied PMT from the standpoint of the risk of not complying with the specified action. The danger of not complying with policy from an IS perspective may expose one's self or organization to potential security breaches. Increased IS training and awareness for employees may help

improve compliance and the employee's conscious control of the situation. Applying repercussions such as withholding wages or threatening termination are extreme but are used to force change and compliance. Keeping wages and employment are good motivators for employees but tend to associate negative connotations with the training and can therefore be detrimental to building a security culture. In today's business environment, adapting to change is constant. Part of organizational change is adapting to new technology.

Information technology (IT) in business is becoming more of a differentiator in the competitive landscape (Molinillo & Japutra, 2017). The adoption of technology can help create efficiencies, reduce cost, improve time to market, and, stimulate innovation (Molinillo & Japutra, 2017). However, simply purchasing and installing technology is not sufficient. Getting the organization to adopt the technology and utilize it efficiently is necessary. Theories, such as innovation theory and diffusion of innovation theory exist to help understand how technology is adopted and integrated within organizations. Using institutional theory as a framework may help IS managers develop policies that improve employee compliance, not how they adopt technologies, so innovation theory and diffusion of technology theory are not directly applicable.

Adoption and diffusion of information technology security standards are not common in the industry (Uwizeyemungu & Poba-Nzaou, 2015). IS managers can use standards to add legitimacy to an organization and help create a stronger security framework. However, Uwizeyemungu and Poba-Nzaou found that human and financial constraints for smaller firms and the lack of demand for standardization between

businesses were a few root causes that limited adoption of standards. An established standard from a legitimate standards organization such as the national institute of standards and technology (NIST) can provide an opportunity for organizations to economically add legitimacy. Similarly, normative pressures exist within technical organizations to hire or develop skilled workers with industry recognizable education and certification underscoring the importance of the human factor within an organization. Understanding and conforming to these different environmental coercive pressures may therefore be a necessary part of the strategy IS managers need to manage to ensure organizational compliance.

Multiple theories exist and have been discussed presently that help explain the different aspects of human behavior as it relates to IS compliance. Safa, Von Solms, and Furnell (2016) introduced social bond theory (SBT) and Involvement Theory (INV) that provided a different view of non-compliance. SBT was developed to help describe the values individuals hold in society. INV theory was developed to better understand a consumer's purchasing decisions. SBT nor INV have a direct correlation to IS or compliance but when an organization is viewed as a microcosm of society, applying SBT and INV has value. SBT postulates that individuals with a strong belief in convention are more likely to follow the rules. INV includes emotion as a component in the decision-making process.

Han, Kim and Kim (2017) explored multiple behavioral theories to help determine why employees comply or do not comply with policy. In addition to general deterrence theory and planned behavior theory, rationale choice (RCT) and psychological

contract theories (PCT) were introduced. RCT assumes that individuals will always make logical choices when deciding about their well-being. PCT is based on the expectations and commitments employers and employees have when entering a relationship. PCTs are generally unwritten rules but typically encourage the employee to believe they will be treated fairly in the employment relationship. IS managers should be aware of the different human behavioral theories when developing IS strategy and policy.

Future direction of institutional theory. The future of institutional theory is taking on a global approach (Scott & Amarante, 2016). As society becomes more and more global and cultures and societies continue to interact and coexist, Scott and Amarante explicate that institutional theory will benefit from both an international and transnational approach, leading to a better understanding of how different countries manage societies as well as organizations. While the current emphasis is not specifically on the organization, Scott and Amarante reiterated that comparing how organizations operate and differentiate themselves can prove beneficial. Comparing how organizations make decisions and manage change was the focus of Chandler and Hwang (2015). In their study, the authors explained some of the reason's organizations practice mimetic isomorphism. Learning from other organizations through imitation or researching other industries or organizations across the industry and not simply regional, a better understanding of best practices can be achieved. Through their study, Chandler and Hwang (2015) were able to develop a framework that can help organizations decide the best time to integrate new behaviors but also which ones to integrate and why.

Potential Strategies for Improving Employee Information Security Training and Awareness

Improving the human element. It is well known within the IS industry that humans are the weakest link in any IS setting (Bauer et al., 2017; Flowerday & Tuyikeze, 2016; Hwang et al., 2017). Applying institutional theory to this study may help determine if employees are institutionalized within the organization, as outlined in Giddens (1984) duality of social structure, and if that institutionalism pertains to IS training and the strategies IS managers use to improve compliance. IS managers face uncertainty with the human element due to the lack of knowledge, training, and resistance to change within the organization (McGovern et al., 2017). IS managers can better manage uncertainty by practicing isomorphism and modeling substantive behaviors or processes (Heras-Saizarbitoria & Boiral, 2015). Adopted behaviors may evolve from mimetic, normative, or coercive pressures that may be applied at the organizational level but IS managers must also understand how to manage and implement behavioral issues at the employee level. Heras-Saizarbitoria and Boiral (2015) surmised in their study on symbolic adoption that if the employees involved in adopting the practices and behaviors of another organization do not fully believe in the value these practices provide, they are less likely to follow them.

Whether humans are the users of information systems, creators of IS policies or maintainers of the underlying technology, the human factor provides the most uncertainty in any IS environment. However, da Veiga and Martins (2015) suggested in their article that the most effective countermeasure to the human factor is awareness, training and

education. Heartfield and Loukas (2018) challenged the assumption humans are the weakest link in the IS chain. The authors proposed a human sensor network that allows users to detect and report social engineering attacks perpetrated against them. Many examples exist where humans have thwarted attacks of a different nature as we can sense things in real-time that machines may not necessarily be able to. However, that is not the norm. A quote from behavioral scientist B.J. Fogg sums up human nature, "3 truths about human nature: We're lazy, social, and creatures of habit" (B.J. Fogg, personal communication, March 31st, 2017). Not complying with policy can be easier and less work than complying. The social aspect of human nature is taken advantage of time and time again through social engineering techniques. As creatures of habit, humans tend to do the same things on a regular basis because it is easier, making humans more susceptible to social engineering. A human sensor network relies on the humans in the network to be responsive, engaged, and relatively tech savvy, contradicting Fogg's assumptions about humans.

In the current environment of constant security threats in the IS domain, many users are simply shutting down and ignoring warnings, requests for updates, changing passwords, etc. Stanton, Theofanos, Prettyman, and Furman (2016) identified this as "security fatigue", where humans reach a saturation point which it simply gets too hard to keep up with maintaining security processes and procedures. People are constantly reminded and bombarded with IS warnings until they become fatigued and stop paying attention. Although Stanton et al. focused their study on the general public, the phenomenon exists in the workplace as well. Training is provided to help facilitate IS

awareness to assist employees with complying with company IS policies. In addition, through training, employees better understand the risks associated with non-compliance and are more likely to follow procedure. However, employees are not immune to the security fatigue phenomenon and generally perform a cost-benefit analysis regarding compliance (Stanton et al., 2016). The cost-benefit of complying with policy is explained as the compliance budget. Once this budget or limit is reached, human nature kicks in and employees find ways to get around policy. Security fatigue can also be considered like decision fatigue.

When individuals are overwhelmed with choices, there is a tendency to make poor tradeoffs or worse, make no decision at all. To the user, this all becomes fatalistic as they begin to believe whatever is going to happen is going to happen or that security is someone else's responsibility. Individuals tend to absolve themselves of responsibility because they believe protection should be provided through the technology and security protocols already in place (Hadlington, 2017). In the same study, 98% of those questioned believed IS was the responsibility of the organization. Managing employee's attitudes and behaviors is something IS managers need to consider when formulating security compliance strategies. In fact, Hadlington posited by understanding the attitude of the user, the IS manager can better develop strategies to reduce gaps in IS security. Overcoming security fatigue is possible if: (a) the number of decisions users have to make about security are limited, (b) always doing the right thing becomes easier and (c) there is consistency with the decision's users do have to make (Stanton et al., 2016).

Fundamentally, practicing good security habits begins at the personal level (Thompson, McGill, & Wang, 2017). Good habits can carry over into the workplace but unfortunately, the average user lacks the knowledge and understanding of the underlying technology they use on a regular basis. In addition, users tend to employ a compliance budget when managing security (Stanton et al., 2016). A compliance budget is a type of decision making that closely correlates to protection motivation theory (PMT), which was developed to help explain individual behavior when confronted with a risky situation (Thompson et al., 2017). Individuals tend to develop a threat appraisal that they use based on their perception of the risk at hand. If individuals believe they can perform a protective behavior (updating software with new security patches for example) that will be effective in making their environment more secure, the more likely they are to practice good security habits (Thompson et al., 2017). However, enhanced security knowledge developed at a personal level does not directly translate to all environments and that training and understanding of the workplace platform and technologies must be considered during training (Stanton et al., 2016; Thompson et al., 2017).

Training employees on the technologies and policies necessary for successful security behavior is essential but Chua, Wong, Low, and Chang (2018) posited that organizations must go further and develop mechanisms to manage employees with access to client data. Chua et al. (2018), agree with Manworren et al. (2016) that most security breaches are caused by employee ignorance on data protection and non-compliance with company policy. Employee negligence with IS is considered a critical factor in overall IS compliance, necessitating the need for better IS policies. Understanding employee

negligence from the point of view of demographics, where differences in social and cultural backgrounds, age, gender or education level can influence individual perceptions of IS may also provide value (Chua et al., 2018). Employee negligence can be minimized by increasing overall awareness of organizational security policy although that is not always the case (Chua et al., 2018). The authors used this contradiction to posit that demographics can play a role in an employee's attitude and behavior toward IS compliance. Indeed, after surveying more than 600 people from different demographic backgrounds, Chua et al. found three demographic factors: age, employment level, and working industry had the biggest impact on employee compliance. The authors also confirmed that policy awareness has a direct and positive impact on compliance, increasing with the age of the employee. The authors found that their results on age related compliance were consistent with Youn's (2009) study where younger workers are less experienced and tend to have lower education levels. The type of industry employees worked in also played a role in compliance. Workers in regulated industries such as financial services, IT, healthcare, and insurance were more likely to comply with policy due to better awareness and training programs that were driven by the need to comply with the appropriate laws.

Increasing security awareness. Weak security awareness programs coupled with poor employee attitude and behavior all contribute to an inadequate IS culture within organizations that can lead to a higher risk of security breaches (Ki-Aries, & Faily, 2017). Mamonov and Benbunan-Fich (2018) postulated in their study on IS threat awareness that a user's self-efficacy to protect themselves online was a strong enough factor to limit

exposure and reduce threats. However, the authors found that self-efficacy alone was not a significant enough factor to have an impact on a user's overall awareness to IS threats. Addressing the human factor in IS is necessary to help reduce risk and build culture and starts by having senior level leadership buying into the program. Senior leadership buy-in helps with overall commitment and cooperation within the organization and should be a fundamental factor IS managers consider when developing strategy (Ki-Aries, & Faily, 2017). However, developing a strategy that only accounts for a one-size fits all security program is not enough. Including processes and policies specific to the business and individual should also be considered when developing strategies (Öğütçü, Testik, & Chouseinoglou, 2016). Continuous reinforcement of IS programs through focused awareness and training may reduce risk and improve culture but it may also add to security fatigue. Developing creative and innovative ways to communicate security related information on a regular basis may help avoid fatigue and employee non-compliance (Ki-Aries, & Faily, 2017). Changing the perception that management is responsible for security to one where all employees are responsible takes trust, communication and cooperation from all involved (Ki-Aries, & Faily, 2017).

Exclusively relying on technology for protection of personal or business information can lead to increased risk of security breaches, particularly for those uneducated or uncomfortable with technology (Öğütçü et al., 2016). As the study by Hadlington (2017) revealed, most users believe effective IS is the responsibility of management. Management reinforces this belief by investing heavily in technology to build stronger firewalls all while ignoring the human connection. Dang-Pham,

Pittayachawan, and Bruno (2017) emphasized this point in their study on the formation of IS groups within organizations. Technology alone is insufficient in protecting a company's information and that the end-user is critical in reducing risk within any IS system. Additionally, Bélanger, Collignon, Enget, and Negangard (2017) found employees that comply with security policy early in the adoption cycle create less organizational stress. Molin, Meeuwisse, Pieters, and Chorus (2018) also found in their study on employee's perceptions of technical security measures, that employees do recognize that stronger security policies and processes do improve security and that it is important to the organization, a fact CISO's can use in developing a comprehensive training or security program. In addition, Bélanger et al. discovered that increased awareness of IS policy also has a positive impact on overall security behavior and compliance. Dealing with the human connection means dealing with uncertainty, something most people are uncomfortable with (Aurigemma, & Mattson, 2017). When adopting technology or adhering to policy, individuals make a threat assessment to determine if adherence is in their best interest based on the risk and effort (Aurigemma, & Mattson, 2017; Stanton et al., 2016; Thompson et al., 2017). IS managers must balance human behaviors of negligence, ignorance and poor behavior with technology when developing a strategy to improve compliance and reduce risk.

IS managers not only have to be cognizant of individual behavioral patterns when developing strategy, they also have to be aware of employee sharing behaviors. Employees tend to share details about an organization or departments culture or subculture and IS is no different (Dang-Pham, Pittayachawan, & Bruno, 2017b).

Informally sharing information regarding departmental security compliance can have both positive and negative consequences. When individuals share knowledge and techniques that lead to less risky behavior that is a positive outcome (Safa & Von Solms, 2016b). However, if only a few employees dominate the flow of information, that can be detrimental to increasing the overall knowledge of the group. Formal training coupled with informal sharing can be an effective strategy in reducing risk within an organization (Dang-Pham et al., 2017b). Using formal and informal methods to develop strategy may also help build a strong security culture that reduces the amount of uncertainty and ambiguity in complying with security policies and procedures (Aurigemma, & Mattson, 2017).

A strong culture of security training and awareness, informal sharing, and formal policies and procedures can also help guard against threats such as social engineering. The threat of social engineering attacks can be reduced through formal training and education (Hatfield, 2018). Social engineering attacks occur both in a professional and private setting but can be mitigated through IS awareness programs. These programs reduce the likelihood that individuals will make poor decisions regarding IS behaviors such as password management, phishing, or leaving a computer terminal unlocked (Hatfield, 2018). As society becomes more dependent on digital information, protecting information becomes essential and addressing the weak links humans represent in becoming victims of social engineering is a continuous challenge (Mouton et al., 2016). Many outside firms are developing tools to simulate social engineering techniques commonly used by attackers. Mouton et al. (2016) proposed a framework that can be

used to train individuals how to respond to different methods of attack to be better prepared when an attack does occur. Frameworks such as these can be used by IS managers to create security awareness material that can be used repeatedly for continuous training. IS managers can take advantage of these tools as part of their strategy to improve compliance with organizational policy but must also take into account human attitudes on privacy. A study by Kokolakis (2017) revealed that individuals are susceptible to immediate gratification bias where a benefit offered in the present is more beneficial than the potential risk exposing information may have in the future. Social engineers can exploit these weaknesses to gain access to secure information.

Perceived social weaknesses can be exploited in other ways as well. While it is commonly known in IS that humans are the weakest link, gender specific differences in IS compliance can also be a factor (Anwar et al., 2017). The authors studied the differences between male and female respondents by applying two prevailing theories: Protection Motivation Theory (PMT) and the Human belief model (HBM). Whereas PMT focuses on an individual's intention to protect themselves based on what they perceive to be a threat, HBM is concerned with perception of the benefits of participating in a health-related behavior. Anwar et al. cited prior research that revealed gender differences were greater with increasing age, with older workers having a stronger perception of technology than younger workers, and that females express a bigger concern for privacy than males do. Developing gender specific training may be warranted based on this information. Anwar et al. determined that self-efficacy in IS compliance was higher in women than in men. A female's confidence and self-efficacy can have a

direct impact on their ability to control their behavior, motivation and social surroundings. Safa, Maple, Watson, and Von Solms (2018) continued this line of thought by postulating that motivation and opportunity are primary factors understanding insider threats and reducing risk. Anwar et al. determined age, experience and education can also have a positive impact IS compliance as well, highlighting the fact that targeted training can be beneficial over a more traditional one-shot approach to training.

Kim, Kim and French (2015) provided a unique look at IS management in the context of need-pull (NP) and technology-push (TP) theories. In the NP model, users' needs are the primary drivers in adopting new technology. TP, where new technology is pushed on the organization because it is perceived as beneficial to increasing overall performance, is often a necessity. However, managing IS is complex and cannot be solved by technology alone. The human component associated with effective security management should involve security awareness and targeted training programs that understand the end user's capabilities and can be more effective than simply pushing out a generic, all for one training program (Kim et al., 2015) or relying on technology.

Coercive, mimetic and normative pressures also exist as social pressures to the individual. Bozan et al. (2015) based their research of individual elderly patients' adoption of electronic health records on the behavioral and cultural components of institutional theory. Understanding how elderly patients behaved when using electronic health records provided a good analogy for understanding how people react to the different pressures when complying with a policy or process. Hu et al. (2016) provided a study of the decision-making process firms used when implementing environmentally

sustainable (green) IT. Firms must also contend with environmental pressures as part of their decision-making process. If enough actors engage in a certain behavior, individual actors are more likely to go along with that behavior, which can be considered a normative behavior (Bozan et al., 2015). If enough individuals conform to this normative behavior, you have the beginning of a homogenous department (Hu et al., 2016). Coercive pressure by the health care providers to use electronic records were also perceived as a factor in conformance and adoption of technology or policy (Bozan et al., 2015).

External business pressures can have an influence on a firm's behavior and decision-making process (Hu et al., 2016). External pressures at the individual and organizational level can also influence a firm's goal of achieving and maintaining legitimacy. Bozan et al., (2015) and Hu et al. (2016) revealed that both coercive and mimetic pressures can have a significant effect on individual compliance. Normative pressures were less significant at the individual level because individuals may already follow engrained processes but organizationally it did have an impact. The findings by Bozan et al. and Hu et al. illustrated that applying the behavioral and cultural components of institutional theory to a study involving the adoption and compliance with training and policy may yield valid results when applied to this study, providing insights that IS managers can use to develop strategies.

IS managers can reduce the uncertainty provided by the human element by developing a security strategy. The strategy should include not falling into a senior management mindset that technology alone can solve the problem by gaining senior

management support for developing and maintaining an effective security awareness and training program. IS managers should develop and implement IS programs that limit the human element by improving awareness through training and compliance. IS managers can counteract the human nature of laziness, need for social interaction, and being creatures of habit by creating a culture of accountability, awareness of social engineering threats and how to mitigate them by providing continuous training to avoid employees from falling into a habit of predictability. By promoting IS awareness as part of the culture, IS managers can reduce security fatigue. Finally, by reducing the number of choices employees have to make on a daily basis when complying with company policies such as password management, computer security, physical security, etc., IS managers can limit decision fatigue.

Improving employee information security compliance. The human component, security training and awareness, and technology are all directly linked to compliance. Achieving compliance is necessary for any organization attempting to gain legitimacy within the industry in which they are competing (Kauppi, 2013). Figure 1 illustrates three different economic variants IS managers can consider when attempting to achieve compliance. Frequency-based imitation, where the actions and practices of organizations that have achieved legitimacy through industry certifications, is one method that can be applied to improve compliance. Copying specific traits of an organization within your industry, known as trait-based imitation, is another tool that can help IS managers achieve compliance. Lastly, outcome-based imitation that copies a behavior that has

proven successful to a similar organization or industry can also help improve legitimacy and achieve compliance.

IS managers must clearly communicate the need for these new processes, policies, and standards in achieving compliance within the industry the organization participates in. In the United States, the national institute of standards (NIST) has developed a cybersecurity framework to comply with the Cybersecurity Enhancement Act (CEA) of 2014. The CEA was established to provide operators of critical infrastructure a framework for managing cybersecurity risks. Currently, adherence to the framework is voluntary. Complying with processes, policies, and standards to improve employee compliance requires managing change. Andrews-Speed (2016) outlined three different types of change associated with institutionalism: layering which involves adding to existing processes and procedures, conversion which adds new goals or actors to change the overall function of the institution, and drift which occurs when negligence in policy compliance gradually takes effect. IS managers must understand that when there is an openness to change within the organization, there is a better likelihood for acceptance and desire to comply (Andrews-Speed, 2016). Compliance through isomorphism helps firms gain legitimacy but can also provide different perspectives for adopting practices and policies as part of an overall strategy (McGovern et al., 2017).

The impacts of not complying with IS policy is well documented in current literature. Human non-compliance with policy was a root cause of the Target breach in 2014 that cost an estimated $400-$500 million (Hemphill & Longstreet, 2016). The security breach was a result of an outside vendor not complying with policy and

approving remote access to the Target network, allowing malware to be introduced into the environment. Target had a state-of-the-art security system with well trained staff but was still the victim of a security breach.

The Target breach would indicate that effective technology and training are not the only factors involved in compliance. Security fatigue, introduced by Lee, Lee and Kim (2016) as information security stress (ISS), awareness and culture are other factors that can impact compliance. The need for employees to constantly remain vigilant on security procedures within the workplace adds a layer of stress to their work environment. The constant stress associated with security compliance leads employees to be less receptive and compliant with IS policies. In this context, a cycle is created where non-compliance leads to more organizational attention and requests for compliance that leads to more stress on the employee that then becomes less receptive and the cycle repeats. Managers can help reduce stress by improving awareness and developing a strong security culture.

When employees are less compliant with security procedures, the organization also loses productivity from the employee. Lee et al. (2016) revealed in their study that close to 64% of respondents to their survey indicated experiencing stress in the workplace associated with IS. Of those surveyed, 43% communicated they had issues completing their work activities due to this stress. Based on their study, Lee et al. (2016) revealed that an increased workload in general was a significant contributor on ISS. As companies continue to shrink workforces, those left behind are seeing their workload increase which fuels this ISS cycle.

IS managers should understand how increased workloads impact compliance as they develop strategies, even if they do not have a direct impact on effecting those workloads. An overworked, over stressed employee can certainly become emotional, leading to poor decisions about IS compliance. Understanding the employee and targeting the training may certainly be something IS managers should consider. The terms overworked and over stressed can be subjective. One person's normal workload might be too much for another person. Similarly, people react to stress differently. Understanding the expectations of employment that include workload and compliance with policy is controllable by management.

IS managers can develop a strategy to improve employee compliance by balancing the need for awareness and vigilance of processes and policies by offering optional refresher training as well as training exercises on a regular cadence multiple times per year as new threats emerge. Managers that understand increased workloads contribute to ISS can develop creative ways to balance work and IS. Managers can take time to understand employee's needs and concerns to help determine what personality types exist and target training accordingly to increase compliance. Finally, managers need to understand how and why people are non-compliant and communicate the necessity for compliance.

Improving employee training. The department of homeland security (DHS) considers training an essential mechanism in IS risk management (Curran, 2015). Education, training and awareness programs are mandated in some industries to either comply with regulatory or contractual requirements. Improving employee training is

closely linked to improving employee compliance. Although not currently required within the industry, IS employee training is another mechanism organizations can use to achieve legitimacy. IS managers can use isomorphism to establish new training programs as part of their overall IS strategy. Learning is seen as efficacious if done in an open and transparent environment that facilitates trust, which is dependent on the organizational culture (Andrews-Speed, 2016). Unfortunately, there is no accepted standard for IS education, training and awareness programs, making it difficult for IS managers to develop a consistent strategy and security culture that encourages training. Regulations are different depending on the industry so organizations that provide IS services to a variety of industries have a unique challenge (Curran, 2015). Coupled with the socio-technical challenge of creating a one-size-fits-all employee compliance policy, IS managers can create effective IS policy by positively framing the message, so it helps increase awareness of the risks associated with non-compliance (de Bruijn & Janssen, 2017).

IS managers must also be educated on the definitions of IS education, IS training and IS awareness (Curran, 2015). IS education combines a mix of passive and active instruction to enhance the employee's overall skill level. IS training is done through standard passive testing techniques and IS awareness focuses on dialogue and collaboration through personal experience to change IS behavior (Curran, 2015). Combining IS education, IS training and IS awareness should be part of any cohesive IS strategy (Curran, 2015). Employees should be educated on the variety of threats and risks that exist, trained on how to recognize and mitigate them and be constantly aware of the

security landscape around them. Regulatory specific training should be done as needed but general IS training and awareness should be done on a regular basis, be part of company policy, and be updated continuously.

Targeted training goes beyond gender (Park, Kim, & Park, 2017). Different professions have different needs when managing IS. In their study on health information security awareness (HISA), Park et al. (2017) studied the behavior of nursing students in disclosing health information that they have access to during their studies. Nursing students are considered vulnerable stakeholders in complying with HIPAA (health insurance portability and accountability act) based on the fact they are regularly exposed to patient information during their studies and clinical practice while simultaneously developing personal values and beliefs regarding the importance of health information privacy. For this reason, nurses suffer from improper, inadequate, or non-existent training. To understand how an individual's behavior may be influenced by education, training and associated sanctions with non-compliance, Park et al. (2017) applied general deterrence theory, which focuses on the consequences of poor behavior. Applying deterrence theory in conjunction with education and training was shown to have a positive impact on a nursing students overall security awareness and compliance (Park et al., 2017), adding further evidence that IS training can help in deterring improper behavior when complying with security policies. Targeted training that comprehends gender (Anwar et al., 2017) and the various levels of IS awareness: being generally aware, having a solid understanding, learning explicitly through training and education, and unconsciously by patterned behavior can have a positive influence on personal

behavior and compliance (Park et al., 2017). Health care professionals are not unique in their needs when it comes to IS management.

How an employee perceives the necessity of IS can be correlated to how well they comply with IS policies and procedures (Kearney & Kruger, 2016). Developing an IS strategy that incorporates the importance of IS built on trust within the organization are seeds for a healthy and effective security culture where users believe the environment is secure (Kearney & Kruger, 2016). Training programs that include organization wide cooperation, coordination, and technical expertise can help strengthen a company's overall IS operations (Bartnes, Moe, & Heegaard, 2016). Users who are more computer savvy and are familiar with security threats that exist online are more likely to exercise better computer security habits than those unfamiliar with current threats (Jeske & van Schaik, 2017). IS managers may benefit from using a quick survey of their employees to see who fits into these two categories before developing a training and awareness program. The survey may easily identify those with advanced IS knowledge and skills that can provide a reasonable prediction of compliance (Jeske & van Schaik, 2017). However, assessing skill levels accurately can be subjective (Kavalaris, Kioupakis, Kaltsas, & Serrelis, 2015). Survey results may be biased based on the population involved and the questions asked so skills assessment are not easily measured.

Employees with advanced IS knowledge and skills are still susceptible to revealing personal and confidential information (Kearney & Kruger, 2016). Cloud based applications and services along with mobile applications are newer technologies that create even more exposure for employees. Revealing personal and confidential

information can lead to a greater risk of social engineering attacks so mitigating this type of risk requires IS managers to focus the development of strategy and policy on awareness and training (Krombholz, Hobel, Huber, & Weippl, 2015). Even so, individuals with a higher perceived IS awareness IQ tend to be more compliant than those with lower IS awareness IQ (McCormac et al., 2017). Increasing IS awareness IQ should start with targeted training that is consistent and continuous. Targeted training can lay the foundation to building a strong security culture

Developing a strategy to improve employee training can take many forms. As part of a comprehensive approach to training, IS managers should become familiar with the differences in IS education, training, and awareness. Education is a mix of passive and active instruction, training is done through standard passive testing, and awareness focuses on dialogue and collaboration to communicate the risks of IS and how to mitigate them. As part of a security training strategy, IS managers can take advantage of industry leaders such as the SANS institute or governmental agencies such as the department of homeland security (DHS) or the National Institute of Standards and Technology (NIST) for insights on IS training. IS managers may benefit by becoming educated on behavioral theories such as general deterrence theory, to gain a better understanding of why certain employee behaviors exist. A comprehensive IS training program should avoid a generic, one-size-fits-all approach and develop training and awareness programs specific to groups or individuals depending on technical ability and industry regulated requirements (e.g., financial, healthcare). Curran (2015) outlined a framework that can be used on an annual basis by IS managers to develop a training program. Safa et al. (2016) suggested

training on a more frequent basis than once a year, which is consistent with current literature. However, Curran's framework provides a realistic and achievable method for developing an IS training program.

In designing an IS program, Curran (2015) suggested following these principles: a) begin any training program by educating the employees of the IS program, b) communicate management's commitment to the training, c) communicate the regulatory and organizational compliance policies and, d) develop and communicate the penalty for non-compliance. Once the objectives of the training are properly communicated, IS managers can develop a variety of testing techniques such as online or in-class training and evaluation. By having training on a more frequent basis, IS managers can help employee's recall previous training and policies and thereby reinforcing the material. More frequent training allows for new material to be presented as well as outlining the desired behavior for compliance along with how non-compliance will be handled. Complimenting Curran's suggestion on educating employees, Bauer et al. (2017) recommended using videos showing the risk and threats associated with IS versus the current method of communicating plainly via email. Bauer et al. (2017) also recommended IS managers a) use a scared straight mentality and create videos that show real-life consequences to real world risks and threats, b) develop realistic metrics that can be used to evaluate and correct awareness and training methods, c) provide mechanisms for employees to provide feedback on the program, allowing for constant improvement and finally, d) customize the training and awareness programs based on the user's differences (location, skill level, areas of responsibility, etc.).

The need for a security culture. Webster's dictionary defines culture as "a set of shared attitudes, values, goals, and practices that characterize an institution; a set of values, conventions, or social practices associated with a particular field, activity, or societal characteristic; and the integrated pattern of human knowledge, belief, and behavior that depends upon the capacity for learning and transmitting knowledge to succeeding generations" ("Culture", 2019). As B.J. Fogg explained, humans are creatures of habit (B.J. Fogg, personal communication, March 31st, 2017). Changing or developing a work culture is not a trivial task. IS managers may be able to take advantage of institutionalism in changing culture. In a study on the current trend of corporations transitioning to a low-carbon energy model, Andrews-Speed (2016) was able to view the change through the lens of institutional theory. The author highlighted the current state of institutionalism by categorizing the different areas the theory applies to. Rational choice institutionalism is more applicable for economic consideration, historical institutionalism is useful when studying the balance of power within organizations and sociological institutionalism is primarily focused on the significance of culture. Andrews-Speed (2016) posited a fourth category of institutionalism, discursive, that can be applied to understanding the role of ideas and discourse within an organization. While all four categories could be examined in the context of this study, sociological institutionalism and the role it plays on shaping culture is the most applicable to understanding how IS managers may be able to create culture by copying symbolism and values used successfully in similar organizations.

In addition, other methods exist for building culture. Applying coercive pressures that are necessary for achieving certification or complying with regulations is one method. If external pressures do not apply, information managers can use mimetic pressures to begin changing the culture. Developing a security culture that allows for shared attitudes and practices for a set of conventions, such as IS compliance, that leads to a patterned behavior of learning and sharing knowledge with new workers should be the goal of every IS manager. AlHogail (2015) proposed organizations take advantage of a known IS culture framework STOPE (Strategy; Technology;, Organization; People; and Environment) in his study, stating that by establishing a strong IS culture within an organization has a positive effect on employee's security behavior than can help reduce internal threats. At the center of the framework are the people, who the author described as being the core of any IS culture. Culture should be embedded in the organization to the point where it can influence employee's behavior (da Veiga & Martins, 2017). Understanding the different attitudes and behaviors of the employees is critical for IS managers developing IS training and awareness strategy (da Veiga & Martins, 2015). The important point to be made, when creating an IS culture, is that senior leadership within the organization must accept the responsibility and expectation that they own it.

IS managers must also include IS awareness, governance, compliance, and audit techniques in addition to behavioral theories as part of the overall policy framework strategy (Densham, 2015). Densham further suggested that developing a framework that continuously assesses and adjusts processes and policies to ensure they remain relevant and effective is fundamental to any IS strategy. Soomoro, Shah, and Ahmed (2016)

confirm Densham's work in their discussion on a holistic approach to managing IS. An effective IS strategy must include processes and policies that integrate both the technical and human aspects (Densham, 2015). However, the human factor remains a significantly complex area that IS managers must continue to focus on. Humans have biases that impact their day-to-day decision making (Tsohou, Karyda, & Kokolakis, 2015). According to Tsohou et al. (2015), individuals are heavily influenced by their cognitive biases and heuristics that they apply to their everyday life. Beyond cognitive bias, Tsohou et al. also posited that compliance with IS policies can also be a factor of the positivity a person feels toward the training, procedures, and policies in place. When employees are ignorant of the potential security threats and associated consequences when threats occur, they will be less prepared to manage them appropriately (Bartnes & Moe, 2016).

Creating a positive experience as part of an IS strategy is consistent with de Bruijn's and Janssen's 2017 study on the need for evidence-based framing strategies. Creating a positive environment for employees to work in can be as simple as hanging up information posters in the office. Tsohou et al. (2015) highlighted this in a poster of a puppy with the caption "someone discovered my password, now I have to rename my dog." Making light of security while at the same time creating a fun atmosphere may help employees realize the importance of IS while at the same time having a positive experience in the office. Djemame, Armstrong, Guitart, and Macias (2016) explored a risk assessment framework based on NIST and the European Network and Information Security Agency (ENISA) guidelines. The article outlined a framework that can be used by organizations to assess security risk within their organization. The assessment begins

by identifying vulnerabilities, identifying threats and monitoring data. Events flagged from the initial assessment are analyzed and quantified based on established parameters. Once the risks are quantified, they are assessed and acted on according to an established decision-making process. Shamala, Ahmad, Zolait, and Sedek (2017) cautioned in their study of information risk management that risk assessment information collected may not always be reliable (i.e., garbage in, garbage out). In their article, the authors suggested implementing information quality (IQ) to the data gathering process to ensure data suggested is more reliable and actionable.

Coupled with an effective risk vulnerability framework, a holistic strategy can be formulated that can lay the foundation for a strong security culture. In their study on risk management frameworks, Joshi and Singh (2017) investigated a variety of currently available risk assessment models, highlighting the strengths and weaknesses of each. The authors agreed that using a risk assessment model to evaluate vulnerabilities within the network, however, they believed that a more comprehensive model that combined the strengths of existing models and reduced or eliminated the weaknesses was a worthwhile effort. In their paper, Joshi and Singh (2017) proposed a recursive risk assessment process. Their model consisted of three phases; 1) identify the weak points in the system, 2) prioritize addressing the weak points based on company strategy, and 3) improve the security position of the organization through actionable plans and fact-based decision making. Repeat these phases continuously to manage new and evolving threats. It is an interesting strategy that mimics product development or software development life cycles in many technical organizations but applied to IS instead of products and software.

The goal of an effective security strategy is to reduce the risk of security breaches within the organization. Safa et al. (2016) recommended building the foundations of a strong security culture by developing processes, standards, and policies that incorporate methods for training and awareness for all employees as part of an overall strategy. In their article on IS policy, Flowerday and Tuyikeze (2016) expanded on Safa et al. (2016) recommendations by including a risk assessment for the organization to develop a starting point. From the results of the assessment, an organization can start developing a strategy on what should be included in the IS policy and how it complements or contradicts company policy. Once the IS policy is developed, IS managers can begin to develop tailored training programs to cover all areas of the organization (Flowerday & Tuyikeze, 2016). Some areas of the company may need specific training on regulatory compliance and other areas may not. Although the policy should be communicated organizationally, training can be individually tailored as needed. Ensuring compliance with policy is part of building a security culture.

Understanding and embracing a subculture. In their study on culture and subculture, da Veiga and Martins (2017) explained that organizational culture is perceived as the dominant culture within an organization and that IS culture can be considered a subculture. The core values of the organization are practiced by most employees in the dominant culture but in a subculture, a smaller group of employees develop and share a culture more specific to their workgroup or department. IS culture can be considered a subculture in this context as different attitudes and behaviors are developed that may not be aligned with the core culture of the organization. Primarily, an

IS culture consists of values and norms associated with protecting information. It is not intended to circumvent the dominant organizational culture and can be an effective complement.

However, if the subculture is deemed as negative and undermining the dominant culture, IS managers must intervene and take steps to align the subculture with the dominant culture (da Veiga & Martins, 2017). In their article on identifying subcultures within an organization, da Veiga and Martins (2017) used an IS assessment tool they developed for an earlier study to help identify if IS subcultures exist within an existing organization. However, while the article provided a way to measure for IS subcultures within an organization, it did not go far enough in explaining how IS managers can include the tool as part of a consistent strategy. Further, the authors only identified that multiple subcultures might exist within organizations but not necessarily how to manage them to provide maximum benefit. The authors could have suggested as part of building a comprehensive security strategy, how the assessment tool could be used in conjunction with an audit tool, to get a clearer picture of the current IS landscape within an organization.

Building a strong security culture. To effectively protect sensitive information within an organization, a strong security culture is necessary (Dhillon, Syed, & Pedron, 2016). Creating a strong IS culture can be a challenge during times of significant change. Technology is currently changing at such a rapid rate that creating and sustaining a strong security culture presents a unique challenge for IS managers (da Veiga & Martins, 2015). To effectively manage change while creating a strong IS culture, IS managers must also

be strong communicators as well. In addition to being effective communicators, IS managers must lead through action. When IS managers stay focused on the important aspects of IS through measurement and control, employees notice, further reinforcing the IS culture (da Veiga & Martins, 2017).

While the importance of management in developing a strong security culture should not be understated, employees who collaborate and share their knowledge of IS with their peers help strengthen the overall culture (Safa et al., 2016). Knowledge sharing and collaboration form the basis of social bond theory (SBT) espoused by Safa et al. (2016). In addition to building a stronger culture, SBT helps improve the level of IS awareness within the organization. Safa et al. (2016) acknowledged in their study that involvement by the individual employee in the overall IS experience is beneficial. The challenge is getting all employees involved. While the article presented positive evidence that collaboration with peers and management in complying with IS policies can help mitigate security breaches, the article does not provide potential suggestions for how an IS manager can begin to create a collaborative environment. However, employee involvement can be improved, based on themes already outlined in this review, with a comprehensive IS strategy that includes clearly communicated policy, formal and informal training on a regular basis, building a culture of awareness and accountability through management sponsored security campaigns, lunch and learns, and other creative ideas encouraging safe security.

Building a strong security culture takes time and patience but IS managers can start by defining a security culture that makes sense for their organization, get senior

leadership buy-in and communicate it. Culture can be defined as a set of shared attitudes, values, goals and practices that characterize an institution. Developing a security culture that encompasses some or all of the shared attitudes, values goals or practices that is communicated and practiced can provide the foundation for a strong security culture (Dhillon et al., 2016). IS managers should develop an organizational baseline by performing a risk assessment. Based on the risk assessment results, IS managers should take the results into account when developing an IS policy that complements company policy. Determining if subcultures exist within the organization should also be part of developing a security baseline (da Veiga & Martins, 2017). If subcultures do exist within the organization, IS managers must decide if these subcultures negate or enhance the security culture they are trying to develop. IS managers should take steps to audit processes and procedures on a regular basis to ensure compliance but also to make adjustments as required. Developing simulations to regularly test employees on policies and procedures is another tool IS managers can use to help establish a security culture. Most importantly, IS managers must be strong communicators and increase user's awareness of IS related topics (Safa et al., 2016). Simple mechanisms such as lunch-n-learn sessions or encouragement of knowledge sharing and collaboration of security related issues, can help reinforce the concept that security is everyone's responsibility.

Future of IS culture. In their article on the future of security in Germany; Gerhold, Bartl, and Haake (2017) discovered risk experts surveyed believe that IS risk awareness by the general population should be managed by state actors instead of accepting the responsibility themselves. Relying on the state or management for security

is a dangerous precedent to set and contradicts what most current literature advocates. While it is desirable for the state or management to be responsible for managing security, the individual must be held accountable for complying with company security policies. Building a strong and effective security culture begins with everyone involved taking responsibility for their own actions and owning security (da Veiga & Martins, 2017).

A more recent approach to IS compliance involving individual accountability and the user's perceived value of the information they manage was the topic of Doherty and Tajuddin's (2018) article. In the article, the authors posit that individuals are likely to comply with security policy if they are aware of the value of the information, they are responsible for. The higher the value, the more likely users are to follow procedures and maintain compliance. This approach, termed value driven IS compliance, aligns with both Gerhold et al. (2017) and da Veiga and Martins (2017) in that users need to assume responsibility. Although it is based on the perceived value of information, the individual is still in control of compliance and has the responsibility. Assigning a value to information is a unique approach to IS compliance and one that IS managers may take advantage of in developing their own strategies. Doherty and Tajuddin (2018) explicate in their study that a value-driven information strategy does not allow for predicting compliance. However, the study did reveal that when users understand the value of the information they are working with, they are more likely to comply with policy. Applying a value to information is a new approach that can be used to improve security compliance. Doherty and Tajuddin (2018) recommend future research distinguish

between personal and organizational data and the value of each as part of a compliance strategy.

The user was front and center in an article by Buchanan (2018). In the article, the future of cyber security training and awareness was shown to be evolving. Buchanan reiterated da Veiga and Martins (2017) that IS within an organization is everyone's responsibility. Most importantly Buchanan mentioned, being aware of the threats and knowing how to deal with them was critical. Simply being aware of the threats and how to manage them is not enough according to the author. There is a critical need for everyone to observe how people react to specific events. Companies are now developing complete training platforms that can simulate IS threats within a standalone environment where users and trainers can be exposed to real-life simulations. The simulations allow the scenario to unfold and be rewound allowing for users to learn in a safe but simulated environment. The author believes training of this type can one day mimic the training pilots currently receive where they are exposed to a variety of scenarios and trained on how to manage them. Buchanan (2018b) goes even further in describing that the current state of software development needs to change to be written with security in mind. Developers should not be immune to continuous learning in the security realm. Similar to proper memory management while writing code, proper security management will need to become part of the standard process developers should use while writing software applications.

Artificial intelligence (AI) is also working its way into cybersecurity training. In an article for CSOonline, Drinkwater (2017) studied the advantages AI can bring to the

IS environment. AI is very good at learning patterns that exist within large datasets and picking up behaviors of users of that data. AI can help pick up on unknown security threats, automate responses and even remediate attack response. Although in the early stages, AI shows promise for applications within IS. Most importantly, AI can be a critical tool in the detection and defense of threats within an organizations network. Although currently seen as assisting humans in IS, AI is becoming more prevalent in a variety of applications that can help process numerous variables, creating the ability for decision makers to analyze a problem faster leading to quicker decisions. AI will not only be useful in fighting security threats, Terranova Security (2019) envisions a future where AI can enhance security training through personalization. By taking advantage of the predictive nature of AI, training material can be updated based on trends uncovered by AI applications as well as creating content specific to each individual learner.

Transition and Summary

In their study of institutional isomorphism, DiMaggio and Powell (1983) developed an understanding of how organizations and institutions can achieve legitimacy and success by mimicking practices, policies, and procedures from other organizations who have used them successfully. Institutional theory can be applied to organizations to help develop guidelines for organizational behavior, practices, policies, and culture. The study by DiMaggio and Powell focused on how organizations can normalize or implement successful practices. Institutional theory considers both social and economic pressures as well as pressures internal and external to the organization that can influence the adoption of practices and policies. The consideration of organizational behavior and

policy adoption makes institutional theory a strong choice for research involving the institutionalization of policies and procedures related to IS.

This literature review investigated the various elements associated with IS within organizations and how the different elements impact strategy development by IS managers. Institutional theory was presented as the conceptual framework to help understand the complexity involved in creating an effective IS strategy. Institutional theory provides a relevant lens to view the implementation of IS practices and procedures and how IS managers apply them as part of an overall strategy within the case study organization. The literature review concentrated on the elements of IS that impact employee compliance; human behavior, security training and awareness, and security culture. Section 2 discusses further aspects of the study such as the role of the researcher, methodology, and design for the study.

Section 2 will discuss further aspects of the study such as role of the researcher, the participants, the justification for the chosen research design and method, the population and sample, aspects of ethical research, data collection, analysis, organization, and the reliability and validity of the study. Section 3 will contain the findings from the study and the presentation of the results based upon all methods of data collection utilized for this study.

Section 2: The Project

This section provides information on the participants, sample, and research methodology while providing justification for decisions made regarding the study. The section will also address ethics and steps taken by the researcher to mitigate factors such as personal and researcher bias. Finally, the following section will describe the approach for data collection and data analysis while discussing reliability and validity.

Purpose Statement

The purpose of this qualitative multiple case study is to explore what strategies IS managers use to improve employee compliance with security training and policy. The participants of the study were IS managers from two technology firms in Western New York. This study may increase IS managers understanding of effective IS strategies that may then be developed into a set of good practices in the area of IS awareness. This study will contribute to social change by highlighting the strategies IS managers have used to deliver improved security awareness programs, leading to better habits in terms of protecting both company and personal data. By being more cognizant of effective IS strategies outlined through a set of good practices, employees and computer users may be able to take advantage of these practices to help reduce the risk of becoming victims of identity theft.

Role of the Researcher

I was the primary instrument in the data collection process for this study. Humans have unique characteristics that qualify them to act as instruments (Guba & Lincoln, 1985). Human characteristics such as responsiveness, adaptability, the opportunity to

clarify and summarize, and the ability to explore responses directly are a few reasons qualifying humans as data collection instruments in a qualitative study. Researchers conducting a case study are responsible for designing the study, developing specific interview questions, understanding and confirming participants' responses, and reducing personal bias and reflexivity (Berger, 2015). My role in this research was to design the study, develop interview questions, and collect, organize, analyze, and report the results. I mitigated bias by presenting the results of the study from the participants' point of view.

I have over 25 years of experience in the software industry. I have never directly worked in the IT field as an IT professional but have worked with IT professionals, IT equipment, and IT infrastructure throughout my career. I regularly attend IS training and comply with IS policies but have never been involved in the development or implementation of IS strategies or policies. Due to my lack of direct involvement with IT during my career, I was able to limit bias in this study. During a research methodology course assignment for this program, I interviewed IT professionals using sample surveys to determine that the organization qualified for this study. I do not have any prior working relationships or interactions with IT professionals I interviewed for this study. I engaged the proper legal and human resource representatives of the target companies for permission to perform research and interview employees. Once a letter of cooperation was signed by both organizations and Institutional Review Board (IRB) approval was obtained (approval number 06-28-19-0542138), I engaged the participants and requested their participation in the study.

I performed this study and data collection ethically and in accordance with the Belmont Report. The Belmont Report distinguishes guidelines and principles for research involving human subjects. The Belmont Report defined research as a formal protocol with a set of procedures and objectives. The protocol consists of basic principles of respect for persons, treating them in an ethical manner, doing no harm, and treating them fairly. All participants were provided adequate information regarding the research and their role, and they provided their informed consent to participate in the study. The information was provided in an organized and professional manner that allowed participants the ability to comprehend the objective of the research. Participants were provided the opportunity to volunteer in the study as well as the ability to withdraw at any time. As a researcher, I completed the Protecting Human Research Participants training course (certification number 2075072).

To avoid personal bias, a researcher must reflect participants' experiences and perspectives while limiting their own experiences and perspectives (Guba & Lincoln, 1985). Researcher bias can reduce the credibility of the study, as it may contribute to manipulation of the collected data to coincide with the researcher's own beliefs (Guba & Lincoln, 1985). By contemplating and understanding my role as a researcher and experience with IS, I was able to mitigate bias by being aware of my own personal experiences and beliefs. I used open-ended semi structured interview questions and recorded each participant's answers. I used member checking as necessary to clarify any answers provided during each interview.

I used an interview protocol to conduct semi structured interviews with participants. The interview protocol contains guidelines the researcher can use to establish reliable results. Establishing consistent and reliable results for all participants is one of the primary reasons for an interview protocol in addition to keeping each interview focused and on track (Lancaster, Kolakowsky-Hayner, Kovacich, & Greer-Williams, 2015). Keeping each interview on track for semi structured interviews allows the researcher to probe each interviewee for further information and gain a deeper understanding of the topic (Ellis, 2016). By having a defined list of questions to follow as part of the interview protocol, researchers can avoid confirmation bias by not selectively collecting and interpreting data based on their own existing beliefs (Roulston & Shelton, 2015).

Participants

An important consideration in determining appropriate participants for this study is the criteria used to determine their eligibility. Selecting an adequate sample is fundamental to research and can help determine the characteristics of a population (Emerson, 2015). Purposive sampling allows the researcher to select participants that are representative of the population to be studied (Guba & Lincoln, 1985). In this study, I was interested in understanding the strategies IS managers use to improve employee compliance with security training and policies. I confined the sample population in my study to IS managers who were responsible for developing organizational strategies for improving employee security compliance. Participants with experience in the phenomena under study can help the researcher better understand the topic (Errasti-Ibarrondo, Diez-

Del-Corral, Arantzamendi, & Jordan, 2018). Therefore, ideal candidates for my study were chief information security officers (CISO) or those in their chain of command who were experienced in developing and implementing IS strategies and policies.

Guba and Lincoln (1985) identified gatekeepers as those who have the authority to contact appropriate individuals at the site of study. The two organizations I used for this study employ CISOs who acted as the gatekeepers for this study. CISOs are responsible for providing expertise and best practices to organizations as well as ensuring compliance with security programs (Karanja & Rosso, 2017). Each CISO was requested to provide access to IS managers within their chain of command and allow them to participate. IS managers had enough knowledge and expertise to adequately answer interview questions. Gatekeepers are typically not involved as participants in the study, as they play the important role of providing authorization for individuals to participate in the study (Kristensen & Ravn, 2015). However, in this study, a deputy CISO for Company A and CISO from Company B were available and willing to participate and provided key executive level insights and knowledge of strategy-building processes. Gatekeepers can also help researchers identify and locate internal documents as secondary data sources (Boblin, Ireland, Kirkpatrick, & Robertson, 2013).

Identifying and engaging gatekeepers can be done using publicly accessible means (Kristensen & Ravn, 2015). Gaining access to participants requires building a relationship with the gatekeeper (Wanat, 2008). The primary strategy I used to identify and engage potential participants was to establish a direct relationship with the CISO's of a two technology firms located in Western New York that acted as the gatekeepers.

Engaging with the gatekeeper helps build credibility with members of their team (Marks, Wilkes, Blythe, & Griffiths, 2017). Once contact was made with the gatekeeper and a relationship established, I asked them to sign a Walden letter of cooperation that outlined their responsibility in the process. Once the letter of cooperation was signed, I worked with the gatekeeper to identify the proper person or persons to interview for the study. Once I received Walden IRB approval for my proposal (approval number 06-28-19-0542138), I then reached out to the intended participants to introduce myself, explain the nature of the study and obtain their formal approval and consent.

Research Method and Design

The qualitative research method was appropriate for this study because the intention was to explore the strategies IS managers use to improve employee compliance and reduce security breaches. A qualitative researcher studies a phenomenon occurring in a natural setting and reflects on how and why the phenomena occurred (Baxter & Jack, 2008; Moser & Korstjens, 2017; Watt, 2007). A quantitative researcher seeks to predict behavior based on measurement and quantitative analysis using numbers (Barnham, 2015; Rutberg & Bouikidis, 2018). The intention of this study was to understand the strategies used by IS managers to improve employee security policy compliance, not predict how someone will react to the strategies, making quantitative method an inappropriate methodology for this study. A mixed method research (MMR) approach combines both quantitative and qualitative methods and requires the collection and analysis of data from both methods (Alavi, Archibald, McMaster, Lopez, & Cleary, 2018; Mabila, 2017). As previously stated, there was no desire to predict human behavior based

on measurement and therefore, MMR was also not being considered as a research methodology.

Research Method

Qualitative research allows for a deeper understanding of the natural setting surrounding the phenomenon under study (Baxter & Jack, 2008; Moser & Korstjens, 2017; Watt, 2007). More specifically, Wahyuni (2012) considers qualitative research as interpretivist (understanding social reality). Understanding and interpreting how IS managers develop and implement strategies makes the qualitative method and interpretive paradigm a stronger choice for this study. Ontology and epistemology define two existing constructs in social research (Wahyuni, 2012). Whereas an ontological construct can be described as reality being independent of the interpretations of actors within that reality, an epistemological construct is described as generating and understanding knowledge that is understood to be valid (Wahyuni, 2012). In this study, the intention was to understand and interpret the strategies IS managers use to improve employee IS compliance and therefore, an interpretive approach is more relevant. For that reason, an epistemological approach to research for this study aligns with a qualitative interpretive methodology.

Quantitative research is considered as positivist (objective understanding through scientific rigor) where reality is ordered and can be studied objectively (Moser & Korstjens, 2017). Quantitative research is inappropriate for this study due to the scientific approach of categorizing collected data and then analyzing the information numerically, which does not allow for interpretation and meaning behind decision making (Wahyuni,

2012). Barnham (2015) advances this line of thinking, stating that quantitative research does not allow for an understanding of how the connections between the collected data are perceived and interpreted.

A mixed method approach combines both a quantitative and qualitative methodology. Whereas positivism is applicable to quantitative methods and interpretivism is applicable to qualitative methods, postpositivism and pragmatism can also be applied to ontological and epistemological research. The focus of pragmatism is on the observable interaction between knowledge and action and although it can be applied to observable phenomena qualitatively, it is better suited with integrating different perspectives associated with a mixed-method study (Wahyuni, 2012). The intention of postpositivism is to seek understanding through inferences and although suitable for qualitative studies (Guba & Lincoln, 1985; Wahyuni, 2012), it is not applicable to this study as understanding and interpretation, not inference, is desired. Therefore, neither positivism nor postpositivism fit neatly with the epistemological viewpoint of this study, making mixed methods an inappropriate research method.

Research Design

A multiple case study design was appropriate for this qualitative study because there was a desire to understand and compare (Baxter & Jack, 2008; Houghton et al., 2013). The strategies IS managers of two different organizations use to improve employee IS compliance within a natural setting were compared. Both organizations serve different purposes but have employees working within each, so understanding the strategies uses in both companies may reveal good practices that can be shared

throughout the IS community. A multiple case study approach allows the researcher to study the differences between the two or more cases using interviews and documentation and compare the results. Yazan (2015) illustrated the importance of using multiple sources by underlying the need to gather as much data as possible to capture the complexity of the research in its entirety.

Narrative research describes the lives or experiences of individuals as told through their own stories (Berry, 2016; Lewis, 2015; Yang & Hsu, 2017). Narrative research design allows the ability to understand multiple perspectives and alternative viewpoints through one's own experiences (Long & Hall, 2018). This approach would be beneficial for understanding how all employees interact with their surroundings in a security setting and how a security culture may evolve. However, the intention of this research was to explore the strategies IS managers use to improve employee security compliance through training and policy, not the personal stories of each employee, making narrative research design an unsuitable choice for this study.

Phenomenological research is appropriate when the desire is to understand an individual's lived experience in a certain setting (Sloan & Bowe, 2015). A phenomenological study could provide interesting information in this context but is based on the researcher being present to observe and describe the experience (Bourne, 2015). As such, phenomenological research does not allow for the collection of information from available documentation, which was a valuable additional data source for this study. In addition to restricting the use of a valuable data source, focusing on an individual's lived experience will not provide enough understanding of the strategies IS officers

develop and implement to improve security compliance for the organization and therefore, phenomenological design was not an appropriate design choice (Bourne, 2015; Grossoehme, 2014; Sloan & Bowe, 2015).

Ethnographic studies are used to understand how certain events may impact a specific culture in a real-life setting and typically requires extended periods of observation in the field through conversations and workshops with participants (Suopajärvi, 2015). Ethnography has been used in information systems research and according to Baskerville and Myers (2015), allows for in-depth research by exposing the researcher to what people do as well as what they say. A benefit of ethnographic research using observation and interaction with the sample population, is that it provides multiple data sources that can help achieve data saturation (Conroy, 2017; Grossoehme, 2014; Suopajärvi, 2015). However, having the researcher inserted into the setting they are studying can make them part of the population under study versus being an unbiased observer. Understanding and observing the culture of an IT organization may provide interesting IS insights, however, that was not the intention of this research study making ethnography also an inappropriate design for this study.

Population and Sampling

The target population for this multiple qualitative case study consisted of IS managers of the security organizations within two technology firms located in Western New York. The selected population in a qualitative study should be comprised of participants that have the most in-depth knowledge and useful information of the topic under study (El-Masri, 2017). Therefore, in this study, the target population were eligible

representatives of the security organization of each firm that had direct knowledge and experience creating, implementing and managing IS strategies and policies within their respective organizations.

Determining the eligibility of participants to be included or excluded in the study was ascertained by asking demographics questions, such as their current role and experience in the IS industry, prior to beginning the interview. Malterud, Siersma, and Guassora (2016) determined that participants should be selected based on their knowledge and experience as it relates to the intended research question. It is equally important that the participants included in the study all share the same knowledge and skill set so responses to similar experiences can be obtained (Hossein, Shaharam, & Ali, 2015). The intended sample of IS managers will be expected to be employed within the IS technology department or division inside the parent organization.

A sample represents a subset of a population for the purpose of understanding the characteristics of the entire population (Gentles, Charles, Ploeg, & McKibbon, 2015). In research, there are generally two sampling techniques, probability and non-probability sampling (Setia, 2016). Setia classified probability sampling consisting of simple, random, systematic, stratified, and cluster sampling. Probability sampling is considered the most relevant technique to use when generalization of the results against the target population is required. The intent of this study was to understand how IS managers create and develop strategies to improve employee compliance for two technology firms in Western New York. Although generalizing the results may yield best practice behavior for the companies under study and may be applicable to others in the industry, it was not

the objective of this study and therefore probability sampling was not considered. Non-probability sampling includes convenience, purposive, quota, and snowball sampling and is a convenient and economic method for obtaining subjects (Carman, Clark, Wolf, & Moon, 2015). For this qualitative study, non-probability sampling will be used so a non-random sample from the defined population of IS managers were studied. Using non-random, convenience sampling can result in selection bias that may limit the generalizability of the study (El-Masri, 2017). Although Robinson (2014) warned against convenience sampling due to the limitations it may have on generalization, limiting the sample size to populations within the same geographic and demographic region favors convenience sampling due to the simplicity of choice. A small target population and anticipated time constraints of the participants were factors in the decision to use non-probability sampling.

Purposive sampling is similar to convenience sampling and is a non-random technique. However, purposive sampling is used to ensure all categories of the targeted population are represented (Robinson, 2014). For this study, there was only one category of the population of interest, the IS manager. In addition, purposive sampling can be used to get a unique perspective. Although individual perspectives in this area may be interesting, the primary interest of this study was to understand how the experience and knowledge of IS managers are used when creating IS strategies. Quota sampling is another variation of purposive sampling and is mainly used to determine if certain criteria about the participants is being met (Robinson, 2014). This study used a specific, non-random sample so quotas were not be necessary.

In snowball sampling, identified participants provide the names of other potential participants (Robinson, 2014). The primary goal of this study was to interview IS managers responsible for developing IS strategy. I established contact with the Chief Information Security Officer (CISO) of the target organizations. The CISOs acted as the gatekeeper and provided contact information for security managers within their organization willing to participate. Experience with the phenomena under study is necessary for understanding (Errasti-Ibarrondo et al., 2018). Therefore, the ideal candidate for my study was the chief information security officer (CISO) or someone in their chain of command, experienced in developing and implementing IS strategies and policies.

The population size for this study was three persons between two organizations. A sample size of one can be enough to achieve data saturation, although there is no rule for sample size (Boddy, 2016). Instead, Boddy reasoned that the homogeneity of the population and the anticipated depth of the interview are key factors. Most importantly, sample size should be representative of the population. In this study, the population was two security organizations responsible for developing and implementing security strategy and a sample size of three participants was a large portion of the population of managers in both security organizations.

Ethical Research

I conducted this research in an ethical and honest manner that did not harm any of the participants. All participants were provided a form detailing the informed consent process that also served as a confidentiality agreement (see Appendix D). Treating

participants with respect and earning their trust is fundamental to obtaining their consent for the study (Bromley, Mikesell, Jones, & Khodyakov, 2015). Honestly informing the participants about the nature of study, that participation was voluntary and confidential, and that they had the right to withdraw from the study at any time are key components in the consent process (Bromley et al., 2015). Participants were able to withdraw from the study in writing or verbally. If the participant withdraws from the study, any data collected from that participant will be immediately destroyed. I worked with the participants to ensure their confidentiality was protected. Beneficence is defined in the Belmont report as maximizing the benefits of the research while minimizing the risk to participants and is fundamental to ethical research (U.S. Department of Health & Human Services, 1979). Minimizing risk to participants was achieved through the informed consent process, which is a formal method used in research, provided in writing, to protect participant's privacy (Elsrud, Lalander, & Staaf, 2016). In addition, the Walden Institutional Review Board (IRB) required approval of any research proposal prior to initiating data collection. A formal submission was made to the Walden IRB board upon committee approval of this proposal and IRB approval was obtained (approval number **06-28-19-0542138**). As part of the consent process, I communicated with the participants how the data will be collected, how it will be used and studied, how long it will be kept confidential, and how the data will be destroyed when the confidentiality window expires or if they chose to withdraw from the study. The standard timeframe for keeping data confidential upon formal approval of the completed study is five years. During that time,

all digital data collected will be stored on a USB drive and locked in a fireproof safe along with any physical data collected. After five years, all data will be destroyed.

To ensure integrity throughout the process, no incentives were offered to the participants for their participation and therefore, participants were allowed to withdraw from the study at any time without penalty. Eliminating incentives allowed the participants to answer freely and avoid any conflicts of interest (Robinson, 2014). There were three participants for the study so masking their identity to ensure confidentiality did not present a challenge. The participants are referred to as manager A from Company A and manager B from Company B to distinguish between each other, but no other identifiable information was used. Grossoehme (2014) recommended protecting the identity of the participants throughout the study and not specifically associating the data collected with either participant to maintain privacy of the participants.

Data Collection

Instruments

I served as the primary data collection instrument for this multiple qualitative case study. Houghton et al. (2013) suggested researchers are prime candidates to be the primary data collection instrument in qualitative research because of their ability to gather data through interactions and interviews with the participants of the study. During the interview process, I asked questions using standardized open-ended interviews (Patton, 1990). Open-ended, semi-structured interviews are beneficial when the intention is to reduce the variation of results between interviewees. Reducing the variation of results between participants was useful in understanding how IS managers develop

strategies for improving employee IS compliance and reducing security breaches. A limitation of open-ended interviews is reduced flexibility and spontaneity during the interview and can be dependent on the skills of the interviewer (Patton, 1990). Based on the established interview protocol, answers provided by the participants during the interview stimulated follow-on questions and mitigated the limitation on flexibility and spontaneity. I developed a basic list of interview questions according to the interview protocol in Appendix D. I reviewed internal documentation as a secondary collection method to assist in validating information gathered during interviews (Boblin et al., 2013).

Data collected from interviews is considered primary data (Thomas, 2015) and data collected from alternative sources such as company documentation and internal websites is considered secondary data (Riegel & Dickson, 2016). Access to secondary data was a requirement for participation. In addition, alternative sources publicly available on the topic of IS strategies such as literature or external company websites were used as secondary data. Use of internal company documentation was helpful to confirm accuracy and validity of the interview data. Triangulation and member checking were also used to confirm and validate results (Johnson et al., 2017).

Morse (2015) suggested member checking allows the researcher to confirm the accuracy and reliability of the data collected by allowing participants in the study to confirm the researcher's interpretation of the collected data. Member checking also allows participants to add to both the interview and interpreted data, even several months after the interview was conducted (Birt, Scott, Cavers, Campbell, & Walter, 2016). By

using member checking, the researcher helps eliminate their own bias and personal knowledge by having participants confirm that their own meanings and perspectives are accurately captured (Birt et al., 2016). In performing the member checking exercise, Birt et al. explicate that the participant has the opportunity to not only validate the accuracy of the data but can also make adjustments based on current circumstances or add new information that was recalled during the review exercise. Additionally, the researcher can validate the data with other participants interviewed to ensure the data is accurate. Member checking can then both remove data no longer relevant and add new data based on the participants recollection of events triggered during the process.

The primary data collected through interviews was recorded on a digital voice recorder and later analyzed using NVivo transcription software. NVivo is considered computer assisted qualitative data analysis software (CAQDAS) allowing for character-based coding (Zamawe, 2015). Coding the transcript allows the researcher to create themes that can be further analyzed and discussed (Patel, Shah, & Shallcross, 2015). NVivo transcribes audio files into text files which can then be reviewed and compared with the audio files for accuracy, validity, and detailed analysis and correlations between themes (Zamawe, 2015). Once reviewed, the transcript files were summarized and provided to the participants for further member checking and validation.

Data Collection Technique

Data collection began once approval has been granted from Walden University's Institutional Review Board (IRB). The data collection technique used to collect the primary data adhered to the interview protocol in Appendix D. The interviews were open

and semi-structured and were recorded on a digital voice recorder. My mobile phone acted as a voice recorder backup to ensure all data was captured without a technical incident. The interviews were all face-to-face. Face-to-face interviews are preferred as they help develop a personal connection and allows the researcher to pick up on important non-verbal clues from the participant (Seitz, 2016). Conducting interviews in a familiar and comfortable setting helps relax the participant and creates an open atmosphere making it easier to share information (Gagnon, Jacob, & McCabe, 2015). There were no other resources such as computers or visual aids, used during the interview and the participants only needed to sign the initial consent form.

Anderson and Paterson (2015) recommend selecting secondary data that aligns with the research at hand. I worked with the gatekeeper and participants to identify documents, videos, training slides, or other artifacts relevant to the study. I worked with the participants to allow me to view the documents on site and in their presence at a time and place convenient for all parties and will make appropriate notes.

The interview was face-to-face and in a setting of the participant's choice, as this helped relax the participant and allowed for more detailed responses (Gagnon et al., 2015). The interviews were conducted according to the interview protocol included in the appendix (see Appendix D). The population size between both organizations was three persons for the individual in-depth interviews. Boddy (2016) explicated that a sample size of one can be enough to achieve data saturation, although there is no rule for sample size. Instead, Boddy reasoned that the homogeneity of the population and the anticipated depth of the interview are key factors. Most importantly, sample size should be

representative of the population. In this study, the population was a security organization responsible for developing and implementing security strategy and a sample size of three participants was a large portion of the population of managers in both security organizations. Interviews were conducted using sampling techniques applicable to the population under study. Smaller sample sizes with participants that are chosen based on their specific purpose should be studied intensely through interviews, member checking, secondary data analysis and confirmation, etc., until data saturation is reached (Malterud et al., 2016).

Saturation can be achieved by triangulating the data and the use of multiple data sources (Fusch & Ness, 2015; Watt, 2007). Triangulation occurs by collecting data qualitatively through interviews and member checking until no new information is generated. Triangulation was achieved by studying documentation associated with the participant and a current review of any available literature on the topic of study. The primary source of data for this study was interview data collected from the participants but internal documentation was also a data source. To achieve data saturation, participants must be added until no new information is generated (Svensson & Doumas, 2013). Face-to-face interviews using the same set of interview questions with each participant helped to expedite data saturation and provide a comfortable environment for participants to provide detailed responses (Fusch & Ness, 2015; Yin, 2014). The Company A participant was extremely knowledgeable on all topics within the IS organization and provided in-depth analysis on all questions so there was no need to continue with other participants as saturation within that organization had been reached.

For Company B, both participants were key stakeholders in their IS organization and also provided detailed answers to all interview questions resulting in saturation. At the point where no new information is generated from the interviews and documentation analysis, it will be assumed that data saturation has been reached (Fusch & Ness, 2015; Houghton et al., 2013; Svensson & Doumas, 2013).

All of the interview data collected was transcribed using NVivo software. Notes and questions were recorded in a journal throughout the process and were used for follow-up or clarification at the end each interview. The journal also recorded thoughts and ideas for the final study. Recording the interviews allows the researcher to return to the interview as many times as necessary to build a complete understanding of the data (Maher, Hadfield, Hutchings, & de Eyto, 2018). Part of the interview protocol included an introduction and brief overview of the study as well as time to establish rapport and make the participants comfortable prior to starting (Gagnon et al., 2015). At the conclusion of each interview, I provided the participant with the opportunity to contribute any additional information they may have regarding the topics discussed. I also asked each participant if there was any relevant documentation that was pertinent to the discussion. Member checking was explained at the conclusion of the interview and follow-up interviews were scheduled. Member checking improves the quality of the data collected as both the researcher and interviewee have an opportunity to clarify any outstanding discrepancies for accuracy (Houghton et al., 2013).

Data Organization Techniques

Organizing the data collected is crucial to enable the researcher to properly explain and share it. In addition, following good data organization habits can help reduce mistakes during analysis (Gorgolewski & Poldrack, 2016). Vaughn and Turner (2016) suggested in addition to using a systematic approach to organize the data, organizing the interview questions by themes can help during the coding and analysis phase. Using an interview protocol also helps maintain structure during the data collection and analysis phases (Sarma, 2015). For this study, I interviewed three people, one from Company A and two from Company B, using an established interview protocol (see Appendix D) to maintain structure and keep the data organized. Secondary data consisted of documentation, videos, and journal entries, etc. I used a systematic approach to organize the data by creating digital folders on a password protected flash drive for each organization involved in the study such as Company A, Company B, etc. I then created directories under each company folder for each participant (eg., participant A, participant B, etc). All digital interview and secondary data collected was also stored under the appropriate participant folder and named CompAParticA, CompBParticB. The descriptive metadata of the participants was masked in a password protected spreadsheet to avoid mixing participant data and confidentiality issues. When the flash drive was not in use, it was securely locked in a file cabinet or safe along with any physical data such as signed consent forms or documentation related to the study. I was the only one with a key to the safe. All data collected for this study will be stored for five years. At that time, all

data related to the study will be destroyed. Hard copy paper artifacts will be shredded, and all electronic data will be deleted.

Data Analysis Technique

Data analysis in qualitative research can be considered as an iterative, interrelated process and can be enhanced using more than one analytic procedure (Kerwin-Boudreau & Butler-Kisber, 2016). I analyzed the data collected in this study through the lens of information theory and the influence institutional isomorphism may have on IS strategy development. Coercive, mimetic, and normative mechanisms are fundamental to institutional isomorphism. Two of the three mechanisms played a significant role in strategy development and how IS managers respond to uncertainty and the potential influence mimetic isomorphism has on the development of security compliance strategies. Belotto (2018) suggested labeling passages within the data with terms related to the research questions, which is consistent with Vaughn and Turner (2016). I have organized the literature review into the following sub-themes that influence strategy: human element, awareness, training, and culture. I used these themes to organize the interview questions and as the basis for my initial analysis. I also used NVivo and its coding tools to analyze the interview data further to determine if other themes may be exposed.

NVivo allows the researcher to transcribe audio files into text that allows the researcher to discover concepts and themes through text or word frequency searches. The coding feature of NVivo allows the researcher to gather all the references to a specific question or topic. As an example, many of my interview questions center on developing

and implementing IS strategies. Categorizing the responses to these questions using NVivo software identified patterns or themes in the data that was not easily identifiable using standard techniques such as reading the text or listening to the audio files. Analyzing the patterns identified by NVivo helped establish correlations within the data and identify potentially new themes. Categorizing and analyzing patterns with NVivo helped create word clouds and frequency diagrams to determine consistency between participant responses. I compared the concepts and patterns NVivo discovered to the themes I created during the literature review. There were no new patterns or key themes identified by the NVivo software. In addition to using thematic analysis techniques outlined here, Houghton & Houghton (2018) recommended reviewing the interview transcripts a minimum of three times to gain a deeper understanding of the data and recommend keeping a reflective diary or journal to capture thoughts and assumptions during the process. I did review the transcripts 2-3 times during the conversion process to ensure I had captured the participant's responses accurately. I used a notebook to capture ideas or questions during the process. A diary can help to capture information has it happens and provide access to specific events (Snowden, 2015). To limit researcher bias in the findings, Leggette and Redwine (2016) explicated that limiting subjectivity and bias can be achieved by allowing the participant to be part of the phenomenon. By expressing the participant's viewpoint of the data and clearly demonstrating any interpretations of the data are those of the participant, there is less room for interpretation from the researcher. I used member-checked versions of transcriptions from interviews rather than the original transcriptions to limit bias as the data was reviewed and approved

by the participant. By following this process, I did not insert my own opinions into the data analysis. To ensure integrity of the data, I only analyzed what was collected via the data collection methods used for this study.

Data triangulation is a procedure that can be used to help achieve accuracy, reliability and saturation and is commonly used in qualitative data analysis. Triangulation occurs by collecting data qualitatively through interviews and member checking until no new information is generated, helping to improve the overall validity of the data using numerous sources (Fusch & Ness, 2015). In addition to interviews and member checking, I performed a comprehensive review of organizational documentation associated with the interviewee and a current review of any available literature on the topic of study as part of the triangulation process. There are multiple types of triangulation used in qualitative research; method, investigator, theory, and data source (Johnson et al., 2017). A combination of method and data source triangulation will be used in this study as data will be collected using interviews of IS managers, analyzing available literature and organizational documentation. Interviews were conducted using sampling techniques applicable to the population under study. Method triangulation involves using mutliple methods of data collection such as interviews and observations. Data source triangulation involves the collection of data from different types of people to gain multiple perspectives. The other two types of triangulation, investigator and theory triangulation, are not applicable to this specific study and will not be used. Investigator triangulation involves using multiple researchers and theory triangulation refers to the use of different

theories in analyzing the data and also does not apply to this study as a single framework, institutional theory, was be applied.

Although triangulation can help achieve consistent and reliable results, Fusch and Ness (2015) warned that it can sometimes lead to inconsistent results due to the variety of sources used, so the researcher must remain cognizant as they synthesize the results for the reader. Ensuring reliable results that are consistent across all data collection processes is critical (Houghton et al., 2013). In addition to using data triangulation, member checking, and literature reviews to ensure data saturation, I implemented the interview protocol in Appendix D to guarantee the same process and questions are used for all participants (Grossoehme, 2014).

Reliability and Validity

In qualitative research, reliability and validity are two essential elements when determining overall rigor (Grossoehme, 2014). Validity can be considered as the measure of the finished product of the research and whether or not that final product represents what it claimed to represent or how accurate it is (Lancaster et al., 2015). Reliability of the results is synonymous with repeatability and is the measure of how repeatable the results would be if another researcher attempted to duplicate the study. Addressing reliability and validity at all phases of the study is essential (Houghton et al., 2013; Patton, 1990). The use of an interview protocol where all participants are asked the same questions within a common timeframe is an important starting point for establishing consistency and repeatability (Lancaster et al., 2015). In addition to using an interview

protocol, member checking is also a tool researchers can use to establish reliability within a study.

Guba and Lincoln (1985) established a list of criteria researchers can use when determining the rigor of their research. Houghton et al. (2013) summarized these criteria as credibility, dependability, confirmability and transferability. Credible research is conducted in a believable manner and is considered internally valid if the research design to be used has withstood the scrutiny of review and has been proven to not include any errors (Lancaster et al., 2015). To help establish credibility and ensure data saturation, I used member checking, observation and triangulation as tools during the analysis phase (Morse, 2015). Member checking is considered the most significant technique in establishing credibility as it allows the participants to confirm the accuracy of the data collected so both the researcher and participant agree (Guba & Lincoln, 1985).

Dependability in qualitative research is often referred to as how stable the data are (Houghton et al., 2013). Dependability is also considered equivalent to reliability and is commonly achieved through use of triangulation (Morse, 2015). Using member checking and triangulation to ensure the reliability and integrity of the research only enhances dependability (Guba & Lincoln, 1985). Another useful tool researchers can use to establish dependability is an audit trail (Houghton et al., 2013). Audit trails can be used to track decisions made during the process and provide clarity into why specific decisions were made during the research process. In addition to an informal journal I have kept during the process with questions and notes, the prospectus, proposal, and literature review matrix captures decisions and rationale used throughout. The audit trail details

how data will be collected and analyzed and the strategy for coding the data into themes for ease of analysis. NVivo software was used during the data analysis phase and provided a trail of the decisions made during the analysis process as well as assisting in achieving confirmability (Houghton et al., 2013).

Confirmability is similar to dependability and refers to the accuracy and objectivity of the process (Houghton et al., 2013). Objectivity is considered similar to dependability, where triangulation and an audit trail can be used to confirm that data collected is accurate and relevant to the study (Houghton et al., 2013; Morse, 2015). Taking detailed notes during the analysis process can help during member checking and limit researcher bias (Connelly, 2016). NVivo can help achieve confirmability through use of comparison analysis and identifying recurring themes within the data to confirm saturation. Establishing credibility, dependability and confirmability of the research helps preserve information from the completed study and establish a foundation for transferring the findings to a similar context.

Whether or not research results can be transferred to a similar context or situation is considered transferability (Houghton et al., 2013). To be considered transferrable to another context, the meanings and conclusions of the study would need to transfer as well. In the context of this study, information and conclusions regarding how IS managers develop and implement strategies to improve employee compliance may be applicable to the development and implementation of other compliant related strategies such as HIPAA implementation. Describing the research so readers can determine if the findings are transferrable is the responsibility of the researcher (Guba & Lincoln, 1985).

Researchers should detail the context, methods, and provide examples of raw data when describing the research to allow for a rich description of the findings so anyone considering the results can make an informed decision (Boblin et al., 2013; Guba & Lincoln, 1985). The final study will include a detailed analysis of the data, trends or themes identified, how the conceptual framework applied and how the organizations under study compare. By comparing the results and providing a detailed description of similarities within the data, transferability can be established.

Transition and Summary

Section 2 restated the purpose statement, and provided information on the participants, sample, and research methodology decisions made in regard to my study. The section also addressed ethics and steps taken by the researcher to mitigate such any potential risks while focusing on reliability and validity of the study. The section also described the approaches taken for data collection, data organization, and data analysis.

Section 3 presents the findings from my research study, describes applications for professional practice, implications for social change, recommendations for future works, and offers reflections from the study conducted.

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 IS managers use to improve employee compliance with security training and policy. I collected data from three individuals at two IS organizations in Western New York, comparing the data and interview results between both organizations. I interviewed one senior IS manager from Company A and two senior IS managers from Company B. The data collected revealed that both organizations operate in heavily regulated industries. All participants indicated that adhering to regulations is a significant factor in developing and implementing effective IS strategies and helped lay the groundwork for new IS policies and procedures. As part of their strategy, each participant expressed the importance of senior leadership support when developing IS programs regarding policy, training and awareness, culture, and compliance. Both companies have been successful in establishing policy, creating and implementing training and awareness programs, and establishing the foundations for a strong security culture. All participants admitted that establishing a cohesive strategy and building a strong security culture across a large organization has presented challenges, and it is a slow process but one that is gaining traction with the support of senior leadership. One area of opportunity highlighted by both organizations is metrics and measurement of employee compliance with policy. Neither organization has established processes for measuring and reporting employee compliance but see it as an area of opportunity.

The sample size for this study was three primary individuals, two of whom were members of the executive leadership team as deputy CISO and CISOs respectively within their organizations. The IS leaders I interviewed were part of a management group with direct reports that had decision responsibility regarding IS, training, and awareness strategies within their respective organizations. In this study, the population was three individuals within two security organizations responsible for developing and implementing security strategies, and a sample size of three participants represented a large portion of the population of managers in both security organizations. I also performed member checking with all three individuals and reviewed IS policy-related documents such as data classification policy documents, acceptable use policies, regulatory documents, and training and security videos. In this study, I used institutional isomorphism theory as the conceptual framework to explore strategies used by organizations to address employee compliance with IS training and awareness policies at the institutional level and close the knowledge gap in available literature.

Data collection was done using semi structured interviews and documentation reviews of materials pertaining to IS training and awareness policies. I used semi structured interviews to ask detailed questions, allowing each participant to discuss and clarify their views. Company documents from the organizations provided triangulation of data that helped provide confirmation and clarification of policies and procedures discussed during the interviews. Company documents included PowerPoint presentations, policy and procedural documentation, training documents, and training videos. Interview

responses were recorded, converted to text, and then loaded into NVivo software, which helped categorize themes from participants' responses.

Presentation of the Findings

The research question that guided this research was: What strategies do IT security managers use to improve employee compliance with security training and policy in order to minimize the risk of security breaches? I used institutional theory and isomorphism as the theoretical frameworks for this study because I wanted to understand if IS organizations practice any of the concepts as outlined within the institutional theory. I found that although there was not a conscious effort to understand and implement institutional theory as part of each organization's IS strategy, there was strong evidence both companies practice isomorphism as part of their overall strategy. Hwang and Choi (2017) found that by developing good habits and mimicking successful organizations, an organization can improve their own culture and norms, thereby increasing their own legitimacy.

Both organizations are required to comply with external regulations within their industry, thereby adhering to coercive forces. Each company is comprised of two separate organizations that have challenges in terms of developing and implementing cohesive companywide strategies. There was little evidence of normative pressures within either organization, but as the interview questions were focused on uncovering evidence of coercive and mimetic forces, the lack of evidence of normative pressure was not unexpected.

Based on the literature review and research question, I was interested in determining if three primary themes would emerge from the data: IS policy, training, and compliance. After converting the interview recordings to text, sanitizing files to remove filler words, time markers, and nonessential discussion, the cleaned file was then put into NVivo for further analysis. Policy and training and awareness were two of the primary areas that emerged from the data along with culture and compliance. The human element, which was a common theme in literature referring to human behavior and actions within an IS community, is certainly an area of concern with both companies, but did not emerge as a specifically discussed issue in the context of behavioral theory. There was no specific effort given to applying any type of behaviorial theories to better understand what motivates or does not motivate employees to comply with policy. Neither organization is staffed to be able to consider that level of analysis. The human factor was implied throughout the interview process by all participants as they discussed establishing policies to guard against human error and negligence. Each company is focused on implementing policies, procedures, and technologies to help prevent the human element from becoming a constant security concern.

All three participants acknowledged that policy and training are key factors in developing and implementing comprehensive IS strategies consistent with current literature. Both companies have strategies in place to manage short and long term IS needs. Company A has a mature IS organization that has been developing and growing their IS policies and procedures for over 12 years and has a fundamental strategy for how to continue to develop and implement new IS policies and procedures. Company B is a

newer organization that is in the process of building up their security team as part of a company merger but also has a strategy in place. It is in the process of evaluating, updating, and replacing legacy policies and procedures. In most cases, legacy policies were not conducive to good security habits, and therefore new CISOs are focused on establishing a baseline with IS acceptable use policies while at the same time developing and implementing security awareness training. Although compliance did not emerge as a frequently discussed topic, it was discussed and is very much part of both companies' overall strategy, as compliance with laws and regulations are required in each of their industries (see Figure 2). Compliance is among the frequently mentioned words, but not as significantly as security, policy, and training.

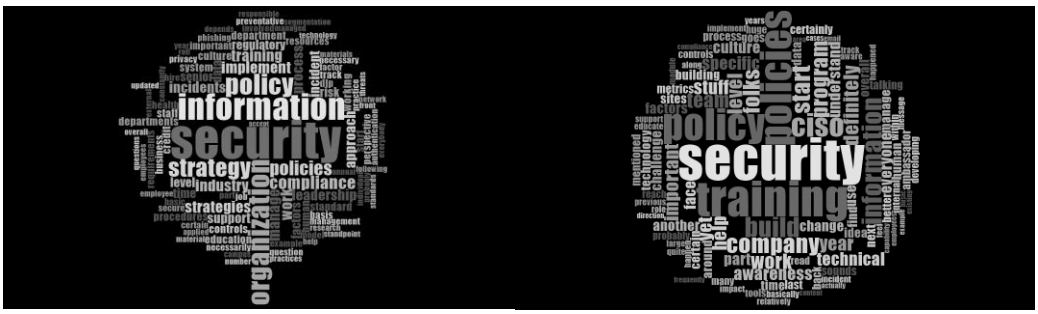

Figure 2. Word cloud comparison.

Theme 1: A Long-Term Security Strategy Begins with Strong Policy

IS policy consistently emerged as an important factor for both organizations as part of their overall security strategy. Both organizations are in the process of developing a company-wide security strategy by redesigning existing policies and procedures based on business needs. As one manager explained, "we want to be the central point of management from a security perspective…to support all that is the underlying policy."

This was confirmed through triangulation of not only current literature but also the amount of secondary data collected from both companies that documented the various policies available for employees. A second manager expressed the importance of establishing and publishing a stable policy, explaining that in doing so "they can set the tone for the organization and provide the ability to enforce compliance". All three participants agreed that establishing processes and policies that encompass the entire company is the long-term strategy (see Table 1). Each organization is heavily regulated and compliance with external and internal regulatory policies is a requirement. Although Company A is further down the path of their long-term strategy with more established training and policies, Company B has a methodological strategy in place to grow their security organization. Both companies have an internal website dedicated to training and policy documentation. Due to their maturity level, in addition to policy documents, Company A's site also includes additional information on training, security tips, and how-to videos. While Company B does have associated documentation on an internal website, it is currently focused on establishing and formalizing a policy baseline so it can communicate what is allowable within the organization.

Table 1

Frequency of references to policy in participant responses and documentation

	Participant		**Document**	
Major Theme	Count	References	Count	References
A Long-Term Security Strategy	3	28	33	2800+

Begins with
Strong Policy

Studies by Chua et al. (2018) and Manworren et al. (2016) explained that employee ignorance and non-compliance with policy are key factors in security breaches. Establishing a policy is critical so employees and management know what they are supposed to do. Training and awareness of new policies can also help reduce or eliminate ignorance. Chua et al. (2018) and Youn (2009) confirmed in their studies that policy awareness and compliance were higher in regulated industries, which was confirmed through these interviews as well. Employees who work in regulated industries are more aware and comfortable in complying with policies. The challenge both companies face is managing uncertainty in a constantly evolving environment. In both companies, new policy and policy updates are governed through an executive committee. Policy updates are primarily driven by new regulations, a security incident not currently covered by policy, or industry best practice. All updates are designed to align with current company policy. The adoption of new technology is also a driving factor in modifying policy. Fundamental to each company's strategy is to make IS pervasive throughout the entire company and ensure compliance with basic acceptable use policies. In addition, implementing technical controls wherever possible to help mitigate the risk of the human element and to help enhance policy coverage in areas that might be understaffed, is also part of the overall strategy.

Angst et al. (2017) cited institutional theory to distinguish between symbolic and substantive adoption of practices. Adopting a policy symbolically to only gain legitimacy

is not a long-term strategy in a regulated industry. Both companies showed significant evidence of substantive adoption of policy, where there was form (policies) with substance (adoption of those polices). Adopting these policies across the organization is evidence of mimetic isomorphism and maps to an outcome-based imitation as shown in Figure 1. This outcome-based imitation is a byproduct of working in a highly regulated industry where culture, behavioral framework and regulations drive strategy and policy and is consistent with the study conducted by Sherer et al. (2016), which studied the impact of institutional environmental conditions on an organization. While the primary strategy for both companies is to increase standardization and coherency across the entire company, Company B is still growing and maturing. It is focused on the short-term strategy of making employees aware of the new IS and policies, changing the mindset of product development to include security as part of their products, and installing technical and security checkpoints that meet both regulatory and customer requirements. Company B also utilizes the National Institute of Standards and Technology (NIST) for an IS framework and is establishing governance and executive roles within the company to help manage and implement their overall IS strategy.

As Bjorck (2004) posited, security with information systems depends on the users of the system. Adopting new policy does involve risk and uncertainty (Schilke, 2018). Implementing institutional isomorphism can help mitigate uncertainty (DiMaggio & Powell, 1983). The need to launch a product can sometimes override the need to comply with a new policy. Current literature suggests individuals make a threat assessment based on the risk of not following policy or the effort it will take to follow policy (Aurigemma,

& Mattson, 2017; Stanton et al., 2016; Thompson et al., 2017). Both executive participants noted a similar philosophy in managing risk. Appropriate risk is accepted based on lack of resources in some cases but also allows for autonomy within the network for employees to follow policy. There are simply too many issues to manage with limited resources, so a risk assessment is done, and a decision is made. Understanding behavioral theories such as Planned Behavior Theory (PBT), Planned Motivation Theory (PMT) and the Theory of Reasoned Action (TRA) have the potential to better understand employees and how they might react to implementing certain policies. However, this is another labor-intensive area and an opportunity for IS organizations.

The socialization of users within the system on how to act, what policies and procedures to follow, for example, are part of an institutionalization within the organization that is reproduced across the company and results in a patterned behavior. As a result of Company A being more mature, there was more evidence of institutionalization than Company B. However, Company B understands the need to institutionalize their policies and has a strategy in place. A study by Andrews-Speed (2016) highlighted a three phased process involved in an organization becoming institutionalized. In the beginning phase, there is a layering that occurs where existing processes and procedures are modified or added to. In the second phase, new goals or actors are added that help change or enhance the institution. The third phase is when drift occurs as complacency with existing policies starts to set in. The first two stages are occurring with Company B. Company A indicated evidence of the third phase occurring

with certain groups and was working on training and awareness to mitigate this type of drift. Training and awareness have consistently been shown to combat complacency (Chua et al., 2018; Manworren et al., 2016; Torten et al., 2018). Company B's current focus is on employee awareness and training with the new policies and procedures, aligning with phase one and two of Andrews-Speed's (2016) study. All three participants have established a reputation across the company as someone who is willing to give seminars or lectures to whoever will listen or asks for their help to counteract complacency.

Theme 2: A Cohesive Information Security Training and Awareness Program is Necessary for Reducing Risk

Training and awareness of IS policy and procedures emerged as an important theme from both organizations. Once an established and cohesive policy is put in place, it is necessary to train employees on those policies. One security manager interviewed explained that when developing an overall training and awareness program, "it should align with existing policy." Another security manager interviewed highlighted the risk associated with the lack of attention to IS policy. By helping employees understand the risks of not following policy through training and awareness, IS managers communicate that "what they are doing is what they believe is best for the firm." The importance of training and awareness was validated through a triangulation of participant interviews, member checking, secondary documentation review, and current literature review.

All participants agreed that establishing consistent policies across the organization with appropriate training and awareness presents a risk-based approach. Providing

consistent policies and procedures helps limit the overall risk by evaluating incidents against policy. When an incident occurs that is not covered by existing policy, that policy is updated and added to the training modules. If an incident occurs and there is existing policy, individuals will be referred to the associated policy and potentially be required to revisit certain training modules. Consistent with current literature, both companies understand the importance of role-based training. Each company serves different customers, have different employee profiles, and therefore have tailored their training programs appropriately. Company B is working on segmenting the training along specific departmental lines whereas Company A has established fundamental training but has also given individual departments some autonomy and latitude on training their individual employees in department specific areas. Different areas are constrained by different regulations, so Company A maintains a general IS policy site that includes both company-wide polices as well as regulation specific polices, videos, and tips on the various security risks associated with their industry.

When comparing the training and awareness programs of each company with current literature, there was strong evidence of alignment with current theory. Designing an IS program should follow four basic principles, according to Curran (2015), a) begin any training program by educating the employees of the IS program itself, b) communicate management's commitment to the training, c) communicate the regulatory and organizational compliance policies and, d) develop and communicate the penalty for non-compliance. Both companies have a strong commitment to educating new employees with an onboarding process that includes privacy and IS training (see Table 2). The three

participants mentioned training or awareness 20 times during the interviews. Participant two of company two mentioned training or awareness 12 times during the interview, which was not surprising as this person was primarily responsible for developing and implementing the training programs. Although training and awareness were frequently mentioned by all participants, the documentation itself did not specifically mention the words training and awareness as the policy and training documents were part of the training and awareness process. Each company has a strong commitment to IS with established CISO's. Each CISO has executive authority and is actively involved in developing and communicating IS strategy and policy. Having senior leadership support and commitment is also cited by Ki-Aries and Faily (2017) as a critical factor in establishing trust and building a strong security culture.

Table 2

Frequency of references to security training and awareness in participant responses and documentation

	Participant		**Document**	
Major Theme	Count	References	Count	References
A Cohesive Information Security Training and Awareness Program is Necessary for Reducing Risk	3	20	33	33

Company A implements more of a push/pull strategy to communicate their security policies and procedures. It employs various push techniques such as monthly

email reminders, security newsletters with security tips, and it has also established a website that includes videos that visualize key tips and issues so employees can pull information as needed. Company B utilizes the NIST framework as their backdrop for training and policy development to take advantage of established principles and techniques. Company B's goal is to have a training module that is general for every employee and then build on that training to develop role-based training based on department needs, data access requirements, job classification, and other role specific areas. This is consistent with current literature suggesting a comprehensive IS training program should avoid a generic, one-size-fits-all approach and develop training and awareness programs specific to groups or individuals depending on technical ability and industry regulated requirements (Curran, 2015). Öğütçü et al. (2016) also recommend developing processes and policies specific to the employee's role in the organization. Role-based training is in the developing stages at Company B as it believes it helps focus the training on the specific environment of the employee instead of trying to generalize it across the company. Like Company A, Company B's CISO has found that face-to-face training can be more effective than computer-based training. Being available in person establishes the importance of the training. It allows for real-time questions and answers and allows the trainer to help understand the audience and who may or may not be actively engaged. Both companies understand the need for training on a regular basis, consistent with Safa et al. (2016), which suggested training on a more frequent basis than once a year. This also aligns with the study by Ki-Aries and Faily (2017) that suggested creating creative ways to communicate IS policies and procedures can help improve

compliance. How the training modules are written can also have an impact on the effectiveness. Both companies understand the need to use simply worded training and policy procedures to avoid confusion or misinterpretation across a multicultural community.

The Department of Homeland Security (DHS) considers training to be an effective tool in managing IS risk and poor compliance. The use of institutional isomorphism is something IS managers can take advantage of when establishing and implementing IS training programs. Establishing a transparent and open environment for learning can build trust and improve the effectiveness of a training program (Andrews-Speed, 2016). Establishing trust and transparency was apparent in both organizations. All three participants understand the need to constantly communicate, help people understand the need for new policies and procedures, and make themselves available for consultation whenever requested. Increasing the awareness by positively framing the message both in person and through training was also advocated in a study by de Bruijn and Janssen (2017).

IS education, training, and awareness all have a slightly different meaning according to Curran (2015). Education uses a mix of active and passive instruction to build skills. Training is done through passive testing techniques, and awareness is done through dialogue and collaboration. Both companies use all of these as part of their repertoire in developing their IS training programs. Educating the users on the risks of poor security habits is achieved with onboarding and annual programs. Training is achieved through reinforcement of policy and active testing such as phishing campaigns,

where users are exposed to insecure situations they need to react to. Most prevalent in each company was the emphasis on awareness through documented policies and procedures, internal websites, and security campaigns. Another important technique each company uses is live training, where people can see the presenter in person, ask questions and get answers in real-time. This is advocated in current literature in a study by Curran (2015) that suggests focusing on dialogue and collaboration can build trust and change behavior.

Building trust within an organization can help form the basis of an effective security culture according to Kearney and Kruger (2016). In addition, programs that have cooperating employees and strong IS coordination and technical expertise prove to be a strong security organization (Bartnes et al., 2016). Each organization showed strong evidence of these attributes. Although Company A is more mature and has a well-established program, it still suffers from personnel challenges where certain departments or employees resist IS training efforts. This is where executive leadership is making a difference. Through patience and continued coordination and dialogue, Company A is making headway. Company B has similar issues. It is building the program essentially from the ground up, but Executive leadership is fully onboard and understands the need for collaboration and dialogue. It also has departments that are slow to implement policies, but the participants interviewed are making progress by making themselves available in person, travelling to tell the story and are part of the executive leadership within the company that helps their legitimacy.

In their study on IS training, Bauer et al. (2017) recommend a four phased approach to building a strong security program. The authors believe that communicating the risks and threats through examples can get people's attention to the seriousness of IS. Executives at both companies employ this through their risk-management process. Executive A communicates through person-to-person dialogues and conferences and executive B communicates more directly with those impacted by clearly outlining the risk if certain procedures are not followed and the impact it will have on the company. If the decision is to move forward against this advice, the risk is at least documented and managed. The second phase centers around metrics that can be established and tracked to make evaluations on overall compliance and effectiveness of the training and awareness programs. Both companies realize the necessity and importance of metrics and see this as an area of opportunity. There are some metrics being gathered but more are necessary and need to be tracked. The third phase is establishing a mechanism for employees to provide feedback for constant improvement of the IS program. Neither company has a dedicated feedback mechanism in place but through openness and communication, both have established channels where department heads or employees can provide input to the process. The last phase recommended by Bauer et al. (2017) is to customize the training and awareness programs based on the user's skill level, area of responsibility, etc. and as discussed earlier, this is consistent with what both companies are striving for. All these phases can help build a security program and form the basis for a strong security culture.

Theme 3: Establishing an Information Security Culture is a Necessary Part of Any Security Program

Establishing a security culture within an organization begins with senior leadership, according to the participants interviewed. One senior manager interviewed stated that "security culture is established by senior leadership. They either accept or don't accept IS strategy. If they accept it, they are promoters." Having senior management being promoters of IS "is the most important part of the culture." Senior leadership promotes the importance of IS throughout the organization, they make employees aware of the various initiatives within the organization, and they help set the tone of what to expect within the organization in relation to IS. Both senior managers interviewed, along with the triangulation of sources of current literature and documentation review, confirmed the importance of senior leadership support. The senior managers practice this theory themselves. The senior managers explained their approach to communicating with the organization as needing to consistently make themselves available through seminars, in person and group consultations, and traveling to different sites to promote policy and help establish culture. In addition to strong senior leadership support, Company A has an established IS program with fully documented policies, videos, training and awareness programs, and other documentation, that has created the fundamentals for a strong security culture. Company B also has strong senior leadership support and is focusing on developing fundamental policies and training programs that will form the basis for a strong security culture.

Culture is defined as a set of shared attitudes, values, goals, and practices that characterize an institution. Current literature suggests institutional theory has been used to help shape organizational culture. Andrews-Speed (2016) highlighted four different

areas of institutionalism: rational choice applicable to economic considerations, historical when managing power within an organization, sociological when focusing on culture, and discursive which attempts to understand the various ideas and discourse within the organization. In the context of culture within an organization, the sociological area of institutionalism is the most relevant to this study. IS managers play a significant role in shaping culture through mimetic isomorphism and the adoption of substantive policies.

Both companies operate in a highly regulated environment and applying coercive pressure on the organization has helped form the basis for a security culture. In addition, customers are becoming more security conscious or must comply with their own industries regulations. This is creating more demand for security within the product itself. While Company A has a more mature, established security organization, Company B is growing theirs by taking advantage of a known IS framework in NIST. Using an established IS framework adds legitimacy, can have a positive effect on an employee's security behavior, and can help reduce internal threats (AlHogail, 2015).

The people or users of the systems are fundamental to creating a strong security culture. Current literature suggests that the goal of an organization is to create a culture that becomes embedded within the employee to a point where it can positively influence their behavior (da Veiga & Martins, 2017). Both organizations discussed how creating a culture is challenging and will take time, but both are seeing positive change. Understanding the different attitudes and behaviors of employees is also something current literature suggests. However, the biggest influence in creating and sustaining a strong IS culture is senior leadership support and their acceptance of owning it, according

to da Veiga and Martins (2017). This was supported by both executive participants as they fully understand their role in developing culture. Both participants agreed that security culture begins with senior leadership, that buy-in from the top creates support, helps promote security policies and initiatives, and sets the overall tone for the organization. Most importantly, according to both executive participants, establishing trust between senior leadership and the employees is critical for implementing policy.

Personal motivation can sometimes be a barrier to culture and implementing policy. Both companies are dealing with this within their organizations. Company A has a unique setup in that it is essentially two organizations within one company with each side dedicated to separate goals. The challenge has been making a universal policy for both entities and getting each organization to conform. There are basic policies that must be followed while others are left to the authority and management of individual departments. Company B also has two organizations but both sides are working toward the same goal. The operations side of the business is more in tune with security policies whereas the product development side has been slower to adapt. The primary issue is motivation. Product development personnel are motivated more by schedule and monetary gains than conforming to policy. This has presented challenges for executive participant B but through constant communication and leadership, they are changing attitudes and culture. At the core of the issue is that employees are trying to do what is best for the organization and conforming to policies that are designed to protect them and the company is new to them and has taken time to get everyone aligned.

Creating a positive experience within the organization also plays a significant role

in building a successful culture. Both de Bruijn and Janssen (2017) and Tsohou et al. (2015) highlighted a positive environment as a critical piece in developing culture. Company A has established a positive culture by providing light-hearted creative videos on different security tips. It has also created a newsletter and email campaign to highlight security issues and concerns in a positive way. Company B is using a different approach in building their culture. It is creating the foundations of a strong security culture by developing process, standards and policies as part of their training and awareness focus by using the NIST framework. This method is consistent with recommendations made in current literature by Safa et al. (2016). An additional study by Flowerday and Tuyikeze (2016) recommends including risk assessment as part of the culture as well. This directly maps to both organizations as risk is assessed and managed daily. Conforming to regulations is absolute but other risks are managed and assessed as necessary.

Each company has been identified as having two internal organizations. Company A has two disparate organizations that must conform to basic policies. Company B has two organizations that were previously governed under legacy policies and processes as two primarily independent organizations that now must become one. In each case, there are subcultures present. Both companies have or are establishing a company-wide culture. However, both companies show evidence of subcultures consistent with a study by da Veiga and Martins (2017). In their study, those authors found evidence that subcultures exist within larger organizations that consist of smaller groups of employees. Subcultures exist within departments that have developed their own norms and values over the years and can be a barrier to adopting a dominant company culture. In each

company, the process has not been to force culture onto each subculture but to understand their needs and issues and to manage the risk of them not entirely following company policy. In some cases, explaining the necessity of a new policy has helped transform the subculture and in other cases, it has been managed as an acceptable risk depending on the issue. In large companies, choosing the battles and managing the risk is more effective than trying to fight and win every battle. There are just not enough resources to manage every issue and trying to manage every issue takes away from important policy development and implementation.

A study by Dhillon et al. (2016) suggests that a strong security culture is an effective mechanism in protecting sensitive information. However, creating and sustaining a strong security culture in times of rapid change can be a challenge for IS managers, according to a study by da Veiga and Martins (2015). To manage change while building a culture, strong leadership with effective communication skills is necessary. All participants understand the need for effective communication and have mechanisms in place such as newsletters, regular emails, and seminars to consistently communicate with employees. In addition to strong communication skills, building a strong security culture requires consistent and sustained action by IS managers. A current study by da Veiga and Martins (2017) confirms that when IS managers are involved and remain focused on the measurement and control of IS, employees notice and stay engaged, helping to reinforce the culture. Employee engagement was apparent with all participants of this study, as the leadership teams were building their security culture through awareness campaigns, constant communication and presence, and continued commitment.

A common theme in current literature when building a security culture is that employees tend to believe that IS is the responsibility of management, that they own it and control it. While it is true that top-down leadership is effective in this area, a study by da Veiga and Martins (2017) found that a strong and effective security culture is the result of everyone being involved and responsible for security, not just management. Although both companies expressed challenges in this area, it was clear that progress was being made by developing policies and awareness campaigns that engage employees, involve them in the process, and constantly stress the importance of IS through various mechanisms. Doherty and Tajuddin (2018) suggest that individuals are more likely to comply with policy if they are aware of the value of the information that they are responsible for. While not specifically aware of Doherty and Tajuddin's study, all participants interviewed understood this at some level. Access to information was typically restricted on a need-to-know basis, creating an atmosphere in both companies that emphasized the importance of the information people are responsible for. Doherty and Tajuddin (2018) posited that when someone understands the value of the information, they are responsible for, the more likely they are to comply with policy.

Theme 4: Improving Compliance Can Help Reduce the Number of Security Incidents

Establishing IS policies, training and awareness, and a strong security culture are fundamental elements for improving compliance with IS policies and procedures. Both companies develop IS strategy based on three fundamental principles: regulatory requirements, incident-based events, and industry best practices. By using this approach,

Company A was able to implement two-factor authentication (2FA) within a few months based on an incident occurring within the organization. As the senior manager explained, “we've tried to leverage incidents that have adversely affected the organization or nearly adversely affected the organization and to leverage those to implement strategies.” While not quantifiable on how many incidents occurred due to this event, by implementing 2FA, the company closed a security gap that existed previously. Employees now must comply with the 2FA policy and the possibility of the incident that precipitated the policy from happening again has been greatly reduced.

Reducing incidents by complying with policy is also consistent with current literature. Manworren et al. (2016) found that 59% of all security incidents were human related, of which 23% were related to phishing. The study revealed that developing effective security strategies that improve policy compliance through training and awareness, reduced the number of phishing security incidents to below 5%. Company B is developing an internal incident response team to similarly update policies and close gaps, thereby also reducing the potential of future security incidents from happening. Company B also has an additional challenge of managing customer incidents through various product requirements. If a customer requires new security features due to incidents, they themselves need to avoid, the IS team works with the product development teams to ensure these features are implemented. Both companies understand that tracking metrics on compliance and incident occurrence is important but consider it a future opportunity as it is a labor-intensive task and resources are stretched thin across

both organizations. Tracking employee compliance with policy can also be helpful to organizations in achieving legitimacy.

Institutional theory provides a framework IS managers can use to help their organization achieve legitimacy and improve compliance. Frequency-based imitation, as shown in Figure 1, is a method that organizations can use to achieve legitimacy through industry certifications. Both organizations have utilized frequency-based imitation by achieving industry certification or validation specific to their line of business. Trait-based imitation, shown in Figure 1, is another economic variant that organizations can use to achieve legitimacy and improve compliance. Trait-based imitation involved copying traits used by other organizations within the industry and can expedite legitimacy within their own industry. Achieving legitimacy along with coercive pressures can provide a foundation for compliance within an organization. The regulated industry that both organizations exist in has been a catalyst for applying trait-based imitation. Outcome-based imitation, also shown in Figure 1, uses mimetic isomorphism to copy behaviors from other organizations, either internal or external, to achieve legitimacy and improve compliance. This type of imitation was also present in both organizations as complying with industry specific certifications was required.

Each organization has established policies relating to compliance within their industry which make it easier to implement new policies that require compliance. However, both organizations struggle with achieving compliance and have implemented internal compliance checks to help enforce policy. Both organizations have different mechanisms in place to manage non-compliance such as re-training, individual guidance,

loss of privileges or even loss of employment. There was agreement between both companies that low compliance of policy does lead to a higher rate of security breaches. To counter this, both companies highlighted the fact that standardizing policy and procedures across the company has reduced the number of security incidents. Although tracking compliance was an area of opportunity for both organizations, incidents are tracked and reviewed. If an existing policy was in place but not followed, re-training may be required. If the incident was not covered by existing policy, a new policy is developed. Company B is working on implementing a risk-management system to trace security incidents back to policy, which is expected to yield more information on compliance and lead to more improvements.

A combination of technology and policy is necessary for an IS program to be effective. A lesser known contributor to poor compliance is information security stress (ISS), also known as security fatigue. Introduced by Lee et al. (2016), ISS is associated with humans becoming additionally stressed in the workplace by needing to also comply with more policies and procedures on top of those that already exist as part of their normal day-to-day workload. Security fatigue was not specifically mentioned by the participants as an issue but can be counteracted by improving awareness and developing and maintaining a strong security culture, which was evident in both organizations. However, the impact on work productivity was mentioned by both organizations. ISS can lead to less productivity in the workplace as employees attempt to manage their normal workload while also maintaining compliance to security policies and procedures. Both companies were cognizant of balancing compliance with policy and productivity. When a

new policy is being developed, appropriate stakeholders are involved and consulted to ensure productivity is not severely impacted.

Applications to Professional Practice

The specific IT problem investigated with this research was the perception that IS managers lacked a strategy for reducing security breaches and improving employee compliance. Current literature suggests that most companies do not have a coherent and effective strategy for reducing security breaches and improving employee compliance. However, the organizations involved in this study would not be considered in the grouping of companies without a coherent strategy. As both organizations operate in heavily regulated industries, responses by the participants indicated adhering to regulations was a significant factor in developing and implementing an effective IS strategy. As part of their strategy, all the participants in this study understand the need for developing and implementing practical and enforceable IS policies, training and awareness, establishing and maintaining a strong security culture where both employee and employer are fully engaged and participating, and managing and tracking compliance. IS managers in both regulated and non-regulated industries may use the results of this study as a guide on developing and implementing a security strategy within their organization.

Implementing any new program within an organization requires commitment from leadership, communication on why the program is necessary, established knowledge of the new program through training and awareness, and strong leadership. Strong leadership and effective communication were evident in both the executive leaders

interviewed for this study. Examples of leadership by executive A was seen with examples of their mastery of the subject matter, pushing out information, making themselves available through conferences, and seminars or consultation. Executive B also exhibited a mastery of the subject matter and is actively involved in communicating the need for security and the associated risks for not following policy with the product development teams. Analysis of the study's findings was done through the lens of institutional theory, specifically institutional isomorphism. As Figure 1 shows, organizations must manage a certain amount of uncertainty. Uncertainty can be mitigated through various methods associated with institutional theory. When a firm is seen as legitimate within their industry, it mitigates a certain amount of uncertainty with how their organization is perceived within their industry. A positive perception can lead to increased business, leading to financial gain. Achieving legitimacy involves social pressures an organization faces when implementing change: coercive, mimetic and normative. Associated with these forces are the economic variants included in the desire for profitability: frequency, trait and outcome-based imitation.

The most apparent pressure both organizations face is coercive due to the highly regulated industries both operate in. Coercive pressures are part of operating in a regulated environment. All participants explained that having an existing infrastructure in place for complying with regulations was an advantage for developing and implementing an IS infrastructure. Employees are trained to comply with policy, so having an existing mechanism in place made it easier when introducing new IS policies and procedures. There was still a need for educating the employees on IS, but each organization was

adding to an established mechanism versus starting from nothing. Establishing new policies and managing the risk and change associated with them in a new unregulated environment was a big part of the challenge. Executive level support was important in this area. Executive level support for new policies allows for easier adoption but still require a focused strategy. In Company A, with an established culture in place, there was more emphasis on compliance across the organization through training and awareness. Company B was more focused on establishing IS policies, making employees aware of the new policies and procedures, and properly training them.

Mimetic pressure was evident in both organizations. Once a process or policy was successfully established in one area of the organization or department, it was then reproduced in other areas mapping to an outcome-based imitation within the company. When a process or policy was successfully reproduced in a new area, it provided more evidence it could work in other areas. However, in some departments, the new policy was not immediately adopted due to a variety of factors that include a subculture existing, resistance to change, or poor stakeholder buy-in to name a few. Resolving this was something the leadership team was doing through awareness, training, and communication. It essentially required changing the culture within these areas or resistance. This could be viewed as examples of trait-based imitation where only specific areas of the parent organization are copied for the gain of the child organization. In some cases, this might be allowed or encouraged and in other cases, depending on the policy, it might not be allowed and would have to be managed.

Normative pressure exists within each organization primarily driven by achieving legitimacy with industry certifications. Normative pressure can also exist within organizations where certain professions exist. Hiring engineers to design and develop products adds legitimacy to a product development organization as does hiring doctors or lawyers within those specific industries. These professions bring legitimacy to their respective organizations but can also apply different pressure from within. These professionals may want to enhance their own legitimacy by continuing their education or becoming certified. This additional certification or education can lead to more legitimacy. Simply bringing these individuals on board and exposing their ideas and processes from other legitimate industries can help new firms achieve further legitimacy internally, gaining support for new policies. There was no explicit evidence of normative pressures within each organization or none that impacted IS strategy.

Through the indirect adoption of institutional isomorphism, both companies involved in this study have developed a strategic approach to implementing IS within their organizations. Consistent between both organizations is a strategy that includes a variety of norms. Organizations that are either just beginning their IS journey or struggling to develop and implement an IS strategy can take advantage of these established norms. First and foremost is establishing executive level support for the IS program. As part of this executive level support, the role of CISO with executive level authority must be established. Ki-Aries and Faily (2017) suggested in their study that senior leadership establishes trust, commitment, and cooperation within the organization that ultimately helps implement new policies.

Having executive level support forms the foundation for creating and sustaining culture within the organization and should be considered the next phase of implementing an effective IS strategy. Building a security culture begins by developing fundamental policies so employees know what is and is not acceptable behavior. Executive level support and fundamental policies form the basis for a strong security culture that needs to be cultivated from the top down in the organization. Cultivating a security culture begins when employees are hired, it continues through constant reinforcement of policy through training and awareness, communicating and educating users of new and existing threats through a variety of different channels, and using technical controls such as implementing least privilege or integrating a tracking system to monitor compliance, to name a few.

Standardizing policies across the organization is also part of an overall strategy that can help build a culture, as standardization can help improve compliance through organizational consistency. Applying industry standards helps legitimize the organization and should be considered. Company B is using the NIST framework to help develop their internal policies, processes, and training programs. Using an established framework avoids re-inventing existing processes, helps establish legitimacy, and reduces the labor involved in creating a new framework. Safa et al. (2016) advocates for using standards as part of an overall IS strategy.

Managing risk is critical in any environment and IS is no different. Safa et al. (2016) recommends performing a risk-assessment for the organization as a start point. The output of the risk-assessment should be used to develop a risk-management plan to

help manage IS incidents. The information gathered from interviewing the IS managers as part of this study confirm that managing risk is an important component of an IS strategy. In the product development space, risk is part of doing business and any risk associated with IS is evaluated, categorized, and managed. For Company B, this means documenting the risk and communicating the outcome if the risk is not accounted for. If the business decides to carry the risk and move forward, it is an educated decision. Company A manages risk through regulatory mandates as well as using a process to evaluate risk through security incidents. If an incident is a result of failing to follow policy, more training and awareness is provided to avoid a recurrence. If the incident is the result of a new threat, policies and training are updated.

Establishing a training and awareness program that communicates changes in IS on a regular basis should go without saying. The larger the organization is, the more difficult this task can become. Both organizations that participated in this study struggle with managing their training and awareness programs across large organizations. That is not to say there are issues but reaching all employees effectively can be a challenge. As a more mature organization, Company A had established policies, websites, procedures and communication mechanisms in place to train and make employees aware of IS. Where it struggled was effectively reaching the various departments within the company that had already established security cultures. Constant communication from executive leadership on the need for new policies across the organization has helped mitigate this issue. Company B struggled with reaching their global partners. The IS team is based in the US and has no official IS presence outside of the country. There is an effort underway to

create a program that will help train key site personnel on the new IS policies and training. The global training effort is expected to make a person responsible at each international site that will be in contact and report back to the US site. Company B sees this as a future opportunity but does have it as part of their strategy.

Compliance metrics is an opportunity that both companies are pursuing. Tracking compliance to manage non-compliance is a labor-intensive operation, which can be a limiting factor to implementing it. Company A sees compliance metrics as a future opportunity but believes it is necessary. Company B also sees metrics as a future opportunity as more resources are added to the team. Company B is implementing technology that can help track security incidents back to policy. Implementing audit mechanisms to ensure compliance is also recommended in a study by da Veiga and Martins (2017). The authors presented an IS assessment tool organizations can use to obtain a current snapshot of their IS organization. Auditing is part of the assessment tool. Although no formal auditing exists with either company in this study, there are informal audits happening on a regular basis. All participants agree that auditing allows for a quick measurement of policy usage but also expressed the process to be labor intensive.

The results of this research highlighted the different strategies each participating organizations consider when adopting IS policies. Applying institutional theory helped frame the discussion on how both organizations are implementing their IS strategy. The interview results and literature review provide a base of knowledge any organization can use to implement or improve their IS organization. Training and awareness is recognized

in both the literature and interview results as being fundamental to establishing policy and creating a strong IS culture.

Implications for Social Change

The implication for social change comes in the form of education and knowledge on the strategies and techniques IS organizations use to improve their organization. Advancing the IS education and knowledge of individuals may improve their own personal security habits. Improving individual security habits can also improve an organizations security habits if employees are more aware of the security risks that are prevalent today. Organizations may also use this study to improve their own IS techniques and strategies.

Documenting strategies that improve organizational security compliance can provide a positive impact on social change. Improved security compliance can lead to better protection of personal identifiable information (PII) for employees and customers. By developing and implementing IS strategies outlined in this study, organizations can better protect employee and customer data by reducing the risk of security breaches. In the highly regulated environment both companies operate in, protecting PII for customers and employees is critical for maintaining compliance with existing laws. Employees within the company that are trained on these new polices and procedures may also benefit from this study outside of their work environment.

As individuals adopt better security habits and share with acquaintances, it can benefit society as well. By being more aware of current threats used by computer criminals and the risks associated with using social media and online commerce,

individuals can reduce the likelihood of becoming victims of identity theft as they use computers in their personal lives. By using information from this study, computer users can reduce the likelihood of becoming targets of security fraud by limiting or eliminating personal information available online, using secure websites, and practicing good security habits such as stronger passwords and anti-phishing methods.

The findings from this study add to the existing IS body of knowledge by providing firsthand information from two active IS organizations and may be of value to society by providing improved IS awareness strategies. The information in this study explains how two different organizations develop and implement effective IS strategies to reduce security breaches and improve employee compliance. This study may also help raise awareness to the challenges of creating and implementing an IS program and how two separate companies are managing these challenges.

Recommendations for Action

Organization IS leaders can use these findings to build their own IS program and culture where IS is considered second nature and can help reduce the risk of employee non-compliance. This study explored the strategies IS leaders use to develop and implement a comprehensive IS program. Starting with executive level support, this study revealed how an effective IS program and culture is created. The study revealed how an IS program can be implemented through constant and thorough communication, using policy, training and awareness, and risk-management to reduce security threats and improve compliance.

Organization IS leaders should consider either providing executive level support or creating the CISO position and providing that person with executive level authority. Executive level support was considered a critical component in building an effective IS program. The lack of executive level support can make it difficult to establish the importance of IS within an organization. Without executive level support, there is little incentive or authority behind policy and implementing a security culture built on trust becomes equally difficult.

Organization IS leaders should include the establishment of a communication plan as fundamental to beginning an IS program. The importance of communication cannot be understated. One of the most important areas for both organizations was making large organizations aware of new and existing policy. Each organization made this a priority and implemented a variety of techniques to make IS information available for general consumption, push it out via different sources, and to make IS managers available for consultation. The communication plan should include who is responsible for what, their contact information, where people can go to get further information, the different methods that will be used to communicate news and information, and the different types of training that are or will be available.

Additionally, IS leaders can improve their culture by instituting a risk-management plan, seeded by a risk-assessment of the organization. Executive level support and strong communication form the basis of any organizational culture and IS is no different. While this study focused primarily on the strategies IS managers can use to improve IS compliance and reduce risk, working hand in hand with the IT department to

integrate with the technical controls in place is an absolute requirement. Technical controls were not the focus of this study but are mentioned here for completeness.

This study may benefit IS managers that are thinking about creating an IS program or are struggling to get one off the ground. IS managers can use this study to gain a deeper understanding of institutional isomorphism and the impact it may have on their own organizational strategy when developing an IS program. A better understanding of coercive, mimetic, and normative forces within an organization may help managers create a more comprehensive IS strategy. A more comprehensive IS strategy can lead to better educated employees that are more cognizant of security risks both inside and outside of their organization. Improving individual security habits can benefit society by reducing the number of identity theft and credit card fraud.

I will disseminate this study to the participants via email. I anticipate sharing the results of this research using appropriate platforms within my classrooms and during lectures. I may use this study to extend the research by writing and presenting papers at relevant conferences. In addition, the output of this study may form the basis for writing and publishing future scholarly journal articles.

Recommendations for Further Study

There are several recommendations for further study. One of the anticipated limitations noted at the beginning of this study was the small number of participants. Future research could expand the population to not only more IS organizations but also more participants. Even though a small population was noted as a limitation, this study benefited greatly from having two executive level participants who were able to provide

detailed results that aligned with current literature. However, adding more participants may reveal additional areas not exposed in this study, further adding to current literature.

Another limitation noted was related to bias introduced by the participants by not answering the interview questions honestly or holding back due to not wanting to expose company information. I believe the participants answered honestly and explained when they could not discuss issues. It is the nature of asking questions regarding IS but a potential solution would be to use anonymous surveys to collect information.

Another area of study that would add to the knowledge base would be to measure metrics around compliance. How many users are or are not complying? This could also be accomplished using anonymous surveys to all the users of the systems. It could provide a picture of compliance even though the results may not be comprehensive or truthful.

A third area of future research that would be interesting, is to survey users of organizational IS policies to determine if the training and policies they are trained on at work, impact their online behavior in their personal lives. Do they practice good habits in their personal lives because of their training at work or do they let their guard down after leaving the work environment?

A fourth area of study that may add value to existing IS literature is a deeper concentration on behavioral theory. Understanding how and why employees act and respond to IS policies and regulations in a work environment would be an interesting addition to research. Ideally, the creation of a Myers-Briggs type of profile focused on IS could add value to an IS organization. Understanding the security profile of each

individual employee may help develop more focused policies, create tailored training and awareness programs, and help focus audit and compliance tracking in specific areas.

Reflections

This doctoral study was the culmination of significant effort and patience. It was never a goal of mine to pursue a doctorate but decided it would be something that would add value as I pursue teaching as a second career. It is true that you do not know what you are capable of until you push yourself. It was less of a technical challenge and more of a mental challenge. The process of defining a problem of significance and researching it at the doctoral level while also raising your critical thinking and writing skills was a unique challenge in itself. It was the discipline and patience to keep going to achieve the final result that was the most difficult. Life gets in the way and family and work commitments take priority. Continuing the journey when life throws you a curveball really challenges you. I was fortunate to have a supportive family along with a reason to finish. During the process of seemingly endless reviews, it seemed like the end would never come. Digging down deep and pushing yourself to finish was something you do not know is inside of you until you are presented with the challenge. It would have been easy to quit after achieving enough credits for a master's degree, but my goal was a doctorate and I wanted to see if I could do it and I did. Patience and perseverance got me through.

Summary and Study Conclusions

IS managers are implementing policies and procedures in their organizations because the threat of security breaches is becoming more and more common. The policies being implemented may or may not have executive level support, may not be part of a

cohesive strategy, and may or may not have effective training and awareness campaigns in place. This study can help IS managers develop a plan for implementing a security strategy that includes executive level support, attention to policy development, the need for consistent and focused training, and elements to help build a security culture. By using established frameworks advocated by NIST and organizational theory, IS managers can add to their toolbox, which they can then use to create a comprehensive strategy.

References

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

Alavi, M., Archibald, M., McMaster, R., Lopez, V., & Cleary, M. (2018). Aligning theory and methodology in mixed methods research: Before design theoretical placement. *International Journal of Social Research Methodology*, *21*(5), 527–540. doi:10.1080/13645579.2018.1435016

AlHogail, A. (2015). Design and validation of information security culture framework. *Computers in Human Behavior, 49*, 567-575. doi:10.1016/j.chb.2015.03.054

Amjad, H. A. R., Naeem, U., Zaffar, M. A., Zaffar, M. F., & Choo, K.-K. R. (2016). Improving security awareness in the government sector. *The Proceedings of the 17th International Digital Government Research Conference on Digital Government Research*. Shanghai, China. doi:10.1145/2912160.2912186

Anderson, K. M., & Paterson, M. (2015). Overview of secondary data analysis with a description of heart failure hospitalizations from the national hospital discharge survey. *Clinical Scholars Review: The Journal of Doctoral Nursing Practice, 8*(1), 130-138. doi:10.1891/1939-2095.8.1.130

Andrews-Speed, P. (2016). Applying institutional theory to the low-carbon energy transition. *Energy Research & Social Science*, *13*, 216-225. doi:10.1016/j.erss.2015.12.011

Angst, C. M., Block, E. S., D'Arcy, J., & Kelley, K. (2017). When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. *MIS Quarterly, 41*(3), 893-916. doi:10.25300/MISQ/2017/41.3.10

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*(Suppl. C), 437-443. doi:10.1016/j.chb.2016.12.040

Aurigemma, S., & Mattson, T. (2017). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security, 73*, 219-234. doi:10.1016/j.cose.2017.11.001

Barnham, C. (2015). Quantitative and qualitative research. *International Journal of Market Research, 57*(6), 837–854. doi:10.2501/IJMR-2015-070

Bartnes, M., & Moe, N. B. (2016) Challenges in IT security preparedness exercises: A case study. *Computers & Security, 67*, 280-290. doi:10.1016/j.cose.2016.11.017

Bartnes, M., Moe, N. B., & Heegaard, P. E. (2016). The future of information security incident management training: A case study of electrical power companies. *Computers & Security, 61*, 32-45. doi:10.1016/j.cose.2016.05.004

Baskerville, R. L., & Myers, M. D. (2015). Design ethnography in information systems. *Information Systems Journal, 25*(1), 23-46. doi:10.1111/isj.12055

Bauer, S., Chudzikowski, K., & Bernroider, E. W. N. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-

compliance with information security policies in banks. *Computers & Security, 68,* 145-159. doi:10.1016/j.cose.2017.04.009

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13*(4), 544-559. Retrieved from https://nsuworks.nova.edu/tqr/vol13/iss4/2

Bélanger, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management, 54*(7), 887-901. doi:10.1016/j.im.2017.01.003

Belotto, M. J. (2018). Data analysis methods for qualitative research: Managing the challenges of coding, interrater reliability, and thematic analysis. *The Qualitative Report, 23*(11), 2622-2633. Retrieved from https://nsuworks.nova.edu/tqr/vol23/iss11/2

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

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

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. doi:10.1177/1049732316654870

Bjorck, F. (2004). Institutional theory: A new perspective for research into IS/IT security in organisations. *Proceedings of the 37th Hawaii International Conference on System Sciences – 2004*. doi:10.1109/HICSS.2004.1265444

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

Boddy, C. R. (2016). Sample size for qualitative research. *Qualitative Market Research: An International Journal, 19*(4), 426. doi:10.1108/QMR-06-2016-0053

Bourne, B. (2015). Phenomenological study of generational response to organizational change. *Journal of Managerial Issues, 27(*1-4), 141-161. Retrieved from Walden University databases.

Bozan, K., Davey, B., & Parker, K. (2015). Social influence on health IT adoption patterns of the elderly: An institutional theory based use behavior approach. *Procedia Computer Science, 63*, 517-523. doi:10.1016/j.procs.2015.08.378

Bromley, E., Mikesell, L., Jones, F., & Khodyakov, D. (2015). From subject to participant: Ethics and the evolving role of community in health research. *American Journal of Public Health, 105*(5), 900-908. doi:10.2105/ajph.2014.302403

Buchanan, B. (2018). SOCLAB - Building the future of cyber security training and awareness. Retrieved from https://medium.com/asecuritysite-when-bob-met-

alice/soclab-building-the-future-of-cyber-security-training-and-awareness-d9232ff9fe53

Buchanan, B. (2018b). The sorry state of secure software development? Retrieved from https://medium.com/asecuritysite-when-bob-met-alice/the-sorry-state-of-secure-software-development-ebbd3eaa8859

Cardinale, I. (2018). Beyond constraining and enabling: Toward new microfoundations for institutional theory. *Academy of Management Review, 43*(1), 132-155. doi:10.5465/amr.2015.0020

Carman, M. J., Clark, P. R., Wolf, L. A., & Moon, M. D. (2015). Sampling considerations in emergency nursing research. *Journal of Emergency Nursing, 41*(2), 162-164. doi:10.1016/j.jen.2014.12.016

Chandler, D., & Hwang, H. (2015). Learning from learning theory: A model of organizational adoption strategies at the microfoundations of institutional theory. *Journal of Management, 41*(5), 1446-1476. doi:10.1177/0149206315572698

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. *Telematics and Informatics, 35*(6), 1770-1780. doi:10.1016/j.tele.2018.05.005

Connelly, L. M. (2013). Limitation section. *Medsurg Nursing, 22*, 325-325, 336. Retrieved from http://www.medsurgnursing.net/cgi-bin/WebObjects/MSNJournal.woa

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing, 25*(6), 435-437. Retrieved from http://www.medsurgnursing.net/cgi-bin/WebObjects/MSNJournal.woa

Conroy, T. (2017). A beginner's guide to ethnographic observation in nursing research. *Nurse Researcher, 24*(4), 10-14. doi:10.7748/nr.2017.e1472

Culture. (2019). In *Merriam-Webster Online Dictionary.* Retrieved from https://www.merriam-webster.com/dictionary/culture

Curran, T. (2015). Information security (IS) training: Instructional design project. *Journal of Applied Learning Technology, 5*(3), 24-30. Retrieved from Walden University databases.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017). Investigation into the formation of information security influence: Network analysis of an emerging organization. *Computers & Security, 70*(Supplement C), 111-123. doi:10.1016/j.cose.2017.05.010

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2017b). Why employees share information security advice? Exploring the contributing factors and structural patterns of security advice sharing in the workplace. *Computers in Human Behavior, 67*, 196-206. doi:10.1016/j.chb.2016.10.025

da Veiga, A., & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security, 49*, 162-176. doi:10.1016/j.cose.2014.12.006

da Veiga, A., & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security, 70(Supplement C)*, 72-94. doi:10.1016/j.cose.2017.05.002

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly, 34*(1), 1-7. doi:10.1016/j.giq.2017.02.007

Densham, B. (2015). Three cyber-security strategies to mitigate the impact of a data breach. *Network Security, 2015*(1), 5-8. doi:10.1016/S1353-4858(15)70007-3

Dhillon, G., Syed, R., & Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security, 56*, 63-69. doi:10.1016/j.cose.2015.10.001

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organization fields. *American Sociological Review, 48*(2), 147-160. doi:10.2307/2095101

Djemame, K., Armstrong, D., Guitart, J., & Macias, M. (2016). A risk assessment framework for cloud computing. *IEEE Transactions on Cloud Computing, 4*(3), 265-278. doi:10.1109/TCC.2014.2344653

Doherty, N. F., & Tajuddin, S. T. (2018). Towards a user-centric theory of value-driven information security compliance. *Information Technology & People, 31*(2), 348–367. doi:10.1108/ITP-08-2016-0194

Drinkwater, D. (2017, March 29). AI will transform information security, but it won't happen overnight. Retrieved from

https://www.csoonline.com/article/3184577/application-development/ai-will-transform-information-security-but-it-won-t-happen-overnight.html

Ellis, P. (2016). The language of research (part 11) -- Research methodologies: Interview types. *Wounds UK, 12*(4), 104–106. Retrieved from Walden University databases.

El-Masri, M. M. (2017). Non-probability sampling: The process of selecting research participants non-randomly from a target population. *Canadian Nurse, 113*(3), 17-17. Retrieved from https://www.canadian-nurse.com/en/articles/issues/2017/may-june-2017?page=2

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

Emerson, R. W. (2015). Convenience sampling, random sampling, and snowball sampling: How does sampling affect the validity of research? *Journal of Visual Impairment & Blindness, 109*(2), 164–168. doi:10.1177/0145482X1510900215

Errasti-Ibarrondo, B., Diez-Del-Corral, M. P., Arantzamendi, M., & Jordan, J. (2018). Conducting phenomenological research: Rationalizing the methods and rigour of the phenomenology of practice. *Journal of Advanced Nursing, 74*(7), 1723-1734. doi:10.1111/jan.13569

Fennell, M. (1980). The effects of environmental characteristics on the structure of hospital clusters. *Administrative Science Quarterly, 25*, 484-510. doi:10.2307/2392265

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*, 169-183. doi:10.1016/j.cose.2016.06.002

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss9/3

Gagnon, M., Jacob, J. D., & McCabe, J. (2015). Locating the qualitative interview: Reflecting on space and place in nursing research. *Journal of Research in Nursing 20*(3), 203-215. doi:10.1177/1744987114536571

Gentles, S. J., Charles, C., Ploeg, J., & McKibbon, K. A. (2015). Sampling in qualitative research: Insights from an overview of the methods literature. *Qualitative Report, 20*(11), 1772-1789. Retrieved from https://nsuworks.nova.edu/tqr/vol13/iss11/5

Gerhold, L., Bartl, G., & Haake, N. (2017). Security culture 2030. How security experts assess the future state of privatization, surveillance, security technologies and risk awareness in Germany. *Futures, 87*, 50-64. doi:10.1016/j.futures.2017.01.005

Giddens, A. (1984). *The constitution of society: Outline of the theory of structuration.* Malden, MA: Polity Press.

Gorgolewski, K. J., & Poldrack, R. A. (2016). A practical guide for improving transparency and reproducibility in neuroimaging research. *PLoS Biology, 14*(7), 1-15. doi:10.1371/journal.pbio.1002506

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

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

Hadlington, L. (2017). Human factors in cybersecurity; Examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), 1-18. doi:10.1016/j.heliyon.2017.e00346

Han, J., Kim, Y. J., & Kim, H. (2017). An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective. *Computers & Security, 66*, 52-65. doi:10.1016/j.cose.2016.12.016

Hatfield, J. M. (2018). Social engineering in cybersecurity: The evolution of a concept. *Computers & Security, 73*(Supplement C), 102-113. doi:10.1016/j.cose.2017.10.008

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security, 76*, 101-127. doi:10.1016/j.cose.2018.02.020

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society, 44*, 30-38. doi:10.1016/j.techsoc.2015.11.007

Heras-Saizarbitoria, I., & Boiral, O. (2015). Symbolic adoption of ISO 9000 in small and medium-sized enterprises: The role of internal contingencies. *International Small Business Journal, 33*(3), 299-320. doi:10.1177/0266242613495748

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational information security strategy: Review, discussion and future research. *Australasian Journal of Information Systems, 21,* 1-17. doi:10.3127/ajis.v21i0.1427

Hossein, J., Shaharam, Y., & Ali, Y. (2015). Investigation the role of medical teacher in education in universities of medical sciences in the country from the viewpoint of medical teachers. *Journal of Medical Education, 14*(3), 106-118. doi:10.22037/jme.v14i3.10257

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

Houghton, F., & Houghton, S. (2018). An appraisal of thematic analysis: Warts and all. *AISHE-J: The All Ireland Journal of Teaching & Learning in Higher Education, 10*(2), 3521-3525. Retrieved from http://ojs.aishe.org/index.php/aishe-j/article/view/352

Hu, P. J.-H., Hu, H.-f., Wei, C.-P., & Hsu, P.-F. (2016). Examining firms' green information technology practices: A hierarchical view of key drivers and their effects. *Journal of Management Information Systems, 33*(4), 1149-1179. doi:10.1080/07421222.2016.1267532

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2-18. doi:10.1108/OIR-11-2015-0358

Hwang, K., & Choi, M. (2017). Effects of innovation-supportive culture and organizational citizenship behavior on e-government information system security stemming from mimetic isomorphism. *Government Information Quarterly, 34*, 183-198. doi:10.1016/j.giq.2017.02.001

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security, 66*, 129-141. doi:10.1016/j.cose.2017.01.010

Johnson, M., O'Hara, R., Hirst, E., Weyman, A., Turner, J., Mason, S., . . . Siriwardena, A. N. (2017). Multiple triangulation and collaborative research using qualitative methods to explore decision making in pre-hospital emergency care. *BMC Medical Research Methodology, 17(1)*, 1-11. doi:10.1186/s12874-017-0290-z

Joshi, C., & Singh, U. K. (2017). Information security risks management framework – A step towards mitigating security risks in university network. *Journal of Information Security and Applications, 35*, 128-137. doi:10.1016/j.jisa.2017.06.006

Karanja, E., & Rosso, M. A. (2017). The chief information security officer: An exploratory study. *Journal of International Technology & Information Management, 26*(2), 23-47. Retrieved from https://scholarworks.lib.csusb.edu/jitim/vol26/iss2/2

Karlsson, F., Hedström, K., & Goldkuhl, G. (2016). Practice-based discourse analysis of information security policies. *Computers & Security, 67*, 267-279. doi:10.1016/j.cose.2016.12.012

Kauppi, K. (2013) Extending the use of institutional theory in operations and supply chain management research: Review and research suggestions, *International Journal of Operations & Production Management*, *33*(10), 1318-1345, doi:10.1108/IJOPM-10-2011-0364.

Kavalaris, S., Kioupakis, F.-E., Kaltsas, K., & Serrelis, E. (2015). Development of a multi-vector information security rating scale for smart devices as a means for raising public infosec awareness. *Procedia Computer Science*, *65*, 500-509. doi:10.1016/j.procs.2015.09.122

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46-58. doi:10.1016/j.cose.2016.05.006

Kerwin-Boudreau, S., & Butler-Kisber, L. (2016). Deepening understanding in qualitative inquiry. *The Qualitative Report, 21*(5), 956-971. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss5/13

Ki-Aries, D., & Faily, S. (2017). Persona-centred information security awareness. *Computers & Security, 70*, 663-674. doi: 10.1016/j.cose.2017.08.001

Kim, S., Kim, G., & French, A. (2015). Relationships between need-pull/technology-push and information security management and the moderating role of regulatory pressure. *Information Technology & Management, 16*(3), 173-192. doi:10.1007/s10799-015-0217-5

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122-134. doi:10.1016/j.cose.2015.07.002

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

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122. doi:10.1016/j.jisa.2014.09.005

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

Lee, C., Lee, C. C., & Kim, S. (2016). Understanding information security stress: Focusing on the type of information security compliance activity. *Computers & Security, 59*, 60-70. doi:10.1016/j.cose.2016.02.004

Leggette, H. R., & Redwine, T. (2016). Using Q methodology in agricultural communications research: A philosophical study. *Journal of Applied Communications, 100*(3), 55-67. doi:10.4148/1051-0834.1230

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health Promotion Practice, 16(*4), 473-475. doi:10.1177/1524839915580941

Long, B. T., & Hall, T. (2018). Educational narrative inquiry through design-based research: Designing digital storytelling to make alternative knowledge visible and actionable. *Irish Educational Studies, 37*(2), 205-225. doi:10.1080/03323315.2018.1465836

Mabila, T. (2017). Postgraduate students understanding of mixed methods research design at the proposal stage. *South African Journal of Higher Education, 31*(5), 136-153. doi:10.28535/31-5-1498

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A comparison of the theory of planned behavior and the theory of reasoned action. *Personality and Social Psychology Bulletin, 18*(1), 3-9. doi:10.1177/0146167292181001

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi:10.1016/0022-1031(83)90023-9

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), 1-13. doi:10.1177/1609406918786362

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

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior, 83,* 32-44. doi:10.1016/j.chb.2018.01.028

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons, 59*(3), 257-266. doi:10.1016/j.bushor.2016.01.002

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. doi:10.7748/nr.2017.e1510

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69,* 151-156. doi:10.1016/j.chb.2016.11.065

McGovern, T., Small, A., & Hicks, C. (2017). Diffusion of process improvement methods in European SMEs. *International Journal of Operations & Production Management, 37*(5), 607-629. doi:10.1108/IJOPM-11-2015-0694

Meyer, J., & Hannan, M. (1979) National development and the world system: Educational, economic and political change, 1950-1970. 1979. (1980). *Educational Studies, 11*(2) 61-262. doi:10.7202/701058ar

Meyer, J. W., & Rowan, B. (1977), Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology, 83*(2). 340-363. doi:10.1086/226550

Mohamed, I. A. H. (2017). Some issues in the institutional theory: A critical analysis. *International Journal of Scientific & Technology Research, 6(*9*),* 150-156. Retrieved from http://www.ijstr.org

Mohammad, R. M., Thabtah, F., & McCluskey, L. (2015). Tutorial and critical analysis of phishing websites methods. *Computer Science Review, 17,* 1-24. doi:10.1016/j.cosrev.2015.04.001

Molin, E., Meeuwisse, K., Pieters, W., & Chorus, C. (2018). Secure or usable computers? Revealing employees' perceptions and trade-offs by means of a discrete choice experiment. *Computers & Security, 77,* 65-78. doi:10.1016/j.cose.2018.03.003

Molinillo, S., & Japutra, A. (2017). Organizational adoption of digital information and technology: A theoretical review. *Bottom Line: Managing Library Finances, 30*(1), 33-46. doi:10.1108/BL-01-2017-0002

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-308. doi: 10.25300/MISQ/2018/13853

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

Moser, A., & Korstjens, I. (2017). Series: Practical guidance to qualitative research. Part 1: Introduction. *The European Journal of General Practice, 23*(1), 271-273. doi:10.1080/13814788.2017.1375

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security, 59*, 186-209. doi:10.1016/j.cose.2016.03.004

Munir, K. A. (2015). A loss of power in institutional theory. *Journal of Management Inquiry, 24*(1), 90-92. doi:10.1177/1056492614545302

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi:10.1016/j.cose.2015.10.002

Oosterhoff, B., Shook, N. J., & Metzger, A. (2018). A matter of fact? Adolescents' assumptions about crime, laws, and authority and their domain-specific beliefs about punishment. *Journal of Adolescence, 62*, 87-95. doi: 10.1016/j.adolescence.2017.11.007

Park, E. H., Kim, J., & Park, Y. S. (2017). The role of information security learning and individual factors in disclosing patients' health information. *Computers & Security, 65*, 64-76. doi:10.1016/j.cose.2016.10.011

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

Patton, M. Q. (1990). *Qualitative evaluation and research methods.* Newbury Park, CA: Sage.

Paul, J., Modi, A., & Patel, J. (2016). Predicting green product consumption using theory of planned behavior and reasoned action. *Journal of Retailing and Consumer Services, 29*, 123-134. doi:10.1016/j.jretconser.2015.11.006

Piña, G., & Avellaneda, C. N. (2018). Municipal isomorphism: Testing the effects of vertical and horizontal collaboration. *Public Management Review, 20*(4), 445-468. doi:10.1080/14719037.2017.1412116

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

Rihoux, B., & Lobe, B. (2015). The case-orientedness of qualitative comparative analysis (QCA): Glass half-empty or half-full? *Teorija in Praksa, 52*(6), 1039-1245. Retrieved from Walden University databases.

Robinson, O. C. (2014). Sampling in interview-based qualitative research: A theoretical and practical guide. *Qualitative Research in Psychology, 11*(1), 25-41. doi:10.1080/14780887.2013.801543

Roulston, K., & Shelton, S. A. (2015). Reconceptualizing bias in teaching qualitative research methods. *Qualitative Inquiry, 21*(4), 332–342. doi: 10.1177/1077800414563803

Rouse, M. (2018). Two-factor authentication (2FA). Retrieved from https://searchsecurity.techtarget.com/definition/two-factor-authentication

Rutberg, S., & Bouikidis, C. D. (2018). Exploring the evidence. Focusing on the fundamentals: A simplistic differentiation between qualitative and quantitative

research. *Nephrology Nursing Journal, 45*(2), 209-213. Retrieved from https://library.annanurse.org/anna/articles/1898/view

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. *Journal of Information Security And Applications, 40*, 247-257. doi:10.1016/j.jisa.2017.11.001

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. doi:10.1016/j.cose.2015.05.012

Safa, N. S., & Von Solms, R. (2016b). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57*, 442-451. doi:10.1016/j.chb.2015.12.037

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

Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management, 22*(3), 176-191. Retrieved from http://www.sajm-amdisa.org

Schilke, O. (2018). A micro-institutional inquiry into resistance to environmental pressures. *Academy of Management Journal, 61*(4), 1431-1466. doi:10.5465/amj.2016.0762

Scott, W. R., & Amarante, J. M. (2016). Institutional theory's past and future contributions to organization studies. *Associacao Nacional de Pos-Graduacao e Pesquisa em Administracao (ANPAD), 13*,1-5. Retrieved from http://www.anpad.org.br/bar

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

Setia, M. S. (2016). Methodology series module 5: Sampling strategies. *Indian Journal of Dermatology, 61*(5), 505-509. doi:10.4103/0019-5154.190118

Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications, 36*, 1-10. doi:10.1016/j.jisa.2017.07.004

Sherer, S., Meyerhoefer, C., & Peng, L. (2016). Applying institutional theory to the adoption of electronic health records in the U.S. *Information & Management, 53*(5), 570-580. doi:10.1016/j.im.2016.01.002

Sloan, A. A. S., & Bowe, B. B. B. (2015). Experiences of computer science curriculum design: A phenomenological study. *Interchange, 46*(2), 121-142. doi:10.1007/s10780-015-9231-0.

Snowden, M. (2015). Use of diaries in research. *Nursing Standard, 29*(44), 36-41. doi:10.7748/ns.29.44.36.e9251

Soomoro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215-225. doi:10.1016/j.ijinfomgt.2015.11.009

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional, 18*(5), 26-32. doi:10.1109/MITP.2016.84

Suddaby, R. (2015). Can institutional theory be critical? *Journal of Management Inquiry, 24*(1), 93-95. doi:10.1177/105649261454530

Suopajärvi, T. (2015). Past experiences, current practices and future design. Ethnographic study of aging adults' everyday ICT practices: And how it could benefit public ubiquitous computing design. *Technological Forecasting & Social Change*, *93*, 112-123. doi:10.1016/j.techfore.2014.04.006

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

Takahashi, A. R. W., & Sander, J. A. (2017). Combining institutional theory with resource based theory to understand processes of organizational knowing and dynamic capabilities. *European Journal of Management Issues, 25*(1), 43-48. doi:10.15421/191707

Terranova Security (2019). Security awareness training in the era of artificial intelligence. Retrieved from https://terranovasecurity.com/security-awareness-training-era-artificial-intelligence

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

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376-391. doi: 10.1016/j.cose.2017.07.003

Torten, R., Reaiche, C., & Boyle, S. (2018). The impact of security awareness on information technology professionals' behavior. *Computers & Security, 79*, 68-79. doi:10.1016/j.cose.2018.08.007

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128-141. doi:10.1016/j.cose.2015.04.006

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

Uwizeyemungu, S., & Poba-Nzaou, P. (2015). Understanding information technology security standards diffusion: An institutional perspective. *2015 International Conference on Information Systems Security and Privacy (ICISSP).* Retrieved from https://ieeexplore.ieee.org/abstract/document/7509923

Vaughn, P., & Turner, C. (2016). Decoding via coding: Analyzing qualitative text data through thematic coding and survey methodologies. *Journal of Library Administration, 56*(1), 41-51. doi:10.1080/01930826.2015.1105035

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods and methodologies. *Journal of Applied Management Accounting Research*, *10*(1), 69-80. Retrieved from http://www.cmawebline.org/jamar

Walsh, R. (2015). Wise ways of seeing: Wisdom and perspectives. *Integral Review*, *11(*2), 156-174. Retrieved from http://integral-review.org/issues/vol_11_no_2_walsh_wise_ways_of_seeing.pdf

Wanat, C. L. (2008). Getting past the gatekeepers: Differences between access and cooperation in public school research. *Field Methods*, *20*(2), 191-208. doi:10.1177/1525822X07313811

Watt, D. (2007). On becoming a qualitative researcher: The value of reflexivity. *The Qualitative Report*, *12*(1), 82-101. Retrieved from https://nsuworks.nova.edu/tqr/vol12/iss1/5

Willmott, H. (2015). Why institutional theory cannot be critical. *Journal of Management Inquiry*, *24*(1), 105-111. doi:10.1177/1056492614545306

Yang, C.-M., & Hsu, T.-F. (2017). New perspective on visual communication design education: An empirical study of applying narrative theory to graphic design courses. *International Journal of Higher Education*, *6*(2), 188-198. doi:10.5430/ijhe.v6n2p188

Yazan, B. (2015). Three approaches to case study methods in education: Yin, Merriam, and Stake. *The Qualitative Report*, *20*(2), 134-152. Retrieved from https://nsuworks.nova.edu/tqr/vol20/iss2/12

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

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs, 43*(3), 389–418. doi: 10.1111/j.1745-6606.2009.01146.x

Zamawe, F. C. (2015). The implication of using NVivo software in qualitative data analysis: Evidence-based reflections. *Malawi Medical Journal, 27*, 13-15. doi:10.4314/mmj.v27i1.4

Appendix A: Human Subject Research Certificate of Completion

Certificate of Completion

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

Date of completion: 05/15/2016.

Certification Number: 2075072.

Appendix B: Permission to Use Figures

From: Lauren Flintoft <lflintoft@emeraldgroup.com>
Sent: Thursday, February 15, 2018 4:25 AM
To: Alan Dawson
Subject: FW: Permission for use of figure

Dear Alan Dawson,

Please allow me to introduce myself, my name is Lauren Flintoft and I am the Rights Executive here at Emerald. Chris has forwarded your query to me.

Subject to full referencing, Emerald is happy for you to use this content within your thesis research. Please note, however, that if in the future you wish to publish your thesis commercially, you will need to clear permission again.

Please note, the above grants permission for content that is '© Emerald Publishing' only. Any content used from the article that makes reference to a copyright holder other than Emerald, will require you to clear permission with that party directly.

I hope this helps, please let me know if you require any further assistance in the future.

Kind Regards,

Lauren Flintoft
Rights Executive| Emerald Group
T: +44 (0) 1274 785227
LFlintoft@emeraldgroup.com| www.emeraldinsight.com

Please consider the environment before printing this email

From: Alan Dawson
Sent: 13 February 2018 18:41
To: Chris Tutill <ctutill@emeraldgroup.com>
Subject: Permission for use of figure

Hello Chris,
I'm a doctoral student at Walden University and in the beginning process of my doctoral study. I have found the article below and would like to reference the diagram in figure 1

on p.1322 in my proposal document. This study will not be used for commercial purposes.

Thank you,

Alan Dawson
Walden University

Katri Kauppi, (2013) "Extending the use of institutional theory in operations and supply chain management research: Review and research suggestions", International Journal of Operations & Production Management, Vol. 33 Issue: 10, pp.1318-1345, https://doi-org.ezp.waldenulibrary.org/10.1108/IJOPM-10-2011-0364
Emerald Publishing Limited, Registered Office: Howard House, Wagon Lane, Bingley, BD16 1WA United Kingdom. Registered in England No. 3080506, VAT No. GB 665 3593 06

Appendix C: Informed Consent Form

Dear Participant:

My name is Alan R. Dawson and I would like to invite you to take part in a research study. I am currently a doctoral candidate at Walden University and conducting this research study is part the doctoral study phase of my degree program. The data that I collect from interviews will be used in order to explore strategies for the implementation of information security (IS) programs that improve employee compliance and reduce the risk of security breaches within the organization. As the primary researcher for this study, I will be interviewing participants with knowledge and experience developing and implementing IS programs. The purpose of this consent form is to inform you of the details regarding participation and to explain your rights so that you may make an informed decision as to whether to participate in this study.

Your participation in this study would be strictly voluntary, and you may withdraw from the study at any time. Should you decide to withdraw, there will be no penalties or repercussions of any kind. You will not be paid for participating in this study. No interviews will be conducted, or any data collected until final approvals have been gained from Walden University's Institutional Review Board.

Background Information

The purpose of this qualitative research study is to explore how IS managers develop and implement strategies to increase employee compliance with company policies to reduce the risk of security breaches within organizations.

Procedures

Should you agree to participate in this study, you will be required to sign this consent form to confirm you have read and accept the terms described. Your participation will involve approximately 60 minutes of your time for an interview. The interviews will be recorded using a digital audio recorder. A second interview may be required for follow up questions based on responses provided during the initial interview. Once all information is gathered and confirmed, there will be a member-checking session after your interview is completed to confirm information gathered during the interview process. The member-checking session should take no more than 15 minutes of your time. It will consist of you validating a summary of the interview responses. Although a transcript will be generated from the recorded interview, you will not be expected to review the entire transcript so one will not be provided.

Provided below are some sample interview questions:

1. What types of policies and strategies do you manage?
2. How does strategy help improve security policy compliance?
3. What prompts the need for information security practices?

Voluntary Nature of the Study:

Participation in this study is completely voluntary. Your information will be kept strictly confidential and participant privacy is a major focus of the researcher. I will take measures to protect your privacy, and all of your answers will be strictly confidential. Neither your name nor the name of the organization will be used in the study. All of the information that you provide is voluntary and there will be no penalty from either myself

as the researcher, the university, or your organization if you decide to exit from participating in this study. Any information that you provide will be used solely for the purpose of this research study. Should you initially accept participation in this study, you may still change your mind at any time without ramifications.

Risks and Benefits of the Study

There is no risk anticipated by your involvement or participation in this study. Rather, your participation in this study could lead to benefits such as a published research study which may have a significant impact in the field, as well as positive outcomes for society. Please feel free to ask me if you have any questions at all regarding the risks or benefits of this study.

Supplemental Contact information

You may feel free to ask me any questions that you have at any time. You may reach me by email. Should you have any private questions or concerns, you may contact a Walden University Research Participant Advocate at 1-800-925-3369, extension 3121210. The Research Participant Advocate is a university representative who can discuss your rights as a participant with you or any concerns that you may have. Walden University's approval number for this study is __-__-__-_____, and it has an expiration date of ##/##/####. Upon completion of this form, I will provide you with a copy for your records.

Statement of Consent

I have read the informed consent form and agree to participate in the study. If I have any questions, I will contact the researcher or the university. I understand that I have

the ability to withdraw participation at any time without penalty. By signing this form, I agree the terms explained above. Thank you for your time in considering participation in this study!

Printed Name of Participant _____

Date of consent _____

Participant's Signature _____

Researcher's Signature _____

Appendix D: Sample Letter of Cooperation

Tailor the yellow highlighted sections and remove red font before having the letter signed.

To the researcher: You must tailor a letter of cooperation for your study and obtain an ink or electronic signature from any organization that is willing to be involved in identifying potential participants or collecting data. Note that the letter of cooperation requirement is waived if the partner's ONLY role is to distribute research invitations (in the form of flyers, packets, or emails) on the researcher's behalf. This waiver does not apply to hospitals, universities, military organizations, or any other organization that has its own ethics/ research approval process; for these organizations, documentation of the site's approval is always required. Please send questions to IRB@waldenu.edu.

If ink signatures are obtained, the signed letters can be e-mailed as attachments to irb@waldenu.edu or faxed to 626-605-0472. Electronic signatures are also acceptable, however if used it is required that the signer of the form either e-mail it directly to IRB@waldenu.edu or be cc-ed upon the submission so the e-signature can be verified.

The letter of cooperation doesn't need to use the specific wording below but it must include the following:

a. Detailed description of any recruitment, data collection, memberchecking, and results dissemination activities that will occur at the site.
b. Detailed description of the involvement of any of the site's personnel, rooms, or resources.
c. Clarity regarding whether the site personnel are providing any supervision of the research activities (particularly if the local personnel will be relied upon to help resolve a crisis situation). If not, then it is assumed that only the remote faculty members are supervising the researcher.
d. For program evaluations and intervention studies: The letter must include clear indication of the facility's role in sponsoring and assuming liability for the program/intervention under study. (Walden cannot sponsor, oversee, or assume liability for any type of program or intervention.) If the site is making any modifications to its standard intervention/program procedures in order to accommodate the research study, the letter needs to confirm that the site is willingly adopting these changes as part of their normal operations during the course of the study.

Sample Letter of Cooperation from a Research Partner

Community Research Partner Name
Contact Information

Date

Dear Researcher Name,

Based on my review of your research proposal, I give permission for you to conduct the study entitled Insert Study Title within the Insert Name of Community Partner. As part of this study, I authorize you to Insert specific recruitment, data collection, memberchecking, and results dissemination activities. Individuals' participation will be voluntary and at their own discretion.

We understand that our organization's responsibilities include: Insert a description of all personnel, rooms, resources, and supervision that the partner will provide. We reserve the right to withdraw from the study at any time if our circumstances change.

Include the following statement only if the Partner Site has its own IRB or other ethics/research approval process: The student will be responsible for complying with our site's research policies and requirements, including Describe requirements.

I understand that the student will not be naming our organization in the doctoral project report that is published in Proquest.

I confirm that I am authorized to approve research in this setting and that this plan complies with the organization's policies.

I understand that the data collected will remain entirely confidential and may not be provided to anyone outside of the student's supervising faculty/staff without permission from the Walden University IRB.

Sincerely,
Authorization Official
Contact Information

Walden University policy on electronic signatures: An electronic signature is just as valid as a written signature as long as both parties have agreed to conduct the transaction electronically. Electronic signatures are regulated by the Uniform Electronic Transactions Act. Electronic signatures are only valid when the signer is either (a) the sender of the email, or (b) copied on the email containing the signed document. Legally an "electronic signature" can be the person's typed name, their email address, or any other identifying marker. Walden University staff verify any electronic signatures that do not originate from a password-protected source (i.e., an email address officially on file with Walden).

Appendix E: Interview Protocol

1. Introduce myself to the participant(s) and describe my role as a student and researcher.
2. Ensure the Informed Consent form has been signed.
3. Remind participants of their voluntary participation in the study and right to withdraw at any time.
4. Briefly provide an overview of the study with the interviewee, explaining the intention of the study is to understand how information security managers develop and implement strategies to reduce security breaches by improving employee compliance with company policy.
5. Remind the participant that the interview will be recorded and inform them when the audio recording is about to begin.
6. Start the interview with the demographic questions and proceed in a semi-structured fashion, allowing for flexibility in re-ordering the questions or asking clarifying or new questions based on the interviewee's responses.
7. At the conclusion of the interview, thank the interviewee for their participation in the study.

Interview Questions:

Demographic Questions

1. What is your current title and role?
2. How did you become involved in information security?
3. What role do you play in managing information security policy and strategy?
4. How many years of experience do you have in this type of role?
5. In your experience, what responsibilities do you have in regards to information security?

Interview Questions

Strategy

1. What types of policies and strategies do you manage?
2. What roles within your organization assist in the development and execution of security policy and strategy?
3. What strategies do you use for information security practices?
4. What strategies have you found to be most effective? What strategies have you found to be ineffective?
5. What factors play a role in the decision of how to implement information security strategies?
6. What are the benefits of implementing information security strategies?
7. What are some of the challenges of implementing information security strategies?

8. What role do external factors or entities, such as a standards body, play in deciding which strategies to implement?
9. What other factors or tactics might you consider adding to improve information security strategies?
10. How do you develop an information security policy or program that does not fall into the “one size fits all” mentality?
11. Do you have the flexibility to create policy based on departmental needs or are there a corporate policies or guidelines that must be followed?

Compliance

12. How might a consistent and coherent strategy help improve security policy compliance?
13. What prompts the need for information security practices?
14. Is employee compliance with information security policies tracked/audited?
15. How is non-compliance enforced?
16. Have you found that there is a direct correlation between low compliance with policy and increased security breaches?

Training/awareness

17. How are employees educated on new threats?
18. How do local cultures/language/slang impact training and policy development?

19. How do you educate yourself on the constantly changing security landscape and use that knowledge to create or update new or existing policies and programs?
20. How often are training programs updated?
21. How do you balance the combination of technological solutions and the human factor in developing a comprehensive information security strategy?
22. How do you manage the need for strong security AND providing employees with a productive work environment (e.g., do security procedures slow down employees from getting their work done?)

Culture

23. What do you believe are the fundamental steps in building an information security culture?

Human Factors

24. What human factors do you believe contribute to poor information security compliance?
25. As an information security manager, how do you guard against the human factor when developing strategies and new training?
26. Are you aware of any behavioral theories, such as Planned Behavior Theory, Planned Motivation Theory and the Theory of Reasoned Action, that may influence policy and strategy development?
27. What's next for information security training and awareness? What new technology or training methods are on the horizon?

28. Is there anything else you would like to add before we close out the interview?