2017

The Training Deficiency in Corporate America: Training Security Professionals to Protect Sensitive Information

Kenneth Tyrone Johnson
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Kenneth Johnson

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. Alexandre Lazo, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Steve Roussas, Committee Member, Doctor of Business Administration Faculty

Dr. Peter Anthony, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

The Training Deficiency in Corporate America: Training Security Professionals to Protect Sensitive Information

by

Kenneth T. Johnson

MS, Trident University International, 2011

MS, Trident University International, 2009

BS, Trident University International, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2017

Abstract

Increased internal and external training approaches are elements senior leaders need to know before creating a training plan for security professionals to protect sensitive information. The purpose of this qualitative case study was to explore training strategies telecommunication industry leaders use to ensure security professionals can protect sensitive information. The population consisted of 3 senior leaders in a large telecommunication company located in Dallas, Texas that has a large footprint of securing sensitive information. The conceptual framework on which this study was based was the security risk planning model. Semistructured interviews and document reviews helped to support the findings of this study. Using the thematic approach, 3 major themes emerged. The 3 themes included security training is required for all professionals, different approaches to training are beneficial, and using internal and external training's to complement each other. The findings revealed senior leaders used different variations of training programs to train security professionals on how to protect sensitive information. The senior leaders' highest priority was the ability to ensure all personnel accessing the network received the proper training. The findings may contribute to social change by enhancing area schools' technology programs with evolving cyber security technology, helping kids detect and eradicate threats before any loss of sensitive information occurs.

The Training Deficiency in Corporate America: Training Security Professionals to Protect Sensitive Information

by

Kenneth T. Johnson

MS, Trident University International, 2011

MS, Trident University International, 2009

BS, Trident University International, 2008

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

August 2017

Dedication

To the greatest man I have ever known, my father! Thank you for challenging me to be a better man. I love you and miss you very much. To my mother who taught me how to write a book report and started me on this journey. You are amazing and I thank you for being a fabulous mother. To my wife and kids, you guys are supportive of my goals and now we can relax for a while and enjoy what is ahead of us. To all of my military men and women who I served with, thank you for your encouragement when my road was tough. To God, I appreciate your patience and understanding while I learned my way!

Acknowledgments

What a journey this has been! I started my education journey in 2006 when I was in the military not knowing what I wanted to accomplish. At the time, I was a single father and knew if I did not have my education, my kids would not have had a role model to look up too. Fast forward 11 years and I am at the pinnacle of my profession.

I cannot help, but think back on the long nights of writing papers, searching for the right reference, and making sure it was in APA format! To the people who have helped me along the way, I thank you more than words can express! To my chair, Dr. Lazo, what an amazing person you are! Thank you for taking the time to help me achieve a dream I never thought to be possible. To Dr. Roussas and Dr. Anthony, thank you for challenging me to perform at a high level.

Lastly, I would like to thank some individuals who are here in spirit and those who had no idea of their contribution to my success. Haywood Johnson Sr., my father. Although, you may not be here to witness me walk the stage, know that your legacy lives on and thank you for every lesson. To my mom, thank you for teaching me how to write a book report. To my kids, you are the reason I wake up and the reason I work so hard, I love you both! Special thanks to my friends Calvin Thomas, Linda McIntosh, and Tina Hampton for being supportive and encouraging during this journey. Finally, my wife, Tina, for the last four and half years you had to put up with me, and you never complained. You supported me when I thought I was going to lose my mind pursuing this degree. I want to thank you because without you none of this is possible as you have been my rock! I love you!

Table of Contents

List of Tables

Section 1: Foundation of the Study

In information technology, having a training plan is essential to the success of the business (Elnaga & Imran, 2013). Senior leaders often called IT leaders, business leaders, or organizational leaders, have a significant role in shaping security professionals as they work to protect sensitive information from exploitation. Training is a common issue among security professionals as it is expensive and requires time away from work (Swarnalatha & Prasanna, 2013). Loyalty was a problem for senior leaders as they invest thousands of dollars in professional training to see individuals leave and go to work for a competitor (Swarnalatha & Prasanna, 2013). Without paying high salaries and providing up to date training, security professionals search for new opportunities providing those amenities. To combat the impromptu reduction of their workforce, senior leaders need to understand the individuals' importance in securing the network from unauthorized attacks (Swarnalatha & Prasanna, 2013).

Background of the Problem

Moone et al. (2014) suggested training is an essential component in providing an employee the aptitude, competencies, and the knowledge necessary to perform complex tasks. The value training has within an organization, companies still revamp, reduce, or eliminate programs to save money (Rida E-Fiza et al., 2015). Senior leaders understand the benefits and ramifications security training can have on a company such as stolen documents and loss of public trust (Amankwa et al., 2014). Senior security professionals can assist junior employees in obtaining useful skills with continual training on specific tasks centric to the mission (Shi, Wang, & Guan 2011).

Shi et al. (2011) suggested creating a professional development program is a lengthy process and needs permission from senior leaders and executives. The training requirements senior leaders place on security professionals do not always relate to situations real-world situations (Mierke, 2014). Implementing a professional development program was critical to the success of the senior leaders and their employees (Tawalbeh & Tubaishat, 2014). Without a proper training program in place, some security professionals have mishaps that could result in loss of sensitive information (Olusegun & Ithnin, 2013). The importance of a training program is critical to business, executives, and employee success (Anthony & Weide, 2015).

Problem Statement

Unauthenticated personnel could penetrate a defenseless system and access sensitive information through vulnerabilities left by untrained security professionals (Homoliak, Ovsonka, Gregr, & Hanacek, 2014). Security breaches are a common event, having cost organizations $145 million in 2014, up 9% from 2013 (Ponemon Institute, 2014). The general business problem was industry leaders do not provide adequate training to security professionals. The specific business problem was that some telecommunication industry leaders lack the training strategies to ensure security professionals can protect sensitive information.

Purpose Statement

The purpose of this qualitative, explorative case study was to explore training strategies telecommunication industry leaders use to ensure security professionals can protect sensitive information. The sample population for the study included senior leaders

in a large telecommunication company located in Dallas, Texas because the company has a large footprint of securing sensitive information. The results of the study could contribute to social change by increasing the success of area industry leaders in training strategies for protecting sensitive information. Data from the study may also have implications to help organizations survive in an environment where security professionals receive minimal training to protect sensitive information. The implications for positive social change could include improved organizational strategy changes in onboarding, continual, and specialized training helping deter cyber criminals from accessing sensitive information. These changes could result in a high quality, an effective cyber team that proactively secures an environment and stops breaches before hackers have an opportunity to steal and exploit sensitive information.

Nature of the Study

By exploring the training security professionals need to protect sensitive information, I believed a qualitative methodology was appropriate for the study. Frels and Onwuegbuzie (2013) noted that qualitative research methods are suitable for exploratory studies where there is a need to describe or explain events. Quantitative researchers concentrate on diving into the specific areas to establish relationships using statistics (Anyan, 2013). The mixed methods research includes both an exploratory qualitative component and hypotheses quantitative component (Frels & Onwuegbuzie, 2013). Park and Park (2016) stated qualitative method researchers concentrate on practical and theoretical findings or discoveries, based on research questions through field study in

natural conditions. I elected to use a qualitative method over quantitative and mixed method, as I did not conduct a hypotheses test.

An exploratory case design is an inquiry that is used by researchers to explore a phenomenon for clarifying the problem (Yin, 2013). A qualitative case study design requires an exceptional amount of research to examine the contents of a real-world problem (Yin, 2013). By utilizing an exploratory case study approach, I asked probing questions to gather information and relate the information to actual situations (Yin, 2011b). The nature of the study provided an opportunity to explore other qualitative designs for relevance and relationship to the phenomena. Per Marshall and Rossman (2011), some qualitative research designs include (a) narrative, (b) ethnography, and (c) phenomenological. Squire, Phoenix, Patterson, and Tambouku (2013) stated that researchers utilizing a narrative approach require the use of field text such as stories, autobiographies, and journals to tell a story. Similarly, the focus of the study was not to tell a story. Therefore, I will not use a narrative approach. Lichterman and Reed (2014) stated that researchers employ an ethnography design when comprehending how individuals use culture to provide meaning to reality and interpret social interactions between people and groups. Culture is not a focus of the study and eliminates ethnography as a possible design. Janesick (2011), stated a phenomenological design is a suitable choice for researchers introducing lived experiences of an individual or group that can provide a detailed and deep understanding of experiences. A phenomenological design was not appropriate for this study due to the requirement of lived experiences and the need for an in-depth understanding of experiences from participants.

Research Question

What training strategies do telecommunication industry leaders use to ensure security professionals can protect sensitive information?

Interview Questions

1. What strategies did you use to address the lack of training security professionals receive in your company?
2. What research and educational training occurred before you made the decision to implement a new training program?
3. What were the deciding factors leading you to implement a new training program for security professionals?
4. What positions in your organization require security training?
5. What benefits have you seen since implementation of the new security training program?
6. What additional information, if any, do you feel is pertinent to the purpose of this study that I did not address in the interview questions?

Conceptual Framework

The conceptual framework for the study followed the security risk planning model from Straub and Welke (1998). The purpose of the security risk planning model is to give managers the full spectrum of concerns and issues relevant to the task of securing sensitive of information in an organization (Straub & Welke, 1998). The security risk planning model has five phases: (a) recognition of security problem or need, (b) risk analysis, (c) alternatives generation, (d) planning decision, and (e) implementation. The

first phase, recognition of security problem or need, requires knowledge of the different security problems that can occur within an organization. The second phase, risk analysis, entails the analysis of how managers identify and prioritize risk. The third phase, alternative generation, involves the consideration of the different options on how to address risks. The fourth phase, planning decision, involves the generation of solutions to address different security risks or issues. The final phase, implementation, involves the realization of the plan that incorporates all the solutions to various security problems.

The security risk planning model applied to the study because the model provided a framework regarding the different components or factors that training security professionals need to know to protect sensitive information (Straub & Welke, 1998). The security risk planning model gave trainers the key components in considering the design of the training program intended to help security professionals secure sensitive information in their organization. Supporting the selection of the model, researchers such as Chen, Ramamurthy, and Wen (2015), Fenz, Heurix, Neubauer, and Pechstein (2014) have used the security risk planning model as a framework for the identification of all concerns and issues managers and administrators consider when securing sensitive information in an organization.

Operational Definitions

Security Professional: A security professional is an individual who implements security controls and performs a risk analysis to protect users of the network and sensitive information (Wang & Guo, 2014).

Leadership: Leadership is the act of using interpersonal skills to motivate and influence others to commit to the goals of a group (Berghel, 2014).

Senior IT Leader: A senior IT leader is an individual holding the title of chief executive officer (CEO), chief information officer (CIO), chief operating officer (COO), executive vice president, president, or vice president who can influence daily operations within the firm (Kawakami et al., 2014).

Training: Training ensures individuals have access to problem-solving tools to learn effectively about any structure or component (Hendrix, Al-Sherbaz, & Victoria, 2016).

Assumptions, Limitations, and Delimitations

Assumptions

An assumption is an aspect believed to be true without verification but are so basic the research problem itself could not exist (Dumangane, 2013; Halkier, 2013). I had four assumptions when conducting this study. The first assumption was each interviewee has a level of interest in the results of the research. The second assumption was that the sample population of interviewees would provide a response that represented most of the organizational leaders with security professionals in positions to protect sensitive information. The third assumption was participants would interpret all questions in the same manner based on the definitions and descriptions in the interview. The fourth assumption was each participant understood he or she had the right to remove himself or herself from the interview at any time.

Limitations

Limitations are characteristics of design or methodology that impact or influence the interpretation of the results of a study (Wei, McCune et al., 2016). My professional background as an engineer could lead to bias and manipulation of the data. To mitigate bias, a researcher can conduct a self-test to ensure bias does not affect the outcome of the research (Yin, 2009). It is natural to have some bias when conducting an interview about the strategies used to effectively training employees. However, to minimize bias, following the research protocol without the insertion of personal views and provide a respondent validation check to address the limitation.

Delimitations

Delimitations are restrictions or boundaries that researchers impose to focus the scope of a study (Wei et al., 2016). The study participants were from a telecommunications company with the titles of positions of director, executive director, and assistant vice president. The participant pool participants reside from a single organization in the Dallas, Texas area.

Significance of the Study

Contribution to Business Practice

The reason I conducted this qualitative case study was to explore training strategies telecommunication industry leaders need to ensure security professionals can protect sensitive information. The study findings may be of value to area telecommunication industry leaders as it could allow the telecommunications industry to increase their overall productivity while reducing the attack vectors hackers use to exploit

networked environments. The inherent vulnerabilities of any network require a highly skilled professional to administer and protect the network from additional exploitation (Gupta, Chaudhari, & Chakrabarty, 2016). Without highly trained security professionals, companies are inviting unauthorized people to attack and steal sensitive information from the network (Stern, 2017). The leaders of companies need to provide continual training to ensure security professionals remain abreast to threats, risks, and vulnerabilities associated with the environment they support.

Implications for Social Change

The findings of this study may assist in positive social change for proactive threat mitigation. Training is an essential part of being a security professional, and without proper training, sensitive information is vulnerable to exploitation (Amankwa, Loock, & Kritzinger, 2014). Business leaders providing training to security professionals may reap the benefits of a more intelligent workforce with lower churn rates resulting in fewer successful attacks. The benefit to the local communities are more sponsor run programs where families can learn how to protect passwords, online banking information, and learn how to detect fraudulent emails.

A Review of the Professional and Academic Literature

The purpose of this qualitative explorative case study was to explore what training security professionals need to protect sensitive information. I interviewed leaders in the telecommunications business located in central Texas, asking for their perceptions about security training for their employees. The results from this study will help to inform

senior leaders in promoting a robust security training program to aid security professionals in advancing their skills to protect corporate resources.

The literature review addressed several themes related to this study. The themes are training as a company strategy, importance, and benefits of employee training, training costs, and security training of senior leaders. Existing studies, as well as peer-reviewed journal articles, provide a context for the research problem. Specifically, the literature review had various themes that provided support to the research problem, the purpose of the study, and the research questions of the study.

There are two main sections in the literature review: (1) definition of training and (2) training programs in organizations. To start the discussion, I focused on defining training. The discussion continued about how training is a company strategy. Training is a major activity of the organization to develop the skills and potential of the employee (Rob, McLorn, & Tural, 2016). In the next phase of the discussion, I focused on security training security professionals require to protect sensitive information. In the final phase of the discussion, factors such as a security training program, the importance of security training program, and the assessment of the effectiveness of the security training programs had a focal point.

The search for related data about security training was exhaustive. The use of various databases was to ensure there were peer-reviewed journal articles included in the literature review. The databases I utilized in the study included EBSCO database, Emerald database, SAGE Journals Online, PsycARTICLES, and Taylor & Francis

Journals, please see table 1 for a complete list. The Walden University librarians provided helpful terminology to aid me in finding relevant articles for use.

Table 1.

List of Host Search Systems Used for Literature Review

Host System
EBSCO
SAGE
Google Scholar
ProQuest
Various Scholarly Books
IEEE
Computers and Applied Sciences Complete
ScienceDirect
Safari Tech Books
Academic Search Complete

I used keywords to collect data about what training security professionals need to protect sensitive information. The keywords used were *company strategy, IT professionals, training, employee training, and effects of security training.* I used several combinations of the keywords to gather as much information as possible. I limited the studies in the literature review to those published from 2013 to 2017 to provide the reader a current context of the problem and the need to explore the research problem. Some studies are older than 5 years and provided value to the study; Table 2 provides a full breakdown of references used in the study.

Table 2.

Summary of References in the Doctoral Study Proposal

Reference type	More than 5 years old 1998-2012	Less than 5 years old 2013-2017	Total
Total Literature used in current study	27	166	193
Dissertation/doctoral studies	0	0	0
NonPeer-reviewed articles	4	8	12
Peer-reviewed articles	23	158	181
Percentage of peer-reviewed and non-peer reviewed articles	13.99%	86.01%	100%

Note: This table summarizes the references used in the entire doctoral study.

Definition of Training

Training has become a popular topic in the world of information technology (Beebe, Young, & Chang, 2014; Suby & Dickson, 2015). There are some jobs that only require certification, as well as a few years of experience to get an interview (Posey, Roberts, Lowry, Bennet, & Courtney, 2013). For most companies, the emphasis is to acquire inexpensive labor and let them learn by handling situations they do not have the skills to handle (Beebe, Young, & Chang, 2014; Suby & Dickson, 2015). This behavior leads to problems that those individuals are unable to resolve (Posey et al., 2013). Proper training comes through experience and a series of academic courses and materials (Suby & Dickson, 2015). New employees should work with an experienced professional to learn the landscape of the environment before taking on tasks without supervision (Suby & Dickson, 2015). Providing the proper training will reduce mishaps related to inexperience (Suby & Dickson, 2015).

Training is a learning process that involves the attainment of knowledge, enhancement of skills, and improvement of the attitudes and behaviors of the employees

to improve their performance (Abawajy, 2014). Another definition by Khattak, Rehman, and Rehman (2014) is training is about evaluating and refining an employee's skills as well as improving their weaknesses. There are some companies who use "training and development" in the workplace to improve the performance of their employees (Khan, 2012). Training programs are also one way to ensure that employees are knowledgeable about the current changes in their industry (Abdul & Asra, 2013).

There are similarities in these definitions. First, the focus of training is on employees. Second, training is all about acquiring knowledge, skills, and abilities. Lastly, training aims to improve the performance of employees.

There are two categories of training: on-the-job or off-the-job (Antonioli & Della Torre, 2015). On-the-job training takes place in a normal workplace. Trainees have access to the actual tools, documents, and materials that they will use when they have finished the training program. On-the-job training is effective for vocational jobs.

On the other hand, off-the-job training is training that takes the trainee away from the usual work environment. One of the advantages of off-the-job training is that the trainee can concentrate more on the training itself. Konings and Vanormelingen (2015) suggested this type of training is effective when the company wants to instill concepts and ideas into the trainees.

In this study, the focus is on-the-job training since it is about security training of the employees. Employees enter training programs to ensure they can handle confidential information at any time. The confidential information is specific to their workplace (Antonioli & Della Torre, 2015).

The demand for training internally instead of externally is due in large part to costs. A company does not want to pay thousands of dollars to send an individual to train if they believe that person will leave shortly after receiving the specialized training (Abawajy, 2014). Internal training can consist of web videos or a certified person teaching peers and giving time to the students to study on their own. External training is something that most employees need because the vendor of the software or hardware has a highly-trained instructor leading discussions and providing real-world situations (Purohit, 2015). The focus of this study was to explore what training security professionals need to protect sensitive information.

Training Programs in Organizations

Training remains a popular topic of conversation in the world of information technology (Beebe, Young, & Chang, 2014; Suby & Dickson, 2015). There are some jobs only requiring certification, as well as a few years of experience to get an interview (Posey et al., 2013). For most companies, the emphasis is to acquire inexpensive labor and let them learn by handling situations they do not have the skills to handle (Beebe, Young, & Chang, 2014; Suby & Dickson, 2015). This behavior leads to problems that those individuals unable to resolve (Posey et al., 2013). An established training program would alleviate unqualified individuals from handling situations suited for experienced professionals (Beebe et al., 2012; Posey et al., 2013).

Proper training comes through experience and a series of academic courses and materials (Suby & Dickson, 2015). New employees should work with an experienced professional to learn the landscape of the environment before taking on tasks without

supervision (Suby & Dickson, 2015). Providing the proper training will reduce mishaps related to inexperience (Suby & Dickson, 2015). Beebe et al. (2012) recommended the use of proper training to reduce accidents or work problems.

The goal of any organization is to have a staff of well-trained employees that can train new talent and provide them ample time to learn about the environment before turning them loose to administer the network (Min, Magnini, & Singal, 2013). Beebe et al. (2012) stated training programs in organizations need to have hands-on experience. Min et al. (2013) emphasized the need for on-the-job training because it pairs a new employee with an experienced veteran.

Training provides different benefits for all kinds of organizations. A good training program is one that can provide the new employee with valuable information about the network that can aid the employee in carrying out tasks (Min et al., 2013).

Several researchers have shown training is necessary to have an adequate supply of employees capable and competent of working in the workplace (Alshery, Ahmad, & Al-Swidi, 2015; Elnaga & Imran, 2013; Yamoah, 2013). Alshery et al. (2015) emphasized the need for a continuous process of professional development among employees in a corporation. Yamoah (2013) argued that training is also one way to develop the career of an individual. Alshery et al. (2015) argued that lack of proper training for employees would be a disadvantage to the company. In their studies, Elnaga and Imran (2013) and Yamoah (2013) concluded that lack of proper training would only lead to problems for the company.

Training is a major program for HR departments and employees will develop based on the content received and their application of the information (Rob, McLorn, & Tural, 2016). In today's competitive world, training would be the key to attaining the objectives of the organization. Training is advantageous to improve the performance and the effectiveness of the organization. Educating and enhancing the performance of employees provides a more intelligent and more efficient employee in a competitive world. Training is both beneficial for the employee and organization because each entity understands the importance training can have when taking on and completing tasks (Niazi, 2011). An employee trained by the organization can face current, as well as future, challenges of the organization. In this sense, a trained employee will contribute to the competitive advantage of the organization. Salas, Shuffler, Thayer, Bedwell and Lazzara (2015) stated that training is beneficial to organizations. Highly skillful and knowledgeable employees are the key to the success of any organization (Salas et al., 2015).

Organizations play a critical role in improving the performance and productivity of an employee to maintain a top of their industry (Salas et al., 2015). This means a significant difference exists between organizations that develop and conduct training programs for their employees and organizations that do not develop and conduct training programs for their employees. McGettrick (2013) suggested a training program provides employees with the necessary tools to perform their professional responsibilities effectively.

Training of employees produces tangible and intangible results (McGettrick, 2013). The impact training has on an organization and employee performance directly relates to the organization being efficient handling risk, expenses and cost, and providing quality training to employees who have a direct effect on security in the company (McGettrick, 2013). However, training must incorporate the vision and mission of the organization (Rob, McLorn, & Tural, 2016).

Trained employees are valuable assets to the organization (McMahon, Serrato, Bressler & Bressler, 2015). Reinsch and Gardner (2014) also conclude that trained employees are assets. One of the reasons for this is because a trained employee can lead to the attainment of long-term objectives of the organization. Moreover, training also leads to the improvement of the interpersonal skills of the individual (Reinsch & Gardner, 2014). Thus, training is beneficial to both the organization and employee, and there should be training available to build and maintain a workforce of workers who are efficient and skilled (McMahon et al., 2015; Reinsch & Gardner, 2014).

Bhatti, Battour, Sundram, and Othman (2013) stated training programs are effective when people are engaged. One of the ways to determine the effectiveness of training programs is training design (Bhatti et al., 2013). A training design is an element of a training program designed to provide structure for the development of instruction (Morgado et al., 2016). Training design deals with the transfer of learning from the training program to the trainee. One of the parts of transfer design focuses on whether the training instruction in the training program aligns with the job requirements of the position. In the literature, the observation of examination of a transfer-oriented training

program would offer the significant information needed to develop training environments more conducive to learning, leading in turn to productivity (Morgado et al., 2016). Identifying the training requirements of the employees, the transfer of training, and the evaluation of benefits of training programs are crucial activities, as well as exploring general training factors that include types of training, selection criteria, instruments, and which trainees would undergo which training (Morgado et al., 2016).

Another factor to consider in measuring training effectiveness is the implementation of the program. To determine what kind of training program to implement, complete an analysis of training needs, a development of training program based on training requirements, execution of the training program, and evaluation of the training program. Bhatti et al. (2013) stated motivated employees participate in training programs if they see there is a need for it. The more motivated the employee, the more quickly the trainee would acquire the new skill or knowledge needed (Bhatti et al., 2013). In the current context of organizations today, there is a need for security training for all employees.

In the workplace, there is more diversity of generations than at any other time in history (Velasco, Villar, Lunar, & Velasco 2016). Due to the influx of diversity, organizations have challenges to ensure equality. A multigenerational workplace would present both challenges and opportunities. To identify the characteristics of each generation, we must comprehend their work ethic and their potential to lead a successful organization (Mencl & Lester, 2014). In the training and development of a multigenerational workforce, HR should understand and appreciate the work style and

personality features of each generation and use those differences to create a stronger, adaptable, and intelligent workforce (Hillman, 2014; Hernaus & Vokic, 2014). As of this writing, three generations exist in the multigenerational labor force: baby boomers, generation X, and generation Y. The different experiences of each generation would influence their various work ethics, attitudes, and differing perspectives on the things in the world.

The multigenerational workforce should focus on retention and motivation (Juras, Brockmeier, Niedergesaess, & Brandt, 2014; Carpenter & de Charon, 2014). Training and development programs would help to retain and motivate employees from different generations (Juras et al., 2014; Carpenter & de Charon, 2014). However, it is important to note that each generation would react differently from the training and development programs (Juras et al., 2014).

Dunlap (2015) suggested that an effective training strategy is vital to company success as it serves as a method to develop individuals and can become an effective recruiting tool. Developing a strategy for training gives the company a competitive advantage over other firms by investing in the employee's education and future (Sung & Choi, 2013). The plan should be comprehensive and flexible as every employee learns differently and provides the best method to maximize the potential of the individual (Kim & McLean, 2014). Utilizing self-directed learning is an effective strategy for those who do not require the attention of an instructor (Bluestone et al., 2013). Kim and McLean (2014) emphasized that training programs must adapt to the needs and learning styles of the individuals.

Improves Competitiveness. To stay competitive in the open market for top talent, investing in education and development of employees is critical to the success of retaining these individuals (Lengnick-Hall & Inocencio-Gray, 2013). Most employers tend to focus on business functions such as downsizing and outsourcing work and expecting the same volume of work without the manpower. Cost and time are major factors as to why most companies do not send their employees to training. The cost of training (depending on the course) can range from hundreds to thousands of dollars, not including the certification test to validate the individual's comprehension of the training (Min, Magnini, & Singal, 2013). Bhatnagar and George (2016) stated the time required to send individuals to class would increase the workload of employees not sent and could lead tension among employees.

Leads to Innovation. One of the key aspects of competition in the market is to have innovative ideas produced by the employees. Training programs are effective when trying to improve the creativity and innovativeness of employees (Sung & Choi, 2013). Organizations with training programs tend to have more creative and innovative employees (Sung & Choi, 2013).

Creativity training is one way organizations can improve the innovativeness of their employees (Sannomiya, & Yamaguchi, 2016). Birdi et al. (2012) reported the effectiveness of "a theory of inventive problem solving (TRIZ)-based creativity training program" in an engineering firm. The authors collected data from a sample of 123 design engineers who will serve as trainees and 96 designers who are non-trainees. After the cross-sectional and longitudinal analyses of the strategies, results revealed that there were

short-term and long-term effects of the TRIZ training for the trainees. The short-term effects include an increase in creative thinking when it comes to problem-solving and an increase in motivating engineers to innovate (Birdi et al, 2012). The long-term effects include the trainees making suggestions about improvements in their work (Birdi et al, 2012). The training program provides engineers with innovative ways to improve their performance (Birdi et al, 2012). A similar study also explored the role of training in developing innovativeness of its employees. Abdullah, Ping, Wahab, and Shamsuddin (2014) collected data from 182 employees from 36 small firms. Based on the analysis conducted by Abdullah et al. (2014), it established that the training programs could explain 28.8% of the variance in the innovativeness of the employees. Abdullah et al. (2014) also emphasized that; "training is proved to be one of the significant predictors of employee innovativeness and all its dimensions (opportunity exploration, idea generation, idea promotion and idea implementation). This finding accentuates the importance of training among small firms, which should go beyond on-job training. In the face of business challenges, small businesses need to promote employee innovativeness through training" (p. 78).

One study concluded that training has an adverse effect on the innovativeness of employees. Saá-Pérez, Díaz-Díaz, and Ballesteros-Rodríguez (2012) carried out an empirical study on 139 small and medium enterprises. The authors concluded that "training per se has an adverse effect on the innovative capacity of SMEs. Only when training interacts with the knowledge assets of the firm does its effect become positive

and highly significant" (p. 230). As such, training programs alone do not have a positive impact on the innovativeness of the employees.

Employee's training affects knowledge creation in an organization that builds itself on the innovativeness of the employees. Kijek and Angowksi (2014) conducted a study with 650 Polish firms about the relationship of employee training and research and development (R&D) activities. The method utilized in the research was the Tobit model. It confirms that innovation-related training programs have a positive impact on employees and the R&D activities of the organization.

Increase Job Satisfaction. Training and development in a company can also affect the job satisfaction of the employees. In several studies, researchers found training and development influences job satisfaction and their intention to stay (Mcphail, Patiar, Herington, Creed, & Davidson, 2015). Choo and Bowley (2007) collected data from 135 frontline staff at one of Australia's largest bakery retail franchises. They used a structured questionnaire. Sixteen items in the structured questionnaire were about the training and development programs of the company, and six items were about job satisfaction. There were several major findings of the study. First, the effectiveness of the training program would be dependent on the quality, design, and experiences of the training program from the perspective of the employees. Second, you can attribute job satisfaction of employees to the company values, work environment, and work responsibilities. If companies want to enhance the satisfaction of their workforce, providing an active development and training program is key to their success.

The satisfaction of employees regarding personal training and development are important to consider in determining whether the training program is effective or not. In Huang, Lee, McFadden, Murphy, Robertson, Cheung, & Zohar (2016) study, they developed a framework to evaluate employee satisfaction with training. Four subscales were significant towards establishing an effective training program. Huang et al., (2016) concluded there was a need for companies to focus on employee capacity and employee development, as it was one of the key aspects of job satisfaction of the employees. Ghosh, Jagdamba, Satyawadi, Mukherjee, and Ranjan (2011) explored what indicators are necessary to conduct an effective training program for managers and non-managers. Ghosh et al., (2011) conducted a factor analysis that generated six factors on how manager and non-managers perceived an effective training program: "clarity of trainer, other facilities, venue of the program, food served, practical application, and communication of trainer." However, there were differences in how managers and non-managers prioritize the factors. It found managers prioritize the communication skills of the trainer, which suggests that the manager could relate better to the trainer if they have excellent communication skills given their intellectual superiority. Van Berkel, Boot, Proper, Bongers, & van der Beek (2014) determined the effectiveness of the training program based on the characteristics of the trainers. They collected data from a structured questionnaire from 80 employees chosen through simple random sampling. Employees found two features that are significant indicators of their satisfaction with the training program, which were the comfort level of the trainer and the rapport of the trainer with

the trainees. In these two studies, an effective training program should include an instructor with effective interpersonal skills and communication skills.

Satisfaction and engagement have a relation with one another. With training, employees are more satisfied and engaged. To have an effective conversation with the human resources department, each person must commit to solving the problem (Arrowsmith & Parker, 2013). The HR department of any organization should also consider the employees are their business partners. Moreover, there should be a purposive approach towards employee engagement, such as developing training programs for the employees. Another way to ensure the satisfaction and commitment of employees is to hear the employee voice (Rees, Alfes, & Gatenby, 2013).

Increases Productivity. Training and development programs also have an impact on the productivity of the employees (Nda & Fard, 2013; Shaheen, Naqvi, & Khan, 2013). There are several definitions of employee productivity in the literature. Fujishiro & Heaney (2017) suggested employee productivity is personnel satisfied with their work and can utilize their entire skillset to affect a positive outcome. Employee productivity is simply about the relationship between the input and output.

In today's workplace, companies must be more productive than in the past because consumers are demanding more products and services (Grip & Sauermann, 2013). Thus, it is important to have trained employees with the appropriate job and the aligned experience and qualification so that the company can survive the competitive market. The success of the business would depend on a workforce that is skilled, knowledgeable and well experienced. One of the main reasons training is necessary is

because it is a fundamental and efficient instrument that helps employees attain their goals and success within the organization. Training not only improves the resources of the employees and the organization, but it also increases the productivity of the employee. Thus, training also increases the productivity of the organization.

Training is an important aspect of enhancing the productivity of the employee and organization (Konings & Vanormelingen, 2015). The research shows training is a core instrument for achieving objectives of the organization and increasing the productivity of the organization (Raza, 2014).

Training is one of the ways to enhance the productivity of the employees and to communicate clearly the goals and mission of the organization (Ahmad, Tariq, & Hussain, 2015). Strohmeier (2013) stated if organizations invest in training employees, they invest in the development of skills in areas of teamwork, interpersonal relationships, decision-making, and problem-solving. This is beneficial to the organization because it enhances the performance of the employees. Training also has an impact on the behavior of employees because they feel more confident about their skills.

In organizations, training plays a crucial role in improving both performance and productivity of the employee that would put the organization in the best position to face competitors and stay at the top of the industry. This means a significant difference exists between organizations that develop and conduct training programs for their employees and organizations that do not develop and conduct training programs for their employees. A training program is something training manager's plan and organizes for employees of

all levels to increase their knowledge, skills, and abilities necessary to perform their job duties.

Previous studies have shown a positive relationship between training and employee performance, as well as employee productivity. As such, training is beneficial for both the employee and the organization (Burgard & Görlitz, 2014; Colombo & Stanca, 2014; Konings & Vanormelingen, 2015). Organizations that are profit-based provide quality service to their stakeholders and consumers, which is the reason these organizations invest in specialized training programs for their employees.

The standards set by the organization provide feedback and measure their skills. Employees measure themselves against the standards established by the organization. Good performance of employees would mean that the employees have performed the task assigned to them. In every company, there is an expectation that employees should provide good performance. When these employees meet the expectations of the organizations, then they are good performers.

Georgiadis and Pitelis (2014) researched explored the impact of training programs to managers and employees in the food industry in U.K. The authors conducted a randomized natural experimental design study. Based on the results of the study, the training program has a stronger positive effect on the employees regarding their productivity and profitability than that of the managers (Georgiadis & Pitelis, 2014). Training is the most effective strategy to improve the commitment of the employee to drive organization performance (Brum, 2007). Khanfar (2011) supports Brum's claim regarding the performance of employees provided through training. Training had a

positive impact on employee motivation and engagement (Georgiadis & Pitelis, 2014). Datta and Davies (2014) endorsed providing sufficient time throughout the work day to train employee's. Datta and Davies (2014) suggested training was important to improve processes within the organization.

Many factors go into influencing the success of an organization; however, human resource is an essential factor. The goal of training is to improve the effectiveness of the organization. It has an influence on the performance of the employees. Training also improves the organizational performance as indicated by the employee performance. Hasan, Zgair, Ngotove, Hussain, and Najmuldeen (2015) stated having training improves the organization's effectiveness, productivity, profitability, and other revenue driven items that link back to training employees. In summary, training, along with other factors, has a positive relationship to the increase in productivity in an organization.

Enhances loyalty to the organization. Employees need to feel that their employers care about their future (Ineson, Benke, & László, 2013). When the managers take a genuine interest in employee development, the results are beneficial. Employees who felt appreciated stayed with the company in tough times as they feel a sense of loyalty (Kumar & Shekhar, 2012). Advancement is a major concern for some employees because people do not work hard to stay in the same position forever. Having a plan to promote individuals will help prove to employees if given the opportunity to take advantage of the training tools the possibilities are available to rise and receive the responsibility they yearn for (Kumar & Shekhar, 2012).

Jehanzeb, Rasheed, and Rasheed (2013) explored the impact of training on the organizational commitment and turnover intentions of employees in the private sector in Saudi Arabia. Jehanzeb et al., (2013) administered a questionnaire to 251 employees of private organizations in Saudi Arabia. The results support that there is a negative relationship between organizational commitment and turnover intention. Moreover, the training of employees positively links with organizational commitment, turnover intentions, and the commitment-turnover relationship (Jehanzeb et al., 2013).

Ineson et al., (2013) collected data from 600 employees of hotels in Hungary and explored the relationship between job satisfaction and employee loyalty. Employees are likely to be loyal to a company if satisfied with their duties and pay (Ineson et al., 2013). Some of the factors that influence job satisfaction and employee loyalty are career development, recognition, salary, treatment of the managers, and social involvement. However, the treatment of managers of the employees and the social involvement factor in the workplace are more influential to employee loyalty more than monetary rewards.

The quality of peers also affects employee loyalty (Carter, Armenakis, Feild, & Mossholder, 2013). When the employees work together, the employee will associate this with a positive work environment (Carter et al., 2013). If there is increased employee loyalty, there is also an increased likelihood that employees would not change jobs. It will also lead to lower turnover intentions (Carter et al., 2013).

Within increasing employee loyalty, the likelihood of an employee recommending products, services, and promoting the workplace environment to prospective employees becomes higher (van der Heijden, Schepers, Nijssen, & Ordanini, 2013). As such, this

would help the recruitment process of the organizations. Employees who would recommend their company might also lead to lower expenses of the company in advertising and recruitment programs.

Increases Employee Retention. Retention of employees was significant and is a crucial aspect of every organization regarding competitive advantage because human resource is an essential and valued asset in today's highly competitive world (Shahin, 2014). The other resources in an organization are effortless; however, to retain talented human resource is the most difficult task for every organization. As such, several organizations concentrated on employee retention, which includes training and development of the employees.

IT professionals need training because they require constant reskilling throughout their profession (Gallagher, Gallagher, & Kaiser, 2013). The field of IT is broad, and the rate of change is quick. Thus, constant expansion and update of skills is a significant part of being an IT professional (Gallagher et al., 2013). The training of IT professionals also leads to increased retention as IT professionals expect various opportunities in their employer. Training of employees results in improved retention, which in turn reduced recruitment costs, as well as reduced the absences of the professionals (Fu & Chen, 2015). Carpenter and de Charon (2014) stated training was a critical retention tool. Carpenter and de Charon (2014) suggested training was part of the psychological contract of the employee to ensure they have opportunities to develop their skills.

Training Programs of IT Professionals. The demand for good IT professionals is high and requires advanced training to complete certain position requirements. A

training strategy provides a baseline and direction for employees to enhance their skills (Sum & Chorlian, 2013). As the IT industry continues to grow, it is important to have an established training program for employees to prevent high turnover and major accidents by not having properly trained employees. By identifying deficiencies in training, the training manager can create a specific training plan for each employee to close the knowledge gap (Sum & Chorlian, 2013).

The market for intelligent IT professionals is relatively small (Diedericks & Rothmann, 2014). Talented IT professionals demand higher pay and other benefits that employers are not willing to pay (Diedericks & Rothmann, 2014). The question remains, how do employers lure an exceptionally skilled IT professional to their business. The answer is not as simple as it seems. Although people need jobs to survive, they do not need jobs that are below their potential and do not interest them. Marketing to hire the right individual is difficult if one is looking for a certain skillset such as a malware analyst or a data loss prevention (DLP) engineer. These positions require highly skilled individuals who know how to read the data and report intelligent findings to upper management (Diedericks & Rothmann, 2014; Korsakienė, Stankevičienė, Šimelytė, & Talačkienė, 2015).

Security Training Programs in Organizations. Information in organizations is confidential. Cyber theft, mobile device loss, identity theft, misappropriation of confidential business information, and unauthorized disclosure of confidential and private data presents the danger to every organization, big or small (Sloan, 2014). It is important that senior leaders, managers, and employees undergo security training to secure private

and confidential information. Researchers and practitioners consider security training as an investment in the employees of the organization as emphasized by the effects of employee training discussion (Ahmad, Bosua, & Scheepers, 2014). Ahmad et al. (2014) suggested security training is a way to protect organizational knowledge and information, especially regarding maintaining the competitive advantage of the organization.

Senior leaders in any organization must warn employees about the importance of information security. Moreover, the organization must have security education and security training provided (Siponen, Mahmood, & Pahnila, 2014). Information security training is important so that the customers would know that the organization is doing everything to ensure that their private information remains protected (Safa et al., 2015). Ensuring the protection of customer's private information was due diligence of the organization (Alcaraz & Zeadallly, 2015).

Hacking events occur in the world (Mukati & Ali, 2014). Organizations and even government institutions have reported being hacked (Mukati & Ali, 2014). Despite organizations investing a considerable amount of money in technology, many of them failed to recognize that the human factor is also the weakest link in cybersecurity (Mukati & Ali, 2014).

Employees recruited from within are not always properly trained to secure confidential information (Flores, Holm, Svensson, & Ericsson, 2014). Hackers use high-tech techniques to acquire sensitive information. Ifinedo (2014) suggested preventing hackers from stealing is difficult, but a training program would help employees detect a potential breach.

Ifinedo (2014) suggested organizations will make mistakes but could avoid them by properly training their employees. One of the greatest security risks in an organization is the employee itself (Ifinedo, 2014). With the lack of adequate security training, hackers could exploit the weaknesses and cripple an organization. One way this could happen is an employees' use of a smartphone connecting to a Wi-Fi hotspot without knowing all the security risks (Mukati & Ali, 2014). Many employees are a victim of a phishing attack, data tampering, and other hacking methods (Flores, Holm, Svensson, & Ericsson, 2014). Because of this, hackers could get sensitive information from the employee that could lead to loss of brand reputation and financial losses of the organization (Lagazio, Sherif, & Cushman 2014).

Reasons Companies Implement Security and Awareness Training.

Mukati and Ali (2014) stated several organizations had implemented security and awareness training as one line of defense against insider threat. Most of the organizations have security and awareness training because of the benefits. The reasons organizations implement security and awareness training are to comply with regulatory requirements or recognize how their business will benefit (Mukati & Ali, 2014).

Fulfill regulatory requirements. There are an increasing number of laws and policies that require organizations to have training and awareness programs (Breaux & Gordon, 2013; Steiker, 2013). However, these programs would depend on the jurisdiction of the government. Per the U.S. Federal Sentencing Guidelines (2013), there are several factors that affect this judgment such as:

- "How frequently and how well does the organization communicate its policies to personnel?
- Are personnel getting effectively trained and receiving awareness?
- What methods does the organization use for such communications?
- Does the organization verify that the desired results from training occur?
- Does the organization update the education program to improve communications and to get the right message out to personnel?
- Does the training cover ethical work practices?
- Is there ongoing compliance and ethics dialogue between staff and management?
- Is management getting the same educational messages as the staff?" (Steiker, 2013, p. 27).

In 1995, the Department of Justice sentenced 111 organizational defendants under these guidelines with 83 cases having to pay necessary fines. In 2001, the organizational defendants rose to 238 with 137 organizational defendants needing to pay fines (Breaux & Gordon, 2013; Steiker, 2013). Moreover, 49 organizational defendants also received both fines and restitution. The average fine was $2.2 million while the average restitution was $3.3 million (Breaux & Gordon, 2013; Steiker, 2013). In 2006, there were 217 organizational defendants (Breaux & Gordon, 2013; Steiker, 2013). Only three organizational defendants had an effective compliance program. One of the inclusions of the compliance program to these guidelines is security training and awareness programs

(Breaux & Gordon, 2013; Steiker, 2013). A regulatory education program should have the following (Breaux & Gordon, 2013; Steiker, 2013):

- Address the interpretation of the company regarding security and privacy laws
- Policies that support activities and programs in the organization that mitigate risk and ensure security and confidentiality of information

Earn customer trust and satisfaction. Privacy breaches in organizations lead to a negative reputation for the organization (Nilashi et al., 2015; Safa et al., 2015). Customers need to feel that the organization is being responsible about their personal information. The organization must implement policies to protect personal information to gain and maintain customer trust (Nilashi et al., 2015; Safa et al., 2015). More than providing security training and awareness to employees, the organization should also keep the customer informed about the security training and awareness programs and security policies they have in store to ensure the protection of private and personal information of the customers (Nilashi et al., 2015; Safa et al., 2015).

The inclusion of some topics in security training and awareness programs include ensuring the consumers and customers receive the proper information. The customer needs to know that security training and awareness programs will result in (Nilashi et al., 2015; Safa et al., 2015):

- The organization protecting the personal information of the client from inappropriate exposure

- Employees' understanding that senior management is strict and serious in the protection of client's personal information
- The protection of the client's personal information through a written contract and compliance audits

All employees should receive security and privacy training and awareness before handling confidential information such as client's information (Nilashi et al., 2015; Safa et al., 2015). Moreover, there should be a refresher training program each year to ensure that employees know the updates. Employees must receive ongoing awareness communications to strengthen security and privacy issues (Nilashi et al., 2015; Safa et al., 2015). The goal is to help employees to embed such practices in their daily work and practices. The security and privacy campaign must communicate that the (1) company is duty-bound to fulfill privacy expectations, (2) employees must be knowledgeable about privacy principles, (3) employees must incorporate security and privacy policies in their daily activities, and (4) employees will face sanction as well as possible termination should they not comply with the security policies of the company (Nilashi et al., 2015; Safa et al., 2015).

Comply to published policies. Organizations are duty-bound to comply with their security and privacy policies (Dunn Cavelty, 2014). If employees do not comply with written policies in an organization, then these policies do not mean anything people outside the organization. Organizations need to train and educate their employees about the published policies, standards, and procedures that ensure security and privacy of the information of the organization (Dunn Cavelty, 2014). The design of the security training

and awareness should support compliance with these published policies. Senior management serves as a role model for employees and heavily influences the extent of employee policy compliance (Dunn Cavelty, 2014). Senior management should show support and show commitment to the security training and awareness events (Dunn Cavelty, 2014).

Exercise due diligence. Due diligence refers to the management of an organization ensuring that assets of the organization have protection in compliance with the legal and contractual obligations (Shackelford, Russell, & Kuehn, 2015; Whitman & Mattord, 2013). One of the examples of such assets is information. Due diligence is one of the powerful motivators for organizations to implement a security training and awareness programs (Shackelford et al., 2015; Whitman & Mattord, 2013).

The U.S. Federal Sentencing Guidelines (2013) and recent amendments have key provisions about organizations needing an effective compliance program and exercising due diligence to ensure prevention of criminal behavior and activities. One way to exercise due diligence is to have an effective information security education program supported by the senior executives of the organization. The sentencing guidelines motivate organizations to develop a program that reduces criminal conduct through an effective compliance program that includes fulfillment of all existing applicable laws and policies (Shackelford et al., 2015; Whitman & Mattord, 2013).

An organization must show its employees that it exercises due diligence not only through compliance, requirements and policies but also to promote a work environment that encourages ethical conduct and a strict commitment to comply with the law

(Shackelford et al., 2015; Whitman & Mattord, 2013). It is important to emphasize that the guidelines describe functional requirements that are clear and concise. The guidelines do not leave room for any other kind of interpretation. It does not matter what the organization calls the program whether it is a compliance program, security program, or ethics program. There are major features in the guidelines that should reflect in the program such as:

- Develop standards to prevent criminal conduct
- Implement procedures to identify and prevent criminal conduct
- Ensure each level has adequate resources for the program
- Perform personnel screening and assessment as applicable to ensure the responsibilities given to each employee
- Ensure effective and proper training and awareness at each level
- Ensure monitoring and evaluating activities to determine the effectiveness of the program
- Implement internal system where individuals could report anonymously to avoid retaliation
- Provide incentives and rewards to individuals who comply
- Enforce discipline to promote compliance at each level
- Review and assess violations to develop reasonable policies to prevent similar violations from happening (Shackelford et al., 2015; Whitman & Mattord, 2013).

The updated guidelines provide the coverage for security training and awareness programs when convicting an organization of a violation (Shackelford et al., 2015; Whitman & Mattord, 2013). The leader of the organization will face rigid sentences and civil penalties unless these leaders provide proof that they have a strict, well-communicated, and well-implemented compliance program (Shackelford et al., 2015; Whitman & Mattord, 2013). Organizational leaders bear the responsibility to ensure that all employees in their organization have a good understanding of the need to comply with the policies and the program. The guidelines require that executive leaders not only show support but also participate in the implementation of the security training and awareness program.

When exercising due diligence, a standard of due care must be observed. Leaders of the organization have a duty to ensure proper implementation of security training and awareness program (Shackelford et al., 2015; Whitman & Mattord, 2013). If leaders do not ensure that employees are trained to handle sensitive and private information and there is a breach or exposure of this information, then both the organization and leader could face legal cases for negligence. Thus, leaders should invest time and resources to ensure and establish an effective information security training and awareness program.

Develop positive corporate reputation. The reputation of the organization is one of its assets (Busch et al., 2016; Greenaway & Chan, 2013). With a good reputation, customers remain loyal, sales increase, and revenue increases. Without a good reputation, customers tend to find another organization, sales decrease, and revenue decreases.

The reputation of the organization must be continually managed (Busch et al., 2016; Greenaway & Chan, 2013). One of the ways to manage a good reputation is to ensure that executives and employees follow the information security precautions to lessen the risk of leaks and breaches in the organizations. Such incidents would lead to media attention harmful to the reputation of the organization. Executives of organizations are taking the issue of reputation very seriously and even includes it in developing the business strategy of the organization.

The security training and awareness programs help ensure the good reputation of the organization in various ways (Busch et al., 2016; Greenaway & Chan, 2013). First, the leaders of the organizations must recognize that there are risks and opportunities that could affect corporate reputation such as information security policies and practices (Busch et al., 2016; Greenaway & Chan, 2013). When a company demonstrates that it could protect and secure sensitive information, then it positively affects the reputation of the organization. On the other hand, when a company has a history of leaks and breaches, then it negatively affects the reputation of the organization. Second, develop government relationships at all levels to assist easily in compliance with various laws and policies (Busch et al., 2016; Greenaway & Chan, 2013). Third, develop security and privacy awareness programs to increase the publicity of the profile of the company (Busch et al., 2016; Greenaway & Chan, 2013). Fourth, organizations must develop different strategies both externally and internally to ensure consistency in its security and privacy policies. Lastly, the organization must establish high standards of security, confidentiality, and

privacy through training programs, campaigns, and activities (Busch et al., 2016; Greenaway & Chan, 2013).

There are several issues that influences corporate reputation that can be addressed through security training and awareness programs (Busch et al., 2016; Greenaway & Chan, 2013). One of the issues is customer complaints (Busch et al., 2016; Greenaway & Chan, 2013). If an employee knows how to handle customer complaints and ensure that the information of the customer is secured, then the customer would praise the organization. Through straightforward security and privacy policies, organizations can increase customer satisfaction levels. Both customers and employees value the perceived strength of the published information security and privacy policies.

The number of reported security incidents also affect the reputation of the organization (Busch et al., 2016; Greenaway & Chan, 2013). Employees are also more likely to adhere to strict security and privacy policies if they see that the organization is strict in implementing them. Employees also perceive the senior executives are role models. Thus, when there are a few security incidents then both employees and customers remain loyal to the organization. Few incidents also lead to a good reputation.

Ensure and promote accountability. Compliance programs ensure and promote accountability of the organization and for the employee regarding the security of information in the organization (Shackelford et al., 2015; Whitman & Mattord, 2013). Employees tend to perform at a much more efficient rate knowing their employers measure their performance. If an organization demonstrates the link between information security compliance and employee performance, then employees would be more

accountable for their behavior and actions and would most likely comply with the guidelines and policies.

Accountability has more influence on company and employee in the 21st century unlike in previous centuries (Shackelford et al., 2015; Whitman & Mattord, 2013). There is a growing number of cases filed against organizations about information security violations. There are times when the organizations are not necessarily the culprits in the violation, but these organizations have weak and poor practices that led to the incident (Shackelford et al., 2015; Whitman & Mattord, 2013). For example, organizations that have been a victim of hackers could also face legal actions because the information in their organization should have been protected even against hackers. Organizations should show proof that they have done everything they could to prevent the hacking incident (Shackelford et al., 2015; Whitman & Mattord, 2013).

Organizations must have effective information security practices in place to ensure the protection of their information (Shackelford et al., 2015; Whitman & Mattord, 2013). Organizations with poor information security practices will be held accountable. The U.S. government encourages organizations to increase employee accountability for information security.

Achieving accountability within an organization; leaders must ensure they have adequate information security training and awareness programs (Shackelford et al., 2015; Whitman & Mattord, 2013). These programs must be well-organized. The executive leaders must show support and participation in these programs. Training programs are ways to make employees accountable. Without support from the executive leaders,

failure of any training program is their burden. The organization must clearly state that it expects all concerned stakeholder to comply with the privacy and security policies.

Topics That Should be Included in the Security Training.

There are lots of topics included in security training. However, in reviewing the literature, there are only a few topics authors mentioned for inclusion. Some of the topics researchers would like to see in a security training plan are the following: (1) the issue that they will come in contact with company secrets and classified information (Ahmad, Maynard, & Park, 2014), (2) responsibilities of the employees in handling sensitive information (some employees need to sign nondisclosure agreements) (Kolkowska & Dhillon, 2013), (3) requirements in proper handling of classified information from the point the individual received them to the point the individual has to destroy the documents (Suby & Dickson, 2015), (4) using passwords or two-step authentication on one's computer (Grosse & Upadhyay, 2013), (5) becoming aware of computer security concerns such as phishing or hacking (Flores, Antonsen, & Ekstedt, 2014), (6) reporting of incidents that risk the security of classified information (Halbert, 2016), and (7) consequences of failing to protect classified information (Halbert, 2016).

Current Strategies to Protect Knowledge and Information.

Ahmad et al. (2014) synthesized several findings in the literature about strategies and mechanisms organizations implement to protect knowledge and information. The synthesis revealed surprising findings. Ahmad et al. (2014) found no evidence of a systematic approach to the identification and protection of knowledge. The approaches of most companies were often random and delegated to the owners of knowledge or

individual employees only. The negative effect of random and delegated training programs may falter if organizations choose this way of managing and protecting sensitive information. Second, the issues about the confidentiality of the operational data of the organization crowded out the attention of the manager to protecting the organization's knowledge and information assets (Ahmad et al., 2014). Based on the findings, organizations sometimes value one matter over another issue, and they cannot protect the confidential data of their customers and their knowledge of information assets (Ahmad et al., 2014). Ahmad et al. (2014) suggested more studies and more comprehensive frameworks to address the needs of every organization in providing training for their employees in handling confidential information of clients and organization.

Similar to Ahmad et al. (2014), Webb, Maynard, Ahmad, and Shanks (2014) assessed the current management strategies of organizations in securing confidential and sensitive information. Webb et al. (2014) identified three deficiencies in security risk management practices of organizations. First, risk assessments are commonly careless. Second, the evaluation of security risks is not comprehensive investigations. Third, the evaluation of risks in an organization is occasional rather than on a continuous basis. Webb et al. (2014) emphasized addressing these deficiencies. Moreover, each training program must incorporate the practices above while improving each training for all employees.

Assessment of security training effectiveness.

In any training program, there must be an evaluation to determine the effectiveness of the training program. However, no study found in the literature explored the assessment of security training effectiveness. One of the possible reasons for this is that information technology security training is a new training program. Lim, Maynard, Ahmad, and Chang (2015) specified there is no unified perspective of recommended security management practices, which is the why an assessment of security training effectiveness is difficult.

Summary

The training of employees was a task of the Human Resources Management (HRM) department. HRM included training and development of employees and associates it with increased work productivity, organizational effectiveness, competitive advantage, satisfaction, innovativeness of employees, and loyalty of employees. The suggestion HRM can increase the capability of companies to select, develop, and motivate a labor force capable of producing superior results. Training employees can relate to increased measures of performance. Most of the training programs have the objective to improve the performance of the employees in the short-term perspective and in the long-term vision to increase the competencies of the employees. Most jobs require knowledge, abilities, and skills that require training.

The productivity of employees helps organizations achieve a competitive advantage. In any industry, competitive advantage is necessary to remain the thought leader in their industry. Owners must understand the association between the success of

their company and the status and condition of their employees. Training provides an increase of productivity helping create a culture of productivity and effectiveness. With a rise in organizational productivity and efficiency, the company profits more money and can provide security training for employees. The primary reason organizations should consider training programs as an investment for their employees to increase productivity, competitiveness, innovativeness, satisfaction, and loyalty.

Employees who are skilled, creative, and productive can contribute to the improvement in the performance of the organization. Training is the most crucial part of human resource management to maintain the effectiveness of human resources. The majority of organizations acknowledge the value of training and is a significant factor that influences the success of the organization.

Training enhanced the knowledge, abilities, and skills of employees adding to the advantage, efficiency, and performance of the organization. Human resources or the employees are the most valuable assets in every organization together with machines and capital. Training is a systematic development of the knowledge, abilities, skills, and behavior of the employees for employees to do their job. Training can take place in several ways, inside the organization, and outside the organization.

Transition

The exploration of training security professionals to amass skills necessary to protect sensitive information requires an organized training program. The purpose of Section 1 was to provide a background of the issue regarding training security professionals to protect sensitive information. A qualitative, phenomenological study was

the foundation of the research on the connection between security professional and the lack of training received to secure sensitive information. Section 2 covers the method and design used to conduct the study and data collection strategies. By invoking a proper plan to measure the findings of the study, I found common themes to connect the reasons security professionals do not receive proper training. The findings and analysis are presented in Section 3.

Section 2: The Project

In this section, I will reiterate the foundation of this study. The general business problem was that industry leaders do not provide adequate training to security professionals. The specific business problem was that some telecommunication industry leaders lack the training strategies to ensure security professionals can protect sensitive information. The central research question was: What training strategies do telecommunication industry leaders use to ensure security professionals can protect sensitive information? In this section of the study, I will present the methodology used for data collection, data storing, and data analysis.

Purpose Statement

The purpose of this qualitative, explorative case study was to explore training strategies telecommunication industry leaders use to ensure security professionals can protect sensitive information. The sample population for the study included senior leaders in a large telecommunication company located in Dallas, Texas because the company has a large footprint of securing sensitive information. The results of the study could contribute to social change by increasing the success of area industry leaders in training strategies for protecting sensitive information. Data from the study may also have implications to help organizations survive in an environment where security professionals receive minimal training to protect sensitive information. The implications for positive social change could include improved organizational strategy changes in onboarding, continual, and specialized training helping deter cyber criminals from accessing sensitive information. These changes could result in a high quality, an effective cyber team that

proactively secures an environment and stops breaches before hackers have an opportunity to steal and exploit sensitive information.

Role of the Researcher

I served as the primary data collection instrument for this study. In qualitative studies, researchers are the primary data collection instrument as their perceptions and presumptions influence the way they ask questions, how they record and interpret answers, and the respondents' attitudes toward the study (Collins & Cooper, 2014). The data collection adhered to a general format based on the interview protocol (attached as Appendix C), but I did allow the flow of communication and took note of verbal and non-verbal cues during the interview. I am familiar with the topic of the study because I worked for the organization and did not receive security training as an employee. I conducted the doctoral study in Dallas, Texas. However, I do not have personal or professional relationships with the selected company or any potential partnerships.

In this study, there was participation by human subjects. As such, I took the necessary measures to ensure the study remained ethical, i.e. that the identity and welfare of participants remain intact (Brakewood & Poldrack, 2013; Harriss & Atkinson, 2013). The process involved three important principles. First, uphold respect for human subjects, I ensured all participants that took part in the study were voluntarily and they understood the purpose of the study and their role and rights as participants (Brakewood & Poldrack, 2013). Second, ensured beneficence, taking part in the study did not result in any harm to the participants; rather, they acquire new knowledge and information on the necessary training security professionals need to protect sensitive information (Brakewood &

Poldrack, 2013). Lastly, related to the principle of justice, I treated all participants equally and provided them with the same rights, respect, and courtesy (Brakewood & Poldrack, 2013).

To address personal bias, Kvale and Brinkmann (2009) advised researchers to produce study results previously cross-referenced and verified. As part of the content analysis, I supported each theme and conclusion generated using data from the interview transcripts as evidence. I conducted member checking to ensure that the interview transcripts accurately depict the views of the study participants. I strictly followed the phases by Straub & Welke (1998) security risk planning model to help facilitate an objective analysis of the qualitative data of this study. Also, I avoided expressing approval or agreement, or disapproval or disagreement, with the participants during interviews, through verbal or non-verbal cues, as recommended by Frels & Onwuegbuzie (2012). I ensured this study complied with three principles described in the Belmont report for ethical research, which as stated by Ross et al. (2013) are respect for persons, beneficence, and justice. I did apply three principles throughout this study using informed consent, assessment of risks and benefits, and through an equitable selection of subjects. The individuals participating in the study did not have their eligibility to participate based on their gender, race, or socioeconomic status. Each person met the inclusion criteria of this study and expressed their interest to participate in the study by signing the consent form.

Participants

In line with the purpose of this study, the study participants included senior IT leaders working in central Texas. My recruitment of the participants for this study, I used a purposive sampling strategy. A purposive sampling strategy is a type of non-probability sampling technique used in qualitative research (Draper & Swift, 2011). The strategy focused on recruiting participants who met a particular set of criteria related to the study (Protheroe, Brooks, Chew-Graham, Gardner, & Rogers, 2013; Merriam & Tisdell, 2015). To participate in the study, individuals met the following criteria: (a) worked at a telecommunication company located in central Texas, (b) had at least ten years of experience in information technology, (c) employed in a managerial position, and (d) had experience with training information security professionals. Aside from any previous relationship with an employee, the choice to select this organization is because the organization is successful in protecting sensitive information.

I gained access to participants by contacting former colleagues through social media to invite them to participate in the study. The use of technology and social media to gain access to participants was acceptable and common in qualitative research (Palinkas et al., 2013). I sent the participants an email containing the introduction letter (Appendix A) to participate in this study. The invitation included the purpose of the study, eligibility criteria for participation, and the nature of involvement expected from the study participants. I gained access to more participants by implementing a snowball sampling strategy, defined by Sanders et al. (2012) as a sampling strategy involving the use of members of a specific population to identify other potential participants for

recruitment. For those who declined to participate, I did not ask them if they could refer other individuals inside the industry who may be interested in taking part in this study. As part of expanding the search beyond the initial selection, I asked the participants to refer other individuals with senior IT leadership experience inside their current organization.

I established a working relationship with the participants through e-mail by answering questions they had about the study. By conversing with the participants before the interview, I established rapport, gained their trust, and, most importantly, ensured they understood the purpose of the study and the interviews (Maunder, Cunliffe, Galvin, Mjali, Rogers, 2013; Phelan & Kinsella, 2013). Qualitative researchers encounter challenges gaining access to participants but recommend methods to address this issue included using establishing links or connections and openness about the study (Opollo, Opollo, Gray, & Spies, 2014). As applied in this study, I focused on recruitment efforts of individuals whom I knew have experience and knowledge in information technology training.

Research Method and Design

Research Method

I used a qualitative case study to explore the training security professionals need to protect sensitive information. In qualitative studies, researchers collect data using the experiences of participants to contribute to the understanding of a particular phenomenon (Morse, 2015). The concept of perspective in qualitative studies is the existence of multiple realities for a single phenomenon, based on the subjective experiences of individuals with the phenomenon under investigation (Barnhill & Barnhill, 2013). The

purpose of using qualitative research methodology was to examine and understand a specific phenomenon (Janesick, 2011). The focus of qualitative studies is on the extraction of contextualized, multidimensional descriptions to add to current knowledge on the phenomenon (Holloway & Wheeler, 2013). Yilmaz (2013) stated qualitative researchers study their natural setting, attempting to make sense of or interpret phenomena regarding the meanings people bring to them. Also, the qualitative method was more appropriate for studies that conduct an exploration of a field that was largely unstudied (Annechino, Antin, & Lee, 2010), as was the case in this research study. Thus, in line with the purpose of the study, which is to explore what training security professionals need to protect sensitive information, I selected qualitative method as the most appropriate research method.

In a quantitative research method, I would need to test theories and relate truth to the numbers (Hussein, 2015). Therefore, quantitative research was not appropriate for this study. In quantitative research, the researcher drafts the methodology based on the research questions and hypotheses formulated to resolve research problems (Hussein, 2015). The focus of the quantitative researcher was to gather numerical data to quantify study variables and using the data to test for statistically significant relationships among the variables (Maltby, Williams, McGarry, & Day, 2014). Based on results of the data analysis, the quantitative researcher draws conclusions and generalizations (Maltby et al., 2014). Likewise, because there is a requirement in mixed methods studies of combining qualitative and quantitative methods (Golicic & Davis 2012), I determined a mixed

method study was inappropriate for this study. Based on the assertions, the quantitative and mixed methods were not appropriate for the study.

Research Design

The options for the research design included a case study, ethnography, narrative, and phenomenology studies. Each of these designs required an accurate data collection method and provides a channel to express thoughts. In phenomenological research, the objective is to explore lived human experiences (Maguire, Stoddart, Flowers, McPhelim, & Kearney, 2014). However, given the focus of the proposed study is to explore what training security professionals need to protect sensitive information, the phenomenology study is not appropriate for this study. Researchers using ethnography aim to comprehend how individuals use culture to offer meaning to reality and interpret social interactions between people and groups (Kriyantono, 2012). Similarly, the focus of this study is not to learn about a particular group. Therefore, ethnography was inappropriate based on the purpose of the study. The narrative research design was not appropriate for this study because I did not combine a participants' life with my own.

In this study, I used a case study research design. Case studies are a research strategy used to study a single phenomenon within a single entity (Yin, 2009). The objective of a case study was to explore an object and report findings (Maguire et al., 2014). Using a case study as the research method allowed me to obtain a deeper understanding of the problem based on the individual knowledge and experiences (Frels & Onwegbuzie, 2013). When I emphasized the importance of a person within a specific context or environment changes occurred where the individual felt empowered to

contribute (James, Cottle, & Hodge, 2010). The data in case study created a centralized account of the experience, with data analysis concentrated on interpreting these experiences about the subjective meanings for individual participants (Sissolak, Marais, & Mehtar, 2011). In this study, the data analyzed will comply with Straub & Welke's (1998) phased approach, discussed in a later subsection. The use of the Straub & Welke's (1998) phased approach will help to ensure that the data analysis is accurate (Yin, 2009).

Saturation in qualitative studies refers to the level of quality data collected in a manner where additional data will no longer contribute to the information and knowledge derived from existing data (Elo et al., 2014; Marshall, Cardon, Poddar, & Fontenot, 2013; Meyer & Ward, 2014). In other words, data saturation signifies comprehension and completeness of gathered data (Elo et al., 2014). To ensure saturation, I conducted a preliminary analysis after the interviews to ensure data completeness (Elo et al., 2014; Marshall et al., 2013; Meyer & Ward, 2014). If I did not achieve saturation, I would have interviewed more participants and created more themes or categories until full saturation of the data was complete (Elo et al., 2014; Marshall et al., 2013; Meyer & Ward, 2014).

Population and Sampling

The sample population for the study was senior IT leaders in a large telecommunications company in Dallas, Texas. I chose this sample population because its members possess adequate knowledge, exposure, and experience on the subject under investigation, which are key characteristics in choosing individuals for a case study (Jahangiri-Rad, Mousavi, & Rafiee, 2014; Merriam & Tisdell, 2015; Tobin & Murphy-Lawless, 2014). I selected the organization because of its leaders' experiences in security

management, which includes protecting sensitive information and addressing security threats, especially in the online environment. Participants in the study had at least ten years of experience in the field of information technology and leadership. I conducted the interviews virtually through Skype.

To gain access to the participants, I used a purposeful sampling strategy. Robinson (2014) defined purposeful sampling as a focus on recruiting efforts of individuals who meet specific inclusion criteria for the study or persons whose knowledgebase covers topics in line with the proposed study. Purposeful sampling strategies in qualitative research provide for the recruitment of information-rich cases about the topic of interest (Palinkas et al., 2013).

I started by contacting former colleagues within the chosen organization and invited them to participate in the study. I used the snowball method of purposive sampling to expand my search beyond the initial recruitment method. A snowball sampling strategy identified interest from people who know other information-rich people (Protheroe et al., 2013). As such, I asked all invitees to either decline or agree to participate, and to refer or recommend other individuals within the same industry with a similar background in information technology and leadership which I can invite to participate in the study.

My goal for sampling was to recruit enough participants to provide saturation for this study, with at least three participants. The sample size was based on several considerations (Robinson, 2014). Abdullah, Wahab, and Shamsuddin (2014) stated that rich information findings would compensate for a small sample size. First, the concept of

saturation was a focal point. Saturating the data ensured the case study had exhausted all avenues that could be pitfalls if examined by other experts in the field of information technology management (Robinson, 2014). Second, the concept of diminishing returns was also an issue, about the point in qualitative studies where the collection of larger volumes of data does not yield new information (Marshall et al., 2013). In the experience of most qualitative researchers, no new information comes from transcripts after interviewing three or more people (Green & Thorogood, 2013). Third, given that data collection and analysis in qualitative studies is more laborious and time-consuming, the use of a sample larger than three might not be viable or feasible (Marshall et al., 2013). Lastly, there was no exact target sample size, but collecting data until saturation was critical to explaining why companies have a lack of training in their organizations. Based on these, I targeted a sample size of three participants for the study. After I had assembled the final list of participants, I interviewed them in a convenient location accessible to the interviewee and me. I briefed the participants on the scope of the study, expectations, and measures to protect their information.

Ethical Research

Resnik (2011) defined ethical research as a method, procedure, or perspective used to determine the behavior and for evaluating complicated situations. Ethics are important to ensure legal requirements remain effective and to help provide a level of creditability to the research. As such, this study steers toward complying with all regulation set forth by Walden University and the IRB committee. Walden University's

Institution Review Board (IRB) assigned me approval number 04-19-17-0409369 after evaluating this study.

In compliance with these regulations, I sent the participants an introduction letter (Appendix A), and I asked participants to sign a consent form indicating their wiliness to participate. The consent form stated the expectations of the participants and the policies and procedures that are in place to uphold participant privacy and protect data confidentiality. In the consent form, I emphasized to the participants they would not receive incentives or rewards in exchange for their participation. I clearly stated the procedures to withdrawal from the study in the consent form. Individuals who wanted to withdraw from the study; simply needed to inform the researcher at any point. No participants withdrew from the study, but if they had, I would have turned over all data collected up to that point and destroyed the data immediately. The information provided to the individuals participating in the study was to ensure they understood the expectations and the corresponding risks and benefits of participation so they could make an informed decision on whether to take part in the study or not.

Each participant acknowledged the procedures for data storage and disposal by signing the consent form, which ensured their privacy and confidentiality. Each participant received a personal number to protect his or her personal information. Protecting the information of the participants is important to maintain confidentiality and integrity (Drtil, 2013). I stored transcripts, audio files, transcribed text, and coding information in a cloud storage folder and labeled it with identifying information known only to me. This procedure will ensure no one will access the information and identify

who the participants were. I will destroy the data after the 5-year anniversary of the study completion.

Data Collection Instrument

I was the primary data collection instrument for this qualitative case study, and I used a semistructured individual interview. Hershberger, Finnegan, Altfeld, Lake, and Hirshfeld-Cytron (2013) stated semistructured interview allows for an open discussion between the interviewer and the interviewee on a subject. I used a semistructured interview technique to focus on a topic and continued to gather information based on what the participant knew and was willing to share during the interview (Vogl, 2013). My process for the participants was to email a copy of the consent form, the introduction letter (Appendix A), a copy of the interview questions (Appendix B), and interview protocol (Appendix C) before the interview. At the start of each interview, I briefly reiterated the purpose of the study and the rights and role of the participants. I then asked the participants each question listed in the interview questions (Appendix B). I followed up questions or clarifications after each of the listed questions in the guide if it was necessary to elicit more detailed responses or explanations from the participants. The interview ended once all the questions in the interview guide, and follow-up questions had a sufficient explanation.

In conjunction with the interview questions, I used a qualitative codebook created in NVivo software, Dragon Dictation software to record and transcribe participants' responses in a web-based software application that assisted in discovering themes. Debbi, Elisa, Nigel, Dan, and Eva (2014) stated the lack of organizational documentation

provided additional evidence the research problem contributed to themes. The use of recording and transcribing added to the observation as a form of physical trace evidence of the personal interview process (Walshe, Ewing, & Griffiths, 2012).

As an added measure to improve the reliability and validity of the gathered data, I conducted member checking. Specifically, after I transcribed each interview, I sent the transcript to the respective participant for review. At this point, they had the opportunity to revise their responses and add supplementary information and comments as they see fit (Ciemens, Brant, Kersten, Mullette, Dickerson, 2014; Coffee, Raucci, Gloria, Faulk, & Steinhardt, 2013; Harvey, 2015). Such member checking process ensured the collected data and its subsequent analysis and interpretation accurately reflected the participants' perceptions and opinions (Ciemins et al., 2014; Coffee et al., 2013; Harvey, 2015).

Data Collection Technique

I was the primary data collection instrument for this qualitative case study, and I used semistructured interviews with open-ended questions. O'Keefee, Buytaert, Mijic, Brozovic, and Sinha (2016) suggested semistructured interviews rely on expertise, skill, ideas, and honesty of the researcher collecting data the for analysis. However, the data received during the interview may have a slightly different meaning to the researcher; seeking clarification of the information will help remove mistakes and save valuable time (Irvine, Drew, & Sainsbury, 2013). The use of interviews for data collection is advantageous as it allows the researcher to generate quotes and stories, establish rapport, and create a deeper and better understanding of participants' perceptions and experiences (Doody & Noonan, 2013; Ferwerda et al., 2013).

In conjunction with the interview questions, I used a qualitative codebook created in NVivo software, Skype for recording interviews, and Dragon Dictation to transcribe participants responses. I did not have to use Cisco WebEx as a backup for recording interviews. The interview recordings provided a simplistic way to transcribe and process data for analysis (Irvine et al., 2013). By using Skype to record interviews, it allowed me to review sections of the recording multiple times to ensure I picked up on key comments that were valuable to the study. A second interview could provide a deeper insight into information not clearly understood during the first interview and provide an opportunity to ask questions that arose in other interviews (Ekanem, 2015). I did not conduct a second interview with any of the participants. I combined my notes with the transcribed data to effectively member check. Marshall and Rossman (2016) stated member checking allows the researcher to approve the credibility of the study and use it as a quality control process to increase accuracy. I used this technique to ensure the views expressed in the transcripts are accurate and reflect the views of the participants. If requested to make additional adjustments in the study, I corrected the errors and requested the participants sign the transcript to indicate their approval of the transcripts used in data analysis.

Data Organization Technique

Gibson, Benson, and Brand (2013) stated to achieve confidentiality and obscurity of each participant, assigning generic codes are critical in the process to maintain privacy. For this study, I used numeric codes to mask the participant's identity. The participants granted me permission to record the interview via Skype by signing the consent form. Each participant had an identifying number in order of their interview. As manual

transcription can be a tedious and time-consuming process, I utilized a software to facilitate transcription (Silva de Araújo & Pedron, 2015; Moylan, Derr, & Lindhorst, 2015). Specifically, I used Voicebase to transcode the Skype audio to text. Ekanem, (2015); Jervis and Masoodian, (2014); Sotiriadou, Brouwers, and Le (2014) suggested by keeping the coded transcripts in a separate folder the researcher can avoid mislabeling. I uploaded the data into NVivo 11 to analyze and code the data using numeric values after I completed member checking.

Each audio file contains a label with name, date, and file type listed as an identifier. I utilized a cloud storage provider to store the data after I finished transcription and coding. After the completion of the study, I encrypted the folder stored on the cloud storage drive. As per Walden University guidelines, after the completion of the study, I will save the transcripts for five years. After this 5-year period, I will destroy all data contents in the cloud storage system by deleting the folder and destroying the encryption key.

Data Analysis

I used NVivo 11 as the analysis software for this qualitative study. The use of NVivo 11 allowed me to code and detect themes extracted from the transcripts of the interviews (Hatani, 2015; Oliveira, Bitencourt, Teixeira, & Santos, 2013). After I imported the transcribed interviews, I used the Straub and Welke's (1998) security risk planning model to analyze the data. I coded the answers using key words to collect specific information about the lack of training employees receive.

The purpose of data analysis was to show themes answering the central research question. Blumer (2016); Onwuegbuzie and Leech (2006); Meyer and Ward (2014) stated data analysis is the most difficult step in qualitative research because the researcher must sort the participant's responses into themes that match the central research question and report based on the analysis of the data. In this case study, the data analysis provided a framework to explore what training security professionals need to protect sensitive information.

After completing data analysis through NVivo 11, I selected the themes that emerged as most prominent or influential among the respondents. I related the themes with the literature review findings, and any subsequently published peer-reviewed article relevant to the study. Based on the findings from the literature review, I identified categories related to strategies and employee effectiveness for coding. Specifically, for strategies, I did use the categories corresponding to types of training provided for security professionals, i.e. on-the-job and off-the-job; and for employee effectiveness, I used the categories of competitiveness, innovation, job satisfaction, and productivity. During my analysis, I did not locate new information, and therefore, did not have to review past interviews for similar information to determine if including the new data would enhance the study or create a new category.

Reliability and Validity

In quantitative studies, the emphasis was on validity and reliability. In contrast, the concern in qualitative studies was upholding credibility, transferability, dependability, and confirmability to maintain the quality of the research study findings (Houghton,

Casey, Shaw, & Murphy, 2013). In qualitative research, credibility refers to using participant viewpoints to define and discuss the subject of interest (Elo et al., 2014; Munn, Porritt, Lockwood, Aromataris, & Pearson, 2014; Trochim, Donnelly, & Arora, 2014). In this study, I implemented two measures to uphold the credibility of my study findings. First, I used open-ended questions to allow the participants to articulate their views using their words. Second, I conducted member-checking through transcript review after each interview. In taking these two steps, the data depicted in this study was accurate based on the views of the participants and allowed the participants to review the results of data analysis.

Transferability pertains to the generalizability of the study findings or the applicability of the findings to other studies (Elo et al., 2014; Trochim et al., 2014). However, case studies are inherently limited regarding transferability because case studies explore a particular phenomenon within a specific context (Elo et al., 2014; Merriam & Tisdell, 2015). I addressed this limitation, by providing a detailed description of the setting and context of the study. The expectation that information is sufficient for future researchers to determine the applicability of the study findings to their respective settings.

About transferability, dependability was a concern in this case study. Dependability refers to the consideration of changes within the context of the study (Elo et al., 2014; Munn et al., 2014). Because the study utilized one specific organization, I acknowledged the conditions in an organization might differ from others, and in turn, affect the views of the study participants regarding the subject. I addressed this limitation

by utilizing follow-up questions asking the participants to provide as much detail during the interviews as possible, mainly to support or provide context for their statements.

Kassam, Sekiwunga, MacLeod, Tembe, and Liow (2016); Trochim et al. (2014) qualitative researchers should also take care to ensure confirmability or the degree in confirming study findings. To ensure confirmability, qualitative researchers must take steps to manage researcher reactivity and bias (Anney, 2014; Howie et al., 2016; Kassam et al., 2016). Anney (2014) defined research reactivity as the potential for the researcher to take control of participants, aiding in changing the results of the study. I addressed the issue of research reactivity by reiterating to the participants their welfare was the priority, and the data they provided for the study would remain confidential. Similarly, I did not use names or identifying information, and the guaranteed anonymity ensured the participants are comfortable sharing their thoughts and experiences.

Researcher bias is also another threat to the confirmability of the study results. In the study, I handled researcher bias using two separate methods. First, I projected a neutral attitude during interviews by not sending verbal or non-verbal cues to affirm or refute the participants' view during the interview. Second, the strict adherence to the steps outlined in Straub and Welke's security risk planning model helped ensure the objective analysis of the data collected for the study.

Lastly, to improve the quality and validity of the research, qualitative researchers must also ensure saturation (Elo et al., 2014; Marshall et al., 2013; Meyer & Ward, 2014). Elo et al., (2014); Marshall et al., (2013); Meyer and Ward, (2014) stated saturation is the point of data collection where a researcher cannot continue to collect and

analyze data for further contribution to the study. To ensure saturation, conducting a preliminary analysis after the first few interviews would help to ensure data completeness (Elo et al., 2014; Marshall et al., 2013; Meyer & Ward, 2014). If I did not achieve saturation, I would have interviewed more participants and created more themes or categories until full saturation of the data was complete (Elo et al., 2014; Marshall et al., 2013; Meyer & Ward, 2014).

Transition and Summary

The purpose of the study was to explore what training security professionals need to protect sensitive information. Section 1 consisted of the background, problem statement, purpose statement, conceptual framework, the research question, and literature review and other elements that contributed to the study. The objective of Section 2 was to detail the qualitative case study design approach and ensure the expectations for the participants, ethical research, and reliability and validity of the data meet the requirements of the study. Specifically, in accomplishing the purpose of the study, I conducted semistructured interviews with managers from a telecommunications firm to gain insight into the training and skills development they provided to their security professionals. I used an interview guide during the interviews, which I conducted virtually through Skype. The NVivo 11 software provided the analysis engine to process the collected data. I followed the necessary steps to ensure credibility, confirmability, creditability, and transferability. More importantly, protecting the participants' identity and well-being throughout the interview process for the study was my top priority.

Section 3 presents the analysis of the data, outcomes and findings, implications and for professional practice, recommendations for future research, and a summary of the study.

Section 3: Application to Professional Practice and Implications for Change

Introduction

The purpose of this qualitative case study was to explore training strategies telecommunication industry leaders use to ensure security professionals can protect sensitive information. Three senior leaders of a large telecommunications firm participated in this research based on the eligibility criteria presented in Section 2. I interviewed each participant in an environment where they felt comfortable providing insight to six semistructured interview questions (see Appendix B). From the data collected, multiple strategies developed that provided insight when other senior leaders in telecommunications can apply when forming their training program.

Presentation of the Findings

The central research question for this study was: What training strategies do telecommunication industry leaders use to ensure security professionals can protect sensitive information? After the data collection process, transcript reviews, and member checking were completed, three themes emerged. The emergent themes were (a) security training required for all professionals, (b) different approaches to training are beneficial and, (c) using internal and external trainings to complement each other.

Emergent Theme 1: Security training required for all professionals

The first theme that emerged among telecommunication senior leaders was security training required for all professionals. After reviewing the participants' responses and inputting the data into NVivo 11, it was apparent that each participant viewed security training as a top priority for the organization. Case participant

Interviewer1 stated, “Cybersecurity training is really essential to reduce the risk that employees can actually be tricked by sophisticated phishing or social engineering methods.” Case participant Interviewer2 stated, “Our organization is intermixed with our chief security office, and our network guys need to understand security and they need to understand the implication of changes they are making in the network.”

The senior leaders focused on certification training as a medium used to help bridge the gap in knowledge, but also present challenges when trying to apply the same methods to different parts of the organization. The findings collected from senior leaders are in line with the conceptual framework and the literature review in the following ways: (a) recognizing the lack of training across the organization, (b) providing different ways of training across the organization, and (c) reasons to implement security training across the organization. Caldwell (2016) suggested there are only a quarter of companies providing security training to employees and another quarter only receive training when joining the company. Without the proper training and different delivery models, the possibility exists employees could receive training that doesn’t fit the role or is conducive to their learning capabilities.

Case participant Interviewer3 stated:

> Our organization leverages a variety of avenues to keep employees current on their skill set. We do a lot of peer training amongst the group, so if the individual has some skills they want to share through a lunch and learn we can accommodate the request. Hands on or virtual training to get employees up to speed not only on

> the product, but the problem that product is trying to solve for our customers is important. Leveraging partners and vendors is essential to train at scale.

Case participant Interviewer2 stated:

> In our company, what we have seen is, as you mentioned, a lack of training for security professionals. Originally, we started training individuals within and across our organization. We focused on product marketing, chief security office, sales, and other sister organizations using just general training programs that are available via SANS certification and other vendor certifications. What we saw was people loved to get certified and learn new things. However, we weren't tying it back to the day to day job people were performing. We started to allow our security professionals to go and get individual certifications and that did not work as well as we had hoped. So, we built a program to ensure people receive a certain amount of competency in a structured environment.

Case participant Interviewer1 stated:

> Cybersecurity training is essential to reduce the risk of tricking employees with sophisticated phishing or social engineering methods. These attacks serve as an unknowingly entry points for cyber criminals to exfiltrate sensitive information. Our partnerships with our internal university allow us to have a robust awareness training program tied to a graduate certificate. We take industry training very serious with our partnerships with the SANS institute. We believe the essential element in developing individuals and teams helps our sellers describe how our products can protect government and commercial institutes from cyber attacks.

Table 3 shows the frequency of participants' comments concerning security training.

Table 3
Number of Times Security training required for all professionals

Theme Security training required for all professionals	*n*	Percentage
Interview1	23	31%
Interview2	40	55%
Interview3	10	14%
	73	100%

Note. n = frequency or number of coding references

Emergent Theme 2: Different approaches to training are beneficial

The second priority for senior leaders was to acknowledge that different approaches to training are beneficial. The theme of different approaches to training are beneficial relates to Straub and Welke (1998) security risk planning model phases alternative generation and implementation. Case participant Interviewer3 stated, "We try to get as much hands-on training and practical use training as we can." Case participant Interviewer1 stated, "The implementation of a tiered, meaning people learn at their own pace. So, we wanted to make sure there was a basic, intermediate, and Ph.D. level of training."

Senior leaders within the organization had different training plans that were different in delivery, but similar in content. Ruhi (2016) stated instructors require an in-depth understanding of practices to facilitate different learning styles. The large community of vendors works with organizations to provide employees hands-on or instructional training to gain the experience and knowledge required to protect sensitive

information (Ruhi, 2016). The conceptual framework and literature review help IT professionals in the areas of planning and proper training programs.

Case participant Interviewer3 stated:

> We have implemented some new training programs for our sales people. Historically, our sales people would go and find business and then bring our team in to help deliver the solution. We break down about eight hours of professional videos (created in house) breaking down cybersecurity into small digestible chunks for sales people. Now it is a requirement for all 7,000 sellers in the organization to have viewed and passed a questionnaire and test on those videos.

Case participant Interviewer2 stated:

> We are in the process of bringing on our first 20 participants into the training program. We want to measure when we get to the end of the training program, how did we develop people. Our biggest concern is retaining the talent we have spent thousands of dollars to training due to our low starting wages. To keep the talent, we have we have started to build security services in the cloud and we have had people get certified to do work in Amazon and Azure. The benefits of this training approach are still ongoing.

Case participant Interviewer1 stated:

> In our new training program, we wanted people to learn at their own pace, so we implemented a basic, intermediate, and Ph.D. level courses. The research we conducted showed professionals in the fortune one hundred and nearly every US government agency needs training to fight against cyber attacks. Regardless of

where you are in the world we delivered a course online. We did a lot of in person training on SCADA, NSIT framework, and about every industry training around cybersecurity.

Table 4 shows the frequency of participants' comments on the different approaches to training are beneficial

Table 4
Number of Times different approaches to training are beneficial

Theme **different approaches to training are beneficial**	*n*	Percentage
Interviewer1	22	30%
Interviewer 2	17	24%
Interviewer 3	33	46%
	72	100%

Note. n = frequency or number of coding references

Emergent Theme 3: Using internal and external trainings to complement each other

The third priority for senior leader was the internal and external training of security professionals. The theme of internal and external training aligns with Straub and Welke's (1998) security risk planning model in the planning decision phase. Gordon (2016) suggested there is no silver bullet to solve all the risks and security issues, but the one thing always within our grasp is training. All three senior leaders talked about different aspects of training within and external to the organization as important practices to ensure the workforce is current with what customer want. Case participant Interviewer1 stated, "Our internal company set up a program to provide information on cybersecurity and provide cybersecurity related training and exercises." Case participant

Interviewer3 stated, “We leverage partners and vendors as much as we can.” Case participant Interviewer2 stated, “People loved to get certified, but they were not tying it back to the day to day job that people are performing.” Ruhi (2016) stated market leaders in the large enterprise space cater to different methods of learning through use partnerships.

Case participant Interviewer1 stated:

> During our research, the training program we came up with we wanted to deliver courses around the world and online. We constantly measured the quality of the students experience and their learning capacity. What the employee learned during class, they could use the moment they returned to the office. Our sales team did not have enough training on newer products. Our customers were asking for more managed security services and more help around their own training program. We finalized on what the customers and sales teams needed and implemented the training program for our security product team, sales team, and customers.

Case participant Interviewer3 stated:

> Our training program is constantly evolving. The lessons learned straight from a book and classroom work, typically, is not the best way to train a security professional. As a sales organization, we look to get as much hands-on training and practical use training as we can. That is why we like vendor support as well as some of the more common classes that are out there that have hands-on labs.

> We have resources come onsite with another resource who has the knowledge and experience, and we do on-the-job training to get our team up to speed.

Case participant Interviewer2 stated:

> We have a program where roughly 15 to 20 participants are bought into a security training program. We utilize a rotational program that runs for 3 years, with each year being a new rotation for the participant. Their path depends on the person and what their interests are. The idea is to move them across different organizations to give them a flavor of what it is like to be a security professional in marketing or chief security office. The goal was to build industry knowledge specific to telecommunications and entertainment. We sent them to conferences such as RSA, Black Hat, and general seminars to further round out their skills.

Table 5 shows the frequency of participants' comments concerning training is different across the company.

Table 5
Number of Times using internal and external trainings to complement each other

Theme Using internal and external training to complement each other	*n*	Percentage
Interviewer1	5	26%
Interviewer 2	6	32%
Interviewer 3	8	42%
	19	100%

Note. n = frequency or number of coding references

Applications to Professional Practice

The findings of this study revealed what senior leaders need to provide security professionals the proper training to protect sensitive information. Each theme exposed insight into the lack of process, but the determination to educate and prepare security professionals to protect sensitive information was evident. The senior leaders' number one priority was to ensure all individuals have the appropriate training required to protect against sensitive information exposure. The results of this study can aid other senior leaders to understand the importance of combining internal and external training efforts to ensure all persons in the organization have the correct level of training before performing their duties.

Implications for Social Change

Senior leaders within an organization may realize that the task of protecting sensitive information is nonexistent without having a fully equipped workforce. Implications for positive social change include senior leaders working with area high schools and colleges to create a cybersecurity program and build talent for future employment. This awareness has the potential to solve multiple problems such as the lack of knowledge known by new employees and the lack of training as these individuals would be highly trained to protect sensitive information. This approach allows the students the opportunity to select different areas of cybersecurity to specialize in and tailor their learnings to fit key areas lacking talent within an organization.

Recommendations for Action

The research findings from this study provided the chance for recommending actions. The results from the study revealed a need to ensure all employees have a foundation on how to protect sensitive information. During the research phase of this study, I found that each organization within the selected company had a different method of providing training to their employees based on position. Based on the findings from this study, senior leaders should define a training program that will work for all organizations within their company.

The intent is to share the findings with the participants. Distributing the result of this study through publications and scholarly journal articles will add to the practice of cybersecurity training. Working with area high school and colleges is another way I intend to distribute the results of this study. Also, the intended plan is to present the findings to my management.

Recommendations for Further Research

This research study had several limitations. My professional background as an engineer could have led to bias, but I removed bias by sticking to the facts. This study explored the lack of training security professionals receive in corporate America. Recommendations for future studies would include effective training programs for cybersecurity professionals, how to retain top talent or competitive salaries for cybersecurity professionals. Future studies should include a larger geographical area comparing U.S. and European cybersecurity professionals.

Reflections

I selected the subject of exploring the lack of training in corporate America because of the training I had while serving in the military. As I collected the data for my study, I assumed my past work experiences in the roles I held as a communications engineer, windows design engineer, network engineer, data loss prevention engineer, technical solutions professional, and now a sales manager would obscure my view during the interview process. However, I discovered my past and present work experiences had no influence on the interview and data collection process. I learned a lot by listening and taking notes during the interview process. I heard the passion for technology and a desire to provide not only security professionals the proper training, but to ensure each person in the organization is mindful of security.

The journey embarked on for this doctoral study has been difficult, exciting, mind torturing, but most of all it has challenged me to become a better student and person. It has been a little over 4 years since accepting the challenge, but with everything that life has thrown at me, I am proud to say I persevered and finished. I will use my Doctoral of Business Administration degree in information technology management from Walden University to help kids less fortunate become interested in technology. I will partner with the chamber of commerce in my surrounding city to make my dream of sharing technology a reality.

Conclusion

I used a qualitative, explorative case study to explore training strategies telecommunication industry leaders use to ensure security professionals can protect

sensitive information. Three senior leaders in the telecommunications industry located in the state of Texas who had experience implementing a training program participated in this research. Data analysis consisted of using NVivo 11, recorded transcripts, and member checking to confirm the responses from the participants were correct. I achieved data saturation when I exhausted all emerging themes. The three main themes emerged from the data included (a) security training required for all professionals, (b) different approaches to training are beneficial and, (c) using internal and external trainings to complement each other. My findings of the study indicated senior leaders did not have a formal plan across the business and heavily utilized external training to bridge the gap in their training program. The need for an internal training program is at the forefront with senior leaders, and they are working internally to ensure cybersecurity professionals receive the proper training whether is it be internally or externally.

References

Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology, 33,* 236–247. doi:10.1080/0144929X.2012.708787

Abdul, A. M., & Asra, M. S. (2013). Training and development of non executives in tourism section - a study of APTDC, India. *International Journal of Management, IT, and Engineering, 3*, 395-414. Retrieved from http://www.indianjournals.com/ijor.aspx?target=ijor:ijmie&volume=3&issue=6&article=033

Abdullah, N.H., Ping, L. L., Wahab, E., & Shamsuddin, A. (2014). Perception on training and employee innovativeness: An evidence from small firms. *2014 International Conference on Management of Innovation and Technology*, (pp.76-80). Singapore: IEEE doi:10.1109/icmit.2014.6942404

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security, 42*, 27-39. doi:10.1016/j.cose.2014.01.001

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*, 357-370. doi:10.1007/s10845-012-0683-0

Ahmad, N., Tariq, M. S., & Hussain, A. (2015). Human resource practices and employee retention, evidences from banking sector of Pakistan. *Journal of Business and*

Management Research, 7, 186-188. Retrieved from http://www.knowledgejournals.com/PDF/66.pdf.

Alcaraz, C., & Zeadallly, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection, 8,* 53-66. doi:10.1016/j.ijcip.2014.12.002

Alshery, W. B. R., Ahmad, F. B., & Al-Swidi, A. K. (2015). The moderating effect of role ambiguity on the relationship of job satisfaction, training and leadership with employee performance. *International Journal of Business Administration*, *6*(2), 30-41. doi:10.5430/ijba.v6n2p30

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions*, (pp. 248-252). New York, NY: IEEE. doi:10.1109/ICITST.2014.7038814

Annechino, R., Antin, T. M. J., & Lee, J. P. (2010). Bridging the qualitative-quantitative divide. *HHS public access*, *22*(2), 115-124. doi:10.1177/1525822X09360760

Anney, V. N. (2014). Ensuring the quality of the findings of qualitative research: Looking at trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies*, *5,* 272-281. Retrieved from http://jeteraps.scholarlinkresearch.com

Anthony, P. J., & Weide, J. (2015). Motivation and career-development training programs: Use of regulatory focus to determine program effectiveness. *Higher Learning Research Communications*, *5*, 24. doi:10.18870/hlrc.v5i2.214

Antonioli, D., & Della Torre, E. (2015). Innovation adoption and training activities in SMEs. *Human Resource Management*, *27*(3), 311-337. doi:10.1080/09585192.2015.1042901

Anyan, F. (2013). The influence of power shifts in data collection and analysis stages: A focus on qualitative research interview. *The Qualitative Report, 18*, 1-9. Retrieved from http://tqr.nova.edu

Arrowsmith, J., & Parker, J. (2013). The meaning of 'employee engagement' for the values and roles of the HRM function. *International Journal of Human Resource Management*, *24*, 2692-2712. doi:10.1080/09585192.2013.763842

Barnhill, G. D., & Barnhill, E. A. (2013). Data security in qualitative research. In M. De Chesnay (Ed.), *Nursing research using data analysis: Qualitative designs and methods in nursing* (pp. 11-18). New York, NY: Springer.

Beebe, N. L., Young, D. K., & Chang, F. R. (2014). Framing information security budget requests to influence investment decisions. *Communications of The Association for Information Systems*, *35*(7), 134-144. Retrieved from http://aisel.aisnet.org/cgi/

Berghel, H. (2014). Leadership failures in the national security complex. *Computer*, *47*(6), 64-67. doi:10.1109/MC.2014.152

Bhatti, M. A., Battour, M. M., Sundram, V. P. K., & Othman, A. A. (2013). Transfer of training: Does it truly happen? An examination of support, instrumentality, retention and learner readiness on the transfer motivation and transfer of training. *European Journal of Training and Development, 37*(3), 273-297. doi:10.1108/.3090591311312741

Bhatnagar, A., & George, A. S. (2016). Motivating health workers up to a limit: Partial effects of performance-based financing on working environments in Nigeria. *Health Policy and Planning, 1*(1), 1-10. doi:10.1093/heapol/czw002

Birdi, K., Leach, D., & Magadley, W. (2012). Evaluating the impact of TRIZ creativity training: An organizational field study. *R&D Management*, *42*, 315-326. doi:10.1111/j.1467-9310.2012.00686.x

Bluestone, J., Johnson, P., Fullerton, J., Carr, C., Alderman, J., & BonTempo, J. (2013). Effective in-service training design and delivery: Evidence from an integrative literature review. *Human Resources for Health*, *11*(1), 51. doi:10.1186/1478-4491-11-51

Blumer, H. (2016). *Internal communication in Bangladeshi ready-made garment factories*. Wiesbaden, Germany: Springer Fachmedien Wiesbaden

Brakewood, B., & Poldrack, R. A. (2013). The ethics of secondary data analysis: Considering the application of Belmont principles to the sharing of neuroimaging data. *NeuroImage*, *82*, 671-676. doi:10.1016/j.neuroimage.2013.02.040

Breaux, T. D., & Gordon, D. G. (2013). Regulatory requirements traceability and analysis using semi-formal specifications. *In Requirements Engineering: Foundation for Software Quality*, (pp.141-157). doi:10.1007/978-3-642-37422-7_11

Brum, S. (2007, January). *What impact does training have on employee commitment and employee turnover?* Retrieved from http://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1022&context=lrc_paper_series

Burgard, C., & Görlitz, K. (2014). Continuous training, job satisfaction, and gender. *Evidence-Based HRM: A Global Forum for Empirical Scholarship*, *2*(2), 126-144. doi:10.1108/EBHRM-11-2012-0016

Busch, M., Patil, S., Regal, G., Hochleitner, C., & Tscheligi, M. (2016). Persuasive Information Security: Techniques to Help Employees Protect Organizational Information Security. *In Persuasive Technology* (pp. 339-351). doi:10.1007/978-3-319-31510-2_29

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

Carpenter, M. J., & de Charon, L. C. (2014). Mitigating multigenerational conflict and attracting, motivating, and retaining millennial employees by changing the organizational culture: A theoretical model. *Journal of Psychological Issues in Organizational Culture, 5,* 68-84. doi:10.1002/jpoc.21154

Carter, M. Z., Armenakis, A. A., Feild, H. S., & Mossholder, K. W. (2013). Transformational leadership, relationship quality, and employee performance

during continuous incremental organizational change. *Journal of Organizational Behavior*, *34*, 942-958. doi:10.1002/job.1824

Chen, Y, Ramamurthy, K, & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. *Journal of Computer Information Systems*, *55*(3), 11-19. doi:10.1080/08874417.2015.11645767

Choo, S., & Bowley, C. (2007). Using training and development to affect job satisfaction within franchising. *Journal of Small Business and Enterprise Development*, *14*(2), 339-352. doi:10.1108/14626000710746745

Ciemins, E. L., Brant, J., Kersten, D., Mullette, E., & Dickerson, D. (2014). A qualitative analysis of patient and family perspectives of palliative care. *Journal of Palliative Medicine*, *17*, 1-4. doi:10.1089/jpm.2014.0155

Coffee, K., Raucci, C., Gloria, C., Faulk, K., & Steinhardt, M. (2013). Perceptions of adolescent wellness at a single-sex school. *International Journal of Health Promotion and Education*, *51*(6), 300-311. doi:10.1080/14635240.2013.829980

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods*, *13*, 88-103. Retrieved from http://ejournals.library.ualberta.ca/index.php/IJQM/article/viewFile/20516/16237

Colombo, E., & Stanca, L. (2014). The impact of training on productivity: evidence from a panel of Italian firms. *International Journal of Manpower*, *35*, 1140-1158. doi:10.1108/IJM-08-2012-0121

Datta, S. T., & Davies, S. (2014). Training for the future NHS: training junior doctors in the United Kingdom within the 48-hour European working time directive. *BMC Medical Education, 14*, S12. doi:10.1186/1472-6920-14-S1-S12

Debbi, S., Elisa, P., Nigel, B., Dan, P., & Eva, R. (2014). Factors influencing household uptake of improved solid fuel stoves in low- and middle-income countries: A qualitative systematic review. *International Journal of Environmental Research and Public Health, 11*, 8228-50. doi:10.3390/ijerph110808228

Diedericks, E., & Rothmann, S. (2014). Flourishing of information technology professionals: Effects on individual and organisational outcomes. *South African Journal of Business Management*, *45*(1), 27-41. doi: 10.1080/14330237.2013.10820618

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

Draper, A., & Swift, J. A. (2011). Qualitative research in nutrition and dietetics: data collection issues. *Journal of Human Nutrition and Dietetics*, *24*, 3-12. doi:10.1111/j.1365-277X.2010.01117.x

Drtil, J. (2013). Impact of information security incidents–theory and reality. *Journal of Systems Integration, 4*(1), 44–52. Retrieved from www.si-journal.org

Dumangane, C. (2013). Conducting multi-generational qualitative research in education: an experiment in grounded theory. *Qualitative Research*, *13*, 379-381. doi:10.1177/1468794113475416

Dunlap, M. (2015). *5 keys to an effective training and development program*. Retrieved from https://www.onefpa.org/journal/pages/jan15-5-keys-to-an-effective-training-and-development-program.aspx.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20,* 701–715. doi:10.1007/s11948-014-9551-y

Ekanem, I. (2015). Entrepreneurial learning: Gender differences. International *Journal of Entrepreneurial Behaviour & Research, 21*, 557-577. doi:10.1108/IJEBR-08-2014-0146

Elnaga, A., & Imran, A. (2013). The effect of training on employee performance. *European Journal of Business and Management*, *5*(4), 137-147. Retrieved from http://pakacademicsearch.com/pdf-files/ech/517/137-147%20Vol%205,%20No%204%20(2013).pdf

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative content analysis: A focus on trustworthiness. *Sage Open*, *4*(1), 1-10. doi:10.1177/2158244014522633

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, *22*, 410-430. doi:10.1108/IMCS-07-2013-0053

Ferweda, M., Van Berugen, S., Van Burik, A., Van Middendorp, H., De Jong, E.M., Van De Kerkhof, P.C.M., & Van Riel, P.L (2013). What patients think about e-health: Patients' perspectives on internet-based cognitive behavioral treatment for patients

with rheumatoid arthritis and psoriasis. *Clinical Rheumatology, 32*, 869-873. doi:10.1007/s10067-013-2175-9

Flores, W. R., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security, 43,* 90-110. doi:10.1016/j.cose.2014.03.004

Flores, W. R., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security, 22*, 393-406. doi:10.1108/IMCS-11-2013-0083

Frels, R. K., & Onwuegbuzie, A. J. (2012). Interviewing the interpretive researcher: An impressionist tale. *The Qualitative Report, 17*, 1-27. Retrieved from http://nsuworks.nova.edu/tqr/vol17/iss30/2

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

Fu, J. R., & Chen, J. H. (2015). Career commitment of information technology professionals: The investment model perspective. *Information and Management*, *52*, 537-549. doi:10.1016/j.im.2015.03.005

Gallagher, V. C., Gallagher, K. P., & Kaiser, K. M. (2013). Mid-level information technology professionals: Skills and traits relevant to fit, individual and

organizational success factors. *International Journal of Social and Organizational Dynamics In IT*, *3*(2), 22-40. doi:10.4018/ijsodit.2013040102

Georgiadis, A., & Pitelis, C. N. (2014). The impact of employees' and managers' training on the performance of small-and medium-sized enterprises: Evidence from a randomized natural experiment in the UK service sector. *British Journal of Industrial Relations* [online]. doi:10.1111/bjir.12094

Ghosh, P., Jagdamba, P. J., Satyawadi, R., Mukherjee, U., & Ranjan, R. (2011). Evaluating effectiveness of a training programme with trainee reaction. *Industrial and Commercial Training*, *43*(4), 247-255. doi:10.1108/00197851111137861

Gibson, S., Benson, O., & Brand, S. L. (2013). Talking about suicide: Confidentiality and anonymity in qualitative research. *Nursing Ethics*, *20*(1), 18-29. doi:10.1177/0969733012452684

Golicic, S. L., & Davis, D. F. (2012). Implementing mixed methods research in supply chain management. *International Journal of Physical Distribution & Logistics Management*, *42*, 726-741. doi:10.1108/09600031211269721

Gordon, A. (2016). The hybrid cloud security professional. *IEEE Cloud Computing, 3*, 82-86. doi:10.1109/MCC.2016.21

Green, J. & Thorogood, N. (2013). *Qualitative methods for health research*. Thousand Oaks, CA: Sage.

Greenaway, K. E., & Chan, Y. E. (2013). Designing a Customer Information Privacy Program Aligned with Organizational Priorities. *MIS Quarterly Executive*, *12*(3). 137-150. Retrieved from EBSCO database.

Grip, A. D., & Sauermann, J. (2013). The effect of training on productivity: The transfer of on-the-job training from the perspective of economics. *Educational Research Review*, *8*, 28-36. doi:10.1016/j.edurev.2012.05.005

Grosse, E., & Upadhyay, M. (2013). Authentication at scale. *Security & Privacy*, *11*(1), 15-22. doi:10.1109/MSP.2012.162

Gupta, S., Chaudhari, B. S., & Chakrabarty, B. (2016). *Vulnerable network analysis using war driving and security intelligence*. Inventive Computation Technologies (ICICT), International Conference (pp. 1-5). IEEE. doi:10.1109/INVENTIVE.2016.7830165

Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society, 32,* 256-268. doi:10.1080/01972243.2016.1177762

Halkier, B. (2013). How to do your case study: A guide for students & researchers. *Journal of Qualitative Research, 13*(1), 107-110. doi:10.1177/1468794111436157

Harriss, D. J., & Atkinson, G. (2013). Ethical standards in sport and exercise science research: 2014 update. *International Journal of Sports Medicine*, *34*, 1025-1028. doi:10.1055/s-0033-1358756

Harvey, L. (2015). Beyond member-checking: A dialogic approach to the research interview. *International Journal of Research and Method in Education*, *38*(1), 23-38. doi:10.1080/1743727X.2014.914487

Hasan, L. M., Zgair, L. A., Ngotoye, A. A., Hussain, H. N., & Najmuldeen, C. (2015). A review of the factors that influence the adoption of cloud computing by small and

medium enterprises. *Scholars Journal of Economics, Business and Management*. *2*, 842-848. Retrieved from http://saspjournals.com

Hatani, F. (2015). Analyzing high-profile panel discussion on global health: An exploration with MAXQDA. *Forum: Qualitative Social Research*, *16*(1), Art. 14. Retrieved from http://nbn-resolving.de/urn:nbn:de:0114-fqs1501148.

Hendrix, M., AlSherbaz, A. and Victoria, B. (2016) Game based cyber security training: Are serious games suitable for cyber security training?. *International Journal of Serious Games, 3*(1), 53-61. doi:10.17083/ijsg.v3i1.107

Hernaus, T., & Vokic, N. P. (2014). Work design for different generational cohorts: Determining common and idiosyncratic job characteristics. *Journal of Organizational Change Management, 27*, 615-641. doi:10.1108/JOCM-05-2014-0104

Hershberger, P. E., Finnegan, L., Altfeld, S., Lake, S., & Hirshfeld-Cytron, J. (2013). Toward theoretical understanding of the fertility preservation decision-making process: Examining information processing among young women with cancer. *Research and Theory for Nursing Practice,* 27(4), 257-275. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4164111/

Hillman, D. R. (2014). Understanding multigenerational work-value conflict resolution. *Journal of Workplace Behavioral Health, 29*, 24-257. doi:10.1080/15555240.2014.933961

Holloway, I., & Wheeler, S. (2013). *Qualitative research in nursing and healthcare.* Chicester, England: Wiley-Blackwell.

Homoliak,I., Ovsonka, D., Koranda, K., & Hanacek, P. (2014). *Characteristics of buffer overflow attacks tunneled in HTTP traffic*, 2014 International Carnahan Conference on Security Technology (ICCST), (pp. 1-6). doi:10.1109/CCST.2014.6986998

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

Howie, E. K., Brewer, A. E., Dowda, M., McIver, K. L., Saunders, R. P., & Pate, R. R. (2016). A tale of 2 teachers: A presschool physical activity intervention case study. *Journal of School Health*, *86*(1), 23-30. doi:10.1111/josh.12352

Huang, Y. H., Lee, J., McFadden, A. C., Murphy, L. A., Robertson, M. M., Cheung, J. H., & Zohar, D. (2016). Beyond safety outcomes: An investigation of the impact of safety climate on job satisfaction, employee engagement and turnover using social exchange theory as the theoretical framework. *Applied Ergonomics, 55*, 248-257. doi:10.1016/j.apergo.2015.10.007

Hussein, A. (2015). The use of Triangulation in Social Sciences Research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*(1). Retrieved from http://journal.uia.no/index.php/JCSW/article/view/212/147

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51,* 69-79. doi:10.1016/j.im.2013.10.001

Ineson, E., Benke, E., & László, J. (2013). Employee loyalty in Hungarian hotels. *International Journal of Hospitality Management*, *32*, 31-39. doi:10.1016/j.ijhm.2012.04.001

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

Jahangiri-Rad, M., Mousavi, M., & Rafiee, M. (2014). Community perspectives on air pollution and its related health risks: A case study of Tehran (2012-2013). *Iranian Journal of Health Sciences, 2*(2), 69-75. Retrieved from http://jhs.mazums.ac.ir/

James, J., Cottle, E., & Hodge, D. (2010). A phenomenological exploration of healthcare chaplains (HCC'S) and registered nurses' (RN's) support of family members during resuscitation of their loved ones. *Scottish Journal of Healthcare Chaplaincy,* 13(2). doi:10.1558/hscc.v13i2.9

Janesick, V. J. (2011). *"Stretching" exercises for qualitative researchers*. Thousand Oaks, CA: Sage.

Jehanzeb, K., Rasheed, A., & Rasheed, M. F. (2013). Organizational commitment and turnover intentions: Impact of employee's training in private sector of Saudi

Arabia. *International Journal of Business and Management*, *8*(8), 79-90. doi:10.5539/ijbm.v8n8p79

Jervis, M., & Masoodian, M. (2014). How do people attempt to integrate the management of their paper and electronic documents? *Aslib Journal of Information Management, 66*(2), 134-155. doi:10.1108/AJIM-01-2013-0007

Juras, A., Brockmeier, J., Niedergesaess, V., & Brandt, D. (2014). Trust and team development to fight chaos: Three student reports. *AI & Society, 29*(2), 267-275. doi:10.1007/s00146-013-0484-9

Kassam, R., Sekiwunga, R., MacLeod, D., Tembe, J., & Liow, E. (2016). Patterns of treatment-seeking behaviors among caregivers of febrile young children: A Ugandan multiple case study. *BMC Public Health*, *16*. doi:10.1186/s12889-016-2813-7

Kawakami, T., Barczak, G., & Durmusoglu, S. S. (2014). Information technology tools in new product development: The impact of complementary resources. *Journal of Product Innovation Management*, *32*, 622-635. doi:10.1111/jpim.12244

Khan, M. I. (2012). The impact of training and motivation on performance of employees. *Business Review,* 7(2), 84-95. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2206854

Khanfar, S. M. (2011). Impact of training on improving hoteling service quality. *Journal of Business Studies Quarterly, 2*(3), 84-93. Retrieved from http://jbsq.org

Khattak, A. N., Rehman, S., & Rehman, C. A. (2014). Realistic job preview (RJP): It's efficiency in recruitment in pharmaceutical industry of Pakistan. Retrieved from http://www.aupc.info/wp-content/uploads/2014/08/V7I1-6.pdf.

Kijek, T., & Angowski, M. (2014). *Enabling knowledge creation: Does employees' training stimulate R&D activities?* Paper presented at the European Conference on Knowledge Management, 2, 556-562. Retrieved from http://search.proquest.com.ezp.waldenulibrary.org/docview/1672881412?accountid=14872

Kim, S., & McLean, G. N. (2014). The impact of national culture on informal learning in the workplace. *Adult Education Quarterly*, *64*(1), 39-59. doi:10.1177/0741713613504125

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *33*, 3-11. doi:10.1016/j.cose2012.07.001

Konings, J., & Vanormelingen, S. (2015). The impact of training on productivity and wages: Firm-level evidence. *The Review of Economics and Statistics*, *97*, 485-497. doi:10.1162/REST_a_00460

Korsakienė, R., Stankevičienė, A., Šimelytė, A., & Talačkienė, M. (2015). Factors driving turnover and retention of information technology professionals. *Journal of Business Economics and Management, 16*(1), 1-17. doi:10.3846/16111699.2015.984492

Kriyantono, R. (2012). Measuring a company reputation in a crisis situation: An ethnography approach on the situational crisis communication theory.

International Journal of Business and Social Science, 3, 214-223. Retrieved from http://www.ijbssnet.com

Kumar, D. N. S., & Shekhar, N. (2012). Perspectives envisaging employee loyalty: A case analysis. *Journal of management research*, *12*(2), 100-112. doi:10.2139/ssrn.1961430

Kvale, S. & Brinkmann, S. (2009). *Learning the craft of qualitative research interviewing*. Thousand Oaks, CA: Sage.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security*, *45*, 58-74. doi:10.1016/j.cose.2014.05.006

Lengnick-Hall, C. A., & Inocencio-Gray, J. L. (2013). Institutionalized organizational learning and strategic renewal: The benefits and liabilities of prevailing wisdom. *Journal of Leadership & Organizational Studies, 20,* 420–435. doi:10.1177/1548051812471723

Lichterman, P., & Reed, I. A. (2014). Theory and contrastive explanation in ethnography. *Sociological Methods and Research, 44*(4), 1-51. doi:10.1177/0049124114554458

Lim, J. S., Maynard, S. B., Ahmad, A., & Chang, S. (2015). Information security culture: Towards an instrument for assessing security management practices. *International Journal of Cyber Warfare and Terrorism*, *5*(2), 31-52. doi:10.4018/IJCWT.2015040103.

Maguire, R., Stoddart, K., Flowers, P., McPhelim, J., & Kearney, N. (2014). An interpretative phenomenological analysis of the lived experience of multiple

concurrent symptoms in patients with lung cancer: A contribution to the study of symptom clusters. *European Journal of Oncology Nursing, 18*(3), 310-315. doi:10.1016/j.ejon.2014.02.004

Maltby, J., Williams, G. A., McGarry, J., & Day, L. (2014). *Research methods for nursing and healthcare*. London, UK: Routledge.

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

Marshall, C., & Rossman, G. (2011). *Designing qualitative research* (5th ed.). Thousand Oaks, CA: Sage.

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

Maunder, R. E., Cunliffe, M., Galvin, J., Mjali, S., & Rogers, J. (2013). Listening to student voices: Student researchers exploring undergraduate experiences of university transition. *Higher Education*, *66*(2), 139-152. doi:10.1007/s10734-012-9595-3

McGettrick, A. (2013). Toward effective cybersecurity education. *IEEE Security & Privacy, 11*(6), 66–68. doi:10.1109/MSP.2013.155

McMahon, R., Serrato, D., Bressler, L., & Bressler, M. (2015). Fighting cybercrime calls for developing effective strategy. Retrieved from http://jupapadoc.startlogic.com/manuscripts/142102.pdf

McPhail, R., Patiar, A., Herington, C., Creed, C., & Davidson, M. (2015). Development and initial validation of a hospitality employees' job satisfaction index: Evidence from Australia. *International Journal of Contemporary Hospitality Management, 278*, 1814-1838. doi:10.1108/IJCHM-03-2014-0132

Mencl, J., & Lester, S. C. (2014). More alike than different: What generations value and how the values affect employee workplace perceptions. *Journal of Leadership & Organizational Studies, 21*(3), 257-272. doi:10.1177/1548051814529825

Merriam, S. B. & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation* (4th ed.). San Francisco, CA: Jossey-Bass.

Meyer, S., & Ward, P. (2014). How to use social theory within and throughout qualitative research in healthcare contexts. *Sociology Compass, 8*, 525-539. doi:10.1111/soc4.12155

Mierke, J. (2014). Leadership development to transform a library. *Library Management, 35*(1), 69-77. doi:10.1108/LM-04-2013-0029

Min, H., Magnini, V. P., & Singal, M (2013). Perceived corporate training investment as a driver of expatriate adjustment. *Contemporary Hospitality Management*, *25*, 740-759. doi:10.1108/IJCHM-May-2012-0079

Moone, R. P., Cagle, G. J., Croghan, C. F., & Smith, J. (2014). Working with LGBT older adults: An assessment of employee training practices, needs, and preferences of senior service organizations in Minnesota. *Journal of Gerontological Social Work*, *57*, 322-334. doi:10.1080/01634372.2013.843630

Morgado, L., Paredes, H., Fonseca, B., Martins, P., Almeida, A., Vilela, A., Peixinho, F., & Santos, A. (2016). A bot spooler architecture to integrate virtual worlds with e-learning management systems for corporate training. *Journal of Universal Computer Science, 22*(2), 271-297 Retrieved from https://www.researchgate.net

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

Moylan, C. A., Derr, A. S., & Lindhorst, T. (2015). Increasingly mobile: How new technologies can enhance qualitative research. *Qualitative Social Work*, *14*(1), 36-47. doi:10.1177/1473325013516988

Mukati, M. A., & Ali, S. M. (2014). The vulnerability of cyber security and strategy to conquer the potential threats on business applications. Retrieved from http://www.jisr.szabist.edu.pk/JISR-C/Publication/2014/12/1/214/Article/JISRC-Vol12-Number1-Paper9.pdf

Munn, Z., Porritt, K., Lockwood, C., Aromataris, E., & Pearson, A. (2014). Establishing confidence in the output of qualitative research synthesis: The ConQual approach. *BMC Medical Research Methodology*, *14*(108). doi:10.1186/1471-2288-14-108

Nda, M. M., & Fard, R. Y. (2013). The impact of employee training and development on employee productivity. Retrieved from https://www.researchgate.net/profile/Dr_Rashad_Yazdanifard/publication/260219097_the_impact_of_employee_training_and_development_on_employee_productivity/links/00b4953030e52c7e4a000000.pdf.

Niazi, B. R. A. S. (2011). Training and development strategy and its role in organizational performance. *Journal of Public Administration and Governance*, *1*(2), 42-57. doi:10.5296/jpag.v1i2.862

Nilashi, M., Ibrahim, O., Mirabi, V. R., Ebrahimi, L., & Zare, M. (2015). The role of security, design, and content factors on customer trust in mobile commerce. *Journal of Retailing and Consumer Services, 26*, 57-69. doi:10.1016/j.jretconser.2015.05.002

Oliveira, M., Bitencourt, C., Teixeira, E., & Santos, A. C. (2013). Thematic content analysis: Is there a difference between the support provided by the MAXQDA and NVivo software packages. In A. Mesquita & I. Ramos (Eds.), *Proceedings of the 12th European Conference on Research Methodology for Business and Management Studies, University of Minhos, Guimaraes, Portugal, 4-5 July 2013* (pp. 304-310). Reading, UK: Academic Conferences and Publishing International

O'Keeffe, J., Buytaert, W., Mijic, A., Brozović, N., and Sinha, R., (2016). The use of semi-structured interviews for the characterisation of farmer irrigation practices, *Hydrology and Earth System Sciences, 20*, 1911-1924, doi:10.5194/hess-20-1911-2016.

Olusegun, O. J., & Ithnin, N. B. (2013). People are the answer to security: Establishing a sustainable information security awareness training (ISAT) program in organization. Retrieved from http://arxiv.org/pdf/1309.0188.pdf.

Onwuegbuzie, A. J., & Leech, N. L. (2006). Linking Research Questions to Mixed Methods Data Analysis Procedures 1. Retrieved from http://nsuworks.nova.edu/cgi/viewcontent.cgi?article=1663&context=tqr

Opollo, J. G., Opollo, D. A., Gray, J., & Spies, L. (2014). Conducting international nursing research: Challenges and opportunities. *Nurse Researcher*, *22*(2), 29-33. doi:10.7748/nr.22.2.29.e1279

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K. (2013). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health And Mental Health Services Research*, *42*, 533-544. doi:10.1007/s10488-013-0528-y

Park, J., & Park, M. (2016). Qualitative versus Quantitative Research Methods: Discovery or Justification? *Journal of Marketing Thought*, 3(1), 1-7. doi:10.15577/jmt.2016.03.01.1

Phelan, S. K., & Kinsella, E. A. (2013). Picture this... safety, dignity, and voice - ethical research with children: Practical considerations for the reflexive researcher. *Qualitative Inquiry*, *19*(2), 81-90. doi:10.1177/1077800412462987

Ponemon, L. (2014). *Cost of data breach study: Global Analysis*. Retrieved from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Posey, C., Roberts, T., Lowry, P. B., Bennett, B., & Courtney, J. (2013). Insiders' protection of organizational information assets: Development of a systematics-

based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly, 37*(4). Retrieved from https://ssrn.com/abstract=2173642

Protheroe, J., Brooks, H., Chew-Graham, C., Gardner, C., & Rogers, A. (2013). 'Permission to participate?' A qualitative study of participation in patients from differing socio-economic backgrounds. *Journal of Health Psychology*, *18*, 1046-1055. doi:10.1177/1359105312459876

Purohit, S. K. (2015). Utilization of Training and Development to Increase Ability and Skill of Employees in Organisations. *The International Journal of Business & Management, 3*(2), 86-94. Retrieved from http://www.theijbm.com

Raza, H. (2014). Training and development impact on organizational performance: Empirical evidence from oil and gas sector of Pakistan. *International of Business and Management, 16*, 67-72. doi:10.9790/487X-16126772

Rees, C., Alfes, K., & Gatenby, M. (2013). Employee voice and engagement: Connections and consequences. *International Journal of Human Resource Management*, *24*, 2780-2798. doi:10.1080/09585192.2013.763843

Reinsch, N. L., & Gardner, J. A. (2014). Do communications abilities affect promotion decisions? Some data from the c-suite. *Journal of Business and Technical Communication*, *28*(1), 31-57. doi:10.1177/1050651913502357

Resnik, D. B. (2011). What is ethics in research & why is it important? *The national institute of environmental health sciences*, Retrieved from http://www.niehs.nih.gov/research/resources/bioethics/whatis/

Rida E-Fiza, S., Farooq, M., Mirza, F. I., Riaz, F., & Ud-Din, S. (2015). Barriers in employee effective training and learning. *Mediterranean Journal of Social Sciences, 6*(3), 240-250. doi:10.5901/mjss.2015.v6n3s2p240

Rob, R., McLorn, G. W., & Tural, T. (2016). Addressing cyber security for the oil, gas and energy sector. *2016 Saudi Arabia Smart Grid (SASG),* 1-7. doi:10.1109/SASG.2016.7849685

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

Ross, L. F., Saal, H. M., David, K. L., & Anderson, R. R. (2013). Technical report: Ethical and policy issues in genetic testing and screening of children. *Genetics in Medicine, 15*(3), 234-245. doi:10.1038/gim.2012.176

Ruhi, U. (2016). An experiential learning pedagogical framework for enterprise systems education in business schools. *The International Journal of Management Education, 14*(2), 198-211. doi:10.1016/j.ijme.2016.04.006

Saá-Pérez, P. D., Díaz-Díaz, N., & Ballesteros-Rodríguez, J. L. (2012). The role of training to innovate in SMEs. *Innovation: Management, Policy, & Practice, 14*(2), 218-230. doi:10.5172/impp.2012.14.2.218

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*(1), 65-78. doi:10.1016/j.cose.2015.05.012

Salas, E., Shuffler, M. L., Thayer, A. L., Bedwell, W. L., & Lazzara, E. H. (2015). Understanding and Improving Teamwork in Organizations: A Scientifically Based Practical Guide. *Human Resource Management*, *54*, 599-622. doi:10.1002/hrm.21628

Sanders, C., Rogers, A., Bowen, R., Bower, P., Hirani, S., Cartwright, M., & Newman, S. P. (2012). Exploring barriers to participation and adoption of telehealth and telecare within the whole system demonstrator trial: A qualitative study. *BMC Health Services Research*, *12*(1), 220. doi:10.1186/1472-6963-12-220.

Sannomiya, M., & Yamaguchi, Y. (2016). Creativity training in causal inference using the idea post-exposure paradigm: Effects on idea generation in junior high school students. *Thinking Skills and Creativity, 22,* 152-158. doi:10.1016/j.tsc.2016.09.006

Shackelford, S., Russell, S., & Kuehn, A. (2015). Defining Cybersecurity Due Diligence Under International Law: Lessons from the Private Sector. *Volume on Ethics and Policies for Cyber Warfare (Oxford University Press, 2015)*. Retrieved from https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10253/SSRN-id2594323.pdf?sequence=1&isAllowed=y

Shaheen, A., Naqvi, S. M. H., & Khan, M. A. (2013). Employees training and organizational performance: Mediation by employees performance. Retrieved from http://journal-archieves35.webs.com/490-503.pdf.

Shahin, N. (2014). Role of employee retention practices in Indian industry - A study of select MNCs in Jamshedpur. Retrieved from

http://www.ijemr.net/August2014Issue/RoleOfEmployeeRetentionPracticesInIndianindustry(206-213).pdf.

Shi, X., Wang, J. X., & Guan, S. (2011). *Analysis on influencing factors of junior staff loyalty of manufacturing enterprises — Empirical study based on manufacturing enterprises in Beijing*. 2011 International Conference on Electronics, Communications and Control (ICECC), China. doi:10.1109/ICECC.2011.6068085

Silva de Araújo, C. C., & Pedron, C. D. (2015). IT project manager competencies and IT project success: A qualitative study. *Organisational Project Management, 2*(1), 53-75. doi:10.5130/opm.v2i1.4142

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, *51*(2), 217-224. doi:10.1016/j.im.2013.08.006

Sissolak, D., Marais, F., & Mehtar, S. (2011). TB infection prevention and control experiences of South African nurses - a phenomenological study. *BMC Public Health*, *11*(1), 262. doi:10.1186/1471-2485-11-262

Sloan, P. (2014). The reasonable information security program. Retrieved from http://jolt.richmond.edu/v21i1/article2.pdf.

Sotiriadou, P., Brouwers, J., & Le, T. (2014). Choosing a qualitative data analysis tool: A comparison of NVivo and Leximancer. *Annals of Leisure Research*, *17*(2), 218-234. doi:10.1080/11745398.2014.902292

Squire, C., Phoenix, A., Patterson, W., & Tamboukou, M. (2013). *Doing narrative research* (2nd ed.). London, ENG: Sage.

Steiker, C. S. (2013). Lessons from two failures: Sentencing for cocaine and child pornography under the federal sentencing guidelines in the United States. *Law & Contemporary Problems*, *76*, 27-52. Retrieved from http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=4345&context=lcp

Stern, G. (2017). Getting with the program to beef up cybersecurity. *Biomedical Instrumentation & Technology, 51*, 70-75. doi:10.2345/0899-8205-51.1.70

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22,* 441-469. doi: 10.2307/249551

Strohmeier, S. (2013). Employee relationship management: Realizing competitive advantage through information technology? *Human Resource Management Review, 23*, 93–104. doi:10.1016/j.hrmr.2012.06.009

Suby, M., & Dickson, F. (2015). The 2015 (ISC)2 global information security workforce study. Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/01/FrostSullivan-ISC%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf.

Sum, V., & Chorlian, J. (2013). Training and the firm's competitiveness: A survey of practitioners. *Economics, Management, And Financial Markets*, *9*(2), 11-26. doi:10.2139/ssrn.2320965

Sung, S. Y., & Choi, J. N. (2013). Do organizations spend wisely on employees? Effects of training and development investments on learning and innovation in organizations. *Journal of Organizational Behavior, 35*(3), 393-412. doi:10.1002/job.1897

Swarnalatha, C., & Prasanna, T. (2013). Leveraging employee engagement for competitive advantage: HR's strategic role. *Global Journal of Commerce & Management Perspective, 2,* 1-6. doi:10.24105/gjcmp

Tawalbeh, L. I., & Tubaishat, A. (2014). Effect of simulation on knowledge of advanced 112 cardiac life support, knowledge retention, and confidence of nursing students in Jordan. *Journal of Nursing Education, 53*(1), 38-44. doi:10.3928/0148434-20131218-01

Tobin, C. L., & Murphy-Lawless, J. (2014). Irish midwives' experiences of providing maternity care to non-Irish women seeking asylum. *International Journal of Women's Health*, *6*, 159-169. doi:10.2147/IJWH.S45579

Trochim, W., Donnelly, J., & Arora, K. (2014). *Research methods: The essential knowledge base*. Mason, OH: Thomson custom

van Berkel, J., Boot, C. R., Proper, K. L., Bongers, P. M., & van der Beek, A. (2014). Effectiveness of a worksite mindfulness-based multi-component intervention on lifestyle behaviors. *International Journal of Behavioral Nutrition and Physical Activity, 11*(9), 1-11. doi:10.1186/1479-5868-11-9

van der Heijden, G. A., Schepers, J. J., Nijssen, E. J., & Ordanini, A. (2013). Don’t just fix it, make it better! Using frontline service employees to improve recovery

performance. *Academy of Marketing Science*, *41*, 515-530. doi:10.1007/s11747-012-0324-3

Velasco, R., Villar, R., Lunar, R., & Velasco, V (2016). Diversity in the workplace. *Journal of Asian Business Strategy, 6*(4), 73. doi:10.18488/journal.1006/2016.6.4/1006.4.73.84

Vogl, S. (2013). Telephone Versus Face-to-Face Interviews: Mode effect on semistructured interviews with children. *Sociological Methodology, 43,* 133–177. doi:10.1177/0081175012465967

Walshe, C., Ewing, G., & Griffiths, J. (2012). Using observation as a data collection method to help understand patient and professional roles and actions in palliative care settings. *Palliative Medicine*, *26*, 1048-1054. doi:10.1177/0269216311432897

Wang, J., & Guo, H. (2014). *A real options pricing framework for valuation of security professionals*. 2014 Seventh International Joint Conference on Computational Sciences and Optimization (CSO), Beijing, China. doi:10.1109/CSO.2014.101

Webb, J., Maynard, S., Ahmad, A., & Shanks, G. (2014). Information security risk management: An intelligence-driven approach. *Australasian Journal of Information Systems, 18,* 391-404. Retrieved from http://journal.acs.org.au/index.php/ajis/article/viewFile/1096/644

Wei, X., McCune, B., Lumbsch, H. T., Li, H., Leavitt, S., Yamamoto, Y., & Tchabaneko, S. (2016). Limitations of Species Delimitation Based on Phylogenetic Analyses:

A Case Study in the Hypogymnia hypotrypa Group (Parmeliaceae, Ascomycota). *Plos ONE, 11*, 1-20. doi:10.1371/journal.pone.0163664

Whitman, M. E., & Mattord, H. J. (2013). Information Security Governance for the Non-Security Business Executive. *Journal of Executive Education*, *11*(1), 97-111. Retrieved from http://digitalcommons.kennesaw.edu/jee/

Yamoah, E. E. (2013). Employee training and empowerment: A conceptual model for achieving high job performance. *Journal of Education and Practice, 4,* 27-30. Retrieved from www.iiste.org/Journals/index.php/JEP/article/download/6771/6884.

Yilmaz, K. (2013). Comparison of quantitative and qualitative research traditions: Epistemological, theoretical, and methodological differences. *European Journal of Education, 48*(2)*,* 311-325 doi:10.1111/ejed.12014

Yin, R. K., (2009). Cas*e study research: Design and methods.* (4th ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2011b). *Qualitative research from start to finish* (3rd ed.). Thousand Oaks, CA: Sage.

Yin, R. K. (2013). Validity and generalization in future case study evaluations. Social Sciences, 19, 321-332. doi:10.1177/1356389013497081

Appendix A: Introduction Letter

Dear Potential Research Participant:

As a security professional, I thank you for your time. I am conducting a doctoral study on business leaders' and why providing proper training for security professionals is lacking. The purpose of this study is to explore what training security professionals need to protect sensitive information.

If you agree to participate in this study, I will conduct an interview with you that will last approximately 30 to 60 minutes. Your participation in the study is completely voluntary. Your information is confidential, and I will not release the specifics of any interview with anyone. I will use the information to determine various trends and relationships along with the other interview data to form conclusions on the best way to provide training to security professionals. After potential interviewees agree to participate in the study, I will be providing more detailed information during the interview.

While the study may be published in the ProQuest Dissertation Database, the individual interviews with each participant will be kept confidential. No individual other than my doctoral study committee at Walden University will have access to the interview transcripts. I will not release information that could impact your position within your organization.

If you have any questions, please contact me at any time. Thank you for your consideration.

Sincerely,

Kenneth Johnson

Appendix B: Interview Questions

The Training Deficiency in Corporate America: Training Security Professionals to Protect Sensitive Information

Interviewee Name:

Date:

Time:

Location:

Central Research Question

What training strategies do telecommunication industry leaders use to ensure security professionals can protect sensitive information?

Interview Questions

1. What strategies did you use to address the lack of training security professionals receive in your company?
2. What research and educational training occurred before you made the decision to implement a new training program?
3. What were the deciding factors leading you to implement a new training program for security professionals?
4. What positions in your organization require security training?
5. What benefits have you seen since implementation of the new security training program?
6. What additional information, if any, do you feel is pertinent to the purpose of this study that I did not address in the interview questions?

Additional Notes:

Appendix C: Interview Protocol

Interview Protocol	
Hello, Mr./Mrs./Ms. (name) My name is Kenneth Johnson. I want to thank you for agreeing to participate in my DBA study and arranging time in your busy schedule to allow me to interview with you.	As I already mentioned on the phone and in the consent form I sent you my study relates to understanding what training strategies do telecommunication industry leaders use to ensure security professionals can protect sensitive information? Do you still agree to participate in my study?
	If a participant wants to back out of the study, make a note and thank them for their time. If participant agrees to proceed with the interview questions.
• Paraphrase as needed • Ask follow-up probing questions to get more in-depth	1. What strategies did you use to address the lack of training security professionals receive in your company? 2. What research and educational training occurred before you made the decision to implement a new training program? 3. What were the deciding factors leading you to implement a new training program for security professionals? 4. What positions in your organization require security training? 5. What benefits have you seen since implementation of the new security training program? 6. What additional information, if any, do you feel is pertinent to the purpose of this study that I did not address in the interview questions?