Walden University

College of Management and Technology

This is to certify that the doctoral study by

Ivadella Walters

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. Carol-Anne Faint, Committee Chairperson, Doctor of Business Administration Faculty

Dr. Craig Martin, Committee Member, Doctor of Business Administration Faculty

Dr. Neil Mathur, University Reviewer, Doctor of Business Administration Faculty

Chief Academic Officer
Eric Riedel, Ph.D.

Walden University
2017

Abstract

Strategies for Recruiting Cybersecurity Professionals in the Financial Service Industry

by

Ivadella Walters

MS, Webster University, 2014

BS, Claflin University, 1983

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

July 2017

Abstract

The cybersecurity market is the fastest growing market in the United States; as such, leaders in financial institutions recognize their businesses are vulnerable, as money is accessible within computerized banking systems. The purpose of this multiple case study was to explore what strategies financial service leaders use to recruit cybersecurity professionals. The conceptual framework for this study was the hierarchy of needs and stakeholder management theory. Data collection involved company archival documents and semistructured, open-ended interviews with 5 financial service leaders in the Midlands area of South Carolina who recruited skilled cybersecurity professionals to support long-term business sustainability. Coding, clustering, and theme development evolved through coding key words and actions, drawing ideas together into clusters, and evolving the prominent ideas into themes. During data analysis, the theoretical propositions underwent a sequential process, which included coding the data by hand. The use of member checking and methodological triangulation increased the trustworthiness of the study. Analysis revealed 3 themes: increased training, broadened social networking, and improved communication. Financial service leaders can use training to educate and recruit new cybersecurity professionals. Also, findings suggest the need for training to improve social networking and communicate as a team to increase profitability. The findings from this study may contribute to social change by helping business owners recruit skilled professionals to prevent or reduce cybersecurity threats.

Strategies for Recruiting Cybersecurity Professionals in the Financial Service Industry

by

Ivadella Walters

MS, Webster University, 2014

BS, Claflin University, 1983

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Business Administration

Walden University

July 2017

Dedication

I dedicate my Doctor of Business Administration degree with a specialization in Project Management to the precious memories of my fiance, the late Sheriff Larry Dalton Williams; my late parents, George and Romell Gaddis Walters; and my late siblings, Michelle Brenda Walters Baxter, and McArthur "Perry" Walters. When my journey seems weary, they were my angels in heaven pulling for me.

I express gratitude to my son, Demond E. Baxter, my siblings, George (Ida Wolfe) Walters, Marian Walters, Isiah (Nicollette) Walters, my entire family, godsons, and friends for their love and support throughout my educational endeavor. I could not accomplish this milestone without their encouragements and my faith in God. Thank you for cheering me on to the finish line and understanding my eccentricities.

Acknowledgments

I must give God all of the Glory. I could not have accomplished this academic process without my faith and constant prayer. It has been a grueling journey in a very difficult time, and through it all, His grace and mercy brought me through. To my committee chair, Dr. Carol-Anne Faint, I cannot thank you enough for your guidance and sincere genuineness. Indeed, your encouragements were instrumental to my success! To my committee members, Dr. Craig Martin, Dr. Al Endres, and Dr. Neil Mathur thank you for your mentorship. I would also like to extend my thanks to Dr. Gene Fusch and Dr. Freda Turner for their guidance as Walden University Program Directors. My editors and consultants, Dr. Ry Henderson-Carter and Mrs. Ida Wolfe Walters, Crucial Eye, LLC thank you for your services and commitment to my success. I am grateful to all of the colleagues, financial service leaders participants, church family, and Representative Terry B. Adams for their confidence in me and unconditional support. Additionally, I would like to acknowledge and thank my pastor, Reverend Dr. Blakely N. Scott, III for his pastoral inspirations and giving me the spiritual assurance that I can complete this educational journey.

Table of Contents

List of Tables

Section 1: Foundation of the Study

As technology evolves, the changes may affect financial institutions and allow threats to online security (Carlon & Downs, 2014). Unfortunately, the expansion of technology creates competitive advantage and new opportunities for people to carry out criminal activities online through cyber-crime, which causes financial burdens on organizations (Lagazio, Sherif, & Cushman, 2014). As the risks increase, financial institutions must continue to seek innovative ways to recruit trained cybersecurity professionals.

Training in various areas of information technology (IT) such as coding, storage, and core systems is important to cybersecurity professionals (Malhotra, 2015). Despite security breaches and identity theft, most research does not reflect the critical vulnerabilities in the global banking and finance industry (May, Koski, & Stramp, 2016). My study might reduce the gaps in strategies that leaders use to hire cybersecurity professionals.

Background of the Problem

Cybersecurity experts expect the trend toward increasingly advanced cyberattacks to continue in the 21st century (Andriole, 2015). The financial service industry is a vital component of the nation's critical infrastructure and remains a prime target for cyber-crime. Homeland Security reported that the United States financial institution cybersecurity market is the largest and fastest growing private sector cybersecurity market (Andriole, 2015). In 2013, information securities' spending on solutions to the

problem totaled $17.1 billion (Von Solms & Van Niekerk, 2013), and rose to $76.9 billion, or by 8.2%, in 2015.

In 2014, leaders at a major United States bank assessed threats to customer security and asserted that spending $250 billion dollars and assigning 1,000 cybersecurity professionals to each incident of threat may not be enough to protect any financial service company from computer attacks (Shields, 2015). However, the issue remains that there is a shortage of trained cybersecurity professionals able to handle these attacks in all businesses; the financial service industry is the most vulnerable because money is readily accessible within banking systems (Andriole, 2015).

Current strategies used to recruit financial service IT professionals consist of job fairs, headhunters, website posting of positions and personal referral (Stoughton, Thompson, & Meade, 2015). In researching the problem, I found no specific studies on the strategies that financial service leaders (FSLs) found helpful in recruiting cybersecurity professionals to defend the banking industry against the threat of cyberattacks. For this reason, I explored what strategies financial service leaders use to recruit cybersecurity professionals.

Problem Statement

There is a shortage of cybersecurity talent in banking institutions in the United States (Carlon & Downs, 2014). Andriole (2015) noted that between April 2013 and May 2014, 93% of financial service organizations experienced cyberthreats. Carlon and Downs (2014) indicated that information security enables a financial institution to meet its business objectives by managing IT related risks. The general business problem was

that shortage of cybersecurity talent resulting in a loss of organizational privacy and profitability. The specific business problem was that some financial service leaders lack strategies to recruit cybersecurity professionals.

Purpose Statement

The purpose of this qualitative multiple case study was to explore what strategies financial service leaders used to recruit cybersecurity professionals. The population of this study consisted of 5 financial service leaders (FSLs) within two financial companies in Columbia, South Carolina, that used successful strategies to recruit cybersecurity professionals. Participants shared strategies they used to recruit cybersecurity professionals. The study findings might help other cybersecurity business leaders recruit skilled professionals, enhance cybersecurity awareness for citizens, and prevent or reduce cybersecurity threats.

Nature of the Study

There are three types of research methods available to researchers: qualitative, quantitative, and the mixed methods. Quantitative, qualitative, and the mixed-method approaches offer different strengths in research (Bryman & Bell, 2015). Quantitative research is a method for investigating variables' relationships, cause-effect phenomenon, and differences in outcomes (Hartas, 2015). I declined to use quantitative research because my intent was to understand strategies participants deploy for integration in their respective processes, and not examine relationships or differences among variables. A mixed method or hybrid approach includes both qualitative and quantitative methods in a single study (Bryman & Bell, 2015). The mixed method approach was not appropriate

because using the mixed method includes quantitative inquiry, which was inappropriate for this study. The qualitative research method was suitable for this study to explore the strategies individuals used to recruit cybersecurity professionals (Hartas, 2015).

In qualitative research, primary designs include: (a) narrative, (b) phenomenological, (c) ethnographic, and (d) case study (Yin, 2014). Narrative researchers explore lifelong (past) stories of individuals. In this study, I sought to understand the current strategies FSLs use to recruit cybersecurity professionals. Therefore, I did not select a narrative study. The phenomenological researcher seeks to explore the meaning of individuals lived experiences (Marshall & Rossman, 2014), which was not the intent of this study. An ethnographic design was not appropriate because studying sociocultural group was not the purpose of this study (Lewis, 2015). A descriptive multiple case study was the most appropriate design for this study because the intent was to explore strategies and individual experiences (Marshall & Rossman, 2014).

Research Question

The central research question was: What strategies do financial service leaders use in recruiting cybersecurity professionals?

Interview Questions

To address the central research question, I proposed the following interview questions (see Appendix A):

1. What strategies do you use to recruit cybersecurity professionals?
2. How were the recruiting strategies to recruit cybersecurity professional deployed and implemented?

3. What challenges, if any, did you experience while using recruiting strategies to recruit cybersecurity professionals? How did you address any barriers to implementing the recruitment strategies?
4. How do you measure the success of your strategies and recruitment processes?
5. What additional information can you provide to help me understand the strategies and processes you've used for employing and maintaining the service of cybersecurity professionals?

Conceptual Framework

The conceptual framework I used for this study was the hierarchy of needs theory established by Maslow in 1943, and Straub and Welke's (1998) stakeholder management theory (SMT). Maslow (1943) explained the motivations of people to first have their lowest-level needs met, such as food and shelter. Once an individual achieves basic needs, higher-level levels needs and goals, such as love and esteem, become their goals. Maslow's hierarchy of needs theory applies to both primary and secondary needs for salary generation and self-actualization. For this study, the primary needs were the job descriptions of cybersecurity positions, the candidates, and current cybersecurity experts: To address when deciding to recruit, accept, and remain in cybersecurity positions with the company. Straub and Welke developed the SMT in 1998, and addressed value creation through business relationships. Use of stakeholder theory enables managers to take responsibility for all stakeholder groups' interests in their decision-making. The principal stakeholders are the hiring managers, applicants, and those needing protection from cybersecurity threats (Straub & Welke, 1998). Lemke and Harris-Wai (2015)

indicated that stakeholder management, consultation and engagement have become increasingly prevalent in the business community as businesses recognize the value of these interactions. Not only is stakeholder consultation a vital component of corporate social responsibility, but businesses that engage with and listen to the needs of their stakeholders consistently outperform their peers.

For the purpose of this study, the principal stakeholders were the hiring managers, cybersecurity applicants, and current cybersecurity experts; however, cybersecurity job descriptions must reflect the needs of a broad range of stakeholders. Stakeholders place trust in the company to protect assets, and business managers respond by recruiting and retaining experts competent to secure cyber activity (Mármol, Pérez, & Pérez, 2016). Using the hierarchy of needs theory as an additional component of the conceptual framework for this study includes addressing the cybersecurity needs of business owners, and identifying the needs of all stakeholders affected by cyberattack. I applied both the hierarchy of needs theory and SMT to the study to understand what strategies business owners require to recruit cybersecurity professionals through identifying the needs for recruiting and retaining successful applicants and current cybersecurity employees.

Operational Definitions

Cyber-crime: Cyber-crime is a deliberate attack, administrative, motivated against information, computer system and programs, and data that lead to violence, against the targets from the international group or undercover agents (Gordon et al., 2015).

Cybersecurity Professional: A cybersecurity professional trains in the protection

of IT systems against threats (Gordon, Loeb, Lucyshyn, & Zhou, 2015). Cybersecurity is the management of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies to protect the environment and organization's assets (Von Solms & Van Niekerk, 2013).

Hacker: Hacker is an unauthorized user who attempts to obtain access to an information system is a crime even if there is no noticeable harm to the network since it is an intrusion (Andriole, 2015).

Information security management (ISM): Information security management is a system used to mitigate the various risks and threats to the information (Lagazio et al., 2014).

Assumptions, Limitations, and Delimitations

In the following subsections, I present assumptions, limitations, and delimitations of the study. Assumptions in the study were presumed true, but not proven. Limitations are a potential weakness of the study, and delimitations are those factors that the researcher can control.

Assumptions

Assumptions allow researchers to remain focused while taking into consideration factors that are important to the study (Leedy & Ormrod, 2013). For this research study, I made three assumptions. First, I assumed that participants of the study would give accurate responses with an understanding that their responses are confidential. The second assumption was that members may articulate experiences related to the topic. The

third assumption was that interviews offered an opportunity to explore what strategies financial service leaders need to recruit cybersecurity professionals.

Limitations

A small sample of participants limits the generalizability of results (Bryman & Bell, 2015). Given the well-known difficulties in gaining information from financial institutions, I decided to follow a qualitative approach, exploring the insights learned from the experiences of leaders with strategies used in recruiting talent. Finally, in this qualitative case study, all aspects pertaining to strategies financial service leaders used to recruit cybersecurity professionals to benefit stakeholders may not convey.

Delimitations

The population for this study included financial service leaders in Columbia, South Carolina. The first delimitation included the population because of the restriction to the area for convenience (Leedy & Ormrod, 2013). The second delimitation included the purposive selection of participants, which is nontransferable to a larger population. The purposeful sample size was a delimitation as the outlooks reflect the experiences of those interviewed and are not generalizable to financial institutions or geographic locations (Bryman & Bell, 2015).

Significance of the Study

The value of the study was to explore what strategies financial service leaders use to recruit cybersecurity professionals. The use of recruiting strategies specifically for cybersecurity professionals in the banking industry may protect individuals and build trust in a sensitive economic climate where everyone is sensitive about fraud (Devi,

2016). A security breach involving customer data may have a devastating effect on an organization (Critchley, 2015). Consumers rely on information systems (IS) to transact their banking needs and purchase their goods (Angel & McCabe, 2015). If criminals are compromising any IS, consumers might lose trust in the organization.

Contribution to Business Practice

The findings from the study may contribute to business practices by providing strategies leaders require to recruit cybersecurity professionals. Financial service leaders may use the findings to evaluate the effectiveness of their current strategies and to reduce costs associated with cybersecurity (Potter & Vickers 2015). It is critical that all financial service leaders understand the issues surrounding computer technology (Fonash & Schneck, 2015). Moreover, investment in organizational security can reduce the financial burden on company leaders and maintain consumer confidence (Adams & Makramalla, 2015).

Implications for Social Change

As cyberattacks increase, public awareness of vulnerabilities also increases (Adnan, Just, Baillie, & Kayacik, 2015). The findings from the study have implications for social change by helping business owner recruit skilled professionals to prevent or reduce cybersecurity threats. The recruitment of skilled professionals could reduce customers' cost and time to address the occurrence of cyber-crime, and increase customer confidence and market share, thus creating greater profits for business owners. Greater profits can benefit community economies (Eckhardt & Bardhi, 2016).

A Review of the Professional and Academic Literature

The purpose of this qualitative case study was to explore what strategies financial service leaders need to recruit cybersecurity professionals. Adnan et al. (2015) reported that cyber-crimes cost business leaders upward of $7.7 million a year. In 2014, the cost of cyber-crimes in the United States increased by 20% compared to other countries (Wilson et al., 2015). The purpose of this qualitative study and literature review was to provide: (a) an overview of the topic, (b) gain a deeper understanding of the topic understudy, (c) create new awareness and research undertaken by others, (d) identify a research question, and (e) summarize the problem (Booyens, 2014). The research question addressed what strategies financial service leaders use to recruit quality cybersecurity professionals.

The literature review contains peer-reviewed references and citations; 97 % of the 145 peer-reviewed articles have a publication date within 5 years of the anticipated graduation date. I examined the following databases: (a) Science Direct, (b) Emerald Management Journals, and (c) ProQuest. The keyword searches included *cybersecurity, internet banking, cyberattacks, vulnerabilities, information technology*, *information security*, *deterrence theory*, *information systems, financial institutions,* and *IT professionals.*

Jasper (2015) explained that general deterrence theory (GDT) seeks to shape one's perceptions of costs and benefits while committing resources, enhancing operations, and using force when necessary. Establishing cybersecurity frameworks is a business necessity. A structure is needed to protect businesses from a cyberattack (Jasper, 2015).

For GDT to be effective, one should rely on: (a) the means leaders' use to influence behavior, (b) credibility by training or influencing the responsibility of others, and (c) communication by sending the right message to the desired audience (Alanezi & Brooks, 2014).

General deterrence theorists view deterrence as implementing strategies to influence the decision makers (Alanezi & Brooks, 2014). The aim of deterrence in the banking industry was to provide restrictions for potential cyber-crime (Cheng, Li, Zhai, & Smyth, 2014). General deterrence theory is most useful in creating constant awareness through training and publicity of possible threats to security (Alanezi & Brooks, 2014).

The first GDT element is the deterrence that focuses on policies, awareness, training, and security (Alanezi & Brooks, 2014). The second element is prevention, which includes obstacles, authentication, devices, firewalls, and procedures. The third part is detection, which concentrates on the process of discovering security breaches, internal system control, and audits trails. General deterrence theorists view deterrence as influencing leaders' decision-making processes, which may require altering or reinforcing how they factor decisions before acting on them (Guzansky & Golov 2015).

The aim of deterrence is to provide disincentives for potential cyberattacks by recruiting trained cybersecurity professionals to mitigate this problem. An estimate of 95% of cyberattacks caused by IT users' mistakes is due to inadequate cybersecurity training (Calton & Levy, 2015). General deterrence theorists suggest that deterrence activities create awareness and inhibit fraud which may stop crime before it happens (Nagin, 2013). Having trained cybersecurity professionals can help leaders facilitate

prevention activities by establishing essential awareness for the operators of the system (Yoo & Chang, 2014). Use of the GDT model aligns with understanding one of the pillars of the cybersecurity strategy in the United States, which was to improve the resilience to cyberattacks by recruiting trained cybersecurity professionals. However, researchers often use Maslow's hierarchy of needs address the frame of reference of stakeholders in their continued use of financial services with increased cybersecurity and protection against theft.

Considered Theory

Extensive theoretical scholars debated the effectiveness of deterrence strategies in preventing and mitigating the consequences of cyber-crimes (Wilson, et al., 2015). Adopting different countermeasures is crucial to decreasing the risk of cyberattacks (Alanezi & Brooks 2014). Wilson et al. (2015) suggested that the main problem associated with a cyber deterrence strategy is the limited capability and intent demonstrated by the legal system, which makes this issue a challenge. because cyberattacks are frequent.

The cyberattack on JP Morgan Chase Bank offers an explanatory case to examine the sufficiency of the GDT strategies (Jasper, 2015). In this case, the hackers compromised a bank employee's username and password to enter the server. With a variety of malware protection, the hackers gained access to 100 servers that stored personal data and 76 million household accounts. For this deterrence by denial, JP Morgan's chairperson admitted that even though the bank has fortified its defenses with $250 million annual security budget, the battle is "continual and likely never-ending"

(Jasper, 2015). Furthermore, the perceptions of cyberattacks has not helped create the necessary awareness to deter and prevent attacks.

Alanezi and Brooks (2014) noted that there is a need to change the perception of trained cybersecurity professionals and create more awareness through training. Social-cultural, industrial, and organizational environment practices have a strong influence on the four components of GDT : (a) deterrence, (b) prevention, (c) detection, and (d) remedy. The goal of deterrence is to reduce cyberattacks (Garg & Camp, 2015). Therefore, I did not use general deterrence theory because my intent was to explore the perceptions of financial service leaders rather than criminals.

Theories used for the Conceptual Framework

Two theories comprised the framework for this research: Maslow's hierarchy of needs and stakeholder management theory (SMT). Value creation is a theme in strategic management and receives attention at both the micro level (individual and group) and macro level (organization and society). Strategic management value refers to the amount people are willing to pay or the time they serve (Tiwana et al., 2014). Examples of theories that describe value creation are the value chain activities, the theory of creative destruction, and transaction cost economics (Crane, Graham, & Himick, 2015). Financial service leaders use the SMT to approach value creation from the perspective that understanding value creation processes are critical tools regarding a firm's relationships (Garriga, 2014).

Previous views of the SMT solely aligned with the financial responsibilities company leaders owed to the business owners (Tiwana et al., 2014). The critics of SMT

claim attempting to balance multiple stakeholder groups' interests are contrary to the responsibilities of the firm (Crane et al., 2015). Jollands et al. (2015) countered this criticism by arguing sustainability in an organization influenced by stakeholders that want successful businesses.

Leaders' relationships with possible stakeholders is largely attributable to their ability to create wealth (Jollands et al., 2015). Stakeholders refer to groups or individuals who contribute, whether substantially or not, to the organization (Eskerod & Huemann, 2013). Thus, stakeholders can be customers, employees, suppliers, investors, financiers, and other groups that contribute to the value creation in the firm. An example of the application of stakeholder theory is when leaders consistently request stakeholders to determine value over time (Alanezi & Brooks, 2014; Zagare, 2013). Therefore, to achieve high performance, an organizational leader should adopt a comprehensive strategy-making perspective, including the needs and demands of multiple stakeholder groups (Garriga, 2014).

The stakeholder is often alone in the process of value creation (Tiwana et al., 2014). The value of each stakeholder group is multifaceted and connected to each other. This connection can create a joint effort by stakeholders with tacit knowledge that their stakes interconnect. The principal task for managers was to facilitate the connection between the different stakeholder groups (Eskerod & Huemann, 2013). For stakeholders' value and welfare, research should enhance options or opportunities that increase the value creation process.

Total utility is the satisfaction obtained from the position individuals have, and marginal utility refers to the pleasure they receive from acquiring or giving away a good or service (Crane et al., 2015). In this way, relationships between stakeholders and business professionals are symbiotic (Garriga, 2014). Value creation opportunities are uncertain. Company leaders can articulate ways for improving stakeholder welfare, due to the total utility function (Davis, 2016).

Researchers indicated that most standards do not address stakeholder management as they focus on SMT to comply with project needs (Eskerod & Huemann, 2013). My research focuses on two stakeholder groups in IT-centric project environments and financial management leaders because business leaders can provide their assessment of a project's overall success. Business leaders may be less knowledgeable about assessing skills that lead to success in a cybersecurity environment. Financial leaders are the primary stakeholders when it comes to addressing issues regarding hiring, and onboarding of all business professionals. Therefore, financial managers are also the ones responsible for recommendations on how development budgets are spent, in IT to which this research contributes (Kafol, 2014).

There is a trend in using management theories in research (Millhollan & Kaarst-Brown, 2014). Kafol (2014) and Adriole (2015) used SMT as the conceptual framework. Theorists also claim that SMT in project management implies, through the combined body of knowledge that touches the multiple processes, tools, and techniques a manager must apply in their profession (Davis, 2016). The concept of SMT describes a stakeholder's ability to select, nurture, and deliver programs effectively (Jollands et al.,

2015). Leaders use strategic SMT to benefit stakeholders, products, and services that help them. Furthermore, SMT is aligned with this study by allowing me to highlighting the importance of recruiting trained and keeping qualified cybersecurity professionals (Andriole, 2015).

The hierarchy of needs, developed by Maslow (1943), had basic goals with the need to achieve higher-level goals. Using Maslow's model of the hierarchy of needs in public and private commercial banks reveals that employees of commercial banks show a great use of lower level needs and moderate use of upper-level needs (Rahman & Nurullah, 2015). Rahman and Nurullah found that employees of private commercial banks have a slightly higher motivational score for Maslow's model, but these motivational differences are significant for safety needs and insignificant for social esteem and need for self-actualization.

Maslow (1943) stated there are 5 needs, which separate into deficit needs, and higher needs. These needs include:

1. Biological and physiological needs: physiological needs - food, drink, shelter, warmth, sleep.
2. Safety needs: - freedom from fear, protection from elements, security, and stability.
3. Love and belongingness need - friendship, intimacy, affection, and love.
4. Esteem needs - achievement, independence, self-respect, and respect for others.
5. Self-Actualization needs: - realizing personal potential, self-fulfillment.

The applicability of Maslow's model is often culture-specific; it requires managerial attention to sustain well-motivated employees in different companies in the various countries globally (Rahman & Nurullah, 2015). The hierarchy of needs consists of different levels, and that leaders use when striving toward a collaborative climate (Jacobsson & Wilson, 2014). According to Jacobsson and Wilson (2014), as their project pertaining to Maslow's model progressed, even the contractors involved themselves in a collaborative way of working.

Researchers use Maslow's hierarchy of needs to better understand human beings and their motives (Hayashi, 2016). The layers related to food and physiological needs are very close, similarly so are the happiness, self-actualization, and transcendence needs (Maslow, 1943). A person must satisfy lower-level needs to meet higher-level growth needs (Singh & Holmström, 2015). Growth needs continue to be felt and can become stronger once need is met (Maslow, 1943). Once growth needs are satisfied, one may be able to reach the highest level: Self-actualization. While every person is capable and has the desire to move up the hierarchy toward a level of self-actualization,

The Maslowian portfolio theory (MaPT) is relevant because researchers' use MaPT to further state that it is not possible to convey human needs into the area of investment (Majewski, 2014). At the primary level, an investor looks for opportunities to secure their financial safety and when that need is being satisfied, the second-tier needs become evident. The second level is still the need for protection where the only criterion in the decision-making process is the possible risk of the decision.

At the lower level of Maslow's hierarchy of needs, one's goals apply, and according to Singh and Holmstrom (2015), individuals are conservative because of the primary survival needs and security. The early majority of managers feel secure in adopting technology and innovative methods of providing financial security to its stakeholders; however, they need confidence and expertise in the required processes and strategies. Early adopters of technology look for the opportunity to recognize a leader, while the innovators and technology developers are creative. The hierarchy of needs applies to various financial security fields, and the fundamental characteristics of Maslow's hierarchy of needs can be easily adapted to suit the financial services industry.

From a technology adoption perspective, innovation-related needs were termed as primary needs, if the adopted the innovation or technology was critical for survival or the sense of belonging to its professional network (Singh & Holmström, 2015). From the viewpoint of multi-disciplinary association, if the network has primarily decided to adopt an innovation, a financial service leader may have to consider the changes to continue doing business within that financial network. Adoption of innovation is consistent with the lower levels of Maslow's needs by providing technology (Hayashi, 2016). On the other hand, secondary needs are the needs that go beyond survival and are akin to the higher- level needs in Maslow's hierarchy (Rahman & Nurullah, 2015).

Motivation strategies and practices are necessary to enhance employee engagement, satisfaction, commitment, and performance in business settings (Devito et al., 2016). D'Souza and Gurin (2016) wrote that Maslow popularized the concept of self-actualization as a lifelong process. Maslow believed people follow a path called *growth*

motivation that allows them to self-actualize and realize their true potential. The significance of the hierarchy of needs theory was to develop models that individuals can follow to reach self-actualization (D'Souza & Gurin, 2016). According to Harrigan and Commons (2015), the hierarchy of needs was a set of mental inferences that account for the hierarchy of needs theory. The hierarchy of needs theory takes the same situations that Maslow wrote of and used behavioral metrics. *Needs*, in this case, are primary and *reinforcers* are secondary factors that change with each stage. Primary reinforcers are basic and secondary reinforcers learned when paired with a primary reinforcer (Harrigan & Commons, 2015). Therefore, individuals who score higher on Maslow's hierarchy should also show higher stages and class in social perspectives.

Hansen and Schaltegger (2016) used the hierarchy of needs in the normative perspective related to deterrence and SMT. Their use of the hierarchy of needs provides a comparable evolutionary model with the stages (for both individuals and organizations) ranging from survival to community values. Financial service leaders used the hierarchy of needs in conjunction with SMT to address social needs related to social equity in stakeholder relations (Kamal, Brown, Sivabalan, & Sundin, 2015). The findings from the Kamal et al., study assisted policymakers in understand the strategies adopted by stakeholders to initiate change.

Theories

The modern-day theory of deterrence is attributable to the early works of Thomas Hobbes (1588–1678), Cesare Beccaria (1738–1794), and Jeremy Bentham (1748–1832) (Jasper, 2015). In protest of the legal policies of Europe from the 1580s to 1830s against

the spiritualistic explanations of crime, these theorists provided a foundation for the general deterrence theory (GDT) in criminology. Although grounded in the field of criminology, Straub and Welke (1998) were the first published theorists to apply GDT to information security (IS), their writing supported the premise that information security was not a top priority for most managers. Using a sample of 1211 randomly selected organizations, Straub and Welke (1998) found that the implementation of security measures decreased organizational risk.

General deterrence theorists suggest the following four elements that provide a framework for avoiding cyberattacks: deterrence, prevention, detection, and remedies of issues. The aim of deterrence in the banking industry was to provide restrictions for potential cyber-crime (Cheng, Li, Zhai, & Smyth, 2014). An estimated 95% of cyberattacks caused by IT users' mistakes are due to inadequate cybersecurity training (Calton & Levy, 2015). Use of the GDT model aligns with understanding one of the pillars of our nation's cybersecurity strategy, to improve our resilience to cyberattacks by recruiting trained cybersecurity professionals; and the researcher considered it for this study (Wilson, et al., 2015).

Adopting different countermeasures is essential to decreasing the risk of cyberattacks (Alanezi & Brooks, 2014). For this deterrence by denial, JP Morgan's chairperson admitted that even though the bank has fortified its defenses with $250 million annual security budget, the battle is frequent and likely never-ending (Jasper, 2015). Furthermore, based on the cultural and social backgrounds of individuals, the perception of cyberattack has not created an innate awareness to deter and prevent these

attacks. Nevertheless, social-cultural, industrial, and organizational environment practices have a strong influence on the four components: (a) deterrence, (b) prevention, (c) detection, and (d) remedy. Therefore, the overarching goal of deterrence is to reduce cyberattacks (Garg & Camp, 2015).

Cybersecurity Workforce

According to Safa, Von Solms, and Furnell (2016), leaders support deterrence by enacting policy. Professionals with expertise in recognizing the risks associated with security breaches within financial institutions have the awareness and knowledge to write policies. Our society, economy and critical infrastructures are IT-driven (Jang-Jaccard & Nepal, 2014). Access to the internet for both business and pleasure is the fundamental element of economic growth and opportunity (Knowles, Prince, Hutchison, Disso, & Jones, 2015). As technology evolves, so does consumer requirements in internet banking. While the services of Internet banking are convenient and flexible it may open customers to theft; unfortunately, banks must provide internet banking services to remain competitive (Mukhtar & Finance, 2015). While businesses must protect their organizational assets, they must also remain vigilant to protect their customers' data.

As cyber-crimes increase, companies must demonstrate awareness of deterrence, (Mukhtar & Finance, 2015). Despite the economic recession, deterrence services within the IT security market increased by 12% in 2010. According to Adnan, Just, Baillie and Kayacik (2015) the United States alone is expected to spend $16.5 billion dollars on deterrence services and expected to exceed $125 billion globally by the year 2015 (Adnan, Just, Baillie, & Kayacik, 2015). Developing the capacity to meet the growing

and changing demands of cybersecurity, financial service markets require trained professionals (Manson & Pike, 2014) to protect the organization and increase profits.

The cybersecurity workforce is not limited to a single occupational category (Burley, Eisenberg, & Goodman, 2014). Burley, Eisenberg, and Goodman noted that cybersecurity is a broad field comprised of numerous IT occupations that include the highly technical fields to upper management levels. Cybersecurity is the protection of cyber systems against cyber threats (Gordon et al., 2015). Cybersecurity is the control of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies to protect the environment and organization's assets (Von Solms & Van Niekerk, 2013).

The roles and responsibilities of security professionals within an organization entail dealing with sensitive information crucial to maintaining a high level of security (Borum, Felker, Kern, Dennesen, & Feyes, 2015). According to Denning and Gordon (2015), the US Department of Defense is actively recruiting cybersecurity professionals. In 2014, employers were only able to fill 900 of its vacant 6,000 positions with qualified, trained cybersecurity professionals. The author noted that 66% of the job openings by 2020 should require post-secondary education training and may rely more on communication and analytic skills than manual skills. These positions, according to Denning and Gordon (2015), require higher levels of education, training, and experience. The demand for cybersecurity professionals is a vocation that encompasses many different job categories with various requests (Campbell, O'Rourke & Bunting, 2015).

Burley (2015) stated that building a highly capable cybersecurity workforce remained President Obama's top national priority during his tenure.

Despite significant efforts to increase the size and quality of the cybersecurity workforce, a recent survey of IT professionals revealed that 86% of security professionals state that the United States faces a shortage in skilled cybersecurity professionals. For companies that provide technical services, recruiting and retaining competent cybersecurity professionals is crucial to protecting corporate assets (Gordon et al., 2015). According to Campbell, O'Rourke, & Bunting (2015), cybersecurity professionals trained in recruiting skilled cybersecurity professionals' face increasing organizational challenges.

A crisis exists in many organizations due to the severe shortage of trained information security professionals (Callan, Johnston, & Poulsen, 2015). According to Phillips and Phillips (2016), one most recognize the importance of the human resources functions in ensuring that the organization has competent cybersecurity professionals. Leaders within human resources have a direct responsibility in supporting and defending the body by seeking and retaining qualified, skilled professionals' talent. The problem, however, is that finding, developing, and retaining individuals that demonstrate valued technical skills is a complicated process. Unfortunately, human resources function has few tools and resources for hiring managers to use (Jeffery, Christen, & Moore, 2015).

Organizational Impact of Cyberattacks

Consumers expect access to on-demand business services and due to these demands; the financial service industry has received an economic boom in internet

banking. According to Gaikwad, Yadav, and Patil (2015), Internet banking is the most popular form of online business service, and because of this popularity, online business services have increasingly become the target of cyberattacks.

A potential attack on information systems can cause substantial losses of data, services, and business operations (Rivera-Ruiz & Ferrer-Moreno, 2015). Security risks present organizational problems such as technical failures, vulnerabilities, human failures, and external events (Mukundan & Prakash Sai, 2014). The speculation is that risks occur due to the availability of information assets. As security technology improves, the security levels of networks from hacking have not seen the same degree of improvement (Jeffery et al., 2015).

Therefore, managing security risks is critical to meet customers' demands and cut costs or spending. One of the industry's components is information-security economics that field of study that combining economic theory models to analyze the benefits for stakeholders (Mukundan & Prakash Sai, 2014). Information-security economics applies to this study through the SMT conceptual framework. The total costs of cybersecurity breaches quantify the expenses, intangible costs, and other spending methods that used the market-efficiency based theory (Bojanc & Jerman-Blazic, 2008). The loss in market value in the days surrounding the announcement of an accident is just an approximate value of a substantial cost of the security breach (Gordon et al., 2015).

Gaikwad, Yadav, and Patil (2015) examined cyberattacks in the financial service industry. Their study looked specifically considered internet banking which the most popular consumer-driven financial service provided by financial institutions. Gordon et

al., (2015) suggested that organizations have not only a legal but also a social responsibility for ensuring that consumers' data is safe. Organizational responsibility includes maintaining competent cybersecurity professionals to preserve the integrity external as well as private financial assets to protect the organization's proprietary information.

Economic Impact

Research presented by Bamara (2015) states that 60% of banks have been targets of cyberattacks. These attacks are in the form of malicious codes and denial of services (DoS); however, credit card breaches, phishing, spoofing, and ATM frauds account for a sizable number of attacks as well. As banks attempt to implement safeguards to protect financial assets, cyberattacks increase in sophistication and complexity. Smith (2015) stated that security methods have changed, and revision should continue because of the increasing intensity of cyber-criminals.

In the early days of hacktivism, there was a difference between a *hacker* and a *cracker*. According to Smith (2015), the term "hackers" is someone interested in the vulnerabilities of a computer system; they were not out to exploit these vulnerabilities for illegal gains. The study further revealed that modern-day "hackers" coordinate gangs whose primary focus is to explicitly exploit these vulnerabilities.

Reliable data is fundamental to the success of a financial institution's revenues and budgets from governmental level, within company boardrooms, and to private stakeholders. Financial services need reliable data on crime to allocate the proportionate amount of revenues so that the cybersecurity measures are cost-effective (Armin,

Thompson, Ariu, Giacinto, Roli, & Kijewski 2015). Revenue spent to resolve cybersecurity breaches could be better on prevention, detection, and curbing security incidences.

Maintaining adequate cybersecurity is crucial for financial services institutions in order to sustain the integrity of its external and internal financial reports, safeguard data, and safeguard customer privacy (Gordon et al., 2015). The fast expansion of sophisticated cyber-threats on a global scale is not only a threat to individual users, but also to national infrastructure and business (Caldwell, 2013). Malhotra (2014) noted that the Internet networks have been gaining concerns in global banking and finance industry over the past decade. Despite the crucial role of financial institutions, both technologically and economically to address cyber-threats, more attention directed toward at the seriousness of vulnerabilities in global banking and finance networks.

Hille, Walsh, and Cleveland (2015) examined that when using the Internet, consumers should transfer their personal and financial data to merchants or third parties when conducting online business transactions. Online transactions that combine personal and fiscal data indicate a person's unique online identity. The growth in online sales coupled with worldwide growth in Internet-based information exchange, social networking, access to mobile devices, and e-commerce is contributing to the rise in cyber-crime.

Fortunately, the inordinate growth in online sales and transactions has created anxiety and awareness of consumers regarding online identity theft. Identity theft is one of the fastest-growing crimes of the 21st century (Ruth, Matusitz, & Wan, 2015). Ruth et

al. (2015) explained that identity theft impacts the personal financial and well-being of victims, and within financial institutions and economy. Identity theft presents challenges for law enforcement agencies and governments worldwide as well. The authors suggest that businesses and organizations can take better measures to protect customers' personal information. Moreover, individuals should be educated regarding their rights, and be vigilant in order to protect their personal information offline and in cyberspace.

Data breaches have involved 70 million Target Store customers and 1.1 million customers from Michaels Store worldwide according to studies conducted by (Hemphill & Longstreet, 2016). Their studies further indicate that Gartner Security analyst reported that the total expenditures to Target that include, civil lawsuits, regulatory investigations, bank breach responses, government fines, financial assessments, revenue loss, and computer network lawsuits may cost the company from $450 to $500 million (Hemphill & Longstreet, 2016). In 2014, the online retail sector broker eBay reported that cyber criminals had accessed $145 million customers' private information.

The research study by Hemphill and Longstreet (2016) also revealed that the 2014 Home Depot data breach affected over 56 million customers' credit and debit cards, with financial losses over $62 million. While retailers have been the primary targets of several cyber-crimes, in 2014, J. P. Morgan Chase and Company had its computers servers intruded by cyber criminals (Hemphill & Longstreet, 2016). J. P. Morgan Chase and Company reported that this cyber-breach affected over 76 million households and 7 million small businesses.

Hemphill and Longstreet (2016) revealed that the cybersecurity breaches cost leaders of financial institutions during 2013 more than $200 million. Additionally, 535 surveyed member banks reported that the average bank loss per debit card is $331 and per credit card $530. The cost related to this type of breach estimated a loss of $148 million, with $38 million of the loss compensated by an insurance payoff. Thus, it is evident that managing the effective security of Internet use has become a strategic business issue for United States retailers and financial service institutions. This research can attest that cybersecurity is a top priority for financial services because of the potential economic impact of the breaches already taking place and because of potential damage from increased cybersecurity threats (Gordon et al., 2015).

Information Technology Turnover

Information technology spending has increased worldwide during the twenty-first century. In 2010, the government on IT hardware and software (Rivera-Ruiz & Ferrer-Moreno, 2015) spent $2.4 trillion. In 2015, IT spending in US dollars increased from 3.8% in the first quarter to 4.2%. Despite the importance of IT in the cyberspace environment and the enormous amount of money invested in IT projects, one in eight of IT projects apply successful based upon research conducted by (McManus & Wood-Harper, 2013). Additionally, cyber-threats pose considerable risk to organizations (Fourie, Sarrafzadeh, Pang, Kingston, Hettema, & Watters, 2014). In contrast, Carlton and Levy (2015) purport that cybersecurity threats are causing substantial financial losses for individuals, organizations, and governments within 72% to 95% of cybersecurity threats to technology due to users' mistakes, and the lack of cybersecurity skills.

When assessing the skill level of IT professionals, computer end-users are weak links in the cybersecurity chain, due to their limited cybersecurity skills (Carlton & Levy, 2015; Shillair et al., 2015). There is an alarming shortage of trained professionals and academic programs to train and produce these professionals (Fourie et al., 2014). The United States, New Zealand, and other countries view this cybersecurity as a human capital crisis (Fourie et al., 2014).

Employee turnover presents considerable challenges within government agencies, businesses, and organizations. These problems these situations present are that the loss of key personnel may impact business profitability (Wang et al., 2015). Competition among industries to gain trained IT professionals is intense within service industries as well as by the federal government, which does not offer salaries as high as the private sector (Korsakienė, Stankevičienė, Šimelytė, & Talačkienė, 2015).

Training

Deterrence focuses on disincentives or sanctions against committing a deviant act and the effect of those actions (McDaniel, 2013). Adopting the *whole organizational approach* must begin with the initial training of individual responsible for creating said sanctions according to Adams and Makramalla (2015). Mission-critical roles in cybersecurity regarding increasing depth of detail are necessary to align with the conceptualization and action of masters, experts, competent practitioners, skilled professionals, beginners, and students.

There is not one cybersecurity professional role with various functions that all fall under the title of cybersecurity. Ben-Asher and Gonzalez (2015) found that a direct

relationship exists between domain knowledge, enhanced by experience and the detection of cyberattacks. Cybersecurity analysts and practitioners are required to have a broad knowledge of network operation as well as information security. However, basic knowledge of information security alone without the knowledge of system operations is not sufficient to defend organizational resources.

Prevention

As deterrence theory suggests, countermeasures are effective in preventing cyber-crimes (Hurlburt, 2015). Gordon et al., (2015) suggested that maintaining adequate cybersecurity is crucial for a company to preserve the integrity of organizational financial reports, as well as to protect the organization's strategic proprietary information. Results of the study concluded that information sharing is a tool whereby all agencies benefit. Furthermore, the exchange of information encourages organizations to be more proactive in their approaches to security, rather than being reactive in their cybersecurity investments. The sharing of information may reduce the tendency of organizations to defer cybersecurity investments.

The basic argument presented in this research is in the perspective of real options perspective of cybersecurity investments. Gordon et al., (2015) wrote that the value of an option to postpone investment in cybersecurity activities increases the uncertainty associated with the investment. One must examine the extent to which information sharing reduces an organization's uncertainty concerning a cybersecurity investment and the value of the deferment option regarding the investment. Meanwhile, the reduction in

the suspension option value may well make economic sense for the organization to make the cybersecurity investment sooner than later.

Knowledge sharing proves to have favorable effects on the education, training, and business sectors (Tamjidyamcholo, Baba, Shuib, & Rohani, 2014). Many professional virtual communities (PVC) have failed because of the lack of interest in sharing knowledge with other members. However, the lack interest was not evident based upon the research whether knowledge exchange in information security can reduce risk.

Tamjidyamcholo, Baba, Shuib, and Rohani (2014) and Gordon et al., (2015) researched the relationship between knowledge sharing and information security that focused on securing data. This study offers recommendations for effective practices in prevention and mitigation of cyberattacks. According to Kim and Park (2014), for information security to be effective, organizations must invest in a committed, competent staff. Further, the information security team must create, articulate, and reinforce security policies. Additionally, training on fair use activities must be a part of the overall cybersecurity plan.

Human vulnerabilities account for 80% of total vulnerabilities exploited by attackers (Gordon et al., 2015). If organizations want to protect organizational resources from cyberattacks, they must train their entire staff (Adams & Makramalla, 2015). According to Adams and Makramalla (2015), just creating corporate awareness is not enough, organizations must make a proactive investment in building cybersecurity skills across all levels of the workforce and leadership by knowledgeable professionals within

the organization. The research introduces the concept of gamification as a framework for organizational development. Using this approach, cybersecurity training and implementation utilize a game-based approach to a far-reaching problem enabling administrative staff to "have fun" while engaging in protecting organizational assets. Further, this type of gaming investment has the potential to reduce the financial burden on businesses from cyberattacks and maintaining consumer confidence.

Adams and Makramalla (2015) presented the anticipated benefits of training utilizing gamification methods. Based upon their research, training enables all employees and organizational leaders not only to understand but to take on the role of various types of attackers to reduce the number of attacks due to personal vulnerability exploitation. Using two separate streams gamification and entrepreneurial perspectives, the researcher presents historical research for building cybersecurity skills while emphasizing the third stream: attacker types to create training scenarios. While offering a thorough overview of using gamification for cybersecurity training, the research is theoretical based and is not in empirical testing or implementation. Adams and Makramalla (2015) revealed that the study lacks solid, tested evidence that cannot produce the expected outcomes and improve employees' abilities to prevent data breaches.

Garcia (2014) also recommended a whole organizational approach to cybersecurity. Defining cybersecurity as a mission-critical role is the essential first step in addressing the challenge of developing a competent workforce that ensures that competent professionals are leaders of financial institutions. Phillips and Phillips (2016)

sought to explain the importance of the Human Resources' function in ensuring that the organization has competent cybersecurity professionals. Human Resource (HR) leaders could add value throughout an organization through innovative, security measures that included securing competent technology leaders, supporting, and defending the organization, and by addressing globalization issues that may impact the organization.

One of the primary issues according to Phillips and Phillips (2016) is that the HR function cannot implement the standard human capital strategies. Providing an updated approach to human capital strategy, the authors presented the typical HR strategy and provided an update to address 12 forces that influence the success of an organization. Of the 12 forces presented in the study, six of the functions relate to (a) investment in organizational capacity, (b) talent management, (c) innovation, (d) technology, (e) recognition of global issues and (f) analytic.

In line with the findings of Gordon et al. (2015), that human intrusion accounts form the clear majority of cyberattacks, the researcher recommended a human capital strategy that addresses cybersecurity. The study supports the findings of Phillips and Phillips (2016) in that the chief information officer must spearhead such organizational efforts of training and policy. A cybersecurity policy must not only protect databases and the privacy of data from employees, customers, and suppliers but must also include a mechanism to control and minimize the impact of cyberattacks (Garcia, 2014).

As stated, cybersecurity policies must not only protect databases and the privacy of data from employees, customers, and suppliers but must also include a mechanism to control and minimize the impact of cyberattacks (Garcia, 2014). In an era of diminished

organizational resources, one problem reported by companies is the misreporting of possible attacks. In other words, detection systems often report a possible attack when there is no threat to organizational resources. Investigations dealing with this type of reporting can be time-consuming (Ben-Asher & Gonzalez, 2015); therefore, there is a need for specific regulatory policy directing the actions of those who suspect data intrusions. According to the research when such policies are in place, there is a decrease in malicious attacks (Ben-Asher & Gonzalez, 2015). Ben-Asher and Gonzalez found that in organizations where specific, situated training and implementation exist, employees reported being able to not only detect possible data intrusions but also to differentiate between the various types of attacks because they train on their network. Using a qualitative approach, the researchers found a moderate relationship between punishment and the severity of the incident. Results of the study provide information regarding organizational policies that set clear network usage and employee responses to policy.

Intrusion Detection

Intrusion detection (ID) and cybersecurity of networks are necessary requirements for maintaining the integrity of wide area monitoring systems (Kim & Park, 2014). Ata and Rao (2014) discussed that wide area monitoring is the role of power systems as a detection mechanism in combating cyber-crimes. Cybersecurity threat technologies thus far are only capable of predicting changes in numerical values after a breach has occurred. Intrusion detection includes a collection of system data and network information in all financial institutions. Kim and Park (2014) indicated that cybersecurity, threat detection using ID involves the identification of ID events, required data of harmful website

information, IP addresses used in enterprises, monitoring operations, collecting event matrix data, and weight values.

According to Ata and Rao (2014), phasor measurement units (PMUs) refer to the collection of data for the smart grid energy systems and analyze the frequency of data to detect possible cyberattacks on the smart grid systems. In this research, the authors offer model-based and signal-based intrusion detection methods as a remedy in detecting the presence of malicious data. The researchers found that the chi-square test and discrete wavelet transforms (DWT) are successful in defending a frequency-based detection. The false data injection attack (FDIA) detected using the extra data.

Armin et al. (2015) explained that government needs reliable data on caber-crime to both devise adequate policies and allocate the correct revenues so that the measures are cost-effective. The detection of the presence of tampered images is significant in digital forensics (Goh & Thing, 2015). The problem, however, lies in the contradictory evidence of its success in the literature. The outcome of this research is a proposal utilizing a hybrid evolutionary framework for evaluating features in image problems for the best feature set. Upon further evaluation and selection, organizations must optimize the feature sets to detect network intrusion.

Remedy

When users are aware that security systems are monitoring organizational assets, the hackers' would-be external entities are less likely to attempt a breach (McDaniel, 2013). However, we know from Gordon et al. (2015) that a high number of data exploits originate internally. The exploitation of the General Information and Communications

Technology (ICT) supply chain is a growing security concern in the industry. According to McDaniel, key elements of the global ICT supply chain security include the development of private businesses and the development of a strategy for education, training, communicate, and awareness about cybersecurity. The foundational elements of the plan are to clarify confusing terminology; further, the establishment of a curriculum and creation of a community of interest is a necessary remedy noted in McDaniel study (2013).

Kim and Park (2014) warned that the constant flood of cyberattacks against financial institutions is increasing. These attacks, according to Kim and Park (2014) are to have greater damages because of advanced persistent threats. The authors explained that *Advanced Persistent Threat* (APT) was not a new way of attacking banks, but a keyword for a trend of recent cyberattacks and those security professionals must be knowledgeable of the APT to create remedies against their attacks.

One is aware through evidenced research that online fraud poses a significant threat to the financial sector as well as to banking customers. Further, cyber-crime has a devastating monetary impact on victims (Cross & Blackshaw 2015; McDaniel 2013). These economic effects surface in the form of stolen identities, fraudulent financial transactions, and fraudulent credit liabilities (Cross & Blackshaw, 2015). While financial organizations struggle to find ways to remedy the situation (considering the shortage of security professionals), a lack of prosecution diminishes the ability of organizations to use law enforcement as a solution to offenses. Cyber-crime poses significant challenges to law enforcement agencies and an exorbitant amount of time to detect and persecute.

Cross and Blackshaw (2015) indicated that the ability to investigate complex financial crimes that occur in a virtual environment is extremely challenging. Law enforcement must incorporate multiple (often-international) jurisdictions. Further, many banks fail to report the breaches due threats of negative responses from the public. Many countries where the most cyber-crimes stem have a very low reporting rate. The authors of the study examined the police responses to online fraud and found that fraud had received little attention and priority from police agencies, thus this exacerbating the online threats.

Bezbarua and Rajkonwar (2015) found a relationship between globalization and cyber-crime. According to their research, globalization has stimulated many financial innovations and has presented tremendous opportunities to the financial service industry. However, threats have increased as well in the financial sector (Bezbarua & Rajkonwar, 2015). The economic sectors and more members of the banking industry are very sensitive to these changes; therefore, the transformation has transferred the traditional brick and mortar banks to that of the core business. Unfortunately, the status of automation in the banking industry in the nation is not uniform.

In a core banking solution (CBS) environment, there exists a complicated and complex network system. The intruders are always on the lookout for loopholes in the system so that they can penetrate it unlawfully (Yoo & Chang, 2014). Bezbarua and Rajkonwar (2015) studied the implementation of security measures along with safety upgrades set in place by the banks for the prevention of unauthorized usage and access to a bank network. Results of the Bezbarua and Rajkonwar study found a culture of silence

and secrecy among organizational officials that hampered any efforts of collaboration between banks in fighting cyber-crime across the globe.

Recruitment Strategies

The primary purpose of corporate recruitment was to convey information regarding an organization to job seekers (Badger, Kaminsky, & Behrend, 2014). Attraction to the business is the most used outcome variables in recruitment research. In cybersecurity, people and organizations do not perceive threats in the same way (Gómez-Cedeño, Castán-Farrero, Guitart-Tarrés, & Matute-Vallejo, 2015). Citizens worry about identity theft, governments worry about global data protection, banks, and infrastructure are concerned about maintaining financial services (for example, payments, and exchanges), and commercial activities (Grau & Kennedy, 2014). Recruitment strategies are similar in cybersecurity, however, that organizations and people do not view them the same way.

Gómez-Cedeño, Castán-Farrero, Guitart-Tarrés, & Matute-Vallejo (2015) indicated innovation, research, and organizational response depend on communication between government and industry, and this communication has a cost. Political and economic advantages motivate the government according to Gómez-Cedeño, Castán-Farrero, Guitart-Tarrés, & Matute-Vallejo (2015). Company leaders must realize that while securing qualified cybersecurity professional within an organization may be costly, the risks associated with loss of revenue from cyberattacks is far reaching. is expensive, but insecurity is costlier in the recruiting of cybersecurity professionals. In the banking

industry, cybersecurity's hiring costs the organization about $150,000 in background checks, training, and salary for each IT professional they hire (Grau & Kennedy, 2014).

Management's concerns with hiring cybersecurity professionals protect the information infrastructure from all possible threats (Chaturvedi, Narain Singh, Prasad Gupta, & Bhattacharya, 2014). Recruitment work determines whether a mediation effect exists on the perceived company's reputation and job characteristics (Badger, Kaminsky, & Behrend, 2014). Job application and selection are decisions with high degrees of legal and social obligations.

Human Resources professionals consider the economic climate when there is an abundance of potential applicants (Lu & Liou, 2015). Human Resources professionals need to seek actively seek the populations of potential employees in which they are interested (Brock & Buckley, 2013). By seeking out recruits, financial organizations can reduce the number of unqualified applicants and increase the diversity of the applicant population. Most human resource professionals hire for cybersecurity positions from within different business occupations, consequently (Brehmer, Lilly, & Tippins, 2013). According to the researchers, when there is no internal staff to fill a position, Human Resources professionals used multiple methods to recruit applicants to include social networking.

Retention of Cybersecurity Professionals

Caldwell (2013) examined that it may take up to 20 years to address the cybersecurity skills gap, and this has translated into a severe shortage of competencies in businesses. Cybersecurity requires three areas of expertise, technical, business,

behavioral and enterprise knowledge. Technical capabilities include knowledge of acquisition and project management processes; regulations and procedures, IT and building technology, and analytical skills (Bish, 2014).

Business capabilities include strategic planning, resource management, and communication support an organization's missions (Conley & Redeker, 2016). Behavioral capabilities involve the leadership, negotiation, and change management skills required to integrate functions and people (Bish, 2014). Enterprise knowledge is an understanding of the facilities portfolio and how to align the knowledge with the organization's missions. Recognition and achievement can encourage employees to produce more, and be loyal (Davidson, Sherman, Barraza, & Marinissen, 2015). On the other hand, workplace friendships relate to the employees' job satisfaction, performance, involvement, and commitment.

Organizational commitment is a variable in the work domain associated with job satisfaction (Davidson et al., 2015). Employees that volunteer to leave is the most necessary people to an organization. Continuance commitment exists because a person cannot find another job or they have a benefit or salary from their current position (Kont & Jantson, 2014). Job insecurity occurs when economic crises become stronger. Job insecurity could lead to reduced commitment and satisfaction. A leader's objective was to convince people to join the organization (Conley & Redeker, 2016). By leaders displaying loyalty, employees also build loyalty and are willing to bind themselves to an organization to achieve long-term goals (Kont & Jantson, 2014). The demonstrated principles and motives of employees regarding business capabilities and organizational

commitment are paramount to an organization's the ability to attract and maintain qualified cybersecurity professionals.

Organizational Policy

Gonzales (2015) indicated that while national security usually focused on the military. All security forces should have standards of accountability. In recent years, the U.S. government has introduced several policy measures aimed at tackling the growing cyber threats facing the country, but many challenges and concerns may arise because of their implementation (Baldino & Goold, 2014). Social networking products such as Twitter, Facebook, Blogs, and YouTube made laws pass through Congress empowering the President to take actions to protect national security (Gonzales, 2015). Cybersecurity staff members have high moral and practical prerequisites (Baldino & Goold, 2014). According to Gonzales (2015), organizational leaders have set their policies to achieve standards.

Qualitative Study

Qualitative research in IT takes on a variety of different designs. Three such studies were qualitative in nature and aligned with my literature. Bouzar-Benlabiod, Bouabana-Tebibel, and Benferhat (2015) explored Intrusion Detection Systems (IDS) and determined IDS are necessary security tools. Deployed in a network to filter traffic data searching for malicious activities, IDS are among another approach to alerts. Qualitative Choice Logic (QCL) integrates the security operator's preferences and continually warns the individual of possible issues with the network (Bouzar-Benlabiod et al., 2015).

Garg et al. (2016) explored Network IDS (NIDS) are the most used IDS. Host IDS (HIDS) are on a machine. Host IDS analyze the host computer activity and return alerts when a suspicious action is detected NIDS graft to the monitored network. Host IDS analyze the network traffic and generate signals when the traffic is malicious. These researchers obtained the data to detect anomalies from the system users. However, the preclusion that Hybrid IDS (HIDS) put together from the systems can allow a global view of the system alerts (Shi, 2014).

Researchers determined the safety net systems that receive funding to pilot a text-based program of their choosing to serve a primary care need (Garg et al., 2016). The researchers obtained ethical approval and created a semi-structured interview guide. Secure electronic protocol attracts increasing attention in the field of information security research (Bouzar-Benlabiod et al., 2015).

Researchers also explored qualitative job insecurity and presented its work stressor with adverse consequences for both the employee and the organization. Employee security is viable (Clopton, 2016). Job security has significant repercussions for employees' strain and may lead employees to withdraw from the job and the organization (Vander Elst et al., 2014). Across many areas of law, national rules apply to questions of procedure.

Researchers use qualitative research to determine social practices and the cultural rules of privacy protection (Kreissl, 2014). The historical implications of modern societies demonstrate one sees that these communities developed along the lines of a theoretical perspective of the political semantics associated with the gradual change in

technology. Technology is problematic when human beings are not involved (Jovanovikj, Gabrijelčič, & Klobučar, 2014).

While the importance of perceived control in explaining the impact of quantitative job satisfaction on both job strain and withdrawal, this was not the case for qualitative job insecurity (Vander Elst et al., 2014). Previous studies on job-related uncertainty during organizational changes have focused on perceived control as a potential mediator of the relationship between job uncertainty and job strain, but have not considered withdrawal (Garg et al., 2016).

For such technology-based security systems to work, they must apply a standardized approach to all issues that may affect stakeholders (Simshaw, 2015). When a deviation occurs, the security-technological system is supposed to produce an alert or react in a pre-determined way. Legally, the American Bar Association (ABA) decided there is an obligation to safeguard information, but they have not published an actual rule (Brooks & Anumudu, 2016).

Transition

Researchers need to pay continued attention to the capacity and capability of the cybersecurity workforce (Burley, Eisenberg, & Goodman, 2014). Section 1 included the background of the problem; the statement of the problem; the purpose statement; and the nature of the study. Furthermore, Section 1 included a review of the literature related to the research topic. Section 2 consisted of the explanation of research reliability and validity, along with the design of my research, strategies used to hire cybersecurity

professionals, and the data collection details. Section 3 results from the data analysis and suggested strategies participants used to recruit IT professionals.

Section 2: The Project

In this section, I will review the research method, design, the researcher's role, data collection, and analysis plans. The purpose of my study was to investigate strategies used to recruit IT professionals. In this section, I will present the methodology used to answer the research question. In this section I also include a description including the population sampling frame and procedure to contact the respondents, instrumentation and construct operationalization, data analysis strategy including reliability, validity issues, and a summary.

Purpose Statement

The purpose of this qualitative multiple case study was to explore what strategies financial service leaders used to recruit cybersecurity professionals. The population of this study consisted of five financial service leaders (FSLs) within two financial companies in Columbia, South Carolina, that used successful strategies to recruit cybersecurity professionals. Participants shared strategies they use to recruit cybersecurity professionals. The study findings might help other cybersecurity business leaders hire skilled professionals, and enhance cybersecurity awareness for citizens. Strategies FSLs used to recruit cybersecurity professionals may reduce financial losses to all stakeholders and the communities in which they live and work.

Role of the Researcher

Sherry (2013) wrote that the role of the researcher was to recognize the sensitivity of research and use that to their advantage in building a relationship with participants. I had prior experience and knowledge on the research topic after working in the banking

industry for over 20 years. The Belmont Report describes four principles of ethical research including moral actions, equal participants, participant benefit, and justice (Bromley, Mikesell, & Jones, 2015). In this research, my responsibility was to respect and act ethically within the parameters of the Belmont Report. The requirement is met through open communication with participants, and participants, abiding by the rules and bylaws set forth through this program of study in addition to feedback from my committee, on how to complete the study and engage my participants.

Furthermore, novel aspects of the participant role were the source of most ethical challenges. As described by Liedtka (2015), to mitigate bias, I identified in the assumptions my personal experiences with the topic, and attitudes towards my research question before data collection. However, I was not employed by and has no business interests with anyone in the banking industry in Columbia, or the surrounding areas. To validate the scientific rigor of qualitative inquiry, a researcher should have an interview protocol (Sarma, 2015). In completing the descriptions of my participants, data collection methods, tools, and resources, I used a systemic process in place to ensure the academic soundness of my research. The interview protocol, which was a written description of how to conduct each interview consistently, supported the data collection process, aided in ensuring the validity of the study, and led to the appropriate data analysis and findings of the study. See Appendix B.

Participants

Eligibility criteria are the guidelines for who can and cannot participate in a study. Having participants with characteristics that are similar ensures that the results of a study align with what is under study, excluding other possible factors (Lewis, 2015; Streagle & Scott, 2015; Marshall & Rossman, 2014). In this way, eligibility criteria help researchers achieve accurate and meaningful results. These standards assure that people who may be negatively affected (i.e. mentally or physically) by participating in the study do not expose themselves to the risk.

The eligibility criteria for study participants of this study were: the individuals were FSLs responsible for the recruitment of cybersecurity professionals, and the FSLs had worked for their respective companies a minimum of 5 years (Miller et al., 2015; McCrae, Blackstock, & Purssell, 2015; Yin, 2014). Additionally, all participants were required to have recruited at least five cybersecurity professionals with *IT Specialist* in their job title, and those employees hired have worked a minimum of 2 years with the company and still employed.

By having comprehensive communication skills and networking ability, I gained access to participants. By promoting a partnership rather than a researcher-subject type of relationship, probing skills can be used to conduct interviews (Lancaster, 2016; Morse, 2014). I used probing skills to conduct interviews. Individuals require a background in their field of study and the ability to communicate (Mikkonen, Kyngäs, & Kääriäinen, 2015; Streagle & Scott, 2015).

Research Method and Design

In the following section, I will outline the research plan and design. Included is an extended review of the choice of investigation method, the justifications for this approach, and the exclusion of other methods. The conclusion between the process, design, and alignment with the conceptual framework used in this study, is justified.

Research Method

In this study, I chose the qualitative method. The qualitative method applies in IT and cybersecurity studies because researchers benefit from the expressed decision-making process of participants and the objective evidence exposed in the interviews (Dağhan & Akkoyunlu, 2014). Often researchers base cybersecurity on ideas of quantitative analysis, assuming the data were numerical in nature. Researchers often forget that humans are still responsible for facilitating IT work. I chose to use the qualitative approach because I am interested in strategies used to recruit individuals in this industry.

Qualitative inquiry is part of the constructivist learning approach and cannot be of use in quantitative studies (Dağhan & Akkoyunlu, 2014). Data diversity supports methodological triangulation. For this purpose, results can be strengthened with nontraditional data collection methods, such as a face-to-face interview (Zhu et al., 2015). I used the face-to-face interview method. Researchers who use quantitative approach do not view participants' experiences, observations, and relevant documentation (Morse, 2014) .

The protocol for mixed methods research includes focus groups, observational study, and data gathered from different tables and documents (Arris, Fitzsimmons, & Mawson, 2015). Quantitative data are not relevant to strategies used to define an outcome, nor would observation be indicative of strategies used by someone to accomplish a result (Hollingsworth et al., 2015). Therefore, mixed methods study was not applicable to my research. A quantitative or mixed methods study incorporates numerical responses (Bryman & Bell, 2015).

Quantitative researchers ignore substantive reasons for decision-making (Parker, 2014). Mixed methods research requires both qualitative and quantitative analysis, which due to the time constraints of this study, and topic understudy, were not appropriate (Burns, 2014). The qualitative method is suitable to researchers' intent and to obtain the lived experiences of the demographic under study (Bryman & Bell, 2015; Marais, 2012).

Research Design

For this study, I chose to use a multiple case study design. A case study design is used by a researcher to exercise control over a study (Thomas, Suresh, & Suresh, 2013). Cases and samples are controls relevant to match within a topic, because potential differences may not exist in qualitative research (Barclay & Stoltz, 2016). Using a case study design offers researchers the advantage of having an actual control group, random in its choosing, without any standard features that may confound associations (Almutairi, Gardner, & McCarthy, 2014; Thomas et al., 2013).

Other research designs considered for this study were narrative, phenomenological, and ethnographic designs. Narrative design is the process of

gathering information through stories (Tong, Raynor, & Aslani, 2014). As there is no way to determine if an individuals' story is true or false: Narrative design is not applicable to my research.

In phenomenological research, researchers try to find the structure and behavior of a group in response to a situation (Koopman, 2015). A phenomenologist researcher is concerned with understanding certain group behaviors from that group's point of view (Henry, Rivera, & Faithful, 2015). I am not interested in an individual situation, but the strategy applied to get the desired result. A phenomenon is not a part of the topic under study, therefore, this approach was not applicable to my research.

The ethnographic research design is the long-term investigation of a group through immersion within their culture (Bryman & Bell, 2015). Based upon the time constraints and the objective of ethnographic research, this design was not appropriate for my study. I chose a multiple case study to obtain living examples of their experiences with strategy and understand the process from which the procedure applies (Hollingsworth et al., 2015). Data saturation was assured through continual inquiry to ensure all information was present until no new information emerged, even when I exceed the number of participants targeted for participation in this study. Data saturation is reached by obtaining referrals of other individuals in this population (snowball sampling) until no new information was there (Rowlands, Waddell, & McKenna, 2015).

Population and Sampling

In qualitative inquiry, the researcher defines the rigor of the population sample (Bryman & Bell, 2015). In the United States, 12 million people generated three million

dollars working in the financial service industry in 2014 (Modlin, 2014). Of those 12 million employees, Columbia, South Carolina has roughly 180 financial service leaders, and 50 employees or less are recruiting professionals. The sample is a subset selected from the larger population, and because the subset in the scope of my research was less than 100, I chose a snowball sample size of five. According to Stivala et al. (2016), a sample size of five to 20 individuals is appropriate for qualitative research. Snowball (chain) sampling is a nonprobability technique that is used by researchers to identify potential subjects in studies when subjects may be difficult to locate (Morse, 2014). Once a participant was identified using the snowball sampling technique, I asked the participant to refer others in the same demographic that may have interest in participating in the research study.

The demographic characteristics of this sample were financial service leaders who oversee recruiting cybersecurity professionals. To ensure data saturation, I continued to ask for referrals of other individuals in this population until no new information emerged, even if the sample used for this research grew beyond the five participants that I sought. The criteria for selecting participants and the use of face-to-face interviews was appropriate for this study because I investigated the lived experiences of participants (Bryman & Bell, 2015). A face-to-face interview assures that I am aware of the social cues of participants, which may convey a deeper or other meaning of their responses.

Ethical Research

Bromley et al. (2015) wrote that the Belmont Report included principles of ethical research. The informed consent process serves to protect participants from harm and

respect a member's privacy (Tam et al., 2015). I offered no incentives for participation in this study. All participants could withdraw from this study at any time during the interview process by stating that they no longer wished to participate, and approving my personal destruction of their informed consent form and or their interview documents.

To assure ethical protection of participants, I participated in the national institutes of health (NIH) series to certify that members' information was protected from risks and avoid the most vulnerable subjects. The measures I chose to assure that the ethical protection of participants was adequate, and not release any personally identifiable information (PII) saved the data on a password encrypted hard drive (Smith-Merry & Walton, 2014). The written data is in a locked file drawer, and all transcribed data and theming are on a password encrypted hard drive for a minimum of 5 years to protect the confidentiality of participants.

The Walden IRB approval number for this study is 03-28-17-0515162 and expires March 27, 2017, one year from the approval date of this study. The name of the companies and participants remained anonymous to guarantee confidentiality (Smith-Merry & Walton, 2014). When Walden University approved this study, I gave a summary of results to the participants and an electronic copy of the research study. This information concluded the ethical research portion of this document.

Data Collection Instruments

I was the primary data collection instrument in this study. I chose to use the peer-reviewed face-to-face interview (PRI) and triangulate using archival data. The purpose of the PRI was to verify that the interviewee was the same person who meets the

eligibility criteria and to confirm that they have a level of knowledge and experience commensurate with what the researcher was investigating (Issitt, 2014).

A confidentiality agreement was not necessary, as I themed the data by hand. The researcher chose a text analysis to interpret the meaning of the data as opposed to a software program. The researcher opted to use interview questions following the interview protocol, located in Appendix B. Qualitative researchers conduct interviews using protocol because they anticipate for surprises (Da Silva et al., 2014). Using an interview protocol can remind me of my questions while allowing unexpected data to emerge (Dağhan & Akkoyunlu, 2014). Member checking enhances the reliability and validity of the data collection processes (Awad, 2014).

Data Collection Technique

The theory is often compelling for collecting and communicating thoughts. However, the technique used such as the qualitative interview can present its problems (Humphrey, 2014). In this study, the researcher chose the qualitative interview method. The disadvantages of using this technique are miscommunication, the trustworthiness of participants, and the academic rigor associated with collecting data via spoken word (Qayyum, 2015).

However, the advantages to using the qualitative interview technique are open-ended questions allowing for conversations to happen, the subject can provide a first-hand account of the topic under study, and a participant may be more honest than with other techniques (Humphrey, 2014). The advantages of using the qualitative interview technique outweigh the disadvantages; thereby I chose a qualitative interview method. A

letter of cooperation granting permission not required since no proprietary data from the business is in this study (Dağhan & Akkoyunlu, 2014). As well, the FSLs interviewed were the top executives of their organizations who have the sole authority to participate in the study.

I chose to access the FSLs' contact information through banking institution websites to obtain confirmation of interest to take part in the study. The FSLs had the full right and authority to choose what information to disclose and who to interviewed (Snowball). A signed informed consent document (Appendix B) was available for all study participants. Pilot studies are a scientific tool for soft research, to conduct a preliminary analysis before devoting resources to a study (Koopman, 2015). As such, a pilot study was unnecessary for my research. The data collection technique follows:
I used the following set of steps as part of the informed consent process that applicable to this study.

a) Before contacting participants, I received approval from IRB.
b) After obtaining IRB approval, I contacted potential participates and asked the FSL for email addresses and telephone numbers of the potential participants.
c) Upon receipt of the informed form, I followed up with potential participants and clarified any questions, and I scheduled the date, time for the face-to-face interview.
d) Before conducting the interviews, I sent the participant via email, the interview questions, and a description of how I would conduct the interviews before replying with the "I Consent."

e) I emailed the new potential participants to provide information about my study, the interview process, confidentiality, and consent form to participate.

f) I ensured consent, time commitment and the rights of participants to answer some or none of the questions, the right to withdraw from the study at any time and the storage process for securing confidential information.

g) I was the only person who has access to their data and that the data is kept in a locked file cabinet in my home and destroyed after 5 years' post-study.

h) The face-to-face interviews began with introductions and an overview of the topic.

i) I informed the participants that I hope to record the interviews to ensure the accuracy of the data collected, but I recorded interviews with participants' permission. I reinforced with the participants that the conversation remains strictly confidential.

j) The interview lasted approximately 45 minutes to obtain responses to five interview questions and follow-up questions if any.

k) I explained the concept of member-checking, ensured each question was thoroughly explained, and confirm the answer provided was their intended statement by contacting participants with transcribed data and request verification of the accuracy of collected information within 5 business days.

l) After confirming answers recorded to the satisfaction of the participants, the interview concluded with a thank you for participating in the study and my commitment to care for the confidential information.

m) I was the only person who has access to their data and that the data is kept in a locked file cabinet in my home and destroyed after 5 years post-study.

The reliability and validity of the data collection process consisted of implementing a triangulation strategy (Noble & Smith, 2015). In the process of triangulation, data collected from multiple sources is used to reliability and validity (Serafini, Lake, & Long, 2015). Three types of triangulations are between-method or the across-method and within-method (Song, Son, & Oh, 2015).

Investigator triangulation such as member checking or peer review is methods to increase credibility (Song et al., 2015). The researcher can establish creditability through examining similar themes in interview transcripts (Thomas & Magilvy, 2011). Between-method involves combining both qualitative and quantitative methods in a study. Within-method is one set of data using different methods to obtain information to compare and crosscheck data collected from people with different perspectives (Vink, Lawrence, McFadden, & Bingham, 2016). Interview questions are present as Appendix A (Humphrey, 2014). To properly use triangulation a researcher uses multiple data sources in an investigation to produce understanding (Qayyum, 2015). I chose methodological triangulation, using archival data on cybersecurity and IT threat management to assure that my methods are suitable to this subject.

Data Organization Technique

The system the researcher chose to use for keeping track of data, and emerging themes for my research was a labeling system. After transcribing text data, including my notes from interviews, the archival documents, I formatted the data for coding in

Microsoft Word (Humphrey, 2014; Oken et al., 2013). This axial coding method used to develop refined themes. By color-coding, the data: *Yellow* (pending), *red* (irrelevant), and *green* (applicable to theory) the researcher refined data using color until no additional information emerges. The successive levels of coding provided the reader information on the underlying information in the themes, as well as allow me to integrate my work efficiently into the final study (Qayyum, 2015). According to the University policy, I am maintaining all raw data in a locked drawer for a minimum of 5 years.

Data Analysis

I chose to rely on theoretical propositions. By following the theoretical propositions that led to this case study, a description of the objective and design of this case study is in the literature review, the qualitative design of the study, and all should be present in the results. To explore the experiences of members the purposive selection method was present. The hand-coding method used for coding and grouping themes from the interviews can show a variety of experience (Saldaña, 2015). The participants of this study were from different organizations, and to get adequate groups of data from those working for various companies this approach is appropriate (Bryman & Bell, 2015; Marais, 2012).

I sequentially processed the data by hand. Hand coding is a way for a researcher or editor to validate and evaluate items by hand using their human capabilities (Marshall & Rossman, 2014). The value in using a hand-coding method is that it can be done anywhere at any time. While there may be more hard data that is locked in a drawer with a key held only by the researcher, the data can also be more relevant to readers. Instead

of computer assisted programs finding themes based on words, a human being can identify issues using complete phrases (Anthony & Weide, 2015). Research procedures ensure privacy during the data collection process.

I did not use participants' names. Each participant was assigned an identifier (code) to protect confidentiality. Information is kept in a locked drawer in the researcher's home and destroyed after 5 years. In the consent form (Appendix A), I included my commitment to care for the confidential information, and the participant's right to answer none of the questions. The participants' reserve the right to withdraw from the study at any time without consequences. I explained to the respondents that my notes are confidential.

I focused on the key themes; correlate the key topics in the literature (*to include novel studies published after writing the proposal*) and the conceptual framework used for this study. Thematic analysis is the simple form of categorization for qualitative data (Walker, 2014). The thematic analysis also encodes qualitative information and develops codes that label the data (Koopman, 2015). The thematic analysis allowed me to match data to themes that exist in my conceptual framework. I continued this process until no data could be themed.

Reliability and Validity

Babbie (2013) stated validity and reliability are critical in ensuring the precision and accuracy of research. Although the two factors do not have the same meaning in qualitative studies, they both rely on various tools such as interview protocol to ensure that the research outcome was consistent and acceptable. The concepts of internal

validity and reliability in quantitative research are equivalent to credibility and dependability of qualitative research (Munn, Porritt, Lockwood, Aromataris, & Pearson, 2014).

Reliability

Specific practices are necessary to assure the design reliability. Reliability is the ability other researchers should repeat the study with consistent results (Humphrey, 2014). Dependability occurs when another researcher can follow the audit trail of the first investigator (Luiz & Stewart, 2014). Audit trails consist of: (a) describing the purpose of the study, (b) describing the selection criteria of the participants in the study, (c) describing the data collection process, (d) explaining how the data was interpreted for analysis, (e) discussing the research findings, and (f) communicating techniques to determine credibility of the data.

To ensure reliability, I provided an interview protocol to identify (page 54-55 in this document) steps taken to conduct the interviews. Following the interview protocol may improve the reliability and repeatability of the study. Additional strategies to ensure reliability include: (a) aligning activities and interview questions with the central research question, (b) documenting and storing data (c) securing data and protecting confidential information (d) applying standard analytical approaches consistent with case studies, and (e) destroying stored, sensitive information after 5 years (Yin, 2014).

Validity

Fassinger and Morrow (2013) suggested three criteria for testing the validity of qualitative research, including credibility, transferability, and confirmability. To ensure

credibility, I described the topic understudy from the view of the participants. Participants are the only people who can determine the integrity of the results, and member check for data integrity. The researcher ensured dependability through member checking of data (Humphrey, 2014). Dependability requires one to account for the changing context within which research occurs and how changes affect the way one approaches a research study (Luiz & Stewart, 2014).

The researcher established creditability through member checking and participant transcript review. The purpose of the qualitative research was to describe or explore the problem of interest from the participant's viewpoint. Therefore, the participants are the only people able to determine the creditability of research (Fassinger & Morrow, 2013).

Transferability to the reader and future research is available by the degree the results of qualitative research can transfer to other contexts (Sanromá, Ramos & Simón, 2015). In qualitative research transferability, is the responsibility of the one doing the generalizing. The researcher may enhance transferability by describing the research context. The researcher addressed confirmability and trustworthiness through triangulation of the results of this study with archival data on the topic under study. The researcher ensured data saturation through continual inquiry to assure all information obtained (Rowlands et al., 2015).

Using triangulation, the researcher validates the study by exploring the topic understudies, using interviews, documentation, and physical artifacts. Marshall and Rossman (2014) suggested providing a conceptual framework to guide the study. The conceptual frameworks used to guide this study are the hierarchy of needs and

stakeholder management theory. According to Rowlands et al. (2015), using a rich, thick description can ensure a deeper understanding of information and breadth in the context of information shared.

Transition and Summary

The objective of Section 2 was to describe the qualitative, single-site, case study approach of within this study. In this part of the study, I described the overview of the purpose, method, design, the data collection methods, and steps to ensuring the reliability and validity of the data collected. Section 3 of the study consists of the presentation of findings applicable to professional practice, the implication for social change, recommendation for action and further study, and the conclusion of the research.

Section 3: Application to Professional Practice and Implications for Change

In Section 1, I discussed the (a) foundation and background of the study, (b) the problem and purpose statement, (c) nature of the study, (d) research question, (e) conceptual framework, (f) operational terms, (g) the significance of the study, and (h) and the literature review. In Section 2, I expanded on the (a) the role of the researcher, (c) the selected participants, (d) a detailed description of the research methodology and design, (e) the population and sampling, (f) ethical research, (g) data collection instruments and technique, (h) data organization technique, (i) data analysis, and (j) reliability and validity. Section 3 contains the (a) findings of the research study, (b) the implications for change (c) recommendations for the action and further research, and (d) the reflections and conclusion.

Introduction

The purpose of this qualitative multiple case study was to explore strategies financial service leaders in the Midlands part of Columbia, South Carolina used to recruit trained cybersecurity professionals. The central research question was: What strategies do financial service leaders use in recruiting cybersecurity professionals? I used a purposeful chain sampling technique to find five participants from the overall population of 22 for this study. Consistent with the literature, participants indicated there is a lack of strategies that FSLs use to recruit knowledgeable cybersecurity professionals. Five members of one population group responded to six open-ended interview questions. The interviews were audio recorded, transcribed, member checked and thematically analyzed to expose key themes. The themes were (a) increased training, (b) broadened social

networking, and (c) improved communication. The literature review exposed a lack of knowledge about strategies FSLs need to recruit trained cybersecurity professionals. Individual abilities should indicate aptitude to perform well in the areas of operational security testing and great threat response when hiring cybersecurity employees (Tobey, 2015). The following section includes a presentation of findings, the application to professional practice, and recommendations for future research.

Presentation of the Findings

The central question for this study was: What strategies do financial service leaders use in recruiting cybersecurity professionals? The interview questions were as follows:

1. What strategies do you use to recruit cybersecurity professionals?
2. How were the recruiting strategies to recruit cybersecurity professional deployed and implemented?
3. What challenges, if any, did you experience while using recruiting strategies to recruit cybersecurity professionals? How did you address any barriers to implementing the recruitment strategies?
4. How do you measure the success of your strategies and recruitment processes?
5. What additional information can you provide to help me understand the strategies and processes you've used for employing and maintaining the service of cybersecurity professionals?

I used Maslow's hierarchy of needs and SMT as the combined conceptual framework for this study (Maslow, 1943; Straub & Welke, 1998). I chose general

deterrence theory as a guide to evaluate the financial position, operational effectiveness, in addition to social performance.

I scheduled a face-to-face semistructured interview. After each interview, I thanked the participants for participating in my research study. I transcribed the recording and performed member checking by providing each participant with my interpretation of the interviews via email for potential closing gaps and correct inaccurate statement. Data collection continued until the study reached saturation, at which point I stopped the interview process.

After I asked participants to verify the transcription of the text data, including my notes from interviews the archival documents, that data formatted for coding in Microsoft Word. I replaced the names of the participants with an identifier (FSL1, FSL2, FSL3, FSL4, and FSL5) to protect their confidentiality. I sequentially processed the data by using hand-coding. After coding the data, I analyzed the data using the pattern-matching technique as described by Dev and Kisku (2016). The similarities in participant responses led me to identify three themes, which were: (a) increased training, (b) broadened social networking, and (c) improved communication.

I used methodological triangulation by combining the interview data from financial service leaders with archival data. I compared archival data for triangulations between my findings in the literature review and similar studies. The third method used is member checking, and I used it to assure data saturation. The findings of this study contain basic strategies financial service leaders may use to recruit trained cybersecurity professionals. I found congruency of all three themes in the peer-reviewed articles

included in the review of the professional academic literature review section of this study. I used the theoretical approach outlined in my combined conceptual framework to process the data. I chose general deterrence theory as a guideline to evaluate the financial position, operational effectiveness, in addition to social performance. As Table 1 indicates, the frequency of occurrence of core themes confirmed that certain recruitment strategies favored in recruiting cybersecurity professionals. In the following sections, I describe the themes evolving through the data analysis process and links each theme to the conceptual framework and literature review.

Table 1

Frequency of Themes for Important Strategies for Recruiting Cybersecurity Professionals

Theme	*n*	% of frequency of occurrence
Increased Training	25	45.4%
Broadened Social Networking	15	28.8%
Improved Communication	13	25.8%

. **Theme 1: Increased Training**

The first major theme that emerged from the data analysis indicated there is a need to increase of training. The development of theme 1 was from all interview questions and company archival documents. Table 1 illustrates 45.4% frequency of occurrence identified in the textual analysis. Training is one of the biggest factors that increased employee commitment, engagement, and job satisfaction (Saleem, Ahmed, & Saleem, 2016).

All (100%) participants indicated that training benefits the organization. A well-trained, stable cybersecurity workforce is critical to protecting the financial service industry. Leaders need to understand and be aware of the factors that influence employee productivity (Aisha, Hardjomidjojo, & Yassierli, 2013). Training is a way for management systems to be effective, which fosters employee satisfaction and company performance. Compared to archival data to include IT reports in the financial service sector from 2014 to 2016 training assures transparency in business (Comizio, Dayanim, & Bain, 2016). Expressed transparency as a fundamental condition needed to improve employee and manager relationships. Alanezi and Brooks (2014) noted that there is a need to change the design and perception of trained cybersecurity professionals and create more awareness through training.

FSL1 reported, "we look at the needs of our company's client base in serving them and how we can meet the needs more effectively." Referencing to training and cross-training, three of the five (60%) participants suggested that the success of a company is measured by how well the employees are trained and cross-trained. A total of four out of five (80%) indicated the principle strategy use to recruit cybersecurity professionals were to focus on the applicant's work history in the field. When specifically looking at the various types of cybersecurity tools they deployed and worked on during their current/ previous employment. FSL4 stated, "we contact internal applicants and ask them to submit resumes if they are interested and if no candidates are identified we publish via headhunters." FSL5 noted that most employees have some weaknesses in their workplace skills. A training program allows employees to strengthen

those skills that they need to improve. Strategies recommended by all (100%) of the participants pertain to both leaders and employees practicing transparency, to advance trust, increasing the likelihood of organizational sustainability.

Each FSL provided their understanding of the first theme. FSL1 mentioned that finding the best combination of experience, education, skill level along with an inner enthusiasm and drive to succeed and grow in the industry. FSL2 noted, "our success is measure in the number of successfully hired candidates with the correct qualifications." FSL3 indicated that the biggest challenge they face is that of a process change that may add requirements for the end user, (customer). FSL4 added, "(That) when staff was stripped of credentials and only allowed to use the new system they adapted." FSL5 elaborated that "if security talent can prove they are proficient in the skillsets I am looking for, then I hire them."

All (100%) of the FSLs also mentioned that the training has improved over the years. Participant responses confirm the findings of Ruvimbo-Terera and Ngirande (2014), who suggested that organizations have found that it is important to invest in employees training to improve deficiencies so that employees can acquire a greater return on human capital investment through increased job commitment and high employee retention (Ruvimbo-Terera & Ngirande, 2014).

Participants' responses and reviews of the company operational policies and procedures (archival documents), demonstrated support for job growth and increased knowledge through the continuance of training. A total of four (80%) of the participants indicated that the employee should take a more assertive role in creating self-

developmental interest in their training. FSL1 argued that the manager should have an ongoing desire to learn and grow professionally and personally. Managers should be actively working on industry and non-industry related certifications such as Security+, CISSP, etc. FSL3 agreed that the most important of any cybersecurity environment was to fully understand the impact of the cybersecurity threat and the deployment of that cybersecurity solution. There must be an open dialogue between the IT department and the stake holder/s as both sides must understand the risks of not doing anything as opposed to applying the cybersecurity solution. FSL5 suggested that cybersecurity professionals want to be working in challenging areas of cybersecurity and know exactly what they're worth.

Application of training to conceptual framework. Participates response was aligned with the conceptual framework of both the hierarchy of needs theory by Maslow (1943) and Straub and Welke's (1998) stakeholder management theory (SMT). Training in both hierarchy of needs and SMT is important to this study because cybersecurity market is the largest and fastest growing market in the United States and financial institutions are prime targets. According to (Adams & Makramalla, 2015), hiring knowledgeable employees for the job is critical for an employer; however, training and retention are even more critical than recruitment, hence the need for organizations to develop and implement effective training practices. By using both SMT and the hierarchy of needs framework will strengthen employee motivation and commitment through training. The hierarchy of needs by Maslow (1943) model presents a means for understanding the

needs of the individual and training makes the worker more secure, can enhance feelings of belongingness and self-esteem, and provides the opportunity for self-actualization.

Findings aligned with existing literature. Researchers indicated that human vulnerabilities account for 80% of total vulnerabilities exploited by attackers (Gordon et al., 2015). If organizations want to protect organizational resources from cyberattacks, they must train their entire staff (Adams & Makramalla, 2015). According to Adams and Makramalla (2015), just creating corporate awareness is not enough, organizations must make a proactive investment in building cybersecurity skills across all levels of the workforce, and people require leadership.

The research introduces the concept of gamification as a framework for organizational development. Using this approach, cybersecurity training and implementation utilize a game-based approach to a far-reaching problem enabling administrative staff to "have fun" while engaging in protecting organizational assets. Further, this type of gaming investment has the potential of reducing the financial burden on businesses from cyberattacks and maintaining consumer confidence. Furthermore, cybersecurity is the control of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies to protect the environment and organization's assets (Von Solms & Van Niekerk, 2013). According to Tamjidyamcholo, Baba, Shuib, and Rohani (2014), knowledge sharing proves to have favorable effects on both the education, training, and business sectors. Whereas both Tamjidyamcholo, Baba, Shuib, and Rohani (2014) and

Gordon et al., (2015) indicated that the relationships between knowledge sharing and training offer effective practices in prevention and mitigation of cyberattacks.

Theme 2: Broadened Social Networking

The second major theme that emerged from the data analysis was broadened social networking. The development of theme 2 was from all interview questions and company archival documents. In Table 1, participates indicated 28.8% of the frequency of occurrence identified in the textual analysis.

Stoughton et al. (2015) indicated that social networking websites such as LinkedIn and Facebook allow employers to gain information regarding applicants which employees may not otherwise share during the hiring process. The data analysis of this study correlated Stoughton et al.'s results were that some leaders' hiring decision did not effect the relationship between screening and hiring. My results suggest organizations should consider the costs and benefits of social media screening which could assist in finding ideal cybersecurity professionals.

A total of three (60%) FSLs indicated to shared their outlook on social networking. Applicants may need to change their social networking websites as well, to make them favorable to an employer (Stoughton et al., 2015). FSL2 recommended we use LinkedIn to find and recruit new talent through our social media campaign. Our company coordinates with the local University recruitment personnel to schedule job fairs when looking for talent. We also posted a job announcement on our web page. FSL4 indicated that we contact internal applicants and ask them to submit resumes if they are interested and if no candidates are identified we publish via headhunters. FSL5 said

we are familiar with social and professional networks LinkedIn, Twitter, and Facebook. You want to find professional social networks that focus on cybersecurity. All five (100%) participants indicated that social networking is critical to recruiting qualified cybersecurity professionals.

Application of social networking to conceptual framework. From the interviews with FSLs were consistent with the conceptual framework presented in both hierarchy of needs theory and stakeholder management theory (SMT). Schuck (2016) suggested that utilizing an employee conduct code rather than the criminal justice system to address offenses is likely to lead to success. The hierarchy of needs lists success amongst higher-level goals. Social networking is a tool that applies to stakeholder management theory, as those who are likely to be a stakeholder also may utilize social networking sites. Ruehl and Ingenhoff (2016) provided that recently corporations have become increasingly active on social networking sites (SNS). From a communication management perspective, SNS have the potential to communicate with stakeholders on online communities directly. The researcher suggested that like Ruehl and Ingenhoff, interconnections of incentive link to possible motivations for participation on corporate pages. Using social networking to recruit cybersecurity professionals is cost effective, and faster than traditional means of having applicants come to a staffer or employer.

Findings aligned with existing literature. Researcher indicated Hille, Walsh, and Cleveland (2015) examined that when using the Internet, the consumers should transfer their personal and financial data to merchants or third parties to carry out online business transactions. Personal and fiscal data combined, constitute a person's unique online

identity. The growth in online sales coupled with the worldwide growth in Internet-based information exchange, social networking, the access of mobile devices, and e-commerce is contributing to the rise in cyber-crime. The online growth has made many consumers anxious about online identity theft. Identity theft is one of the fastest-growing crimes of the 21st century (Ruth, Matusitz, & Wan, 2015). Ruth et al. (2015) explained that identity theft impacts the personal finances and well-being of victims, and on the financial institutions and economies of countries. Identity theft presents challenges for law enforcement agencies and governments worldwide.

Ruth (2015) advocated that businesses and organizations can take measures to protect personal information better and that individuals should be educated regarding their rights, and be vigilant and protect their personal information offline and in cyberspace. Likewise, Saridakis, Benson, Ezingeard, and Tennakoon (2016) indicated that social networking users are at a high-risk propensity to become victims of cyber-crime. The results of this study indicated to control information shared on social networking platforms has adverse effects on recruiting qualified candidates because part of knowing an applicant was to know everything about them.

Theme 3: Improved Communication

Improved communication is the final theme found through textual analysis and it is essential in every area within every strategy. Working together as a team improves business processes and profitability, and market share (Daneshgari & Moore, 2016). Compared to archival data regarding business communication: Communication makes people feel confident in their role as an employee, and by providing guidelines to

strengthen interaction between leaders and staff, both grow together as a team (Bruyer, Jacobs, & Vandendaele, 2016).

In the respondents' answers, proved that the team should work toward the same goals for innovations to be successful. One must make a change to practice in business and assure that communication is important to everyone involved in an organization (Webb & Roberts, 2016). All five (100%) participants' responses indicated that communication requires strengthening to recruit cybersecurity professionals.

Communication is salient to all five (100%) of the participants interviewed. FSL1 indicated that project managers meet with the customer to assess the plan and set milestones to address these challenges. The manager then meets with his staff to plan and set goals and address issues as they arise. FSL2 mentioned my strategy was deployed using technology and recruiters. FSL3 noted that the region implements a Regional Change Control Board, (RCCB) that governs the deployment of a new cybersecurity hardware/software. The product was tested against a select subset of platforms throughout the region to identify any issues that may occur. If no issues occur, then an Action Item was then submitted for a full rollout. FSL4 acknowledged we used a research team to decide what changes in our staffing are needed based on cost effectiveness, then we communicate the change to staff involved, and implement the change through agile methodologies. FSL5 revealed that we found young new talent and helped them realize the potential to engage in challenging work, as well as growth and development.

A total of four (80%) participates provided their response to stakeholder consideration and three of four (75%) indicated they want more stakeholder involvement. FSL1 mentioned from the feedback, "we received from our customers on how their needs are met overall and if the staff is knowledgeable". FSL3 noted by "evaluating the knowledge of the recruit on their ability not only to follow established procedures once trained but also identify new and upcoming technologies and finding ways to prepared for them before these technologies being deployed throughout the enterprise. We do this because we understand that security of our networks and data are a continuous process." FSL4 indicated "the productivity of employees measures our success and how much data is secured versus how much is compromised, and the satisfaction of our customers." FSL5 stated that "to be sure to put performance measures in place to determine how successful your response plan was to the cyber threat. Find out how long it would take your organization to quarantine or mitigate the breach through different scenario plays. If you are successful or not, continue to update the business security protocol.

Application of communication to conceptual framework. Communication in both SMT and the hierarchy of needs is important to this study as well as to the use of the combined conceptual framework in the future. According to Nagin (2016), the most significant error in communication is the failure to communicate risk to both would be criminals and those in defense and the policing of the same criminals. Based on participant FSL3's entire response series to the six interview questions there is a constant flow of communication to both higher and lower level employees. In response to question 5, how the success of strategies and recruitment processes are measured, FSL3

stated by evaluating the knowledge of the recruit on their ability not only to follow established procedures once trained but also identify new and upcoming technologies and finding ways to prepared for them before these technologies applies throughout the enterprise. We do this because we understand that security of our networks and data are a continuous process.

Demonstrating a communication process, that goes above them as a financial service leader, and directly to the cybersecurity professional. I find that there is not a lack of disclosure in this case from the free population, but a lack of recruiting strategy in the sole reliance on social media to attract and test would be cybersecurity professionals. The data resulting from this research demonstrates that customers' perceptions of customer-related corporate social responsibility (CSR) and ethical issues have a positive impact on both customer identification and stakeholder satisfaction with banking companies. Resonating with Pérez and Rodríguez del Bosque (2016) findings that perceptions of stakeholder-related CSR boost customer satisfaction, due to frequent agile communication.

Findings aligned with existed literature. Researchers indicated that the exploitation of the General Information and Communications Technology (ICT) supply chain is a growing security concern in the industry. According to McDaniel (2013), key elements of the global ICT supply chain security include the development of private businesses and the development of a strategy for education, training, communicate, and awareness about cybersecurity. The roles and responsibilities of security professionals within an organization entail dealing with sensitive information (Borum, Felker, Kern, Dennesen,

& Feyes, 2015). Denning and Gordon (2015) indicated that the US Department of Defense is actively recruiting cybersecurity professionals. In 2014, employers filled 900 of 6,000. The authors mentioned that 66% of the job openings by 2020 and should require post-secondary education and may rely more on communication and analysis skills than on manual skills.

Table 2.

A sample of participants' perspectives from identified themes (cont.)

Theme	Participant: Experience
Increased Training	FSL1: Finding the best combination of experience, education, skill level along with an inner enthusiasm and drive to succeed and grow in the industry. The prospective staff member should have career oriented goals and be driven to learn and succeed. FSL2: Our success is measure in the number of successfully hired candidates with the correct qualifications. FSL3: The biggest challenge we face is that of a process change that may add a requirement for the end user, (customer). In most cases, this change requires buy-in and acceptance from the local Union representatives and additional training to the customer.
Broadened Social Networking	FSL2: We use LinkedIn to find and recruit new talent through our social media campaign. Our company coordinates with the local University recruitment personnel to schedule job fairs when looking for talent. We also posted a job announcement on our web page. FSL5: We are familiar with social and professional networks LinkedIn, Twitter,

Table 2 continues	and Facebook. You want to find professional social networks that focus on cybersecurity.
Improved Communication	FSL1: Project managers meet with the customer to assess the plan and set milestones to meet these challenges. The manager then meets with his staff to plan and set goals and address issues as they arise. FSL2: My strategy was deployed through the use of technology and recruiters. FSL3: The region implements a Regional Change Control Board, (RCCB) that governs the deployment of a new cybersecurity hardware/ software. The product is then tested against a select subset of platforms throughout the region to identify any issues that may occur. If no issues occur, then an Action Item is then submitted for full rollout. FSL4: We use a research team to decide what changes in our staffing are needed based on cost effectiveness, then we communicate the change to staff involved, and implement the change through agile methodologies. FSL5: We found young new talent and helped them realize the potential to engage in challenging work, as well as growth and development.

Applications to Professional Practice

The purpose of this qualitative multiple case study was to explore what strategies financial service leaders need to recruit trained cybersecurity professionals. The populations for this study consisted of five FSLs Columbia, South Carolina. These FSLs responsible for the recruitment of cybersecurity professionals have worked for their

respective companies a minimum of 5 years and have recruited at least 5 cybersecurity professionals with *IT Specialist* in their job title. The population provided information on how to recruit and retain trained cybersecurity employees. The information furnished by the 5 FSLs contributed to social change through sharing strategies they use to recruit and retain cybersecurity professionals. There is an abundance of research which provided reasons for recruiting professionals, but limited research on strategies to specifically recruit and retain people in the IT field. Financial service leaders can use this research to create additional innovative ideas on how to retain and recruit IT professionals.

The themes which emerged during data collect are increased training, broadened social networking, and improved communication. The FSLs, in this case, expected cybersecurity professionals to possess already the skills they needed to work in an IT environment noted by FSL3 and FSL 5 (40%). The results of my study could contribute to business practices by encouraging leaders in the financial service industry to be transparent in training and hiring practices. The FSLs, who participated in this study, conveyed that having ready to work employees has lasting benefits for the cybersecurity industry and that on the job training could include organizational goals. Training may promote employee behaviors consistent with the values of the organization. Business leaders may find results of this study affect organizational and social change by encouraging business practices that influence their stakeholders to contribute to data security efforts.

Social networking to recruit employees was also a strategy utilized by FSL2 and FSL5 (40%). Prospective cybersecurity professionals could use this information to clean

up their online footprint to attract IT recruiters and promote their services. Communication is salient to all five (100%) of the participants interviewed. Open communication and a top-down approach to communicating change increases transparency and establishes trust amongst management and employees. The FSLs in this case, described to their supervisors and subordinates to assure the proper information is the same throughout the organization, and everyone understood the reasons for the change and fluctuation of security efforts.

The researcher will provide any company interested with a summary of the findings including suggestions for professional practice, and how my results can apply to their organization. The implication for positive social change will arise from a gained knowledge base of how to find and recruit IT professionals and those with IT related skills. The intended contribution to existing research was to provide knowledge to the banking industry on the importance of strategies to have the best encryption and security of all internal and external data to protect themselves, and their stakeholders.

Implications for Social Change

The primary objective of this study was to explore strategies FSLs use to retain and recruit cybersecurity professionals. The retention of professionals has been an increasing concern for the cybersecurity industry (Campbell, Saner, & Bunting, 2016). The implementation of the strategies identified by FSL1, FSL2, FSL3, and FSL4 (80%) such as using social media to look for and recruit IT professionals) should serve as a precedence for young social networkers to make their pages professional (Jethwani, Memon, Seo, & Richer, 2016). The use of recruiting strategies specifically for

cybersecurity professionals, in the banking industry can protect individuals and build trust in an economic climate where everyone is sensitive about fraud (Devi, 2016).

The results of my study may contribute to social change, and business practices as leaders reach greater company financial performance goals, through retention of cybersecurity professionals. Business executives can find areas of weakness in data security, create more jobs, and invest financial gains into the infrastructure of the local community. Through the creation of profit, a greater economic development is possible as more job applicants relocate to areas where there are growing economies and a secure job base. Business leaders might develop and sponsor college scholarships as the organizational need for cybersecurity professionals rising, and spur those institutions to train students on the data security to fit needs of the banking industry.

The more members of the community that attend college, the more society benefits (Lile, Ottusch, Jones, & Richards 2017). There is a likelihood that college graduates earn more, contribute more to the community, have better health coverage, and are likely to contribute back to the society from which they came. Institutions of higher learning enhance economic development through research programs and partnerships with business and governmental entities. Business leaders may find results of this study affect organizational and social change by encouraging business practices that influence young people to use their technology skills in ways that benefit themselves and society.

Recommendations for Action

My recommendation is that future researchers further the understanding of phenomena – this may be a strategy for business owners. The high number of data

breaches in the banking industry stifles organizational profitability and can damage the morale of the existing customers. Employers should interview IT specialists to ensure not only their job skills are proficient; however, but to understand the personality of the job applicant fits well with the organizational culture and the employee is willing to learn. Communicating clear and consistent hiring practices helped build trust with stakeholders, and restore confidence in the banking industry.

Business and government leaders should apply the findings of this study because cybersecurity breaches affect business profitability and sustainability. Managers should not overlook the importance communicating is in their work environment and the benefit social media can have on recruiting, retaining, and the production of cybersecurity professionals. Results can assist leaders with recruiting, training financial service organizational leaders, and building stakeholder relationships focusing on retention, motivation, and performance.

Recommendations for Further Research

Researchers could benefit from the social change concepts offered in this research study by applying the audit trail to repeat and expand the understanding of the phenomenon. The advantage to repeating a study is identifying to recruit and retain cybersecurity professionals to maintain data security. There are numerous industries in the field of business, and assessing the value of IT strategy may be different for all of them. Utilizing a qualitative case study method would be ideal because it is the method used in the current research.

Other study designs, such as phenomenological, ethnographic, and grounded theory, would be inductive and allow for ongoing data collection and analysis (Latham, 2013). The following recommendations for future study are for individuals interested in exploring topics comparable to my research that chose to use similar methodologies. Organizational leaders may use my research about retaining cybersecurity professionals, to attract and hire trained, cybersecurity IT specialist.

In other businesses, the strategies presented here may assist in securing financial data, and that change would be specific to each industry. My recommendation is that stakeholders may change their behavior based on what strategies they perceive as valuable. The findings resulting from this study inform a business problem focused on the concept of organizational benefit. Based on the responses provided by participants, not only did I discover possible answers to the research questions, but also these results assisted in identifying what professionals believe are the traits required to be competent in their field.

Reflections

With limited experience with Walden University and the dissertation writing process, Walden and writing a dissertation, I started this process with some preconceived ideas and values of how this study was going to be. As a banker, I wanted my dissertation to be something I would be passionate about and have the accessibility to conduct research. My research topic also led to concerns over how the citizens in South Carolina were affected by South Carolina Tax Commission (SCTC) hacking problems.

After that, cybersecurity became a topic of intense public discussion because these issues affect me personally.

With the understanding that SCTC did not have a designated cybersecurity professional before the cyberattack occurred and the agency reported the incident 14 days after the attack, I began to think that other governmental agencies and financial institutions may not have a cybersecurity security professional on staff as well. My thoughts were that financial institutions employ security officers, however not a person who handles only the IT risks and vulnerabilities created by possible cyberattacks.

Another preconceived idea was that I would be taking online courses and not have someone to help if I have problems with my doctoral study. Now I can honestly say; Walden University has given me all the tools I need to be fruitful and to complete this journey. I am thankful for my Chair, and the committee selected for me, that knew so much about my topic; as well as the reviewers and methodologists that assisted with the development of the study.

Driven by the competition among financial institutions to offer new products and services, organizations are rapidly adopting new technology. Collectively, innovation of new technology and the data that financial institutions generate along with the funds they maintain and convey every day make financial institutions attractive targets for cyberattacks. New vulnerabilities in both hardware and software apply daily; making it difficult to protect systems from cyberattacks may be a reason why financial institution has difficulty hiring cybersecurity professionals.

Conclusion

Leaders should use multiple strategies including being honest and transparent to hire cybersecurity professionals and establish trust with all stakeholders. By increasing managers' ability to communicate through social media, and events-young, trained IT professionals are more likely to be found. Individuals interested in IT and specifically cybersecurity should train in the field before looking for positions; the U.S. military is a great place to gain experience, connecting with Carolina Cluster Pathway Program (C^2P^2) at Claflin University, Benedict College, and Voorhees College, or a Science, Technology, Engineering, and Mathematics (STEM) Internship Program.

The findings and recommendations from my research provide a framework to address how to recruit and retain cybersecurity professionals in the banking industry. General deterrence theory and social support theory as they relate to management effectiveness can change stakeholders' perception of employees within an organization. Through ethically meeting the demand for cybersecurity professionals, financial service leaders may have, a strategy could then deploy in businesses to create sustainable management of security threats, communication with stakeholders, and increase transparency in business.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1), 5-14. Retrieved from http://timeview.ca

Adnan, M., Just, M., Baillie, L., & Kayacik, H. G. (2015). Investigating the work practices of network security professionals. *Information & Computer Security*, *23*, 347-367. doi:10.1108/ICS-07-2014-0049

Aisha, A., Hardjomidjojo, P., & Yassierli. (2013). Effects of working ability, working condition, motivation and incentive on employees' multi-dimensional performance. *International Journal of Innovation, Management and Technology, 4*, 605-609. doi:10.7763/IJIMT.2013.V4.470

Alam, M., Gale, A., Brown, M., & Khan, A. I. (2010). The importance of human skills in project management professional development. *International Journal of Managing Projects in Business, 3*, 495-516. doi:10.1108/17538371011056101.

Almutairi, A. F., Gardner, G. E., & McCarthy, A. (2014). Practical guidance for the use of pattern-matching technique in case-study research: A case presentation. *Nursing & Health Sciences, 16*, 239-244. doi:10.1111/nhs.12096

Alanezi, F., & Brooks, L. (2014). *Combatting online fraud in Saudi Arabia using general deterrence theory (GDT).* Paper presented at the Twentieth Americas Conference on Information Systems Savannah, GA. Abstract retrieved from http://aisel.ainet.org

Andriole, S. J. (2015). Who Owns It? *Communications of the ACM*, *58*(3), 50-57. doi:10.1145/2660765

Angel, J. J., & McCabe, D. (2015). The ethics of payments: Paper, plastic, or bitcoin. *Journal of Business Ethics*, *132*, 603-611. doi:10.1007/s10551-014-2354-x

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*(2), 24-33. doi:10.18870/hlrc.v5i2.214

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015, August). *2020 cyber crime economic costs: No measure no solution.* Paper presented at the Tenth International Conference on Availability, Reliability and Security (*ARES),* 701-710. doi:10.1109/ARES.2015.56

Arris, S. M., Fitzsimmons, D. A., & Mawson, S. (2015). Moving towards an enhanced community palliative support service (EnComPaSS): protocol for a mixed method study. *BMC Palliative Care*, *14*(1), 1-8. doi:10.1186/s12904-015-0012-4

Ata, A., & Rao, V.S. (2014). Detection and protection against intrusions on smart grid systems. *International Journal of Cyber-Security and Digital Forensics, 3*(1), 38-48.

Awad, G. (2014). Motivation, Persistence, and Crosscultural Awareness: A Study of College Students Learning Foreign Languages. *Academy of Educational Leadership Journal, 18*(4), 97-116.

Babbie, E. (2013). *The basics of social research*. Boston, MA: Cengage.

Badger, J, Kaminsky, S., & Behrend, T. (2014). Media richness and information

acquisition in internet recruitment. *Journal of Managerial Psychology, 29*(7), 866. doi:10.1108/JMP-05-2012-0155

Baldino, D., & Goold, J. (2014). Iran and the emergence of information and communications technology: the evolution of revolution? *Australian Journal of International Affairs*, *68*(1), 17-35. doi:10.1080/10357718.2013.840263

Bamrara, A. (2015). Evaluating database security and cyber attacks: A relational approach. *Journal of Internet Banking & Commerce*, *20*(2). doi:10.4172/1204-5357.1000115

Barclay, S. R., & Stoltz, K. B. (2016). The life-design group: A case study assessment. *The Career Development Quarterly, 64*(1), 83-96. doi:10.1002/cdq.12043

Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51-61. doi:10.1016/j.chb.2015.01.039

Bezbarua, R. K., & Rajkonwar, A. (2015). Cyber Crime–with special reference to banking industry of Assam. *Asian Journal of Research in Banking and Finance, 5*(8), 81-88. doi:10.5958/2249-7323.2015.00103.

Bish, A. J., Newton, C. J., Browning, V., O'Connor, P., & Anibaldi, R. (2014). An exploration of the professional competencies required in engineering asset management. *European Journal of Engineering Education*, *39*, 432-447. doi:10.1080/03043797.2014.895701

Bloomberg, L. D., & Volpe, M. (2012). *Completing your qualitative dissertation: A roadmap from beginning to end*. Thousand Oaks, CA: Sage.

Bojanc, R., & Jerman-Blazic, B. (2013). A quantitative model for information-security risk management. *Engineering Management Journal, 25*(2), 25-37.

Booyens, M. (2014). A Student's Experience of Gaining Access for Qualitative Research. *Notes from Practice/Uit Die Praktyk*, *1*, 146-151. doi:10.15270/50-1-17

Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information & Computer Security*, *23*, 317-332. doi:10.1108/ICS-09-2014-0064

Bouzar-Benlabiod, L., Bouabana-Tebibel, T., & Benferhat, S. (2015). Instantiated First Order Qualitative Choice Logic for an efficient handling of alerts correlation. *Intelligent Data Analysis*, *19*(1), 3-27. doi:10.3233/IDA-140693

Brehmer, A., Lilly, B., & Tippins, M. J. (2013). Improving salesperson recruitment: Examining practices of screening candidates for potential success versus potential failure. *The Journal of Applied Business and Economics, 15*(1), 29-38.

Brock, M. E., & Buckley, M. R. (2013). Human resource functioning in an information society: Practical suggestions and future implications. *Public Personnel Management, 42*, 272-280. doi:10.117/0091026013487047

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

Brooks, A. K., & Anumudu, C. (2016). Identity development in personal branding instruction social narratives personal branding instruction social narratives and

online brand management online brand management in a global economy. Global Economy. *Adult Learning*, *27*(1), 23-29. doi:10.1177/1045159515616968

Bryman, A., & Bell, E. (2015). *Business research methods*. New York, NY: Oxford University Press.

Bruyer, T., Jacobs, G., & Vandendaele, A. (2016). Good Pharma? How Business Communication Research Can Help Bridge the Gap Between Students and Practitioners. *Business and Professional Communication Quarterly*, *79*, 141-153. doi:10.1177/2329490615610776

Budría, S., & Moro-Egido, A. (2014). Overqualification, skill mismatches and wages in private sector employment in Europe. *Technological and Economic Development of Economy*, 20, 457-483. doi**:**10.3846/20294913.2014.883341

Burley, D. L. (2015). Cybersecurity education, part 2. *ACM Inroads*, *6*(2), 58-58. doi:10.1145/2746407

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM*, *57*(2), 24-27. doi.10.1145/2556936

Burns, J. (2014). Qualitative management accounting research in QRAM: Some reflections. *Qualitative Research in Accounting and Management, 11*(1), 71-81. doi:10.1108/QRAM-02-2014-0017

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*, *2013*(7), 5-10. doi:10.1016/S1361-3723(13)70062-9

Callan, V. J., Johnston, M. A., & Poulsen, A. L. (2015). How organisations are using

blended e-learning to deliver more flexible approaches to trade training. *Journal of Vocational Education & Training*, *67*, 294-309. doi:10.1080/13636820.2015.1050445

Campbell, S. G., O'Rourke, P., & Bunting, M. F. (2015). Identifying dimensions of cyber aptitude, the design of the cyber aptitude and talent assessment. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *59*, 721-725. doi:10.1177/1541931215591170

Campbell, S. G., Saner, L. D., & Bunting, M. F. (2016). Characterizing cybersecurity jobs: applying the cyber aptitude and talent assessment framework. In *Proceedings of the Symposium and Bootcamp on the Science of Security,1*(3), 25-27. doi:10.1145/2898375.2898394

Carlon, D. M., & Downs, A. (2014). Stakeholder valuing: A process for identifying the interrelationships between firm and stakeholder attributes. *Administrative Sciences, 4*, 137-154. doi:10.3390/admsci4020137

Carlton, M. & Levy, Y. (2015). Expert assessment of the top platform independent cybersecurity skills for non-IT professionals. *Proceedings of the IEEE SoutheastCon, Fort Lauderdale, Florida*, 1-6. doi:10.1109/SECON.2015.7132932

Challenges to Enrollment and Participation in Mindfulness-Based Stress Reduction Among Veterans: A Qualitative Study. *The Journal of Alternative and Complementary Medicine*, *21*, 409-421. doi:10.1089/acm.2014.0324.

Chaturvedi, M., Narain Singh, A., Prasad Gupta, M., & Bhattacharya, J. (2014). Analyses of issues of information security in Indian context. *Transforming Government:*

People, Process and Policy, 8(3), 374. doi:10.1108/TG-07-2013-0019

Cheng, L., Li, W., Zhai, Q., & Smyth, R. (2014). Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior*, *38*, 220-228. doi:10.1016/j.chb.2014.05.043

Clopton, Z. D. (2016). Territoriality, Technology, and National Security. *University of Chicago Law Review*, *83*(1), 45-63. Retrieved from https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=2635173

Comizio, V. G., Dayanim, B., & Bain, L. (2016). Cybersecurity as a global concern in need of global solutions: An overview of financial regulatory developments in 2015. Journal of Investment Compliance, 17, 101 – 111. doi:10.1108/JOIC-01-2016-0003

Conley, S., & Redeker, N. (2016). A systematic review of self-management intervention for inflammatory bowel disease. Journal of Nursing Scholarship. doi:10.1111/jnu.12189

Corruption, South African multinational enterprises, and institutions in Africa. *Journal of Business Ethics, 124*, 383-398. doi:10.1007/s10551-013-1878-9

Cowley, J. A., & Greitzer, F. L. (2015). Organizational impacts to cybersecurity expertise development and maintenance. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 59*, 1187-1191. SAGE Publications. doi:10.1177/1541931215591185

Crane, A., Graham, C., & Himick, D. (2015). Financializing stakeholder claims. *Journal*

of Management Studies, *52*, 878-906. doi:10.1111/joms.12147

Critchley, T. (2015). Why DTMF masking is critical to payment security. *Computer Fraud & Security*, *11*, 8-10. doi:10.1016/S1361-3723(15)30101-9

Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing, 9*, 119-128. doi:10.1093/police/pau044

Da Silva, G. F., Morano, M. T., A., Sales, M. P., U., Olegário, N.,B., . . . B. (2014). Comparison of face-to-face interview and telephone interview administration of COPD assessment test: A randomized study. *Quality of Life Research, 23*, 1193-1197. doi:10.1007/s11136-013-0563-x

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

Dağhan, G., & Akkoyunlu, B. (2014). A qualitative study about performance based assessment methods used in information technologies lesson. *Educational Sciences: Theory & Practice*, *14*, 333-338. doi:10.12738/estp.2014.1.2005

Daneshgari, P., & Moore, H. (2016). Organizational transformation through improved employee engagement– "How to use effective methodologies to improve business productivity and expand market share". *Strategic HR Review*, *15*(2), 57-64. doi:10.1108/SHR-02-2016-0007

Davis, K. (2016). A method to measure success dimensions relating to individual stakeholder groups. *International Journal of Project Management*, *34*, 480-493. doi:10.1016/j.ijproman.2015.12.009

Davidson, B., Sherman, S., Barraza, L., & Marinissen, M. J. (2015). Legal challenges to the international deployment of government public health and medical personnel during public health emergencies: impact on national and global health security. *Journal of Law, Medicine & Ethics, 43,* 103-106. doi:10.1111/jlme.12229

Denning, P. J., & Gordon, E. E. (2015). A technician shortage. *Communications of the ACM*, *58*(3), 28-30. doi:10.1145/2723673

D'Souza, J., & Gurin, M. (2016). The universal significance of Maslow's concept of self-actualization. *The Humanistic Psychologist*, *44*(2), 210. doi:10.1037/hum0000027

Dev, D. S., & Kisku, D. R. (2016). HPV guided object tracking: Theoretical advances on fast pattern matching technique. *Perspectives in Science*. doi:10.1016/j.pisc.2016.06.005

Devi, S. (2016). Emergence of Cyber Security and transformations in the World Order. *International Journal of Innovative Knowledge Concepts*, *2*(3) 53-72.

Devito, L., Brown, A., Bannister, B., Cianci, M., & Mujtaba, B. (2016). Employee motivation based on the hierarchy of needs, expectancy and the two-factor theories applied with higher education employees. *International Journal of Advances in Management, Economics and Entrepreneurship*, *3*(1), 20. Retrieved from http://nsuworks.nova.edu/hcbe_facarticles/267/

Eassey, J. M., & Boman, J. H. (2016). Deterrence Theory. *The Encyclopedia of Crime & Punishment*. doi:10.1002/9781118519639.wbecpx115

Eckhardt, G. M., & Bardhi, F. (2016). The relationship between access practices Access Practices and economic systems. Economic Systems. *Journal of the Association*

for Consumer Research, *1*,(2), 210-225. doi:10.1086/684684

Edwards, B. (2015). Escaping the false dilemma of strategic nuclear and biological deterrence. *Contemporary Security Policy*, *36*, 371-373. doi:10.1080/13523260.2015.1061751

Erturk, A. & Vurgan, L. (2015). Retention of IT professionals: examining the influence of empowerment, social exchange, and trust, *Journal of Business Research* 68(1): 34–46. doi:10.1016/j.jbusres.2014.05.010

Eskerod, P., & Huemann, M. (2013). Sustainable development and project stakeholder management: What standards say. *International Journal of Managing Projects in Business*, *6*(1), 36-50. doi:10.1108/17538371311291017.

Fassinger, R., & Morrow, S. (2013). Toward best practices in quantitative, qualitative, and mixed-method research: A social justice perspective. *Journal for Social Action in Counseling and Psychology*, *5*(2), 69-83.

Flynn, S. V., Duncan, K. J., & Evenson, L. L. (2013). An emergent phenomenon of American Indian secondary students' career development process. *The Career Development Quarterly*, *61*, 124-140. doi:10.1002/j.2161-0045.2013.00042.x

Fonash, P., & Schneck, P. (2015). Cybersecurity: From months to milliseconds. *Computer*, (1), 42-50. doi:10.1109/MC.2015.11

Fourie L., Sarrafzadeh, A., Pang, S., Kingston, T., Hettema, H. & Watters, P. (2014). The global cybersecurity workforce: An ongoing human capital crisis. *Global Business and Technology Association*. Retrieved from http://hdl.handle.net/10652/2457

Freeman, R. B. (1999). The economics of crime. *Handbook of labor economics*, *3*, 3529-3571. doi:10.1016/S1573-4463(99)30043-2

Gaikwad, S. B., Yadav, A. A., & Patil, P. H. (2015). The study of e-security in internet banking. *International Journal of Advanced Research in Computer and Communication Engineering, 4*(8), 1-4. doi:10.17148/IJARCCE.2015.4840

Garcia, D. (2014). Not yet a democracy: establishing civilian authority over the security sector in Brazil – lessons for other countries in transition. *Third World Quarterly*, *35*, 487-504. doi:10.1080/01436597.2014.893489

Garg, V., & Camp, L. J. (2015). Why cyber crime? *ACM SIGCAS Computers and Society*, *45*(2), 20-28. doi.10.1145/2809957.2809962

Garg, S. K., Lyles, C. R., Ackerman, S., Handley, M. A., Schillinger, D., Gourley, G., & ... Sarkar, U. (2016). Qualitative analysis of programmatic initiatives to text patients with mobile devices in resource-limited health systems. *BMC Medical Informatics & Decision Making*, *16*(1), 12. doi:10.1186/s12911-016-0258-7

Garriga, E. (2014). Beyond stakeholder utility function: Stakeholder capability in the value creation process. *Journal of Business Ethics, 120*, 489-507. doi:10.1007/s10551-013-2001-y

Goh, J., & Thing, V. L. (2015). A hybrid evolutionary algorithm for feature and ensemble selection in image tampering detection. *International Journal of Electronic Security and Digital Forensics*, *7*(1), 76-104. doi::10.1504/IJESDF.2015.067996

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: a real options perspective.

Journal of Accounting and Public Policy, *34*, 509-519. doi: 10.1016/j.jaccpubpol.2015.05.001

Gómez-Cedeño, M., Castán-Farrero, J. M., Guitart-Tarrés, L., & Matute-Vallejo, J. (2015). Impact of human resources on supply chain management and performance. *Industrial Management & Data Systems, 115*, 129. doi:10.1108/IMDS-09-2014-0246

Gonzales, A. R. (2015). Advising the President: The growing scope of executive power to protect America. *Harvard Journal of Law & Public Policy*, *38*, 453-507.

Grau, D., & Kennedy, C. (2014). TIM lecture series - the business of cybersecurity. *Technology Innovation Management Review, 4*(4), 53-57.

Guzansky, Y., & Golov, A. (2015). The rational limitations of a nonconventional deterrence regime: The Iranian case. *Comparative Strategy*, *34*, 169-184. doi:10.1080/01495933.2015.1017349

Hansen, E. G., & Schaltegger, S. (2016). The sustainability balanced scorecard: A systematic review of architectures. *Journal of Business Ethics, 133*, 193-221. doi:10.1007/s10551-014-2340-3

Harrigan, W. J., & Commons, M. L. (2015). Replacing Maslow's needs hierarchy with an account based on stage and value. *Behavioral Development Bulletin*, *20*(1), 24. doi:10.1037/h0101036

Hartas, D. (2015). *Educational research and inquiry: Qualitative and quantitative approaches*. (2nd ed.) New York, NY: Bloomsbury Publishing. New York, NY.

Hayashi Jr., P. (2016). Tattvabodha and the hierarchical necessity of Abraham Maslow.

Journal of Management, Spirituality & Religion, *13*(2), 82-93. doi:10.1080/14766086.2015.1076735

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

Henry, M., Rivera, J., & Faithful, G. E. (2015). The four principles of phenomenology. *Continental Philosophy Review, 48*(1), 1-21. doi:10.1007/s11007-014-9313-1

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. *Journal of Interactive Marketing*, *30*, 1-19. doi:10.1016/j.intmar.2014.10.001

Hollingsworth, T., Adams, E., Anderson, R., Atkins, K., Bartsch, S., Basáñez, M., & ... Irvine, M. A. (2015). Quantitative analyses and modelling to support achievement of the 2020 goals for nine neglected tropical diseases. *Parasites & Vectors*, 81-28. doi:10.1186/s13071-015-1235-1

Humphrey, C. (2014). Qualitative research - mixed emotions. *Qualitative Research in Accounting and Management, 11*(1), 51-70. doi:10.1108/QRAM-03-2014-0024

Hurlburt, G. (2015). Cyberhuman Security. *Computer*, (5), 88-91. doi:10.1109/MC.2015.127

Issitt, C. (2014). The peer review interview aspect of the IPD process. *The Safety & Health Practitioner, 32*(1), 24.

Jacobsson, M., & Wilson, T. L. (2014). Partnering hierarchy of needs. *Management Decision*, *52*, 1907-1927. doi:10.1108/MD-02-2014-0075

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80*, 973–993. doi:10.1016/j.jcss.2014.02.005

Jasper, S. (2015). Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly*, *9*(1), 60-85. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA617847

Jeffery, A. D., Christen, M., & Moore, L. (2015). Beyond a piece of paper: Learning to hire with synergy. *Nursing Management*, *46*(1), 52-54. doi:10.1097/01.NUMA.0000452008.64591.fb

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2016). "I can actually be a super sleuth." Promising practices for engaging adolescent girls in cybersecurity Education. *Journal of Educational Computing Research 9*, 130-139. doi:10.1177/0735633116651971

Johnson, B. (2014). Ethical issues in shadowing research. *Qualitative Research in Organizations and Management, 9*(1), 21-40. doi:10.1108/QROM-09-2012-1099

Jollands, S., Akroyd, C., & Sawabe, N. (2015). Core values as a management control in the construction of "sustainable development". *Qualitative Research in Accounting and Management, 12*, 127-152. doi:10.1108/QRAM-04-2015-0040

Joshi, K. (2015). Continuity planning: the importance of including digital property. *Strategic Direction*, *31*(3), 33-36. doi:10.1108/SD-01-2015-0017

Jovanovikj, V., Gabrijelčič, D., & Klobučar, T. (2014). A conceptual model of security

context. *International Journal of Information Security*, *13*, 571-581. doi:10.1007/s10207-014-0229-x

Kafol, C. (2014). Multi-Layer Project Cycle Management Model for Complex Projects. *DAAAM International Scientific Book*, 279-294. doi:10.2507/daaam.scibook.2014.23

Kamal, O., Brown, D., Sivabalan, P., & Sundin, H. (2015). Accounting information and shifting stakeholder salience: An industry level approach. *Qualitative Research in Accounting and Management, 12*, 172-200. doi:10.1108/QRAM-04-2014-0028

Kim, Y., & Park, W. H. (2014). A study on cyber threat prediction based on intrusion detection event for APT attack detection. *Multimedia Tools and Applications, 71*, 685-698. doi:10.1007/s11042-012-1275-x

Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cybersecurity management in industrial control systems. *International Journal of Critical Infrastructure Protection*, 9, 52-80. doi:10.1016/j.ijcip.2015.02.002

Kont, K., & Jantson, S. (2014). Organizational Commitment in Estonian University Libraries: A Review and Survey. *New Review of Academic Librarianship, 20*, 296-319. doi:10.1080/13614533.2014.898671

Koopman, O. (2015). Phenomenology as a potential methodology for subjective knowing in science education research. *Indo - Pacific Journal of Phenomenology, 15*(1), 1-10.

Korsakienė, R., Stankevičienė, A., Šimelytė, A., & Talačkienė, M. (2015). Factors driving turnover and retention of omology professionals. *Journal of Business*

Economics and Management, *16*(1), 1-17. doi:10.3846/16111699.2015.984492

Kreissl, R. (2014). Assessing Security Technology's Impact: Old Tools for New Problems. *Science & Engineering Ethics*, *20*, 659-673. doi:10.1007/s11948-014-9529-9

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

Latham, J. R. (2013). A framework for leading the transformation to performance excellence part I: CEO perspectives on forces, facilitators, and strategic leadership systems. *The Quality Management Journal, 20*(2), 12-33. doi:10.1348130549

Lancaster, K. (2016). Confidentiality, anonymity and power relations in elite interviewing: conducting qualitative policy research in a politicised domain. *International Journal of Social Research Methodology, 1*, 1-11. doi:10.1080/13645579.2015.1123555

Leedy, P. D., & Ormrod, J. E. (2013). *Practical research: Planning design* (10th ed.). Upper Saddle River, NJ: Pearson Education.

Lemke, A. A., & Harris-Wai, J. N. (2015). Stakeholder engagement in policy development: Challenges and opportunities for human genomics. *Genetics in Medicine*, *17*, 949-957. doi:10.1038/gim.2015.8

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice*, *2*(4), 23-41. doi:10.1177/1524839915580941

Liedtka, J. (2015). Perspective: linking design thinking with innovation outcomes through cognitive bias reduction. *Journal of Product Innovation Management*, *32*(6), 925-938. doi:10.1111/jpim.12163

Lile, J. R., Ottusch, T. M., Jones, T., & Richards, L. N. (2017). Understanding College-Student Roles: Perspectives of Participants in a High School/Community College Dual-Enrollment Program. *Community College Journal of Research and Practice*, 1-17.

Lu, H., & Liou, H. (2015). Impacts of business companies' recruitment advertisements, publicity, sponsorship, and word-of-mouth on graduating students' job pursuit intentions. *Journal of Accounting, Finance & Management Strategy, 10*(1), 115-145.

Majewski, S. (2014). The Maslowian portfolio theory versus the pyramid portfolio. *Folia Oeconomica Stetinensia, 14*(1), 91-101. doi:10.2478/foli-2014-0107

Malhotra, Y. (2014). A risk management framework for penetration testing of global banking & finance networks voIP protocols. doi:10.2139/ssrn.2555098

Malhotra, Y. (2015). Bridging Networks, systems and controls frameworks for cybersecurity curricula & standards development. In *2015 NY Cyber Security & Engineering Technology Association Conference, 1*(22), 25-38. doi:10.2139/ssrn.2792636

Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *ACM Inroads*, *5*(1), 47-52. doi:10.1145/2568195.2568212

Marais, H. (2012). A multi-methodological framework for the design and evaluation of

complex research projects and reports in business and management studies. *Electronic Journal of Business Research Methods*, *10*(2), 64–76. Retrieved from www.jbrm.com

Mármol, F. G., Pérez, M. G., & Pérez, G. M. (2016). I Don't Trust ICT: Research Challenges in Cyber Security. *IFIP International Conference on Trust Management, 473*, 129-136. doi:10.1007/978-3-319-41354-9_9

Marshall, C., & Rossman, G. B. (2014). *Designing qualitative research* (6th ed.). Thousand Oaks, CA: Sage Publications, Inc.

Maslow, A. "Hierarchy of needs: A theory of human motivation [Kindle]." *Psychological Review, 50*, 370- 396. Retrieved from www.amazon.com

Maule-ffinch, B. Martinez, M. E., Kearney, D. J., Simpson, T., Felleman, B. I., Bernardi, N., & Sayre, GKey trends in information security. *Network Security*, *2015*(11), 18-20. doi:10.1016/S1353-4858(15)30102-1

May, P. J., Koski, C., & Stramp, N. (2016). Issue expertise in policymaking. *Journal of Public Policy*, *36*, 195-218. doi:10.1017/S0143814X14000233

Mbowe, J. E., Zlotnikova, I., Msanjila, S. S., & Oreku, G. S. (2014). A conceptual framework for threat assessment based on organization's information security policy. *Journal of Information Security, 5*, 166-177. doi:10.4236/jis.2014.54016

McCrae, N., Blackstock, M., & Purssell, E. (2015). Eligibility criteria in systematic reviews: A methodological review. *International journal of nursing studies*, *52*, 1269-1276. doi:10.1016/j.ijnurstu.2015.02.002

McDaniel, E. A. (2013). Securing the Information and Communications Technology

Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness. *Issues in Informing Science & Information Technology, 10*, 313-324.

Miller, A., Moon, B., Anders, S., Walden, R., Brown, S., & Montella, D. (2015). Integrating computerized clinical decision support systems into clinical work: a meta-synthesis of qualitative research. *International journal of medical informatics*, *84*, 1009-1018. doi:10.1016/j.ijmedinf.2015.09.005

Mikkonen, K., Kyngäs, H., & Kääriäinen, M. (2015). Nursing students' experiences of the empathy of their teachers: a qualitative study. *Advances in Health Sciences Education*, *20*, 669-682. doi:10.1016/j.ijnurstu.2015.06.004

Modlin, S. (2014). Collecting and Disbursing: Increasing cash management efficiency through the utilization of bank services. *Public Finance and Management, 14*(3), 357-370. Retrieved from http://search.proquest.com/openview/86990515fb9d07ba3e222e47900af775/1?pq-origsite=gscholar

Mok, K. Y., Shen, G. Q., & Yang, J. (2015). Stakeholder management studies in mega construction projects: A review and future directions. *International Journal of Project Management*, *33*, 446-457. doi:10.1016/j.ijproman.2014.08.007

Morse, J. (2014). Sampling in Qualitative Research. *The SAGE Encyclopedia of Social Science Research Methods, 1,* 20. doi:10.4135/9781412950589

Mukhtar M., & Finance, M. B. A. (2015). Perceptions of UK based customers toward internet banking in the United Kingdom. *Journal of Internet Banking and*

Commerce, *20*(1). Retrieved from *http://www.arraydev.com/commerce/jibc/*

Mukundan, N. R., & Prakash Sai, L. (2014). Perceived information security of internal users in indian IT services industry. *Information Technology and Management, 15*(1), 1-8. doi:10.1007/s10799-013-0156-y

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

Nagin, D. S. (2013). Deterrence in the twenty-first century. *Crime and Justice*, *42*, 199-263. doi:10.1086/670398

Nagin, D. S. (2016). What We've Got Here Is Failure to Communicate. *Criminology & Public Policy, 15*(3), 1-13. doi:10.1111/1745-9133.12227

Napier, N. P., Keil, M., & Tan, F. B. (2009). IT project managers' construction of successful project management practice: a repertory grid investigation. [Article]. *Information Systems Journal, 19*, 255-282. doi:10.1111/j.1365-2575.2007.00264.x.

Noble, H., & Smith, J. (2015). Issues of validity and reliability in qualitative research. *Evidence Based Nursing*, *18*(2), 34-35. doi:10.1136/eb-2015-102054

Oken, E., Switkowski, K., Price, S., Guthrie, L., Taveras, E. M., Gillman, M., . Dietz, P. (2013). A qualitative study of gestational weight gain counseling and tracking. *Maternal and Child Health Journal, 17*, 1508-17. doi:10.1007/s10995-012-1158-9

Orojloo, H., & Azgomi, M. A. (2014, September). *A method for modeling and evaluation*

of the security of cyber-physical systems. Paper presented at Eleventh International ISC Conference on Information Security and Cryptology, Tehran. doi:10.1109/ISCISC.2014.6994036

Parker, L. (2014). Qualitative Perspectives: Through a methodological lens. *Qualitative Research in Accounting and Management, 11*(1), 13-28. doi:10.1108/QRAM-02-2014-0013

Pérez, A., & Rodríguez del Bosque, I. (2016). The stakeholder management theory of CSR-a multidimensional approach in understanding customer identification and satisfaction. *International Journal of Bank Marketing*, *34*(5). doi:10.1108/IJBM-04-2015-0052

Phillips, J. J., & Phillips, P. (2016). How HR can have an impact in non-traditional areas. *Strategic HR Review*, *15*(1), 5–13. doi:10.1108/SHR-11-2015-0092

Potter, L. E., & Vickers, G. (2015). What skills do you need to work in cybersecurity: A look at the Australian market. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, USA,* 67-72. doi:10.1145/2751957.2751967

Qayyum, Z. U. (2015). Image retrieval through qualitative representations over semantic features. *Multimedia Tools and Applications, 74*, 1935-1959. doi:10.1007/s11042-013-1731-2

Rahman, H., & Nurullah, S. M. (2014). Motivational need hierarchy of employees in public and private commercial banks. *Central European Business Review*, *3*(2), 44-53.

Requirements Capture and Comparative Analysis of Cloud Security Techniques.

International Journal of Grid and Distributed Computing, *8*, 285-308. doi.10.14257/ijgdc.2015.8.2.25

Rivera-Ruiz, I., & Ferrer-Moreno, E. (2015). The relationship between strategic leadership, human IT infrastructure, project management, project success, and firm performance. *International Journal of Information, Business, and Management, 7*(2), 77-84.

Rowlands, T., Waddell, N., & McKenna, B. (2015). Are we there yet? A technique to determine theoretical saturation. *The Journal of Computer Information Systems, 56*(1), 40-47.

Ruehl, C. H., & Ingenhoff, D. (2016). Community management on social networking sites: Why and how stakeholders use corporate Facebook pages. *2016 49th Hawaii International Conference on System Sciences, 5*, 2216-2226.doi:10.1109/HICSS.2016.278

Ruth, T., Matusitz, J., & Wan, T. T. (2015). Understanding predatory organised crime network governance theory. *Social Change*, *45*, 587-604. doi:10.1177/0049085715602790

Ruvimbo Terera, S., & Ngirande, H. (2014). The impact of training on employee job satisfaction and retention among administrative staff members: A case of a selected tertiary institution. *Sosyal Bilimler Dergisi/Journal of Social Sciences*, 39(1), 43-50. Retrieved from http://journal.nku.edu.tr/index.php/BJSS Russell,

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security, 56*, 70-82.

doi:10.1016/j.cose.2015.10.006

Saldaña, J. (2015). *The coding manual for qualitative researchers*. New York, NY: Sage.

Sanromá, E., Ramos, R., & Simón, H. (2015). Portability of human capital and immigrant overeducation in Spain. *Population Research and Policy Review, 34*, 223-241. doi:10.1007/s11113-014-9340-y

Saleem I., Ahmed R. & Saleem N. (2016). Mediating role of work exhaustion: The missing linchpin to address Employee's Turnover. *Journal of Behavioural Sciences,* 26, 156-173

Saridakis, G., Benson, V., Ezingeard, J. N., & Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change*, *102*, 320-330. doi:10.1016/j.techfore.2015.08.012

Sarma, S. K. (2015). Qualitative research: Examining the misconceptions. *South Asian Journal of Management, 22*, 176-191. doi:10.1732041530

Shields, K. (2015). Cybersecurity: Recognizing the risk and protecting against attacks. *NC Banking Inst.*, *19*, 345. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/ncbj19&div=17&id=&page=

Sherry, E. (2013). The vulnerable researcher: Facing the challenges of sensitive research. *Qualitative Research Journal, 13*, 278-288. doi:10.1108/QR J-10-2012-0007

Shi, W. (2014). A provable secure sealed-bid multi-attribute auction scheme under semi-honest model. *International Journal of Communication Systems*, *27*, 3738-3747.

doi:10.1002/dac.2571

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199-207. doi:10.1016/j.chb.2015.01.046

Schuck, A. M. (2016). Evaluating the Impact of Crime and Discipline on Student Success in Postsecondary Education. *Research in Higher Education*, 1-21. doi:10.1007/s11162-016-9419-x

Simshaw, D. T. (2015). Legal Ethics and Data Security: Our individual and collective obligation to protect Client data. *American Journal of Trial Advocacy*, *38*, 549-574.

Singh, V., & Holmström, J. (2015). Needs and technology adoption: Observation from BIM experience. *Engineering, Construction and Architectural Management, 22*(2), 128. doi:10.1108/ECAM-09-2014-0124

Singh, A., & Teng, J. T. (2016). Enhancing supply chain outcomes through Information Technology and Trust. *Computers in Human Behavior*, *54*, 290-300. doi:10.1016/j.chb.2015.07.051

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

Song, Y., Son, Y. J., & Oh, D. (2015). Methodological issues in questionnaire design. Journal of Korean Academy of Nursing, 45(3), 323-328.

doi:10.4040/jkan.2015.45.310.4040/jkan.2015.45.3.323 .323

Stivala, A. D., Koskinen, J. H., Rolls, D. A., Wang, P., & Robins, G. L. (2016). Snowball sampling for estimating exponential random graph models for large networks. *Social Networks*. doi:10.1016/j.socnet.2015.11.003

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology*, *30*(1), 73-88. doi:10.1007/s10869-013-9333-6

Smith-Merry, J., & Walton, M. (2014). Research governance as a facilitator for ethical and timely research? Learning from the experience of a large government-funded multisite research project. *Australian Health Review, 38*, 295-300. doi:10.1071/AH13173

Storey, V. C., Straub, D. W., Stewart, K. A., & Welke, R. J. (2000). A conceptual investigation of the e-commerce industry. *Communications of the ACM, 43*, 117-123. doi:10.1145/341852.341871

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

Streagle, K., & Scott, K. W. (2015). The alternate assessment based on alternate achievement standards eligibility decision-making process. *The Qualitative Report, 20*, 1290-1312.

Tam, N., Huy, N., Thoa, L., Long, N., Trang, N., Hirayama, K., & Karbwang, J. (2015).

Participants' understanding of informed consent in clinical trials over three decades: Systematic review and meta-analysis. *World Health Organization. Bulletin of the World Health Organization, 93*, 186-198H. doi:10.2471/BLT.14.141390

Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, *43*, 19-34. doi:10.1016/j.cose.2014.02.010

Thomas, S., Suresh, K., & Suresh, G. (2013). Design and data analysis case-controlled study in clinical research. *Annals of Indian Academy of Neurology, 16*, 483-487. doi:10.4103/0972-2327.120429

Tiwana, A., Konsynski, B., & Venkatraman, N. (2014). Information technology and organizational governance: The IT governance cube. *Journal of Management Information Systems (Special Issue) 30,* 3 (Winter 2014), 7–12.

Thomas, E., & Magilvy, J. K. (2011). Qualitative rigor or research validity in qualitative research. *Journal for Specialists in Pediatric Nursing*, *16*, 151–155. doi:10.1111/j.1744-6155.2011.00283.x

Tobey, D. H. (2015). A vignette-based method for improving cybersecurity talent management through cyber defense competition design. In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research,6*(27), 31-39. ACM. New York, NY. doi:10.1145/2751957.2751963

Tong, V., Raynor, D. K., & Aslani, P. (2014). Design and comprehensibility of over-the-

counter product labels and leaflets: A narrative review. *International Journal of Clinical Pharmacy, 36*, 865-872. doi:10.1007/s11096-014-9975-0

Vander Elst, T., Richter, A., Sverke, M., Näswall, K., De Cuyper, N., & De Witte, H. (2014). Threat of losing valued job features: The role of perceived control in mediating the effect of qualitative job insecurity on job strain and psychological withdrawal. *Work & Stress*, *28*, 143-164. doi:10.1080/02678373.2014.899651

Vink, W. D., Lawrence, K., McFadden, A. M. J., & Bingham, P. (2016). An assessment of the herd-level impact of the Theileria orientalis (Ikeda) epidemic of cattle in New Zealand, 2012–2013: a mixed methods approach. New Zealand veterinary journal, 64(1), 48-54. doi:10.1080/00480169.2015.1090893

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity. *computers & security*, *38*, 97-102. doi:10.1016/j.cose.2013.04.004

Wahl, M. & Prause, G. (2013). Toward understanding resources, competences, and capabilities: business model generation approach. *Entrepreneurship and Sustainability*.1(2): 67−80. doi:10.9770/jesi.2013.1.2(1)

Walker, R. (2014). Sampling in Qualitative Research. *The SAGE Encyclopedia of Social Science Research Methods, 1,* 102-103. doi:10.4135/9781412950589

Wang, X., Wang, L., Zhang, L., Xu, X., Zhang, W., & Xu, Y. (2015). Developing an employee turnover risk evaluation model using case-based reasoning. *Information Systems Frontiers*, 1-8. doi:10.1007/S10796-015-9615-9

Webb, S. H., & Roberts, S. J. (2016). Communication and social media approaches in small businesses. *Journal of Marketing Development and Competitiveness, 10*(1),

66.

Wilson, R., Whitmoyer, G., Pieper, M., Astrachan, H., Hair, F., & Sarstedt, M. (2014). Method trends and method needs: Examining methods needed for accelerating the field. *Journal of Family Business Strategy*, *5*, 4-14. doi:10.1016/j.jfbs.2014.01.011

Wilson, T., Maimon, D., Sobesto, B., & Cukier, M. (2015). The effect of a surveillance banner in an attacked computer system additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency*, *52*, 829-855. doi:10.1177/0022427815587761

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

Yoo, J., & Chang, H. (2014). Public IT service strategy for social information security in the intelligence all-things environment. *Electronic Commerce Research*, *14*, 293-319. doi:10.1007/s10660-014-9155-2

Zagare, F. C. (2013). Deterrence theory, then and now: There is no going back. *St Antony's International Review*, *9*, 157-167. doi:10.1093/obo/9780199743292

Zhu, M., Xia, J., Yan, M., Cai, G., Yan, J., & Ning, G. (2015). Dimensionality Reduction in Complex Medical Data: Improved Self-Adaptive Niche Genetic Algorithm. *Computational & Mathematical Methods in Medicine*, 1-12. doi:10.1155/2015/794586

Appendix A: Interview Questions

1. What strategies do you use to recruit cybersecurity professionals?
2. How were the recruiting strategies to recruit cybersecurity professional deployed and implemented?
3. What challenges, if any, did you experience while using recruiting strategies to recruit cybersecurity professionals? How did you address any barriers to implementing the recruitment strategies?
4. How do you measure the success of your strategies and recruitment processes?
5. What additional information can you provide to help me understand the strategies and processes you've used for employing and maintaining the service of cybersecurity professionals?

Appendix B: Interview Protocol

Interview Time:
Place:
Location:
Interviewee Number:
Interview Introduction

Before we begin, I want to thank you again; your participation is highly appreciated. My name is Ivadella Walters. I am a doctoral student enrolled in the D.B.A. program of Walden University. The purpose of the meeting is to identify strategies used to recruit cybersecurity professionals in the financial service industry. The interview will last 45 minutes. Is this still a convenient time to talk? (If no, please let us reschedule for_____.) If, yes I continue.

First, please note that a) this interview is audio recorded for use as data for coding and analysis, b) the treatment of your answers is confidential and your identity confidential, c) the study will not report on individual participations, and you may withdraw at any time.

I appreciate you taking time from your busy schedule to help me with my research. The interview design helps me to gain insight from FSLs to gain strategies to recruit cybersecurity. Please note there are no right or wrong answers. If you believe you are not in a position to answer any question (or set of questions) for any reason, simply inform me. After a few questions acknowledging your background and experiences, I asked you a set of open-ended questions. Please feel free to elaborate or illustrate any way you feel fit when answering the open-ended questions. When I ask follow up questions, I am seeking to present clearly, what I ask in the question since some of the questions could be interpreted differently. Please ask me to restate any question that may need clarification.

I want to remind you that your participation is voluntary and you may choose not to answer any questions during the interview. I be taking notes as you respond. I would also reiterate this interview is being digitally recorded in order not to miss any of your answers. Would that be Okay? (If no, I not record the interview. If yes, I will start the recording now.)

General Notes & Comments