2020

Exploring Cybersecurity Awareness and Training Strategies To Protect Information Systems and Data

Michael Hanna
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Michael Hanna

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. Bob Duhainy, Committee Chairperson, Information Technology Faculty
Dr. Constance Blanson, Committee Member, Information Technology Faculty
Dr. Gary Griffith, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

Exploring Cybersecurity Awareness and Training Strategies To Protect Information Systems and Data

by

Michael Mohsen Hanna

MS, Walden University, 2019

MS, University of Calgary, 2011

BS, University of Calgary, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2020

Abstract

Ineffective security education, training, and awareness (SETA) programs contribute to compromises of organizational information systems and data. Inappropriate actions from users due to ineffective SETA programs may result in legal consequences, fines, reputational damage, adverse impacts on national security, and criminal acts. Grounded in social cognitive theory, the purpose of this qualitative multiple case study was to explore strategies hospitality organizational information technology (IT) leaders utilized to implement SETA successfully. The participants were organizational IT leaders from four organizations in Hampton Roads, Virginia. Data collection was performed using telephone and video teleconference interviews with organizational IT leaders (*n* = 6) as well as secondary data analysis of documents related to SETA programs (*n* = 31). Thematic analysis was used to analyze and code the data, which resulted in three themes. Consistent, persistent, and relevant awareness and training was the first theme to emerge. Awareness and training based on threats, vulnerabilities, and risks was the second theme to emerge. Disclosing expectations and taking appropriate actions towards employees based on behavior was the third theme to emerge. A recommendation is that SETA should be performed regularly throughout the year while using employee rewards and punishments to promote desired behavior. The findings of this study may promote positive social change by providing information to IT leaders to develop SETA programs and reduce security risks within organizations across various industries. Improved SETA may contribute to improved cyber practices at home and better protect family members.

Exploring Cybersecurity Awareness and Training Strategies To Protect Information Systems and Data

by

Michael Mohsen Hanna

MS, Walden University, 2019

MS, University of Calgary, 2011

BS, University of Calgary, 2005

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

June 2020

Dedication

I dedicate this study to my father, Moe, my mother, Nana, and my son, Matthew. First, to my father, who passed away two years before completing this study. He was a PhD in Chemical Engineering and always emphasized the importance of education. He always had an analogy for everything, and many of them related to education. When I completed my bachelor's degree, he once joked with me and said he would be impressed when I finished a doctorate degree. I know he was always proud of me, but this accomplishment means so much to me. He taught me the meaning of preserving through the greatest of challenges and the importance of education. I will never forget you, and I will always love you dad.

To my mother, she always taught me the importance of realizing there is more to life than just work and school. She was the other half to my development, and I would not be the man I am today without her.

Last, I would like to dedicate this to my one-year-old son. Even though my son cannot read yet, I want him to understand the importance of pushing through the challenges life presents us with. Matthew, I promise you that I will always be there for you.

Acknowledgements

I could not have made it to this point of my academic and professional life without my incredible wife, Ryann. My wife and I have gone through the challenges of deployment, building a life together with our son, and completing doctoral programs together. We have both sacrificed so much to get to this point, and I couldn’t have done this without you. Your love, coaching, and support have meant so much to me from the moment we met. Once again, to my son, Matthew. Just watching you grow up and develop throughout the early stages of your life, you have really shown me what is important in life. I hope the example I try to make and the value I place on education, grit and resiliency are concepts my son takes with him throughout his life. My ability to persevere came from my parents, and I am so thankful that they have had my back my entire life.

I must also thank my doctoral committee for the support and guidance they have provided me. Thank you Dr. Duhainy, Dr. Blanson, and Dr. Griffith. This has been one of the most significant journeys of my life and it would have not been possible without my doctoral program committee.

Table of Contents

List of Tables v

Section 1: Foundation of the Study 1

Background of the Problem 1

Problem Statement 2

Purpose Statement 2

Nature of the Study 3

Research Question 5

Interview/Survey Questions 5

Conceptual Framework 6

Operational Definitions 7

Assumptions, Limitations, and Delimitations 8

Assumptions 8

Limitations 9

Delimitations 9

Significance of the Study 10

Contribution to Information Technology Practice 10

Implications for Social Change 10

A Review of the Professional and Academic Literature 11

Social Cognitive Theory 13

Components and Modes of Human Agency 16

Triadic Reciprocal Determinism Model and Constructs 20

Contrasting and Similar Theories 30

Cybersecurity Awareness and Training 34

Human Factor in Cybersecurity 41

Security Education, Training, and Awareness Research 48

Transition and Summary 49

Section 2: The Project 52

Purpose Statement 52

Role of the Researcher 53

Participants 56

Research Method and Design 60

Method 60

Research Design 63

Population and Sampling 67

Ethical Research 73

Data Collection 75

Instruments 75

Data Collection Technique 79

Data Organization Techniques 81

Data Analysis Technique 83

Reliability and Validity 86

Reliability 86

Validity 87

Dependability 87

Credibility 88

Transferability 89

Confirmability 89

Data Saturation 90

Transition and Summary 90

Section 3: Application to Professional Practice and Implications for Change 92

Overview of Study 92

Presentation of the Findings 92

Theme 1: Consistent, Persistent and Relevant Training and Awareness 93

Theme 2: Awareness and Training Based Off Threats, Risks and Vulnerabilities 99

Theme 3: Consequences and Disclosed Expectations 105

Applications to Professional Practice 112

Implications for Social Change 116

Recommendations for Action 118

Recommendations for Further Study 120

Reflections 122

Summary and Study Conclusions 123

Appendix A: Interview Protocol 174

Appendix B: Interview Questions 177

Appendix C: Letter of Invitation 178

Appendix D: Informed Consent Form 180

List of Tables

Table 1. Frequency of First Major Theme in Participant Responses and Documentation……………………………………………………………..96

Table 2. Frequency of Second Major Theme in Participant Responses and Documentation…………………………………………………………..……..101

Table 3. Frequency of Third Major Theme in Participant Responses and Documentation………………………………………………………………108

Section 1: Foundation of the Study

In this section, I will present the background of the problem, problem statement, purpose statement, and nature of the study. I will delineate the assumptions, limitations, and delimitations of the study. Also, I will present the research question, conceptual framework, and significance of the study.

Background of the Problem

Organizations utilize a combination of technical and nontechnical security measures to protect information systems and data through a multilayered, defense-in-depth strategy (Conteh & Schmick, 2016). According to Conteh and Schmick (2016), a defense-in-depth strategy consists of security policies, network guidance, audits and compliance, technical solutions, physical security, and security education, training, and awareness (SETA). The weakest layer in an organization's defense-in-depth strategy is related to the user's unawareness of cybersecurity best practices, cybersecurity threats, and vulnerabilities (de Bruijn & Janssen, 2017). The purpose of cybersecurity awareness and training programs are to ultimately protect an organization from the harm posed by cybersecurity vulnerabilities, threats, and attacks by improving employee education, training, and awareness (Beuran et al., 2018a). The need for better cybersecurity awareness and training strategies are demonstrated by 58% of employees not knowing how to protect an organization from malicious activity, and 98% incorrectly believing security responsibilities are delegated to the system administrators (Hadlington, 2017). Effective SETA strategies are needed to protect users and organizational information systems and data.

Problem Statement

Humans are the weakest layer in an organization’s cybersecurity program, and their unawareness contributes to an organization’s vulnerabilities (de Bruijn & Janssen, 2017). The need for better cybersecurity awareness and training strategies are demonstrated by 58% of employees not knowing how to protect an organization from malicious activity, and 98% incorrectly believing security responsibilities are delegated to the system administrators (Hadlington, 2017). The general information technology (IT) problem is that ineffective employee cybersecurity awareness and training programs contribute to compromises of organizational information systems and data. The specific IT problem is that some corporate hospitality IT leaders lack strategies to implement cybersecurity awareness and training programs to protect organizational information systems and data.

Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore strategies used by corporate hospitality IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data. The population consisted of corporate hospitality IT leaders including the chief executive officer (CEO), chief operating officer (COO), general managers, chief information officer (CIO), chief information security officer (CISO), and IT directors in Hampton Roads, Virginia, who have implemented cybersecurity awareness and training strategies within their organization. Implications for positive social change include the potential improvement to awareness and training programs that contribute to better cybersecurity practices, which may protect national security, guard critical infrastructure, and prevent disclosure of sensitive information due to compromise that may harm citizens. The improvement of cybersecurity awareness and training also has the potential of protecting these same employees and their families, including children at home, as a result of effective education. The lessons learned at work through awareness and training programs can be retaught at home, which may protect families from crime and nefarious intent. There is also the potential to contribute new knowledge and insights that may lead to discovery, such as new strategies and tactical level implementations that may protect organizations from damaging events and ultimately improve the cybersecurity culture at a macrolevel.

Nature of the Study

My intent in this qualitative exploratory multiple case study was to explore organizational cybersecurity awareness and training strategies used to educate employees on practices to protect organizational information systems and data. Multiple case studies enable researchers to acquire a deeper understanding of a phenomenon (Zach, 2006). My intent in this study was to provide depth in understanding the strategies of cybersecurity awareness and training used to educate employees on practices to protect organizational information systems and data. A qualitative research method was suitable for this study because I focused on multiple organizations and their successful implementation of cybersecurity awareness and training programs. Qualitative research promotes the generation of detailed and rich responses to intricate subjects (Cope, 2014). Therefore, I decided not to collect numerical data to evaluate my research questions, which is explicitly required in a quantitative study. A quantitative study is appropriate when numerical data is used to describe a phenomenon (Carr, 1994). Mixed methods research encompasses the incorporation of qualitative and quantitative methods and should only be utilized if the combination of methods better explains the research question than a single approach alone (Halcomb, 2019). Because I intended to explore this phenomenon and not describe it with numerical data, quantitative research was not appropriate for this study. Also, I decided not to utilize mixed methods because the integration of quantitative methods did not more fully answer the research question of this study than just using qualitative approaches.

The use of a multiple case study was the chosen design for this study. Case studies and, more specifically, multiple case studies enable researchers to acquire a deep understanding of a phenomenon (Zach, 2006). Moustakas (1994) stated that phenomenological studies examine the experiences of individuals that have shared an experience (as cited in Ward & Webster, 2018). Furthermore, phenomenology is used to better understand human beings through their perceptions (Qutoshi, 2018), which may be a beneficial research design, but it did not allow me to focus on the specific details of an organization’s cybersecurity awareness and training strategies and the consequences these strategies had in promoting the protection of data and information systems. Ethnography focuses on the culture of a population through immersion, so an actual representation of the context can be achieved (Flacking & Dykes, 2017), which was not my intent in this study because I was more interested in the how and why cybersecurity awareness and training strategies are implemented within organizations. Last, a narrative study allows for the gathering of data and stories from personal experiences (Haydon, Browne, & van der Riet, 2018). As mentioned, I was more interested in examining the why and how cybersecurity awareness and training strategies are implemented by IT leaders, rather than the personal stories about their experiences within the constructs of a cybersecurity awareness and training program. Therefore, the use of a narrative study was not an appropriate design for this particular study.

Research Question

What strategies are used by corporate IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data?

Interview/Survey Questions

1. What aspects of cybersecurity interest you most?
2. What are the components of your cybersecurity program?
3. What cybersecurity awareness strategies have you used to promote the protection of organizational information systems and data?
4. How do you determine which cybersecurity awareness strategies are used to promote the protection of organizational information systems and data?
5. How do you determine what cybersecurity concepts are most important in your organization's cybersecurity awareness and training program?
6. How do you determine that employees have been adequately trained through cybersecurity awareness strategies to protect organizational information systems and data?

7. What methods worked best in cybersecurity awareness strategies to promote the protection of organizational information systems and data?
8. How do you enforce cybersecurity compliance and conduct remediation training?
9. How do you measure success of your cybersecurity awareness and training program?

Conceptual Framework

The conceptual framework of this study was social cognitive theory (SCT) developed by Albert Bandura in 1986. SCT uses a triadic model consisting of personal, behavioral, and environmental determinates, all of which interact with each other to shape human behavior (Bandura, 2001a). The four primary constructs of SCT are self-efficacy, self-regulation, social learning, and outcome expectancy (Lowry, Zhang, & Wu, 2017). Self-efficacy is the belief an individual has in themselves to accomplish something or overcome a challenge (Uszynski et al., 2018). Self-regulation refers to an individual being able to self-assess their actions (Benight, Harwell, & Shoji, 2018). Social learning refers to the persuasions incurred from negative and positive social influences which impact an individual's learning (Lowry et al., 2017). Outcome expectancy is related to an individual's ability to assess the rewards versus consequences of taking action (Schoenfeld, Segal, & Borgia, 2017).

I selected this conceptual framework because it aligned well with the implementation of cybersecurity awareness and training programs. The basis of implementing a cybersecurity awareness program within an organization is based on mandated requirements placed by government or industry regulations (Kortjan & Von

Solms, 2014). The behavior and learning of an individual are based on intrinsic and extrinsic factors, as presented in the triadic model. Regulated standards, such as the Payment Card Industry Data Security Standard (PCI DSS), represent an environmental factor in the form of frameworks, which IT leaders must consider and instill on the employees of the organization. Awareness and training programs in a corporate atmosphere may fail at teaching regular user's cybersecurity principles (Ricci, Breitinger, & Baggili, 2018). Examining cybersecurity awareness and training strategies of IT leaders to improve user self-efficacy is important, and SCT is applicable. Successful cybersecurity programs require a mechanism to measure the success of objectives (Bozkus Kahyaoglu & Caliyurt, 2018) and applies to the goal-setting construct of SCT. Finally, social learning is a mechanism to deter the misuse of information systems by emphasizing the consequences of inappropriate actions (D'Arcy, Hovav, & Galletta, 2009). By examining the strategy of user accountability in a cybersecurity training and awareness program, I will explore its effectiveness in this exploratory study. Therefore, SCT is an appropriate theory to apply to the conceptual framework in examining cybersecurity awareness and training strategies in organizational use by IT leaders.

Operational Definitions

The following operational definitions, which I utilized in this doctoral study, may assist readers understand the content better.

Cybersecurity awareness: The level of cognizance and understanding of concepts related to cybersecurity such as threats, vulnerabilities, and risk (Berkman, Jona, Lee, & Soderstrom, 2018).

Cybersecurity training: Actions aimed to improve the skills and abilities of others (Beuran et al., 2018a).

Organizational IT leader: An individual that leads other IT employees within the organization and manages the implementation of strategy, policy, and technology related to IT, such as a CEO, COO, CIO, CISO, IT director, IT manager, or general manager (Hickman & Akdere, 2018).

Sensitive data: Data that are, in essence, considered sensitive or data in which sensitive details about an individual can determined or extrapolated (Shabani & Borry, 2018).

Assumptions, Limitations, and Delimitations

Assumptions

Assumptions are concepts or facts imposed on the study that are accepted as true (Uprichard & Dawney, 2019). In this study, I assumed that the participants possessed a strong understanding and knowledge of cybersecurity awareness and training programs. I also assumed that the participants responded in a truthful, accurate, and honest manner to the open-ended questions. I assumed that the use of a qualitative research methodology would be effective in providing the data needed to answer the research question. I constructed the interview questions in a manner to facilitate a discussion to acquire possibly used cybersecurity awareness and training strategies to protect organizational information systems and data.

Limitations

Limitations of a study are potential weaknesses of a research study that may require future work to resolve or opportunities to perform additional research (Hall & Martin, 2019). The first limitation of this exploratory multiple case study was that I examined the implemented cybersecurity awareness and training strategies of at least three cases. Furthermore, the geographic study location was Hampton Roads, Virginia, which may produce results that may not be generalized nor transferable to other locations. I examined cybersecurity awareness and training strategies of the hospitality industry and may not be applicable to other industries. Last, the participants of the study included organizational IT leaders, which may result in responses and observations that do not apply to other leaders and employees of the organization.

Delimitations

Delimitations are constraints and boundaries that researchers impose in qualitative studies to scope the study (Alpi & Evans, 2019). First, participants of the study included organizational IT leaders who possessed the knowledge and/or experience of implementing cybersecurity awareness and training strategies at their organization. Second, the interviews were open-ended to promote the open and transparent sharing of their experiences and observations about the implementation of cybersecurity awareness and training programs at their organization.

Significance of the Study

Contribution to Information Technology Practice

From the perspective of contributing to the IT practice, organizations strive to instill strong cybersecurity programs to protect the assets of the organization. The results of this study may provide much-needed insights into the strategies that hospitality IT leaders utilize to implement, manage, and measure cybersecurity awareness and training strategies to promote the protection of information systems and organizational data. As organizations are faced with numerous attacks each year, organizational IT leaders must take the appropriate steps to ensure they have effective strategies to protect their organizations. Organizational leadership implementing cybersecurity awareness and training programs must examine the effectiveness of educational strategies that promote employees knowingly protecting organizational information systems and data. The results and insights of this study may aid organizations of various domains to consider the factors that positively contribute to an organization's cybersecurity awareness and training program.

Implications for Social Change

The implication for positive social change was that the lessons taught through organizational cybersecurity awareness and training programs may be retaught at home. Families and children are spending more time on connected systems, which exposes them to numerous threats. Employees may take the lessons learned from cybersecurity awareness programs at work to educate their families. These lessons might protect their families from the dangers that surround them in cyberspace. Protecting families, including children, incurs an immediate positive social contribution and one that is invaluable. Children live in a highly connected world, which implies the need for cybersecurity education due to the potential cyber-related risks, but little is known of youth cybersecurity education (Edwards et al., 2018). Even with the lack of research, youth cybersecurity education is necessary, and the awareness acquired by parents or guardians may be presented to children. For example, concepts related to attack vectors towards devices used by children and young adults may be taught about potential dangers. Furthermore, the parents of these children may not come from backgrounds suited to understand the best practices of cybersecurity so that they can pass this knowledge on to their families at home for protection. By determining strategies utilized to implement cybersecurity awareness and training programs, the findings will be available to organizations within academia, government, and corporate. The organizations in these sectors may use the findings of this research to improve their cybersecurity awareness and training programs. In turn, by improving the knowledge base of employee cybersecurity practices at work, these same employees may better educate their families. Additionally, the findings of this study can be used to develop cybersecurity awareness and training programs at the elementary, middle, and high school levels.

A Review of the Professional and Academic Literature

The purpose of this qualitative multiple case study was to explore strategies that organizational hospitality IT leaders use for cybersecurity awareness and training programs to protect organizational information systems and data. The focus of the literature review was the research question: What strategies are used by corporate IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data? I explored the current cybersecurity awareness and training strategies across multiple industries. Afterward, I explored strategies researchers have studied to address the educating and awareness of human beings, to include the enforcement of teaching using the four constructs and three determinants of SCT.

Keywords used in searching for the appropriate literature included: *cybersecurity, information security, data breach, data compromise, confidentiality, integrity, availability, non-repudiation, cyber behavior, human factor, vulnerabilities, risk, cybersecurity awareness, cybersecurity training, cybersecurity education, social cognitive theory, human agency, triadic reciprocal determinism model, behaviorism, cognition,* and *constructivism.* Additionally, I have conducted searches using various permutations of these keywords to promote relationships that may have an impact on this study. These sources will provide academic and industrial perspectives on the strategies of implementing cybersecurity awareness and training programs.

This literature review contains references from 131 articles, journals, and conference proceedings. The primary research libraries and databases included the EBSCOhost Computers and Applied Sciences Complete, EBSCO Business Source Complete, Sage Journals, Google Scholar, ScienceDirect, IEEE Xplore Digital Library, ResearchGate, ProQuest Computing, Emerald Insight, ProQuest Nursing & Allied Health Source, Ovid, and ProQuest Dissertations and Theses Global. I verified the peer-reviewed status of articles using UlrichsWeb Global Serials Directory and individual journal websites. I reviewed 131 articles, of which 131 (100%) were peer-reviewed, and 120 (91.6%) were published within 5 years of my anticipated graduation date.

The literature focused on three key areas: (a) SCT, (b) cybersecurity awareness and training strategies, and (c) impacts of the human factor in cybersecurity. The review of the four components and three determinants of SCT focused on the educating and awareness of human beings, including the enforcement of teaching. The four constructs consisted of self-efficacy, self-regulation, social learning, and outcome expectancy. The three determinants consisted of personal, behavioral, and environmental factors. The research into cybersecurity awareness and training involved current events, consequences of compromise, and strategies to mitigate against negative outcomes. Finally, the research of human factors within the domain of cybersecurity were examined.

Social Cognitive Theory

Albert Bandura extended his original social learning theory (SLT) in 1986 and defined it as SCT, which accounted for characteristics that behaviorist theory could not (Locke, 1987). According to Bandura (1986), the actions of an individual are a product of personal, environmental, and behavioral factors. SCT assumes an agentic stance, which assumes that human beings are enabled and have the power to take the necessary steps to improve their situation (Bandura, 2019). Rather than assuming a unidirectional relationship between the individual and environmental influences or internal influences, SCT describes psychosocial functioning through a triadic bidirectional model (Wood & Bandura, 1989). The triadic model is known as triadic reciprocal determinism, and it describes the triadic, bidirectional relationship between an individual’s behavior, personal factors, and the environment (Lo Schiavo, Prinari, Saito, Shoji, & Benight, 2018). In addition to the triadic reciprocal determinism model, SCT consists of four constructs, which are self-efficacy, self-regulation, social learning or modeling, and outcome expectancy (Lowry et al., 2017). SCT delineates that the development of an individual is not due to unidirectional influences, but rather through bidirectional relationships that interact with each other, and are further influenced by the key constructs of self-efficacy, self-regulation, social learning, and outcome expectancy.

Human behavior and learning are constantly influenced by internal factors, personal characteristics, the individual’s behavior, the behavior of others, and the environment, all while being constantly reassessed by the individual. The model of triadic reciprocal determinism is maintained through a self-regulatory mechanism that impacts the relationship between environment, personal factors, and behavior to varying degrees (Bandura, 1991). The self-regulatory system of SCT delineates the mechanism in which human beings adjust their behavior based on various influences (Bandura, 1991). The strength between the relationship of personal, behavioral, and environmental factors is not equal to each individual and may change from one time period to the next. (Font, Garay, & Jones, 2016). It is also not assumed that the relationships of the triadic reciprocal determinism model are occurring at all times (Wood & Bandura, 1989). The ability to produce a desired behavior or learning outcome is related to properly managing behavioral, environmental, and personal factors (Lo Schiavo et al., 2018). When attempting to achieve a desired outcome within an organization and increasing the likelihood of knowledge acquisition, a careful examination of individual characteristics, employee behaviors, and the organization's culture and environment is needed to implement the most effective training strategy.

Human agency is a key component of human behavior as it relates to an interactive relationship between personal factors, the environment, and behavioral factors from a SCT perspective. SCT assumes the premise of an agentic perspective, which implies that human beings able to adapt from various influences rather than being a product of their external environment (Bandura, 2006). Human agency denotes a human being's capability to influence the circumstances surrounding them as well as determining their actions based on various factors (Bandura, 2006). According to Bandura (2006), human beings contribute to the status of their life and are not simply a result of the circumstances surrounding them.

There are four core properties of human agency, which are intentionality, forethought, self-reactiveness, and self-reflectiveness (Bandura, 2001a). In addition to the four core properties of human agency, there are three different modes of human agency (Sanders, Stensland, & Juraco, 2018). The three modes of agency are individual agency, proxy agency, and collective agency (Bandura, 2006). Humans are influenced by their environment and they influence the environment around them through the four core properties of human agency and the three modes of human agency. Organizations that effectively manage the concept of human agency may be able to promote positive and desired outcomes.

Components and Modes of Human Agency

Individuals maintain the ability to act on their own accord, within the constraints of their environment, but are influenced by the relationships of the triadic reciprocal determinism model. Intentionality is an individual's deliberate decision to act (Bandura, 2006). According to Bandura (2001a), intentionality does not assume that the deliberate action will always result in a positive outcome because there are instances in which an individual will incorrectly forecast the outcome of an action. Additionally, intentionality does not occur in a vacuum, but may also include external entities and a coordinated effort may be necessary to achieve the desired outcome of the pursuit (Bandura, 2006). Intentional action of human agency is constrained by social constructs and institutional requirements, and as such, intentionality is influenced by allowable and unallowable regulations of the social environment (Schoon & Heckhausen, 2019). The ability for an individual to be intentional in their endeavors and actions is not done in isolation, but rather is guided by social constructs, laws, regulations, constraints, and opportunities.

Forethought is the creation and refinement of future plans based on individual goals and mentally assessing the outcomes of performing the forecasted action (Bandura, 2006). Individuals will develop alternative courses of action and select the best option based on their individual goals, with the general intent of developing solutions with high reward, while limiting or not selecting actions that have a negative impact on the individual (Bandura, 2001a). The mental development of potential future outcomes against individual goals provides internal guidance within the framework of their environment (Bandura, 2018). Forethought interacts with the triadic reciprocal determinism model in a manner that provides an individual with the possibility to will a desired future within their present situation (Bandura, 2018). Forethought serves as an internal human mechanism to visualize potential actions with associated outcomes and based on individual goals and outcome expectancy, and an individual will select one of the developed mental courses of action.

Self-reactiveness refers to an individual's ability to adapt and modify their course of action based on internal and external factors (Bandura, 2006). Self-reactiveness is strongly related to an individual's motivations and their internal regulatory mechanism to alter their course of action based on various factors (Motl, Pekmezi, & Wingo, 2018). External feedback and other factors will influence an individual's choices and alter their course of action, which contributed to the agentic property of self-reactiveness (Miraglia, Cenciotti, Alessandri, & Borgogni, 2017). Self-reactiveness operates in relation to forethought because an individual will use forethought to plan and select a course of action, but through constant evaluation of perceived outcome at a particular moment, an individual will adjust their execution if necessary (Bandura, 2001a). The self-reactive mechanism of human agency operates within the framework of self-monitoring, performance against personal standards, and corrective actions (Bandura, 2001a). Self-reactiveness is an important characteristic of human agency that describes the internal mechanisms that allow a human being to adjust their actions based on personal, behavioral, and environmental factors.

The most fundamental human agentic core property is that of self-reflectiveness, which is the self-examination of an individual's core internal characteristics (Bandura, 2018). Through internal reflection, an individual will assess internal characteristics such as values, key motivational factors, and self-purpose (Bandura, 2001a). During the cognitive framework of self-reflectiveness, an individual examines numerous factors, which include the accuracy of their perceived outcome to the occurring outcome, and how others will react (Bandura, 2001a). Another contributor to an individual's self-reflective nature is utilizing prior knowledge and inferencing outcomes based on prior knowledge (Bandura, 2001a). Human beings do not just execute an action and not think about it any further. Rather, an individual will examine and evaluate circumstances against internal factors and prior knowledge, which is used to develop conclusions for future reference or refined action.

An individual's daily operation is shaped and influenced by three modes of agency, which are individual, proxy, and collective (Anderson et al., 2019). Within SCT, the individual mode of agency refers to an agent's belief to influence the environment they are operating within and have control of their personal functioning (Bandura, 2006). Within the constructs of SCT, the individual mode of agency stipulates that an individual not only believes they have control of achieving a specific outcome, they believe that they can command a result (Anderson et al., 2019). The examination of the individual mode of human agency is focused on the scope of actions that are controlled specifically by the individual (Bandura, 2018).

Individuals may not have the means, ability, or resources to achieve the outcome they desire or influence the desired effect on their own so they may require using a proxy (Bandura, 2018). In circumstances such as this, an individual will leverage the abilities, resources, and means of someone else to achieve the outcome that they ultimately desire (Bandura, 2006). Examples of proxy modes of agency include a child needing their parents or an employee leveraging the influence of their boss (Bandura, 2001a). Proxy agency is not strictly constrained to situations in which an individual lacks the ability, knowledge, or means to accomplish a task, but it may be a situation in which the agent believes someone else can perform the task better (Bandura, 2001a). There may be circumstances in which an individual is not able to achieve the outcome they desire, so they may need the influence or assistance of someone else to accomplish the desired outcome. Additionally, proxy agency is not a unidirectional relationship, but rather it is related to a circumstance in which an individual can benefit through the characteristics of another. This implies that a parent may turn to a child to produce a desired result, such as instilling sympathy.

The last mode of agency is collective agency. Collective agency occurs when the desired outcome can only be achieved through the efforts of a group (Bandura, 2018). Collective agency is a product of the belief that the collective group has in its ability to produce a result (Bandura, 2001a). Of importance, collective agency is not determined by the sum of fragmented and unrelated beliefs, but rather, collective agency is a product of the shared belief of the group to accomplish an outcome (Bandura, 2001a). Collective agency consists of both individual and proxy agency (Zinette, Manfred, & Andrew, 2019). An example of collective agency was the circumstance involving a group of Chinese physics teachers that joined together to initiate curriculum reform and through the process, positively influenced individual agency (Fu & Clarke, 2019). In the occurrence of circumstances in which the desired outcome cannot be achieved through individual or proxy agency, the sum of a collective group may be able to produce the desired outcome and instill the change needed in a given circumstance or to achieve a specific objective.

Triadic Reciprocal Determinism Model and Constructs

SCT is based on the premise that human beings are agents within a framework in which their behavior is influenced by the bi-directional relationships between an individual's behavior, personal factors, and environment within the triadic reciprocal determinism model (Bandura, 1991). The strength of the relationships between personal, behavioral, and environmental factors is fluid, not always of equal strength, nor are all relationships occurring at the same time (Font et al., 2016). The factors of the triadic reciprocal determinism model and relationships between each other are influenced by self-efficacy, self-regulation, social learning or modeling, and outcome expectancy (Lowry et al., 2017). The response and behavior of human beings is the result of a dynamic bi-directional relationship between the environment, personal factors, and behavioral factors that are further influenced by the key constructs that also interact with each other, which will be further discussed in the following sections.

Within SCT, the environment consists of factors associated with the physical and social environment surrounding the individual that may impact the behavior of that individual (Bennett et al., 2018). There are three environmental structures with SCT, which are the imposed environment, selected environment, and constructed environment (Bandura as cited in Bandura, 2001a). The social environment incorporates social and sociodemographic factors to include social interactions, social support, and cultural environment (Ikeda, Hinckson, Witten, & Smith, 2018). Sociodemographic characteristics are characteristics that combine social and demographic factors to include education level, marital status, age, gender, and income level (Geoffroy et al., 2018). Within the two environmental constructs of physical and social environments, there are three environmental structures that are relevant within SCT. Within the imposed environment, an individual can assess, act, and respond at will within the environment, but they cannot control the environment (Zhang, Y., Zhang, M., Luo, Wang, & Niu, 2019). The selected environment refers to an individual's choices of the social environment, their activities, and connections to reach a desired outcome (Zinette et al., 2019). The constructed environment refers to the environment that an individual will experience without explicit choice from the individual and requires effort on the individual's part to understand (Anaya-Reig, 2018). The three environmental frameworks that an individual interacts with can be influenced by the individual, or the environment may influence the individual.

Personal factors from a SCT perspective are associated with characteristics specific to the individual and influenced by many factors. Personal factors include attitudes, personal beliefs, previous experiences to include outcomes, personal motivations, and self-efficacy (Amico, Mugavero, Krousel-Wood, Bosworth, & Merlin, 2018). Personal factors, such as cognitive, affective, and biological events impact environmental and behavioral factors of the triadic model (Bandura, 2001a). Personal factors are also influenced by other personal factors, such as personal motivations being influenced by outcome expectation, which in turn is influenced by prior experience and familiarity (Wang, Hung, & Huang, 2019). Research has demonstrated that individuals with higher levels of self-efficacy set higher goals and envision positive outcome expectations, which may be physical, social, or emotionally benefiting (Beauchamp, Crawford, & Jackson, 2019). Personal factors are constantly influenced by other personal factors, which in turn influences behavioral and environmental factors in a dynamic fashion.

Human behavior is managed by internal mechanisms, which are impacted by personal and environmental factors (Bandura, 2001a). Bandura (2001a) presents the example that human behavior is influenced by economic conditions, family structure, and status because it impacts an individual's standards, level of self-efficacy, and other influences managed by an individual's internal mechanisms. Behavioral factors include internal mechanisms such as self-observation and judgment in one's actions or actions surrounding them (Amico et al., 2018). Within SCT, behavioral factors also include and are influenced by the awareness of one's thoughts, which is known as metacognition (Tur-Porcar, Roig-Tierno, & Llorca Mestre, 2018). Metacognition consists of the elements of self-efficacy and self-regulation, which are two of the four key constructs of SCT (Tur-Porcar et al., 2018). The self-regulatory system functions off internal psychological factors and self-evaluation. The motivation of an individual to perform an action is related to their ability to self-evaluate (Bandura, 1991). Self-evaluation is a complex task, which is influenced by an individual's personal values, current environment, and perceived level of importance of the task against the outcome of the task (Bandura, 1991). An individual’s internal framework impacts the decisions and actions of the individual. The self-regulatory system of an individual is a process in which an individual’s belief to accomplish a task is impacted by individual characteristics such as upbringing, personal standards, and overall judgment. The undertaken action is then self-evaluated within the self-regulatory system, which in turn influences future actions and decisions.

The belief in one’s own abilities is a key characteristic in performance, judgment, and personal motivations. Self-efficacy is an individual’s belief in themselves to take action, overcome constraints, and accomplish a task satisfactorily (Brooks et al., 2019). In the context of career performance, self-efficacy is impacted by contextual influences, such as organizational support and assistance entities (Bolkan, Pedersen, Stormes, & Manke, 2018). In turn, self-efficacy influences outcome expectations, personal goals, and ultimately, overall personal performance (Bolkan et al., 2018). It has been demonstrated that past performance can also influence self-efficacy (Khorakian & Sharifirad, 2019). When examining self-efficacy, there is also an influential relationship with the “big-five” personal traits, which are conscientiousness, openness, agreeableness, extraversion, and neuroticism (Stajkovic, Bandura, Locke, Lee, & Sergent, 2018). Self-efficacy is a core determinant of personal motivation, personal judgment, and behavior (Bandura, 2004). Organizations may positively impact self-efficacy by focusing on the development of other personal characteristics. Additionally, the efforts in improving self-efficacy can be aligned to improve personal goals, better decision making, and improve personal performance within an organization.

There are different forms of self-efficacy such as response efficacy and task self-efficacy, which are influenced by an organization’s information security program and contribute to an effective SETA program. Response self-efficacy refers to an individual’s belief that their behavior makes a difference in reducing risk (Meijers, Remmelswaal, & Wonneberger, 2018). An individual’s experience and knowledge with cybersecurity has a significant influence on response efficacy and overall self-efficacy (Li et al., 2019). Task self-efficacy refers to an individual’s ability to complete a task (as cited in Graham, Li, Bray, & Cairney, 2018). It has been demonstrated that hands-on activities and training have improved self-efficacy in the domain of cybersecurity education (Jin, Tu, Kim, Heffron, & White, 2018). Formulating training that not only relies on presenting information may improve self-efficacy, which may positively influence an individual’s level of cybersecurity awareness.

Self-efficacy and the effectiveness of an organization’s SETA program are related to each other. The effectiveness of organizational SETA programs has a significant influence on self-efficacy, and self-efficacy has a significant influence on security compliance intent (Yoo, Sanders, & Cerveny, 2018). Negative personal characteristics, such as upbringing, income, and mental health, may negatively impact personal self-efficacy (Bingöl, 2018). Senior management buy-in and organizational practices and policies related to cybersecurity awareness and training programs significantly influenced employee self-efficacy of cybersecurity principles (Cuganesan, Steele, & Hart, 2018). According to Bandura (2012), self-efficacy is developed through mastery experiences, social modeling, social persuasion, and personal state. Mastery experiences refers to an individual’s ability to succeed through difficult circumstances instead of succeeding through simple tasks (Bandura, 2012). Social modeling refers to an individual observing others succeeding (Bandura, 2012). Social persuasion refers to an environment in which individuals are taught to believe in themselves, and in turn, will overcome challenges (Bandura, 2012). Finally, self-efficacy is improved by improving the emotional and physical states of individuals, such as reducing anxiety (Bandura, 2012). Self-efficacy within the domain of cybersecurity and SETA programs are shown to improve employee information security practices. Furthermore, cybersecurity self-efficacy can be influenced through various initiatives, and organizations must focus efforts to promote employee development and education.

An individual’s ability to monitor, assess, and adjust their actions is a critical contributor to self-efficacy, personal actions, and personal development. Self-regulation is a critical characteristic to examine in terms of failure to obey standards (Baumeister, Tice, & Vohs, 2018). Self-regulation is a dynamic internal process made up of the self-monitoring, self-diagnostic, self-motivating, judgmental, and reactive systems (Bandura, 1991). An individual can self-observe their actions, evaluate those actions against a delineated standard, and react accordingly (Benight et al., 2018). Organizations must examine the impacts their training programs and culture have on the self-regulatory framework on an individual to improve overall behavior.

An individual’s self-regulatory system is made up of various constructs that influence their behavior. Self-regulation can be broken down into cognitive, motivational, and behavioral self-regulation, and the correct learning strategy based on these characteristics is important (Hoch, Scheiter, & Schüler, 2019). Cognitive self-regulation refers to an individual’s decision to select an appropriate reasoning strategy, motivational self-regulation refers to an individual’s reliance on their own abilities, and behavioral self-regulation is an individual’s decision to invest sufficient effort (Hoch et al., 2019). In the education domain, self-regulation and motivation are related constructs, which are influenced by goal-setting, topic interest, and, most of all, self-efficacy (Lau, Kitsantas, Miller, & Rodgers, 2018). Organizations must understand the self-regulation system of an individual and create an organizational culture and training strategy that aligns to promote more beneficial behaviors. On the other hand, individuals must understand the accepted standards within an organization, grasp acceptable behaviors, and be able to self-regulate their actions to act in their best interest and the interest of the organization.

An individual’s ability to satisfactorily self-regulate promotes an improved organizational cyber posture and effective cybersecurity awareness and training program. The inability to properly self-regulate is directly related to an increased likelihood of committing an inappropriate information assurance action, which may increase the cyber risk towards an organization (Vishwanath, Harrison, & Ng, 2018). SETA programs are an effective educational construct which impacts human behavior by influencing self-regulatory constructs (Herath, Yim, D’Arcy, Nam, & Rao, 2018). Mastery of teaching material and achievement of organizational goals is directly related to individual self-regulation (Sitzmann & Weinhardt, 2018). Furthermore, training effectiveness is influenced by applying rewards and punishments during the training cycle, which impacts an individual’s self-regulatory system by influencing the feedback they receive (Sitzmann

& Weinhardt, 2018). Self-regulation can be improved by providing verbal feedback (Ho, Uy, Kang, & Chan, 2018) and interactive group settings (Guo, Tang, Wiley, Whittemore, & Chen, 2018). Behavioral strategies such as self-monitoring, problem-solving, goal setting, and planning can positively impact individual self-regulation systems (Kahan, Wilson, & Sweeney, 2018). By applying various training strategies to positively develop individual self-regulation, with the use of rewards and punishments, organizations are able to promote more effective cybersecurity awareness and training programs to protect organizational information systems and data.

Outcome expectation influences an individual's decision making, actions, and effort toward accomplishing a task. Outcome expectation refers to an individual's assessment of the positive and negative implications of an action or decision (Bandura, 2006). Outcome expectation can be generalized into one of three categories, which are physical effects, social effects, and self-evaluation effects (Bandura, as cited by Lin & Chang, 2018). Physical effects refer to physiological pleasure and discomfort, social effects refer to positive and negative social recognition, and self-evaluative effects refer to personal levels of satisfaction (Lin & Chang, 2018). Individuals are more likely to perform an action or series of actions if they believe that they are capable of performing the action and that the outcome expectancy is positive (Pinnell et al., 2018). Negative outcome expectations disincentivize an individual's willingness to perform a specific action (Sessford et al., 2019). Bandura (2012) suggests that outcome expectation is directly influenced by an individual's self-efficacy, while outcome expectation directly influences personal goals and behavioral motivations. Organizations must satisfy the prerequisite of ensuring individuals are aware of how to perform specific actions and believe in their capabilities to promote a more significant impact from outcome expectancy to modify behavior. By utilizing the appropriate makeup of physical, social, and self-evaluative outcome expectations, organizations may promote behaviors that align with organizational goals. Delineation of outcome expectations to employees has positively impacted the learning outcomes of information assurance principles and are enhanced by incorporating the monitoring of network activity (Ahmad, Ong, Liew, & Norhashim, 2019). The appropriate use of outcome expectation, rewards, and punishments may promote better cybersecurity decisions from employees.

Utilizing observational learning is an additional method to promote the acquisition of knowledge by individuals. Observational learning refers to learning acquired by an individual through observation (Merlin et al., 2018). Observational learning is directly influenced by the perceived value of the information to be acquired ,and if the information can be easily understood by the individual (Merlin et al., 2018). An individual's behavior can be enhanced through observational learning (Carcea & Froemke, 2019). Organizations that promote positive behavior and emphasize the value of desired actions may improve an individual's behavior and learning acquisition through observational learning.

The dynamic subfunctions of observational learning contribute to an individual's ability to regulate, learn, and recall past behaviors. Observational learning consists of four subfunctions, which are attentional processes, retention processes, production processes, and motivational processes (Bandura, 2001b). The attentional process refers to focusing on the behavior to be learned, and more attention is given to behaviors perceived as more attractive to the individual (Carroll, Sankupellay, Rodgers, Newcomb, & Cook, 2018). The retention process of observational learning refers to an individual's ability to convert the behaviors focused on during the attentional process into a form stored in human memory (Bai, Lin, & Liu, 2019). The production process recalls the learned behavior from memory and attempts to accomplish the previously observed behavior (Mulyaningsih, Suwandi, Setiawan, & Rohmadi, 2018). The motivational process accounts for the fact that individuals do not learn everything they see, but rather, is influenced by direct, vicarious, and self-produced incentives (Bandura, 2001b). To promote the benefits of observational learning, practitioners need to appropriately use the four subsystems of the observational learning framework while ensuring that learners of the material perceive the teaching process and the learned information as valuable.

In addition to utilizing observational learning, the appropriate use of the three motivational influences to educate and inform individuals are needed to promote positive learning outcomes. Vicarious motivating influences are founded on outcome expectation and based on reward and punishment of modeled teachings (Wood & Bandura, 1989). Self-produced motivators are learned over time and through experience, such as learning that touching hot surfaces bring discomfort (Bandura, 2006). Direct motivation is a product of self-evaluated results at the moment the result of the action was encountered (Bandura, 2001b). Information security awareness programs that utilize orientations to enforce learned procedures and the application of taught principles while addressing motivational factors have positively impacted an individual's ability to abide to information security practices to protect sensitive information (Park, E., Kim, Wiles, & Park, Y., 2018). The expectation of regret in the future based on an action, such as punishment and emotional hardship, significantly influenced an individual’s behavior to take proper actions to protect sensitive information (Chen & Li, 2017). Incorporation of motivational influencing factors from the observational learning framework may improve organizational SETA programs to protect sensitive information through improved employee behavior.

Contrasting and Similar Theories

Experiential learning theory and social cognitive theory. Experiential learning theory (ELT) is used to describe the process in which individual learning is the product of experience (Brown, Willett, Goldfine, R., & Goldfine, B., 2018). The foundation of the ELT process is within an individual’s environment and consists of an individual personally performing an activity, collecting data from the activity, and reflecting on what has occurred to ultimately create knowledge (Angstmann, Rollings, Fore, & Sorge, 2019). ELT focuses on experience and a problem-based learning style (Beccaria, Kek, & Huijser, 2018).

Within ELT, the self-reflective phase consists of personal reflection, and the forethought phase consists of goal-setting, self-efficacy, and outcome expectancies to modify future performances (Nakabayashi, 2018). Experiential learning has been applied in cybersecurity awareness through simulations and virtual reality (VR), in which individuals personally experience scenarios through VR, respond, and develop cybersecurity knowledge (Seo et al., 2019). Overall, ELT assumes that an individual can self-reflect and regulate future behavior, which aligns with the agentic perspective of SCT. The learning mechanism of ELT also aligns well with the self-efficacy construct of SCT and both theories posit the importance of the environment on the individual throughout the learning process. Outcome expectation also aligns within the construct of ELT because when an individual reflects on prior actions and modifies future actions, outcomes of the prior event contribute to the overall learning experience. ELT does not explain how individuals learn through social observation, and that internal and behavioral factors contribute to the overall learning process. SCT accounts for demographics, personality, and outside influences, such as the organization and social pressures from peers to influence learning, which describes the organizational force and potential factors in exploring organizational SETA programs, whereas ELT is less or not impacted by these factors.

Discovery learning theory and social cognitive theory. Discovery learning (DL) suggests that an individual learns concepts through self-discovery and personal examination (Bakker, 2018). The use of DL is strongly dependent on the problems developed by instructors to improve knowledge acquisition and the transference of knowledge (Abrahamson & Kapur, 2018). Furthermore, improvement in knowledge acquisition does not imply a change in personal attitudes (Abrahamson & Kapur, 2018).

A primary concern with discovery learning is effectiveness, which is influenced by return-on-investment, quality of lesson planning, and the requirement to educate through discovery (Bakker, 2018). The use of DL implies little intervention when training individuals so that they may explore various impacts with specific actions (Kulasegaram, Axelrod, Ringsted, & Brydges, 2018). Also, DL has been shown to be more effective with the use of another form of teaching, such as directly instructing individuals (Kulasegaram et al., 2018). DL and SCT align well in terms of outcome expectation because as individuals work through problems in DL, they learn from the outcome and attempt a different approach until a satisfactory outcome has been achieved. DL does not explain how individuals learn through social observation, and that internal and behavioral factors contribute to the overall learning process. SCT accounts for demographics, personality, and outside influences, such as the organization and social pressures from peers to influence learning. DL places individuals in a difficult situation in acquiring cybersecurity knowledge because it relies on personal exploration to discover relatively difficult concepts. Furthermore, DL would require other teaching methods so that individuals would have an understanding of what to look for in terms of cybersecurity education.

Transformational learning theory and social cognitive theory. The theory of Transformational learning (TLT) posits that an individual assesses and reassess their current perspective to discover potentially new knowledge (Hovey, Jordan, Bedos, Rodriguez, & Apelian, 2018). A major critique of TLT is that it focuses on personal cognition and places little to no importance on social and personal factors (DeCapua, Marshall, & Frydland, 2018). Within TLT, there remains an emphasis on a particular experience to trigger the assessment, which may produce a transformation in an individual's knowledge (Blewitt, J. C., Blewitt, J. M., & Ryan, 2018). As in SCT, self-efficacy is a key factor within transformational learning because an individual with a higher level of self-efficacy is more likely to perform actions, which may result in a transformational event (Blewitt et al., 2018).

TLT aligns with SCT in terms of self-efficacy increasing the likelihood of performing an action and that the results of an actual experience can shape future behaviors. Also, TL and SCT share similarities in terms of outcome expectation because based off the result of an experience from a TLT perspective, the individual will account for this result in future similar experiences. TLT places emphasis on the individual as an agent, but ignores that social learning, and that the triadic factors influence knowledge acquisition, which is related to mechanisms organizations utilize to implement SETA programs. TLT does not explain how individuals learn through social observation, and that internal and behavioral factors contribute to the overall learning process. TLT is strongly contingent on the individual going through the experience, rather than learning from other individual's experiences.

SCT provides a good framework to analyze education, training, and awareness programs, but there are several limitations that organizational IT leaders must consider regarding SCT. Firstly, the strength between the relationship of personal, behavioral, and environmental factors is not equal to each individual and may change over time. (Font et al., 2016). Due to the fact that personal and behavioral characteristics may be influenced differently over time or due to a specific set of circumstances, the effectiveness of SETA programs may change for each individual of the organization at different times. SCT implies that the environment influences human behavior and learning significantly (Rubenstein, Ridgley, Callan, Karami, & Ehlinger, 2018). This is an important note because organizational cultures are different from each other and may be different across various industries. The factors of the triadic reciprocal determinism model and relationships between each other are influenced by self-efficacy, self-regulation, social learning or modeling, and outcome expectancy (Lowry et al., 2017). This is important to note because organizations place different levels of importance on these factors. For example, organizations may place different levels of importance on social learning or implement different punishments for information security violations, which in turn, influences the strategies used to implement organizational SETA programs.

Cybersecurity Awareness and Training

The purpose of cybersecurity awareness and training programs is to ultimately protect an organization from the harm posed by cybersecurity vulnerabilities, threats, and attacks by improving employee education, training, and awareness (Beuran et al., 2018a). A vulnerability is a potential weakness within a system that may be exploited to cause undesired outcomes (Sheehan, Murphy, Mullins, & Ryan, 2018). A cyber threat is the potential occurrence of an undesired event, such as data loss or malicious inject (Wang & Johnson, 2018). An attack consists of actions attacking the security mechanisms of a system, which is a result of conducting vulnerability discovery, then exploitation development, followed by exploitation delivery, and repeating this process (Huang, Siegel, & Madnick, 2018). Cybersecurity awareness and training programs are intended to inform, educate, and frame human behavior to understand the potential harm that they and the organization face and how to protect themselves and the organization's information systems and data.

Cybersecurity awareness refers to the practices and policies utilized to improve overall cognizance of cyber-related vulnerabilities, threats, and attacks, from both an intentional and unintentional perspective (Berkman et al., 2018). Protecting an organization’s information systems and data is a shared responsibility with every member of the organization, and cybersecurity awareness is an important component in developing an employee’s understanding to know how to protect the organization (Kim, 2017). Users are presented with key decisions throughout their day, which may impact the security posture of an organization, such as revealing critical information in a social engineering attempt or clicking a link presented in a phishing attempt and it is their awareness that may prevent being exploited (Kim, 2017). Overall, cyber awareness programs are necessary to ensure the safety of the user, and in turn, protect the information systems that they are utilizing (Balhara, Harshwardhan, Kumar, & Singh, 2018). Cybersecurity awareness is a critical initiative to ensure users are mindful of the problems residing in cyberspace that may negatively impact the organization or the user.

Cybersecurity training refers to the process of conveying how to perform an action or set of actions through activities to transfer skills to protect against cyberattacks (Beuran et al., 2018b). Training through exposure within the domain of information security is a necessity in educating users in cybersecurity compliance and principles (Park, E., Kim, & Park, S., 2017). The overarching organizational program designed to reduce the number of information assurance events through employee education is also known as SETA (Yoo et al., 2018). SETA is the combination of cybersecurity education, awareness, and training, with the intent of supporting the organization’s initiatives to protect employees, and organizational information systems and data from intentional or unintentional compromise (Yoo et al., 2018). Overall, an organization educates its workforce on cybersecurity-related policies, procedures, and tactics to reduce the risk to the organization's information systems and data from malicious activity.

The manner in which SETA is designed and implemented within an organization is dependent on the industry and the laws and regulations surrounding it. In the United States, the strategic vision of cybersecurity awareness and training is provided by the National Initiative for Cybersecurity Education (NICE) (Kortjan & Von Solms, 2014). NICE is a collaborative effort between government, academia, and the private sector focused on cybersecurity education, awareness, and training for organizational use (Hodhod, Wang, & Khan, 2018). In fact, the NICE framework is intended to serve as a baseline for organizational use in respect to cybersecurity awareness and training (Coulson, Mason, & Nestler, 2018). NICE consists of seven major categories, which are made up of abilities, knowledge, and skills subcategories to guide organizations on SETA initiatives (Coulson et al., 2018). The specialty area of training, education, and awareness is associated with the "Oversee and Govern" category of the NICE Cybersecurity Workforce Framework (Dawson & Thomson, 2018). National direction, such as governmental regulations, influence industry regulations (Kabanda, Tanner, & Kent, 2018). Different industries, such as healthcare, finance, business, and education are concerned with different forms of sensitive data and must be protected according to specific regulations and practices (Pendley, 2018). National-level initiatives form the foundation of industrial regulations, and cybersecurity awareness programs must account for industry-specific guidelines and national level directives to appropriately protect organizational information systems and data.

Various industries that maintain and utilize sensitive information must abide by specific regulations and appropriate practices, which need to be taught effectively to promote better cybersecurity practices. The “Training, Education, and Awareness” (TEA) specialty area of “Oversee and Govern” is under-represented in terms of available training resources for security professionals (González-Manzano & de Fuentes, 2019). Passively communicating and educating users on proper cybersecurity practices must address more than warnings of inappropriate actions but must use appropriate teaching methods to maximize individual learning (Alohali, Clarke, & Furnell, 2018). Improving overall organizational awareness of appropriate regulations is an important component of protecting organizational information systems and data (Pendley, 2018). Industry-specific regulations include the Gramm-Leach-Bliley Act (GLBA) and Financial Information Security Management Act (FISMA) within the financial industry, the Health Insurance Portability and Accountability Act (HIPAA) within healthcare, and the Family Educational Rights and Privacy Act (FERPA) within education (Pendley, 2018). The European Union’s General Data Protection Regulation (GDPR), which is concerned with protecting the personal information of European citizens and also impacts organizations within the United States (Falco, Noriega, & Susskind, 2019). Additionally, the Payment Card Industry Data Security Standard (PCI DSS) imposes regulations specific organizations that maintain credit card information (Catota, Morgan, & Sicker, 2019). Industries from various domains are mandated to perform specific actions and maintain standards to protect organizational information systems and data based on regulatory guidance. Organizations can promote improved cybersecurity practices by educating employees on laws and regulations, and may need to focus on the further development of underdeveloped SETA programs.

Properly implemented and managed cybersecurity awareness and training programs contribute to the success of organizations and incur several benefits. The implementation and disclosure of cybersecurity awareness and training programs have demonstrated a $2.30 increase in stock price in firms overseen by the Securities Exchange Commission (SEC) (Berkman et al., 2018). SETA programs contribute to a manager's ability to properly assess the cybersecurity risks within their organization and to properly allocate necessary resources, which further protects stakeholders (Jalali, Siegel, & Madnick, 2019). Small-to-medium sized businesses reduce the risk of falling victim to cybercrime by properly implementing SETA programs (Bada & Nurse, 2019). Cybersecurity awareness and training programs within the domain of healthcare may reduce cybersecurity risks through unintentional user behavior and improve equipment availability (Schwartz et al., 2018). The proper function and availability of healthcare equipment due to a reduction in cyber incidents may be enhanced through SETA programs, which avoids patient harm, further injury, or even death (Schwartz et al., 2018). Organizational cybersecurity and awareness programs are not meeting requirements due to several reasons (He & Zhang, 2019). The effective design and implementation of SETA programs may incur significant benefits to business operations, promote protections to stakeholders, and enhance customer experiences, but SETA programs are not achieving the goals of organizational leaders.

Organizations have difficulty providing effective cybersecurity and awareness training programs due to the resources required to educate employees on a constantly changing subject. End-users must be able to assess, identify, and properly report phishing emails to designated organizational representatives, but employees continue to inadequately achieve these objectives (Miranda, 2018). Employees are inadequately trained to evaluate phishing attempts because there is a lack of complete training programs addressing phishing awareness entirely (Miranda, 2018). Educating employees on dynamic attack vectors such as social engineering is difficult due to the constantly changing strategies of malicious actors (Aldawood & Skinner, 2019). Furthermore, organizations have difficulty providing cost-effective training for dynamic attack vectors, which places an economic constraint on SETA programs (Aldawood & Skinner, 2019). Organizations are conflicted with the return-on-investment of cybersecurity measures and awareness programs (de Bruijn & Janssen, 2017). Findings from the Global Security Awareness Report from SANS highlighted that poor employee engagement, problems with training time, and inadequate resources negatively impacted organizational SETA programs (Sabillon, Serra-Ruiz, & Cavaller, 2019). Organizations are faced with a difficult challenge of educating employees on a rapidly changing domain, and organizations may only have limited resources available or lack the desire to allocate necessary resources to protect organizational information systems and data.

An organization’s culture and the belief of the employees, including leadership actions, contribute to an organization’s SETA program effectiveness. Ricci et al. (2018) determined that employees are willing to undergo additional cybersecurity awareness training, but being provided a time that does not conflict with other obligations was an employee concern. Cases exist in which organizations assume that the technology alone will protect the organizations information systems and data, therefore inadequately investing in employee education and awareness (Hadlington, 2017). Overall, an organization’s cybersecurity culture is related to an employee’s cybersecurity awareness (Flores & Ekstedt, 2016). The guidance and actions taken by leadership within an organization are directly correlated to the cybersecurity awareness of employees (Flores & Ekstedt, 2016). Organizations that waive employee punishment of small information assurance infractions increase the likelihood that an employee will commit a graver offense in the future (Hess & Cottrell, 2016). Several factors related to an organization’s implementation of SETA programs directly impact overall employee effectiveness. Organizations must emphasize leadership buy-in, afford greater resource availability to support SETA programs, and foster a culture that values cybersecurity.

Information security is one of the top challenges and priorities of organizational IT leaders. Organizational IT leaders are concerned with information security and rate it as one of their top concerns (McLaughlin & Gogan, 2018). According to McLaughlin and Gogan (2018), the damages incurred by a security incident may be dire, and examples of damages include damage to reputation, impact to overall business operations, a monetary loss. Contributing to the criticality of information security to the organization is the importance and value of an organization’s data (Kolkowska, Karlsson, & Hedström, 2017). To reduce the likelihood of an information assurance event or compromise, adherence to an organization’s information security policy is a vital characteristic of a healthy organizational cybersecurity posture (Bauer, Bernroider, & Chudzikowski, 2017). To improve adherence to organizational information security policies, organizational IT leaders rely on implemented SETA programs to educate their employees on methods to protect organizational information systems and data from compromise (Bauer et al., 2017). Ensuring compliance to an organization’s information security policy is critical to the protection of the organization, and the success of an organization’s SETA contributes to the optimal function of the organization while limiting the negative impacts associated with compromise.

Human Factor in Cybersecurity

Organizations utilize a layered approach to protect information systems and data from unauthorized access, and it is important for organizational leaders to implement a security solution that addresses technical solutions and addressing the human factor, together. Organizations utilize a combination of technical and nontechnical security measures to protect information systems and data through a multi-layered, defense-in-depth strategy (Conteh & Schmick, 2016). According to Conteh and Schmick (2016), a defense-in-depth strategy consists of security policies, network guidance, audits and compliance, technical solutions, physical security, and SETA. The weakest layer in an organization’s defense-in-depth strategy is related to the user’s unawareness of cybersecurity best practices, cybersecurity threats, and vulnerabilities (de Bruijn &

Janssen, 2017). Organizational cybersecurity efforts are strongly reliant on software solutions, but human interaction with information systems and software presents the greatest opportunity for malicious actors to exploit and infiltrate information systems of an organization (Sawyer & Hancock, 2018). With the emphasis on software and algorithms to protect an organization's information systems and data, it is paramount that organizational leaders address the human factors of cybersecurity to protect the organization.

Organizations must utilize an appropriate combination of technical and nontechnical cybersecurity solutions to protect an organization's information systems and data. The human aspects of an information security model describe the relationships between individuals, organizations, and intervention factors with the behaviors, education, and awareness related to information security (McCormac et al., 2017). Both IT professionals and all remaining employees of an organization influence the level of risk from a cybersecurity perspective (King et al., 2018). In many instances, the defense against information assurance events is solely through software (Sawyer & Hancock, 2018). An analysis of the human factor within an organization's cybersecurity program is a necessary complement of an organization's hardware and software security measures (Ani, He, & Tiwari, 2019). Certain attack vectors, such as social engineering, can only be prevented through appropriate actions from the user because no technical solution can prevent a user from providing sensitive information to a malicious actor over the phone (Ghafir et al., 2018). Although technical security solutions are critical in protecting an organization's information systems and data, the importance of addressing the human factor cannot be ignored because in some instances, it is the only measure that can protect an organization from intentional or unintentional harm.

In cases, the method of access to an organization's information systems and data is through its employees, which warrants attention being placed on educating employees on potential cybersecurity risks. Attack vectors and malicious actors rely on the ignorance of employees to gain unauthorized access (Ghafir et al., 2018). When employees are aware of the potential cyber risks, they are less likely to be exploited or introduce malicious cyber activity within the organization (Phillips & Tanner, 2019). A critical error common to organizations is that cybersecurity awareness and training leads assume that conducting the training once on specific topics suffices to protect the organization (Phillips & Tanner, 2019). Cybersecurity awareness and training should be incorporated into daily tasks because 90% of training sessions are forgotten within one week (Ghafir et al., 2018). According to Ani et al. (2019), 97% of industrial workforce participants did not possess any security training. This is believed to be the result of the organization being comfortable with the risk incurred from the level of employee cybersecurity proficiency or a lack of understanding of how quickly the cybersecurity domain changes (Ani et al., 2019). Employee cybersecurity education programs must be carefully constructed to train on specific risks and in a manner that promotes retention of knowledge. Organizations must appropriately address the content and quantity of cybersecurity education.

The cybersecurity knowledge of an employee is one of the strongest predictors of appropriate cybersecurity behavior, which ultimately benefits the organization's cybersecurity posture. An individual’s level of information security awareness is related to knowledge, attitude, and behavior (Parsons et al., 2017). Individual’s self-efficacy and level of experience in the field of information security are strongly related to the behaviors of an individual from a security standpoint (Blythe & Coventry, 2018). Employee cybersecurity knowledge was strongly related to security behavior with a correlation of 0.73 from an information security awareness study of 505 employees (McCormac et al., 2017). Employee knowledge shares one of the strongest relationships to employee cybersecurity behavior (McCormac et al., 2017). A lack of cybersecurity knowledge has been demonstrated by employees from several domains, which increases the likelihood of exploitation and potential compromise of organizational information systems (Yan et al., 2018). Some organizations foster an environment in which employees are not provided adequate training and must focus their efforts on increasing employee knowledge of information security principles, which in cases, provides the greatest benefit in protecting the organization from cybersecurity risks.

In order to promote positive cybersecurity behavior, the attitudes of employees must be positive, and their beliefs accurate, which is promoted by indirectly addressing cybersecurity attitudes. Employees are more likely to engage in risky cybersecurity behavior if they possess an incorrect or poor perspective on information security (Hadlington, 2017). Employees have been shown to incorrectly believe that the technical solutions of an organization will protect any action they take on an information system (Hadlington, 2017). An employee’s understanding of why they must abide by organizational cybersecurity principles or their attitude is strongly related to their overall level of knowledge in information security (McCormac et al., 2017). Additionally, an employee possessing a positive attitude towards cybersecurity, increased their likelihood of adopting organizational cybersecurity practices and policies (Ani et al., 2019). Cases exist in which the delta between employees of an organization that are aware of an organization's information security policy and those that are not are significant (Li et al., 2019). To improve the organization's overall cybersecurity awareness, leadership must offer regular information security training throughout the year, within an understandable format (Li et al., 2019). Organizational leadership must implement a SETA program that educates employees on a regular basis and incorporate why employees should engage in specific cybersecurity behaviors, rather than just how to perform those actions. Additionally, to decrease the level of risky behavior and decrease the likelihood of information system and data compromise, organizational SETA programs should address the limitations of technical solutions in protecting the employee and organizational assets.

The main concern of organizational SETA programs is promoting more appropriate behavior among employees, and ultimately lower the risky behavior engaged. The overall success of an organization's cybersecurity program is directly related to the behavior of its employees, and issues with organizational cybersecurity programs are the result of human interaction (Öğütçü, Testik, & Chouseinoglou, 2016). Organizations should not consider all users as a single group, but rather, group users based on their perceived level of risk (Yan et al., 2018). Employees that are unaware of cybersecurity risks or share a negative attitude of cybersecurity have a higher likelihood of engaging in risky and inappropriate behavior (Hadlington, 2017). Also, lower levels of cybersecurity awareness increase the likelihood of risky behavior on different technological platforms, such as cellphones (Koyuncu & Pusatli, 2019). Inappropriate employee behavior and practice on online social networks at work, such as Facebook, increases the risk to organizational information systems and sensitive data (Terlizzi, Meirelles, & Viegas Cortez da Cunha, 2017). Furthermore, ineffective SETA programs increase the likelihood of behaving inappropriately and falling victim to social engineering attacks (Miranda, 2018). Öğütçü et al. (2016) demonstrated that more employees are aware of cybersecurity risks, the more conservative they were in their behavior. The goal of organizational SETA programs is to change and maintain employee behavior so that risky actions are limited across all information system platforms. Furthermore, SETA programs should focus on educating employees, as different groups, on the dangers of behaviors that may be exploited by malicious actors on all software applications, including social media, to prevent harm to the employee and the organization.

Organizational SETA programs should avoid framing SETA programs as a "one-size-fits-all" approach because personal characteristics influence cybersecurity awareness and behavior. Personal characteristics of employees, such as upbringing, demographics, and cultural background, influence cybersecurity behavior (Yan et al., 2018). Men demonstrated higher levels of cybersecurity self-efficacy and behaviors than women (Anwar et al., 2017). Older employees generally demonstrated more positive cybersecurity attitudes, which may be related to their increased level of conscientiousness (Hadlington, 2018). Younger employees also demonstrated higher levels of risky cybersecurity behavior than older employees (Hadlington, 2018). In addition to women demonstrating less optimal cybersecurity behavior, women were less proactive in improving cybersecurity awareness (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). An employee's personality also impacts their behavior in terms of self-reporting cybersecurity issues, more specifically, their levels of conscientiousness and openness (Shappie, Dawson, & Debb, 2019). When organizational leaders design and implement cybersecurity awareness and training programs, they must analyze the demographics, personal characteristics, backgrounds, and personalities of their employees to design an effective SETA program.

Inappropriate behavior of employees may result in grave consequences to the organization. The compromise of the Office of Personnel Management (OPM) and its stored background checks was the result of compromised user credentials (Gootman, 2016). The OPM security breach caused grave damage to United States national security because it negatively impacted intelligence operations and disclosed sensitive information of United States government employees (Gootman, 2016). The Target hack of 2013 was also the result of compromised user credentials (Plachkinova & Maurer, 2018), which resulted in a $10 million lawsuit settlement, high costs to network infrastructure, and significant reputational damage (Jeong, Lee, & Lim, 2019). The Equifax hack was the result of poor, human-induced, security practices, which resulted in losses to the company in excess of hundreds of millions of dollars, but increased likelihood of consumer fraud due to the loss of over 140 million customers (Wang & Johnson, 2018). By increasing cybersecurity awareness knowledge of employees, organizations can expect improved cybersecurity behavior and a lower likelihood of compromise (McCormac et al., 2017). Intentional and unintentional user behavior may result in significant compromises and consequences to the organization and its customers, which can be prevented through cybersecurity awareness and training programs.

Security Education, Training, and Awareness Research

Research on organizational SETA programs across various domains and geographic locations have been performed. Molok, Ahmad, and Chang (2018) conducted a multiple case study of a university, statutory body, public service organization, and security firm with Malaysia to examine information security due to online social networking (OSN) leakage. Organizations may mitigate risks due to OSN information security concerns by implementing a SETA program, and that awareness of the specific threat is promoted among employees in a frequent and consistent manner (Molok et al., 2018). Examination of three cases from the financial sector within Central Eastern Europe determined that organizations should utilize various forms of media and training approaches to promote information security awareness (Bauer et al., 2017).

The research from Bauer et al. (2017) determined that information security leaders should strive to implement frequently occurring training sessions, customized to specific user groups to promote improved cyber behavior. Nasir, Arshah, Hamid, and Fahmy (2019) conducted an exhaustive search of eight databases and analyzed 79 studies on information security culture and determined that an organization's culture towards information security influences the security of the organization. It was also determined that no consensus on exact factors of culture could be determined to fully describe information security culture, but the incorporation of SETA was correlated to a positive cyber culture (Nasir et al., 2019). A cross-cultural examination of information security behavior from various industries between the United States and Ireland, consisting of 19 semistructured interviews, demonstrated that organizational leaders that valued cybersecurity implemented SETA programs and technical controls more stringently than leaders that did not value information security (Connolly, Lang, & Wall, 2019).

Based on the review of prior research on SETA programs, cyber behavior, and organizational information security strategies from this literature review, I hypothesize several potential themes from my data collection. First, I hypothesize that consistent and frequent security education and training to employees will be a theme. Second, I hypothesize the use of various training methods and media will be a theme. Third, I hypothesize that senior leader cybersecurity emphasis and importance will be another theme.

Transition and Summary

This section included background and review of the literature regarding SCT, SETA programs, and the human factor of cybersecurity. The cybersecurity behavior of employees is a critical component of the organization's overall cybersecurity program. The design and implementation of organizational SETA programs must not only address the technical solution but must ensure that the cybersecurity knowledge and attitudes of employees are appropriately addressed. By ensuring an appropriate level of knowledge and a positive attitude towards cybersecurity, the organization may better promote positive and less risky cybersecurity behaviors from employees. By ensuring that cybersecurity knowledge, attitude, and behavior are addressed, an organization can increase its likelihood of protecting organizational information systems and data. Therefore, organizational leaders must be able to provide effective SETA programs to ensure that the organization, its employees, and its customers are protected.

SCT assumes the perspective that human beings are agents, which are influenced by their environment, individual factors, and behavioral factors. Furthermore, the triadic reciprocal determinism model is influenced by the constructs of self-efficacy, self-regulation, social learning or modeling, and outcome expectancy. Improving self-efficacy and self-regulation through organizational SETA programs and policy can promote safer cybersecurity behaviors and better protect organizational information systems and data. Improved knowledge and awareness can be promoted through social learning and enforced through the use of outcome expectation. An organization's SETA program is a critical component in supporting a defense-in-depth strategy. Organizational leaders must acknowledge the importance of SETA programs and support the implementation and execution of educational programs to ensure the protection of the organization, the employees, and customers.

Section 2 includes an outline of my intent, role of the researcher, research design, population sample, data collection techniques, and data analysis techniques used for the study of organizational cybersecurity awareness and training program design and implementation. Section 3 will include an overview of the study and a presentation of findings from the analysis of the collected data. Section 3 will also include the discussion of applications of the research to professional practice, the implications of social change, and the presentation of recommendations, reflections, and conclusions resulting from this research study.

Section 2: The Project

In this section, I will restate the purpose of this study and discuss the research and the main reasons for pursuing a qualitative multiple case study. Section 2 includes the purpose of this study, a discussion of the role of the researcher, an explanation of the participants, the research method and design, the population and sampling, and ethical research. Section 2 also includes the data collection methods, data collection techniques, data instruments, and data analysis. The end of Section 2 includes a discussion of reliability and validity of data.

Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore strategies used by corporate IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data. The population consisted of hospitality IT leaders including the CEO, COO, CIO, CISO, general managers, and IT directors in Hampton Roads, Virginia, who have implemented cybersecurity awareness and training strategies within their organization. Implications for positive social change include the potential improvement to awareness and training programs that contribute to better cybersecurity practices, which may protect national security, guard critical infrastructure, and prevent disclosure of sensitive information due to compromise that may harm citizens. The improvement of cybersecurity awareness and training also has the potential of protecting these same employees and their families, including children at home as a result of effective education. The lessons learned at work through awareness and training programs can be retaught at home, which may protect families from crime and nefarious intent. There is also the potential to contribute new knowledge and insights that may lead to discovery, such as new strategies and tactical level implementations that may protect organizations from damaging events and ultimately improve the cybersecurity culture at a macrolevel.

Role of the Researcher

In this qualitative study, I was the primary research instrument in collecting data. One of the researcher's objectives when performing research is to collect accurate and quality data. When performing a qualitative case study, the researcher will thematize, design the study, develop interview questions, conduct and record the interview, transcribe the recordings, analyze the data, verify the data analysis, and report the findings, all while protecting the participant and data (Sutton & Austin, 2015). I developed the interview questions, coordinated all efforts to solicit participants that satisfy eligibility requirements, collected and reviewed the data, conducted any necessary follow-ups to ensure accuracy of data to promote quality, and reported the findings. In this study, the interview questions were open-ended in order to promote open and detailed dialogue, as suggest by Roulston (2018). During the interview process, I recorded the responses and observations of the interviewee. Observation is a frequent method of data collection within a qualitative study, and a researcher must focus their efforts during observation because it is difficult to observe everything (Moser & Korstjens, 2018). Participant observation is a dynamic process, which requires constant evaluation of the setting, what observation was made, how does it occur, and why does it happen, which provides insight into the participant's feelings (Moser & Korstjens, 2018).

In addition to conducting interviews, I examined documents from the organization that the interviewee is employed at. I was critical in my efforts to focus my observations on promoting high-quality data collection. I have 15 years of IT experience, and of those 15 years, 11 years involve work within the domains of cybersecurity and information assurance. I also have 4 years of experience teaching computer science and cybersecurity principles. I have no relationship, nor contacted any participant, prior to receiving official approval from the Walden University Institutional Review Board.

The Belmont Report (National Institutes of Health, 1979) served as the ethical foundation and standards for my study by providing the ethical framework by which I operated by while conducting my study. I strictly adhered to the ethical principles and applications delineated in the Belmont Report, which included treating all participants with respect and protecting participants. Protecting participants explicitly implies protecting participants from any form of harm, which includes maintaining their privacy and confidentiality throughout the study (National Institutes of Health, 1979). Additionally, I provided participants with all necessary information to make an educated, informed and voluntary agreement to participate by providing full and honest disclosure to all participants as recommended by the National Institutes of Health (1979).

Researcher bias is an inherent concern when performing a qualitative study and must be mitigated for to ensure and promote the validity and quality of a qualitative study (Johnson, Adkins, & Chauvin, 2019). Researcher bias may be introduced due to personal experiences, views of the world, various perspectives, and societal upbringing (Wadams & Park, 2018). Researchers must exercise caution and utilize sound practices when collecting, analyzing, interpreting, and reporting qualitative data in order to mitigate against bias (Rettke, Pretto, Spichiger, Frei, & Spirig, 2018). Bias introduced by researchers may negatively impact the validity of a study, and researcher self-awareness is critical in reducing bias (Cypress, 2017). Self-assessment and documentation of preexisting assumptions, prior experiences, and viewpoints, followed by comparing this self-evaluation to analyze data to ensure that analysis is not being impacted by assumptions decreases researcher bias (Bayne & Branco, 2018). I mitigated personal biases by taking a self-inventory of my prior education, experiences, values, and perspectives in relation to this study. I utilized open-ended interview questions to capture the participant's perspective on the phenomenon. Furthermore, I did not delineate or impose my personal views, experiences, and beliefs on the subject in order to avoid influencing the data collected and avoid bias throughout this study.

I utilized an interview protocol as a framework while conducting interviews for this study. A well-constructed interview protocol is critical in promoting high-quality data within a qualitative study (Yeong, Ismail, R., Ismail, N., & Hamzah, 2018). According to Yeong et al. (2018), it is paramount to align the interview protocol with the research question. Within the framework of an interview protocol, it is beneficial to apply socially accepted rules to promote open dialogue, focus on gaining information relevant to the research question, draft a script to aid in the execution of the interview, and utilize follow-up questions (Castillo-Montoya, 2016). The interview protocol proposed by Rivard, Fisher, Robertson, and Mueller (2014) consists of five steps: building rapport, avoid asking leading questions, avoid interrupting the interviewee, allow for pauses between and during questions, and using follow-up questions to satisfy gaps in responses. I utilized the same interview protocol for all participants and asked nonleading, semistructured, and open-ended questions so that I ensured consistency throughout interviews. Additionally, my interview protocol focused on participant experiences while maintaining self-awareness of personal assumptions to minimize personal bias. Participants were provided adequate time to respond to interview questions and provided thoughts on cybersecurity awareness and training strategies to protect organizational information systems and data. I used follow-up questions as necessary to ensure participants elaborate on their responses in relation to the research question. As a result, interviews will be the primary instrument for exploring participant's cybersecurity awareness and training strategies to protect organizational information systems and data. The interview protocol is delineated in Appendix A and includes the interview questions for this multiple case study.

Participants

In this multiple case study, I used a contact for each organization to act as a mediator and assist me in gaining access to potential research participants after Walden University IRB approval. A gatekeeper is a member of an organization, independent of the relationship with the researcher, that can solicit members within the organization to participate in the study (Peticca-Harris, deGama, & Elias, 2016). A gatekeeper can be an individual who can serve any position within the organization that may assist me in locating potential participants or be a participant themselves. The gatekeeper evaluated the participant eligibility for this study and provided a set of potential participants, if available. There may be scenarios in which organizational leaders may be reluctant to allow access to qualitative data and documents because they consider these sources as sensitive (Ivanova-Gongne, Koporcic, Dziubaniuk, & Mandják, 2018). Gatekeepers can improve the likelihood that researchers can gain access to the organization and qualitative data by reducing employee hesitations (Okumus, Altinay, & Roper, 2007). Hesitations may occur because a perceived outsider is querying employees and examining internal documents related to the research question (Okumus et al., 2007). I used a gatekeeper to assist me in gaining access to participants and organizational documents relevant to my study. I pursued gatekeepers that are members of the Virginia Beach Hospitality Association (VBHA), which incorporates the hospitality industry of Hampton Roads, Virginia.

Organizations that maintained a chief information security officer, or equivalent leader responsible for enforcing information security are more likely to implement an organizational SETA program (Kappelman et al., 2018). Organizations across various industries utilize various reporting structures to satisfy information security concerns, but top leadership, to include CEOs, CIOs, CISOs, CISO equivalent, or other designated agent maintain responsibility of the organization's information security program (Karanja, 2017). The age of information security leaders can vary from under 10 years of experience to over 21 years of experience (Na, Park, Yu, Kim, & Chang, 2019). The importance of information is strongly related to the security classification and restrictive nature of the data (Na et al., 2019). The eligibility criteria of participants are that they are an organizational leader with the designated responsibility of ensuring information security for an organization that processes or maintains sensitive data.

The process of establishing and maintaining a working relationship with participants consists of several steps. First, I requested that the gatekeeper forward my email invitation (see Appendix C) and consent form (Appendix D) to eligible participants. Gatekeepers are able to leverage their standing within the organization and trust with internal employees to coordinate participation with a research study (Amundsen, Msoroka, & Findsen, 2017). A gatekeeper possesses the influence to create access with research participants and promotes a working environment between the researcher and participant at a specific location (Lund, Panda, & Dhal, 2016). It is critical to create an environment between the researcher and participant that is not authoritative in order to promote a positive working environment (Råheim et al., 2016). After I received an email from the potential participant stating that they are willing to voluntarily participate in my research study, I coordinated a time and place to conduct the interview. I also offered to meet or discuss areas of concern with the participant prior to the interview, if applicable. If participants did not sign the consent form prior to the interview, I reminded them via phone or email to complete the consent form. Furthermore, I reminded participants via phone or email, and via the consent form, about the study's background, procedures, key terms, voluntary nature of the study, benefits, risks, and privacy surrounding the study. I did not begin any interviews until I had received consent from the participant.

Each participant had the opportunity to address any questions or concerns via email or phone prior to the commencement of the interview to ensure that they understand the study and are comfortable with proceeding. Developing trust between the participant and the researcher is a major factor in earning participant consent (Kongsholm & Kappel, 2017). The proper dialogue between researcher and participant, which addresses concerns, can build trust and improve the likelihood of consent (Sil & Das, 2017). Describing the benefits of research and reporting findings to participants, while also explaining the mechanisms in place to protect their privacy improves trust between researcher and participant (Goodman et al., 2017). During the scheduling of the interview and prior to conducting the interview, I described the interview process, the purpose of the study, and mechanisms to protect their privacy. I ensured that they are comfortable with the interview process and willing to proceed prior to commencing the interview. I reiterated the interview process with participants by referring to the interview protocol in Appendix A. I also reiterated to participants that participation in this study is entirely voluntary and that the personal information of the participant and any details regarding the organization will always remain confidential.

I developed and maintained a strong working relationship with participants founded on trust and transparency by creating an environment that fosters participant education and comfort. The researcher can increase trust between the researcher and participant by being transparent with informed consent and reiterating the methods that will be used to protect the participant (Hart-Johnson, 2017). Additionally, a give-and-take relationship between the participant and researcher is necessary to create a sense of depth, and true concern for the interests of the participant are needed to create an environment of trust (Leggett, 2018). Utilizing prolonged engagement and appropriately allocating time to build trust with participants, preparing for the interview, and becoming familiar with the interview location may promote credibility (Moser & Korstjens, 2018). I strived to develop and maintain the trust of all participants by ensuring their comfort, maintaining full transparency through every phase of the interview, and allocating the appropriate effort and time to build trust.

Research Method and Design

I performed a review of research methods that are suitable for this study with the intent of selecting the appropriate method for this study. I reviewed three research methodologies, which are qualitative, quantitative, and mixed methods (Levitt et al., 2018). The qualitative method provides increased flexibility in understanding a phenomenon (Lucero et al., 2018). Unlike a quantitative methodology, the use of qualitative methods may provide insights into the how and why of a phenomenon (Bush, Persky,& Amechi, 2019). After a critical review, I decided to utilize the qualitative methodology and exploratory multiple case study design to answer the research question.

Method

The goal of qualitative research was to explore and acquire a strong understanding of real-world problems by examining a phenomenon through participant experiences and rich data (Moser & Korstjens, 2017a). Qualitative data consists of static and dynamic forms of rich data, such as static text within documents and descriptions of rich, dynamic experiences (Bansal, Smith, & Vaara, 2018). Researchers are able to delve into and collect data-rich experiences and insights from participants in qualitative research (McHugh et al., 2019). Qualitative research is well suited to examine phenomena within a particular scenario and not about generalizing across a population (Singer et al., 2019). Data can be collected in qualitative research through interviews, focus groups, and observation (Saunders et al., 2018). Interviews performed in qualitative studies are beneficial in focusing efforts and acquiring great detail from participants regarding the how and why of implementing policies and strategies, which quantitative methods cannot accomplish (Lancaster, 2017). Furthermore, semistructured interviews are an approach in which key characteristics of the phenomenon in question can be focused on through explicitly coordinated questions throughout the interview to pursue greater detail (Gill, Stewart, Treasure, & Chadwick, 2008). The protocol of interviewing also affords the participants the ability to further elaborate on any topic they believe to be pertinent to their experiences (Yeong et al., 2018). I utilized a qualitative research method to explore the strategies used to implement cybersecurity awareness and training programs in Hampton Roads, Virginia, to protect organizational information systems and data. I examined various forms of rich data and conducted semistructured interviews to gain a deep understanding of the research question.

I considered utilizing a quantitative method for this study. Quantitative research focuses on collecting, manipulating, analyzing, and quantifying data (Goertzen, 2017). Quantitative research generally utilizes larger sample sizes and promotes generalizability across a population, but it fails to gather deeper explanations and experiences (Rahman, 2017). Quantitative research is not suited to provide insights into human experiences because of the inability to objectively quantify personal experiences (Bagdonienė & Zemblytė, 2005). My intent in this research study was to examine the insights into participant experiences about cybersecurity awareness and training strategies to protect organizational information systems and data. Quantitative research uses numerical data to analyze and deduce trends through statistical analysis (Queiros, Faria, & Almeida, 2017). Numerical data was not suited to provide details and a deep understanding of personal experiences in implementing cybersecurity awareness and training strategies to protect organizational information systems and data. Therefore, I did not utilize numerical data to explore the research question and explain the phenomenon. Also, researchers utilizing a quantitative research method will test against a null and alternate hypothesis (Roloff & Zyphur, 2018). My intent in this study was not to test against a null and alternate hypothesis, therefore, a qualitative study was not appropriate. For these reasons, a quantitative research method was not selected for this study.

I considered utilizing a mixed methods research method for this study. Mixed methods research combines components of quantitative and qualitative research in a specified manner within a single study (Regnault, Willgoss, & Barbic, 2018). A mixed-methods study should only be used when the data collected from both quantitative and qualitative methods are necessary to adequately answer the research question (Halcomb, 2019). Researchers leverage various degrees of qualitative and quantitative methods within a mixed-method study depending on the researcher's intent (Halcomb, 2019). Also, various degrees of quantitative and qualitative data analysis techniques are used in mixed-method studies (O'Sullivan & Howden-Chapman, 2017). Quantitative data analysis methods include descriptive, inferential statistical techniques, and multivariate analysis (O'Sullivan & Howden-Chapman, 2017). Due to the fact that quantifying data will not be required to answer the research question of this study, neither a quantitative nor mixed methods approach is necessary to complete this study. The purpose of this study was to collect data related to the personal experiences of the participants in regard to the strategies used to implement cybersecurity awareness and training programs to protect organizational information systems and data. As a result, a qualitative method was best-suited to acquire a deeper understanding of the strategies used to implement cybersecurity awareness and training programs.

Research Design

An exploratory multiple case study design was selected for this qualitative research study. Qualitative research design types include narrative, ethnography, narrative, and case studies (Squires & Dorsen, 2018). Multiple case study design is an approach to compare the findings of more than one case study (Ridder, 2017). A case study design may be used by a researcher to examine a phenomenon from the perspective of the participant in great depth (Ebneyamini & Moghadam, 2018). A case study approach is beneficial when conducting exploratory studies (Bosley, Appleton, Henshall, & Jackson, 2019). The use of semistructured interviews can be used to collect data within a case study design (Castka & Balzarova, 2018). I utilized an exploratory multiple case study design to obtain a deep understanding and explore the strategies used to implement cybersecurity awareness and training programs to protect organizational information systems and data. I conducted semistructured interviews to gain insight into the personal experiences of participants in regard to the strategies used for developing cybersecurity awareness and training strategies.

Case study research designs are very well suited to understand the how and why of a phenomenon (Fàbregues & Fetters, 2019). Furthermore, a case study approach allows for the opportunity for a researcher to examine complex phenomena and gain an understanding of the phenomena (Heale & Twycross, 2018). A case study design incorporates a detailed analysis of an individual and organization (Moser & Korstjens, 2017b). Also, qualitative case studies may incorporate the analysis of organizational documents to further analyze a phenomenon (Elias, Hendlin, & Ling, 2018). I utilized a multiple case study approach and include how and why related questions during participant interviews and during organizational document reviews to acquire a deeper understanding of the phenomenon. I selected a multiple case study design to explore the complex phenomenon of cybersecurity awareness and training strategies to protect organizational information systems and data. This multiple case study explored the strategies to implement SETA strategies utilized by organizational hospitality IT leaders at multiple organizations to protect organizational information systems and data by conducting interviews and examining company documents to gain a thorough understanding of the experiences of the participants.

I considered utilizing an ethnographic research design for this research study. Ethnographic research is intended to analyze a specific culture (Capous-Desyllas & Barron, 2017). I will explore the strategies used by organizational hospitality IT leaders to implement SETA programs, and I do not want to understand a particular culture. Data collection of ethnographic studies is mostly in the form of observing the group of individuals associated with the culture of interest and conducting informal interviews (Moser & Korstjens, 2017b). Researchers will deeply immerse themselves in a culture and observe the culture in their natural surroundings to learn about the group and culture (Jones & Smith, 2017). I used interviews and examined organizational documents during the data collection phase of my study and do not need to observe the individuals of a culture. Therefore, an ethnographic study was not suitable for my intended research.

I considered utilizing a phenomenological research design for this study. Phenomenology research consists of the primary characteristic of examining a phenomenon through the evaluation of lived experiences related to the phenomenon (Ghaffari & Lagzian, 2018). Two categories of phenomenological research are descriptive phenomenology and interpretive phenomenology (O'Halloran, Littlewood, Richardson, Tod, & Nesti, 2018). Descriptive phenomenology is focused on describing the lived experiences related to a phenomenon (O'Halloran et al., 2018). Interpretive phenomenology means that the researcher intends to understand the meaning and essence of the lived experience (Matua & Wal, 2015). The culture evaluated in a phenomenological study will have shared an experience (Molley et al., 2018). I did not select the phenomenological research design because I do not intend to understand how shared experiences of a culture implement strategies for SETA programs to protect organizational information systems and data.

I also considered utilizing a narrative research design for this study. The researcher utilizing a narrative approach examines past experiences through the personal accounts and stories of participants (George & Selimos, 2018). Narrative research approaches consist of an open dialogue between the researcher and the participant, in which the participant shares their experience through personal stories in verbal or textual format (Moen, 2006). Narrative research focuses on the stories presented by the participant about themselves or a particular event (Mohajan, 2018). The stories of participants are not solely constructed by facts, but by the meanings they interpret at the time, which influences the stories they construct (Shamir & Eilam, 2005). Ultimately, a narrative approach focuses on discovering and interpreting the meaning of stories presented by the participant (Nolan, Hendricks, Williamson, & Ferguson, 2017). Although participant stories regarding experiences may contribute to this study, it is not required to explore the strategies that organizational hospitality IT leaders utilize to implement SETA to protect organizational information systems and data. I focused on the strategies to implement SETA and organizational documents to understand the phenomenon instead of attempting to understand participant experiences through personal stories. Therefore, I did not select a narrative approach because it does not meet my intent for this research study.

I examined and included multiple sources of data in my research study in order to achieve data saturation. During the data collection process and interactions with participants, data saturation is achieved once no new information is produced (Saunders et al., 2018). Researchers will recruit participants throughout a study until no new information is produced, at which point data saturation has been achieved (Squires & Dorsen, 2018). A researcher will cease recruiting participants and reviewing other sources of data once data saturation has been achieved (Moser & Korstjens, 2018). Since I conducted a multiple case study, I interviewed participants from numerous organizations and evaluate organizational documents until no new information is produced. I will maintain a record and awareness of all collected data, and once I have determined that only redundant findings are being discovered, I will assess that data saturation has been achieved.

Population and Sampling

The population of my research study consisted of organizational hospitality IT leaders at several organizations in Hampton Roads, Virginia. Organizational IT leaders include positions such as a CEO, CIO, CISO, IT director, IT manager, or General Manager (Hickman & Akdere, 2018). I explicitly targeted organizations that maintain sensitive data and have implemented SETA programs. Selecting participants must be a deliberate process in which the researcher has access to such participants, and the participants possess the prerequisite knowledge and experience with the phenomenon (Moser & Korstjens, 2018). In qualitative research, it is important to deliberately select participants with characteristics that ensure the researcher can answer the research question (Cleary, Horsfall, & Hayter, 2014). The population for my research study was individuals that are responsible for the implementation of SETA programs within their organization and possess experience implementing cybersecurity awareness and training programs to protect organizational information systems and data.

The set of potential participants that make up the study population is produced by implementing inclusion and exclusion criteria (Martinez-Mesa, Gonzalez-Chica, Duquia, Bonamigo, & Bastos, 2016). Inclusion and exclusion criteria for participants is a critical component of research (Patino & Ferreira, 2018). Inclusion criteria refers to participant characteristics that are important to the researcher to answer the research question (Patino & Ferreira, 2018). Exclusion criteria refers to participant characteristics that may negatively impact the success of the research (Patino & Ferreira, 2018). Inclusion criteria is used to set constraints to promote a researcher's ability to focus on participants that may contribute to answering the research question (Magny-Normilus, Mawn, & Dalton, 2019). A set of inclusion criterion is necessary to focus my efforts on a specific population for this research study. The eligibility criteria for participants in this research study were (a) being over the age of 18 years old, (b) occupies an organizational hospitality IT leadership position for at least one year, (c) volunteers to share their experiences, (d) works at an organization that maintains sensitive data, and (e) possesses knowledge or perceptions of cybersecurity awareness and training strategies to protect organizational information systems and data.

I selected purposive sampling for my qualitative research study as the approach to obtain participants for my study. Purposive sampling means that the researcher uses their best judgment in selecting participants that can best answer the research question (Moser & Korstjens, 2018). Purposive sampling is beneficial in situations in which the researcher does not intend to generalize across a population (Fletcher & Friedel, 2018). Purposive sampling is a nonprobabilistic sampling method and also known as judgmental sampling, selective sampling, or subjective sampling (Sarstedt, Bengart, Shaltoni, & Lehmann, 2018). Purposive sampling is useful for situations in which the researcher seeks to deliberately examine participants with a specific skill set, expertise, or experience (Fletcher & Friedel, 2018). Purposive sampling is a nonprobabilistic sampling technique, which means the probability of selection of participants is unknown (Pandey, 2018). Purposive sampling promotes the ability to focus on participants that may provide data-rich content to answer the research question (Phoenix et al., 2018). The population of my study consisted of organizational hospitality IT leaders in Hampton Roads, Virginia, that were responsible for the implementation of SETA programs within their organization and possess experience implementing cybersecurity awareness and training programs to protect organizational information systems and data.

Sample sizes for qualitative research studies are reached once data saturation has been achieved (Saunders et al., 2018). Sim, Saunders, Waterfield, and Kingstone (2018) examined four approaches of attempting to determine sample size in exploratory qualitative studies a priori through rules of thumb, conceptual models, numerical guidelines, and statistics, but doing so is extremely difficult, and data saturation remains the threshold. Researchers must ensure that both data saturation has been achieved and that enough participants have been involved in answering the research question (Blaikie, 2018). The sample size of a qualitative study is not uniform and is dependent on the data needed to be gathered, and until data saturation has occurred (Mei & Lantai, 2018). The sample size for this exploratory multiple case study cannot be determined a priori and was dependent on achieving data saturation.

Saturation is the event in which little to no new information is produced during the data collection process of the study (Namey, Guest, McKenna, & Chen, 2016). Data saturation is the threshold in which qualitative studies are held in determining the appropriate sample size, but there is a dispute on the meaning of data saturation in the academic community (Hennink, Kaiser, & Marconi, 2016). Achieving data saturation is an iterative process performed by the researcher in which the researcher identifies concepts during data collection and acquires additional participants to explore these presented concepts until no new information is produced (Hennink et al., 2016). In a study performed by Hennink et al. (2016), they discovered that data saturation was achieved after nine interviews. The research by Namey et al. (2016) produced similar results in which data saturation was reached within eight interviews. Attempting to assign a general sample size guideline for data saturation is troublesome, especially with a loosely agreed-upon concept, but data saturation is considered achieved when the data collected is not contributing to answering the research question and is redundant (Sim, Saunders, Waterfield, & Kingstone, 2018b). Data saturation is achieved sooner in a small study (Fusch & Ness, 2015). Fusch and Ness (2015) state that performing interviews and focus groups contribute to achieving data saturation. Interviews achieve data saturation sooner than focus groups (Namey et al., 2016). The relationship between data saturation and collected several sources of data for triangulation is strong (Fusch & Ness, 2015). I conducted interviews in an iterative manner, examine several sources of data for triangulation, and continued until little to no new information or themes were produced.

In-depth interviews possess the characteristic of asking open-ended questions in order to understand personal experiences, opinions, and knowledge, with the ability to ask follow-up questions (Rosenthal, 2016). Interviews, including face-to-face interviews, are a highly utilized data collection method in qualitative research (McGrath, Palmgren, & Liljedahl, 2018). Interviews should be conducted at a time and location that is convenient for the participant with little to no disruptions (McGrath et al., 2018). The interview should be performed in a manner that promotes the comfort of the interviewee (Rosenthal, 2016). Protecting the respondent's privacy and maintaining the confidentiality of responses is a critical requirement of qualitative research (Fomby & Sastry, 2019). Interviewees locating a private setting to conduct interviews promote more accurate and detailed responses (Fomby & Sastry, 2019). Also, telephone interviews promote more open dialogue (Fomby & Sastry, 2019). The use of telephones as an interview medium is not a disadvantage even though nonverbal cues cannot be viewed (Oltmann, 2016). Researchers that do not examine nonverbal cues can incur some advantages because the researcher is not susceptible to misinterpreting nonverbal cues, and the interviewer is still able to notice deviations in response times and audible cues (Oltmann, 2016). Conducting interviews over video teleconferencing is an alternative to face-to-face interviews, which promotes open dialogue and allows for the observation of nonverbal cues (Irani, 2019). Video teleconference interviews should also be conducted in a private location with little to no interruptions (Irani, 2019). I conducted interviews with participants via face-to-face, video teleconference, or telephone. In cases in which the interview was performed via video teleconference or telephone, the participant was provided with an electronic copy of the informed consent form via email. The participants consented by responding to the email and stating, "I consent". The mode of the interview was decided upon by the interviewee to promote the comfort, privacy, and protection of the participant. The location of interviews will be conducted in a private location with little to no disruptions to either the interviewer or interviewee. In cases in which the interview was conducted via video teleconference or telephone, the participant and I coordinated a time and personally selected locations that ensure privacy and little to no disruptions after informed consent has been acquired. Prior to commencing the interview, I asked the participant if they were satisfied with the privacy of both of our locations at the time of the interview. Also, I asked the participant if they foresee the possibility of any interruptions during the scheduled interview, and if so, we will reschedule to a more opportune time.

As discussed in this section, interviews were conducted until data saturation had occurred. Interviewees were sourced from four cases. Each case consisted of at least one site within Hampton Roads, Virginia, with at least one individual in charge of information security. Multiple case studies consist of more than one case and allow researchers to evaluate and assess relationships from findings (Eisenhardt & Graebner, 2007). Multiple case studies are preferred in terms of determining relationships, and if two or more cases are able to demonstrate similar findings, then replication may be claimed (Zimmermann, Rentrop, & Felden, 2017). Multiple case studies related to information security management should have between two and six cases (Eisenhardt, as cited in Molok et al., 2018). For this qualitative, multiple case-study, I utilized four cases, each of which may consist of more than one physical site and may have had more than one individual responsible for information security.

Ethical Research

After I received IRB approval from Walden University, I invited potential participants to contribute to my research study via email. I contacted the gatekeeper via email or telephone prior to emailing potential participants. The email consisted of the informed consent document, the purpose of the study, a list of the interview questions for prior review, and my contact information to discuss any questions or concerns the participants may have. Informed consent is a process between the researcher and participant with the primary goals of describing the measures to protect the participant, their privacy, and delineating all appropriate information to the participant (Murray, Bierer, Hirschfeld, Klein, & Davis, 2018). I provided the informed consent form, as delineated in Appendix D, which denotes the background of the study, procedures, expectations of participating, voluntary nature of participating, risks and benefits of participating, disclosure of no compensation to participate, privacy details, questions and concerns, and providing consent. The ethical standing of the study can be improved through the informed consent process by ensuring that participants are given adequate and understandable information to make an informed decision (Alahmad, 2018). Also, it is critical to emphasize that participation is entirely voluntary during the informed consent process in order to maintain the autonomy of a participant (Pierre, 2018). It is highly recommended to receive a written and signed informed consent form and review the details of the consent form with the participant prior to conducting an interview (Nusbaum, Douglas, Damus, Paasche-Orlow, & Estrella-Luna, 2017). The informed consent form outlined the purpose of the study, the criteria for participating in the study, the researcher’s role in the study, the process for withdrawing from the study, protective measures of data, disclosure of incentives, and the intent to publish findings. Every participant was required to read and sign the informed consent form prior to participating in the study.

All participants were informed that their participation in the study is entirely voluntary and that they have the right to withdraw at any time with no consequence. This information was also be delineated in the informed consent document. I ensured that I maintained honesty and transparency with every participant and that they fully understood the informed consent process as well as the process to formally withdraw from the study. Adherence to the informed consent process is critical when conduction research with human subjects (Shepherd & Macklin, 2018). I did not offer any form of incentives to participants to participate in this study. Incentives have been shown to impact the informed consent process because participants may be willing to accept greater risk (Manton, Gauld, White, Griffin, & Elliott, 2019). The impacts on data quality when providing incentives are varied because some instances improve quality and others decrease data quality (McGonagle & Freedman, 2017). As a result, I will not offer any incentives to participants.

In order to maintain the highest level of ethical soundness and protection of participants, I adhered to all IRB legal and ethical regulations and requirements as delineated by Walden University. The identities and personal information of all participants and organizations participating in this study will be kept confidential. Two methods of ensuring the protection of participants are to anonymize the participant and secure the data collected. Pseudonyms can be used to protect the identities of participants (Butler, Copnell, & Hall, 2019). It is strongly recommended to store research data in a secure manner (Shelly & Jackson, 2018). Participants will be given a pseudonym such as P1, P2, and P3. Additionally, no personally identifiable information nor organization name will be used throughout this study. All data will be stored securely in accordance with IRB requirements as delineated by Walden University by storing all research data in a locked file cabinet. All electronic data will be stored on a password-protected, encrypted external hard drive. All collected research data on the external hard drive will be permanently destroyed, as well as any audio recordings and paper records after five years from the date of publication of this study as denoted in the “Ethical Research” section, Walden University IRB requirements, and informed consent (Appendix D).

Data Collection

Instruments

I was the primary instrument during the data collection for this research study. Within a qualitative study, the researcher is considered the primary data collection instrument (Clark & Vealé, 2018). Barrett (2007) states that the researcher’s knowledge base, outlook, and subjectivity during data collection is are important characteristics in completing a qualitative study. Primary methods of data collection within qualitative research include interviews, document analysis, and observation of participants by the researcher (Melin & Axelsson, 2016). It is critical that the researcher remain unbiased throughout all forms of data collection to ensure a quality qualitative study.

Interviewing of participants is a method of data collection within qualitative research. Conducting individual interviews provides participants with the opportunity to reflect internally and share their personal experiences (Mavhandu-Mudzusi, 2018). Semistructured interviews are an approach in which key characteristics of the phenomenon in question can be focused on through explicitly coordinated questions throughout the interview to pursue greater detail (Gill et al., 2008). The interview questions will be open-ended in order to promote open and detailed dialogue, as suggest by Roulston (2018). Conducting semistructured interviews in a one-on-one setting with participants is an ideal method in collecting data for this qualitative research study.

The use of interview protocols promotes reliability within a qualitative study. The interview protocol proposed by Rivard et al. (2014) consists of five steps: building rapport, avoid asking leading questions, avoid interrupting the interviewee, allow for pauses between and during questions, and using follow-up questions to satisfy gaps in responses. Utilizing an interview protocol is a strategy that may improve reliability (Wixted, Mickes, & Fisher, 2018). An interview protocol promotes a consistent interview process throughout the research study and increases the overall effectiveness of data gathering (Yeong et al., 2018). A copy of the interview protocol is included in Appendix A, and a copy of the original interview questions are located in the Research Question section of this study. I utilized an interview protocol to maintain consistency throughout this qualitative research study. Pre-interview activities will consist of a personal introduction, verification of proper completion of informed consent forms, disclosure that the interview is recorded, and review of study confidentiality. The interview began with turning on the recording device, then introducing the researcher, and identifying and stating the participant's code with date and time. Afterward, I commenced the interview and ended with asking the participant if they have any additional inputs they would like to disclose. At the end of the interview, I stopped the recording device. The post-interview process included an explanation of the member checking process, scheduling a follow-up meeting to validate data collected and interpretations from the interview, thanking the participant for their time, and providing the participant with my Walden University contact information.

Written notes and observations are beneficial augmentations to interviews. Utilizing note-taking during an interview reminds participants that they are undergoing an academic interview (Jentoft & Olsen, 2019). Additionally, the gap in time created from note-taking provides an additional opportunity for participants to reflect further and possibly provide more detail (Jentoft & Olsen, 2019). Participant observation is a dynamic process, which requires constant evaluation of the setting, what observation was made, how does it occur, and why does it happen, which provides insight into the participant's feelings (Moser & Korstjens, 2018). Maintaining notes of participant responses and observations are critical components of data collection because it promotes the gathering of rich data (Phillippi & Lauderdale, 2018). Following transcription, notes taken throughout data collection should be incorporated to add nonverbal content (Phillippi & Lauderdale, 2018). Transcription allows for repetitive review to verify data saturation and data analysis for theme discovery (Sugihara, Fujinami, Jones, Kadowaki, & Ando, 2015). Interviews will be transcribed with additional notes added to create detailed descriptions. Each interview was transcribed within 14 days and checked for accuracy. The use of semistructured interviews and participant observation with note-taking was utilized to improve reliability, validity, and overall quality of the research study.

Member checking is a key method in validating data collected and interpretations made from data collection. Member checking provides participants with the opportunity to verify and correct any misinterpretations from data gathering, which validates the correctness of the data (Iivari, 2018). Member checking promotes triangulation within a qualitative study (Van Horne & Murniati, 2016). Agnew, Marks, Henderson, and Woods (2018) argue that an additional benefit of member checking is that it improves the quality of the study because participants can make corrections to inaccurate interpretations by the researcher or identify errors in data collection. Member checking is an effective method in ensuring the accuracy of data and interpretations, which promotes a higher quality study. I continued to member check with participants until they agree that the data collected, and interpretations accurately reflected their experiences.

A review of organizational documents promotes the analysis of a phenomenon and triangulation. Qualitative case studies may incorporate the analysis of organizational documents to further analyze a phenomenon (Elias et al., 2018). Documents serve as an additional data source that can be used for triangulation and support data collected from interviews (Siegner, Hagerman, & Kozak, 2018). Utilizing multiple data sources such as interviews and organizational documents allow researchers to conduct data triangulation and improve reliability and validity (Moser & Korstjens, 2018). I collected data through interviews and additional data sources, such as organizational documents to complete this qualitative research study.

Data Collection Technique

When conducting qualitative research, data sources include interviews, participant observation, direct observation, documents, and artifacts (Polkinghorne, 2005). Ethical principles and applications are delineated in the Belmont Report, which includes treating all participants with respect and protecting participants (National Institutes of Health, 1979). When conducting interviews, it is critical to retrieve initial approval from the participant, ensure that the interviewee's privacy is protected, and provide necessary conveniences for the participant (Bolderston, 2012). I acquired IRB approval and a memorandum of agreement from the organizations that participated in the study prior to collecting data. Once the memorandum of agreement was signed, I coordinated with the gatekeeper to acquire email addresses of organizational hospitality IT leaders that will participate in my research study. Once I acquired the email addresses, I sent out emails requesting permission to conduct interviews. Once permission was given to conduct interviews, I sent out information that delineated the research study and their ability to withdraw at any time. The letter of invitation for this research study can be located in Appendix C.

I conducted semistructured interviews, which allowed me to focus my efforts on the research question. There are benefits and disadvantages to utilizing semistructured interviews in a qualitative research study. Semistructured interviews are an approach in which key characteristics of the phenomenon in question can be focused on through explicitly coordinated questions throughout the interview to pursue greater detail (Gill et al., 2008). Open-ended questions within a semistructured interview promote open and detailed dialogue (Roulston, 2018). The disadvantage of semistructured interviews is that some participants will have difficulty engaging in open conversation, as well as be reluctant to share personal details (DeJonckheere & Vaughn, 2019). Conducting interviews over video teleconferencing is an alternative to face-to-face interviews, which promotes open dialogue and allows for the observation of nonverbal cues (Irani, 2019). Video teleconference interviews should also be conducted in a private location with little to no interruptions (Irani, 2019). Therefore, to provide convenience and comfort to participants, I conducted semistructured interviews over video teleconference or telephone.

Organizational document analysis was another data source for qualitative research. As with interviews, there are advantages and disadvantages to utilizing documents as a data source. The benefit of documents as a data source is that they can be referred to at any time and used to conduct data triangulation to improve reliability and validity (Moser & Korstjens, 2018). There may be scenarios in which organizational leaders may be reluctant to allow me to access qualitative data and documents because they consider these sources as sensitive (Ivanova-Gongne et al., 2018). For this study, I coordinated with the mediator to access organizational documents as a data source and ensured that the privacy of these documents is enforced. Document analysis included email, standard operating procedures, policies, instructions, and training material related to the research question.

After each interview was completed, the recording of the interview was transcribed within 14 days and reviewed for accuracy. Member checking provides participants with the opportunity to verify and correct any misinterpretations from data gathering, which validates the correctness of the data (Iivari, 2018). Member checking promotes triangulation within a qualitative study (Van Horne & Murniati, 2016). Agnew et al. (2018) argue that an additional benefit of member checking is that it improves the quality of the study because participants can make corrections to inaccurate interpretations by the researcher or identify errors in data collection. Providing participants with the opportunity to review transcribed interviews during member checking promotes research validity (Usman, 2018). To ensure accuracy, the transcribed interview was reviewed against the recorded interview. Additionally, the transcribed interview was member checked by the participant to ensure accuracy. The transcribed interview was only be used for this research study after the participant has verified accuracy. If the participant determined that the transcribed interview or any interpretations are inaccurate, I requested that the participant provide corrections, which will be added as notes. Afterward, I examined the inputs to determine if any new themes are generated or if the inputs only provided additional clarity.

Data Organization Techniques

Data organization is a process that must be incorporated throughout a study because it may promote effective data management and archiving, which contributes to protecting participant information (Sherif, 2018). Inappropriate use of collected data may result in the loss of data throughout the study and leave the researcher susceptible to data compromise due to reduced security (Myneni et al., 2016). One of the most critical requirements of data organization is ensuring consistency throughout the study (Broman & Woo, 2018). Data organization techniques include the development of data, secure storage, and sharing within the constraints of laws and regulations (Zhou, 2018). Data organization also includes code development and implementation of data, as well as transcription (Neale, 2016). I utilized data organization techniques to construct, organize, codify, and securely store the data collected throughout the study. I utilized Microsoft Word documents to construct consent forms and document the interview process with participants. Following each recorded interview, I transcribed each interview and stored them in a password-protected Microsoft Word document. I also utilized a password-protected Microsoft Excel spreadsheet to consolidate and manage study artifacts. I created a folder for each participant on an encrypted external hard drive. Each folder was labeled with a pseudonym for each participant and interview data and recordings, and organizational artifacts collected via the corresponding interviewee were stored in a single folder.

The researcher is responsible for protecting participants and collected data during and after the study (Surmiak, 2018). The researcher maintains a legal and regulatory requirement of securing research data appropriately and strictly adhering to protecting the study participants (Chauvette, Schick-Makaroff, & Molzahn, 2019). Data from research studies are stored for three to ten years, depending on the educational institution, research facility, or organization (Lin, 2009). To meet the requirements of Walden University, I will store all data in a locked cabinet for five years. After five years from the completion of this study, I will destroy the data.

Data Analysis Technique

In this section of the research study, I will delineate the data analysis techniques to be used in order to analyze data collected concerning organizational strategies to implement cybersecurity awareness and training programs to protect organizational information systems and data. I utilized a qualitative multiple case study and gathering, preparing, analyzing, and interpreting data are critical requirements. Thematic analysis is well suited for qualitative data analysis (Nowell, Norris, White, & Moules, 2017). The six stages of thematic analysis are data familiarization, generation of initial codes, assessment of themes, theme review, the definition of generated themes, and reporting (Robertson et al., 2018). Analyzing data with thematic analysis requires the researcher to examine the collecting data and understand the key concepts that relate the findings with each other (Clarke & Braun, 2018). The understanding and relation of data to key concepts rather than data prevalence contributes to the flexibility of thematic analysis in discovering themes within qualitative research (Lin, 2019). After the transcribed interview has been reviewed and accepted by the participant to be accurate, I performed thematic analysis with all other collected data, to include documents. The primary research question, interview questions, and respective answers were inputted into NVivo. Also, a copy of the original interview questions is located in the Research Question section of this qualitative study, as well as in Appendix B.

Conducting thematic analysis throughout this research study will require operating within six stages. The six stages of thematic analysis are data familiarization, generation of initial codes, assessment of themes, theme review, the definition of generated themes, and reporting (Robertson et al., 2018). Following data collection, data familiarization consists of reviewing and rereading transcriptions and other data sources the data and annotating initial ideas that can be used to develop codes in the second stage (Deighton-Smith & Bell, 2018). During this phase, I read and reread transcribed interviews and documents repeated times until I had become familiar with the content. Stage two consists of the generation of initial codes, which requires grouping data with the same meaning into the appropriate group (Palos-Sanchez, Saura, Reyes-Menendez, & Esquivel, 2018). It is important to ensure that adequate data is grouped into a code so that perspective is maintained, and data can be grouped into multiple codes (Palos-Sanchez et al., 2018). Within stage two, I reviewed the collected data and group it into codes that represented the essence of the data.

Stage three consists of grouping the codes from stage two into themes that represent the meaning of the codes (Kentischer, Kleinknecht, Spirig, Frei, & Huber, 2018). Stage four consists of reviewing themes that consist of verifying the themes against the generated codes across the entire data set (Scharp & Sanders, 2019). During these stages, I used the codes from stage two and grouped them into appropriate themes that accurately reflect their meaning and compare them against the entire data set. The definition of themes in stage five is an iterative process in which the researcher must assess and reassess the collected data against produced themes and refine accordingly

(Patton & Henry, 2019). The last stage in thematic analysis is writing the report which describes each theme in detail (Chen, Draucker, & Carpenter, 2018). After validating that all themes have been defined accurately, I produced the final report, which fully describes each of the themes produced from the thematic analysis.

Triangulation with all collected data from various evidence sources was used to verify findings and improve the quality of the study. Additionally, qualitative data analysis requires that the researcher assess various data sources in order to discover patterns in the collected data. Qualitative data analysis is strongly concerned with analyzing various data sources to discover pertinent patterns (Moser & Korstjens, 2018). By utilizing multiple data sources such as interviews and organizational documents, researchers are able to conduct data triangulation to improve reliability and validity (Moser & Korstjens, 2018). Methodological triangulation can be used to validate results by comparing multiple data sources (Kelle, Kühberger, & Bernhard, 2019). To support data analysis requirements, I utilized the NVivo software package to code the transcribed interviews. I also utilized Microsoft Excel to categories organizational documents. NVivo is a useful tool to perform qualitative data analysis, to include coding (Maher, Hadfield, Hutchings, & de Eyto, 2018). NVivo provides researchers with the functionality of sorting and filtering data, discovering and associating relationships, defining themes and categories, visualizing data analysis, and reporting (Phillips & Lu, 2018). In addition to NVivo functioning as an appropriate qualitative data analysis tool and able to assist in key concept discovery, it is well suited for an exploratory study (Wilk, Soutar, & Harrigan, 2019). Due to the benefits provided by NVivo in exploratory qualitative data analysis, I utilized the application as a primary data analysis tool. Pertinent information related to the research topic was included in the qualitative data analysis, to include information related to SETA.

Reliability and Validity

In this study, I implemented reliability and validity strategies to promote and produce a qualitative study of high quality. Appropriately establishing reliability and validity are critical requirements in demonstrating rigor in a qualitative study (Smith & McGannon, 2018). Qualitative researchers must enforce the concepts of trustworthiness, rigor, and quality in a qualitative research study (Squires & Dorsen, 2018). Trustworthiness and quality are promoted by enforcing dependability, credibility, transferability, and confirmability (Forero et al., 2018). This section includes a description of the strategies I implemented to ensure that validity and reliability are addressed in this study.

Reliability

The reliability of data is a primary requirement during this doctoral study process. Reliability must be considered throughout the entire qualitative research study. Reliability refers to the ability that a researcher can demonstrate consistency between the analysis of data across the spectrum of all participants (Spiers, Morse, Olson, Mayan, & Barrett, 2018). Reliability also takes time into account because reliability refers to the consistency and accuracy of data over time and across the population of the study (Carminati, 2018). Utilizing an interview protocol is a strategy that may improve reliability (Wixted et al., 2018). Reliability was achieved by utilizing process and strategies from within a framework

Validity

Establishing validity within qualitative research requires careful planning and adherence to critical qualitative research concepts. Validity refers to the accurate representation of the experiences described by the participants (Spiers et al., 2018). The validity of a qualitative study is enforced by ensuring that dependability, confirmability, transferability, and credibility are satisfied (FitzPatrick, 2019). Adherence to research methodology, appropriate sampling, and continuous collection and analysis of data contribute to qualitative validity (Morse, Barrett, Mayan, Olson, & Spiers, 2002). Validity was established by ensuring that dependability, confirmability, transferability, and credibility are achieved.

Dependability

The trustworthiness of data that is collected and analyzed throughout this study is a critical requirement of a high-quality qualitative research study. Dependability refers to the fact that the findings of a qualitative study are repeatable when performed within the same construct (Forero et al., 2018). An interview protocol is well suited for semistructured interviews and improves the dependability of the study by reducing bias while collecting high-quality data (Castillo-Montoya, 2016). The use of member checking increases the dependability of a qualitative study (Flynn & Korcuska, 2018). Member checking provides participants with the opportunity to verify and correct any misinterpretations from data gathering, which validates the correctness of the data (Iivari, 2018). The use of an audit trail is a strategy utilized to ensure the dependability and confirmability of a research study (Moser & Korstjens, 2017a). Managing a precise record of the entire data collection process is necessary in maintaining an audit log (Forero et al., 2018). Member checking was utilized in this study to promote dependability. The entire process of collecting data throughout this qualitative study was fully documented, which included recordings and all notes taken. An interview protocol was incorporated into this study to further promote dependability.

Credibility

Credibility refers to a level of confidence that the results are an accurate representation of the participant's experiences (Forero et al., 2018). Member checking is a strategy that promotes credibility by allowing participants to verify that the information obtained during data collection is accurate, and any interpretations are representative of the delineated experiences (Moser & Korstjens, 2017a). Member checking provides participants with the opportunity to review the interview responses and interpretations from data collection and provide inputs to whether the results accurately represent their experience (Smith & McGannon, 2018). During the interview process, I recorded all interviews so that I may review the data collected at a later time. Interview questions remained the same, and the interview protocol was enforced at all times with all participants. These efforts promoted credibility and avoided misinterpreting the data collected throughout this study.

Transferability

Transferability refers to the ability of the researcher to generalize the research across different scenarios by using the same research process (FitzPatrick, 2019). The incorporation of purposeful sampling with open-ended interview questions promotes transferability (Liu, Tang, Wang, & Lee, 2013). Transferability is enhanced by ensuring rich descriptions of the participants, their experiences, and the research process are maintained (Moser & Korstjens, 2017a). Transferability was promoted by maintaining detailed records of collected data from the participants and maintaining rich descriptions of the research process. The interview protocol utilized in this study incorporated open-ended questions and purposeful sampling.

Confirmability

Confirmability refers to the extent that the findings of a research study can be confirmed by other researchers (Forero et al., 2018). Confirmability also implies that the collected data and interpretations of the researcher are accurate (Moser & Korstjens, 2017a). As with dependability, confirmability is enhanced by maintaining an audit trail (Ellis, 2019). Additionally, triangulation is a critical strategy in promoting confirmability within a qualitative research study (Abdalla, Oliveira, Azevedo, & Gonzalez, 2018). Confirmability will be enhanced by ensuring the entire process of collecting data throughout this qualitative study will be fully documented, which will include recordings and all notes taken. Triangulation through collecting data from interviews, organizational documentation, and field notes were utilized.

Data Saturation

I examined and included multiple sources of data in my research study in order to achieve data saturation. During the data collection process and interactions with participants, data saturation is achieved once no new information is produced (Saunders et al., 2018). Researchers will recruit participants throughout a study until no new information is produced, at which point data saturation has been achieved (Squires & Dorsen, 2018). A researcher will cease recruiting participants and reviewing other sources of data once data saturation has been achieved (Moser & Korstjens, 2018). Since I conducted a multiple case study, I interviewed participants from numerous organizations and evaluated organizational documents until no new information was produced. I maintained a record and awareness of all collected data, and once I had determined that only redundant findings were being discovered, I assessed that data saturation was achieved.

Transition and Summary

In this section of the study, I presented the research method and design that will be used to conduct this study. Also, I presented the role of the researcher, participants, population and sampling, ethical considerations, data collection, reliability, and validity. Additionally, I reviewed data collection instruments, data collection techniques, and data analysis techniques. In respect to reliability and validity, I addressed dependability, credibility, transferability, confirmability, and data saturation.

In Section 3, I will expand on the qualitative study with an emphasis on the overview of the study, presentation of the findings, application to professional practice, and implications for social change. Afterward, I will present recommendations for action and further study. Last, I will present personal reflections for this qualitative study.

Section 3: Application to Professional Practice and Implications for Change

Overview of Study

The purpose of this qualitative exploratory multiple case study was to explore strategies used by corporate IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data.

Presentation of the Findings

In this study, I sought to answer the overarching research question: What strategies are used by corporate IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data? I conducted semistructured interviews with seven participants and performed member checking to validate the data and used purposeful sampling to select the participants. Purposeful sampling supports the researcher's ability to select desired qualities in participants and examine appropriately data rich organizations that satisfy study requirements (Goodrich, 2019). I utilized SCT as the conceptual framework because I intended to understand if organizational cybersecurity awareness and training programs employed any of the concepts outlined within SCT. I found strong evidence that the cases in this study practiced elements of SCT as a part of their SETA strategy.

In addition to semistructured interviews, I collected organizational documents related to the organization's SETA program. I performed triangulation by used the semistructured interviews and collected organizational documents. I transcribed the interview recordings to text, sanitized files to remove filler words, time markers, and irrelevant interview discussions. Afterward, the collected documents and sanitized files were inputted into NVivo for analysis. Data analysis revealed three dominant themes: (a) consistent, persistent, and relevant training and awareness; (b) training based off risk; and (c) disclosed outcomes and consequences.

All four organizations are required to comply with federal and state laws, as well as industry regulations, thereby being influenced by external entities. Each hospitality organization maintained and processed sensitive information, which incurs a requirement to protect sensitive information. Sensitive information for all organizations included employee and customer information. Therefore, each organization is challenged in developing and implementing effective cybersecurity awareness and training strategies.

In the following section, the three major themes that emerged during the data analysis phase are evaluated against the review of the literature and examined through the lens of Albert Bandura's SCT, which served as the conceptual framework for this study.

Theme 1: Consistent, Persistent and Relevant Training and Awareness

The theme of consistent, persistent, and relevant training and awareness was the first theme to emerge during the data analysis stage of this study. The findings of this study demonstrate an alignment of consistent, persistent, and relevant training and awareness with existing literature. Hands-on, scenarios-based cybersecurity awareness and training approaches demonstrated effective transference of knowledge and appropriate behavior across 173 non-IT professionals across the southeast United States (Carlton, Levy, & Ramim, 2019). Challenge-based cybersecurity problems and hands-on lab-based sessions promoted the transference of concepts and practical knowledge (Smith & Ali, 2019). Basic cybersecurity education is insufficient to promote appropriate security behaviors, but rather simulators and hypothetical scenarios are shown to increase knowledge transference (Zwilling et al., 2020). A critical component of successful and effective cybersecurity awareness and training programs is ensuring that training and messaging are performed consistently (Abawajy, 2014). Cybersecurity education in the hospitality industry must provide relevant teachings to minimize damage to hospitality operators (Chen & Jai, 2019). All participants across four organizations indicated their organization's SETA strategy included problem-based training, which was relevant to the operators and pertinent to their job functions and performed consistently. This finding was also demonstrated in the collected documents and training materials from the organizations.

Protecting an organizations' information systems and data is a shared responsibility with every member of the organization, and cybersecurity awareness is an important component in developing an employee's understanding to know how to protect the organization (Kim, 2017). All four organizations have implemented an information security awareness and training program that provides consistent, persistent, and relevant cybersecurity education to its employees. All participants indicated that consistent, persistent, and relevant cybersecurity training and awareness is a philosophy of their organization's SETA program (see Table 1). This was confirmed through triangulation of current literature and the secondary data collected across all four organizations that documented the use of consistent, persistent, and relevant training. A consistent, persistent, and relevant cybersecurity awareness and training program was essential and necessary to satisfy industry regulations and protect sensitive organizational and customer data. One organizational IT leader (P1) described the importance of implementing a cybersecurity awareness and training program that educates the end-user and validates their understanding of the material in relation to a dynamic threat landscape. The consistent, persistent, and relative cybersecurity awareness and training strategy included annual cybersecurity training, Payment Card Industry Data Security Standard Training, and periodic cybersecurity notices to organizational employees.

All participants across the four organizations indicated the use of consistent, persistent, and relevant training to support SETA program requirements. The organizational IT leader, P3, described the employees of the organization as “a shield” that protects the organization from potential threats and adheres to company policies through appropriate security practices. Participant P3 indicated that appropriate security practices were taught through relevant training that addresses current threats and reiterated accordingly throughout the year. Participants P1, P2, P3, P5, and P6 indicated that employee cybersecurity awareness and training began from the moment of onboarding. Although participant P4 did not indicate training at onboarding, they indicated consistent training occurred. Participant P6 indicated that employees only acquire network access once they had completed basic security training. Each organization is regulated, and compliance standards are delineated by external and internal entities to appropriately monitor and protect sensitive information systems and data. The appropriate employee behaviors to satisfy external and internal compliance standards is promoted through SETA programs.

Table 1

Frequency of First Major Theme in Participant Responses and Documentation.

	Participant		Document	
Major Theme	Count	References	Count	References
Consistent, Persistent, and Relevant Cybersecurity Awareness and Training	6	48	25	127

Relevant and pertinent cybersecurity awareness and training is necessary to improve employee knowledge and promote appropriate behavior to protect critical assets. According to ISO 27032, cybersecurity is maintaining the confidentiality, integrity, and availability of information systems and data (Hermogeno, 2019). Cybersecurity is a difficult concept to understand, and users generally do not feel physical pain from inappropriate behavior, which decreases the user's willingness to improve awareness (de Bruijn & Janssen, 2017). Further, cybersecurity is a difficult concept to understand, and it is necessary to create an environment that promotes the transfer of knowledge to employees, which encompassing consistent and relevant training (de Bruijn & Janssen, 2017). Participant P6 indicated that they reexamine organizational cybersecurity training material multiple times a year to evaluate relevancy to employees and the current environment. All participants indicated the inclusion of training material that was relevant to their job function and environment. A critical component of successful and effective cybersecurity awareness and training programs is ensuring that training and messaging are performed consistently (Abawajy, 2014).

SETA programs that do not consistently and periodically address employee cybersecurity knowledge generally lack maturity, effectiveness, and incur increased risk to the organization (Sabillon et al., 2019). Regularly produced and administered cybersecurity training is a best practice in the implementation of organizational SETA programs (He & Zhang, 2019). At a minimum, annual cybersecurity awareness training has been shown to improve the level of cybersecurity knowledge (Krasznay & Hámornik, 2019). All six participants indicated that their organization's cybersecurity awareness and training strategies included annual training, at a minimum, to educate users.

When examining this theme through the lens of SCT, an organization with a consistent, persistent, and relevant cybersecurity awareness and training program will increase an organization's cyber posture and promote increased levels of employee cybersecurity knowledge. Self-efficacy is one of the pillars of SCT. Self-efficacy is the belief an individual has in themselves to take appropriate action, overcome challenges, and satisfactorily accomplish a task (Brooks et al., 2019). An individual's level of self-efficacy is influenced by organizational training, education, support, and assistance (Bolkan et al., 2018). The participants of all organizations indicated that they implemented and followed cybersecurity awareness and training programs to improve the employee's ability to appropriately act in the face of cyber threats. According to participant P6, the goal of their SETA program is to have participants understand the risks they face and appropriately react, which includes informing IT of any malicious activity or emails they may receive. Organizational IT leaders should select appropriate cybersecurity awareness and training strategies that improve an employee's cybersecurity knowledge base in order to accomplish business requirements while safely navigating through the threats found in the cyber domain.

From the context of SCT, there are two forms of self-efficacy that an organization can strive to improve. The two forms of self-efficacy are response and task self-efficacy. Response self-efficacy refers to an individual's belief that their behavior makes a difference in reducing risk (Meijers et al., 2018). An individual's level of cybersecurity education positively influences their level of response self-efficacy (Li et al., 2019). Participant P3 referred to the intent of the organization's SETA program to teach employees how to respond to events such as receiving phishing email attempts or locating unknown external devices. Task self-efficacy refers to an individual's ability to complete tasks appropriately (as cited in Graham et al., 2018). All responses from the interviewees were in alignment with improving task self-efficacy with the use of proper awareness and training. All participants indicated that their annual cybersecurity training consisted of test questions and scenarios to pass annual tests. Research has indicated that hand-on activities such as scenario-based problems can improve cybersecurity self-efficacy (Jin et al., 2018), which aligns with the participant responses.

An organization's ability to protect its organizational information systems and data is influenced by the decisions employees make each day (Kim, 2017). SETA programs are a necessary component in ensuring the protection of organizational information systems and data (Balhara et al., 2018). When viewed through the lens of SCT, an organization with an effective SETA program will improve the cyber posture of the organization through desired employee behavior. Based on the findings of this study, a successful SETA program will take into consideration the need to improve an employee’s ability to act and respond. To accomplish this requirement, organizational IT leaders must implement effective strategies to increases employee self-efficacy, which is one of the pillars of SCT.

Theme 2: Awareness and Training Based Off Threats, Risks and Vulnerabilities

The theme of awareness and training based on threats, risks, and vulnerabilities was the second theme to emerge during the data analysis stage of this study. The second theme that emerged from interviews and collected documents from this study aligned with the findings in the literature. According to Bada and Nurse (2019), small-to-medium sized businesses at a city level must implement cybersecurity awareness and training programs that account for existing threats and risks and inform employees of these concepts. Technical and nontechnical controls, which include SETA programs, are based on existing cyber threats, risks, and vulnerabilities (Agrafiotis, Nurse, Goldsmith, Creese, & Upton, 2018). Increasing cybersecurity knowledge has been correlated to increased cybersecurity awareness and appropriate behavior, independent of the country (Zwilling et al., 2020). Zwilling et al. (2020) indicate that it is critical to educate users on pertinent threats, risks, and vulnerabilities, and expand upon basic levels of security knowledge to promote desired behavior. The findings of this study confirmed existing literature that employees are educated on cybersecurity concepts through SETA programs that emphasize risks, threats, and vulnerabilities. All six participants indicated that their SETA programs educate employees by emphasizing existing threats, risks, and vulnerabilities.

Cybersecurity awareness refers to the level of knowledge and understanding of the concepts: threats, vulnerabilities, and risk within the cyber domain (Berkman et al., 2018). Conducting a risk assessment that examines technical and social vulnerabilities, including the human factor, are necessary to understand how to best protect all aspects of society, to include organizations (King et al., 2018). All four organizations have implemented SETA programs that deliver training and awareness based on risk and perceived vulnerabilities to the organization. All participants indicated that their training materials referred to threats, vulnerabilities, and risks that employees in the hospitality industry encounter in their day-to-day requirements (see Table 2). This finding was confirmed through examination of literature and training material collected in this study, which documented the implementation of a cybersecurity awareness and training program founded on addressing risks, threats, and vulnerabilities. A SETA program that educates users on potential threats, vulnerabilities, and risks are a necessary component of cybersecurity education to protect information systems, and employee and customer data. Participant P4 indicated that cybersecurity training must address protecting passwords and maintaining the physical security of the organization to protect sensitive data.

Table 2

Frequency of Second Major Theme in Participant Responses and Documentation.

	Participant		Document	
Major Theme	Count	References	Count	References
Awareness and Training Based Off Threats, Vulnerabilities, and Risk	6	45	26	149

The findings of this study demonstrate an alignment of cybersecurity awareness and training programs based on threats, vulnerabilities, and risks. An organization's weakest layer in its information security strategy is due to user's unawareness of threats and vulnerabilities (de Bruijn & Janssen, 2017). The purpose of an organization's SETA program is to protect the organization's information systems and data posed by vulnerabilities, threats, and risks by improving the level of cybersecurity knowledge of employees (Beuran et al., 2018a). Protecting sensitive data is dependent on stakeholders understanding trends and current threats that incur risk (Kruse, Frederick, Jacobson, & Monticone, 2017). Participant P1 indicated that their SETA program and training material is influence by the results of a risk assessment of the company and the industry as a whole. Employees that are unaware of cybersecurity risks have a higher likelihood of behaving inappropriately from a cybersecurity standpoint (Hadlington, 2017).

A vulnerability is a potential weakness within an information system that may be exploited (Sheehan et al., 2018). Effective policies, and cybersecurity awareness and education of potential vulnerabilities are critical in promoting a strong information security program (Tambo & Adama, 2017). Participant P3 delineated that their SETA program strives to promote appropriate employee behavior, adhere to company policy, and protect the organization. An effective SETA program must ensure that awareness and training are aligned to an employee's day-to-day tasks and the risks they may encounter (Sabillon et al., 2019).

The education of employees on critical attack vectors and vulnerabilities may better protect organizations. Employees must be adequately educated on phishing through SETA programs to protect the organization (Miranda, 2018). All participants indicated the importance of educating users on phishing. The organizational IT leader, P2, indicated that the organization's SETA program promotes the awareness of phishing and spoofing threats. Weak and improperly managed passwords, such as writing passwords down, increases the risk to information systems and data (Timms, 2017). Participant P3 described the importance of ensuring that proper password management is incorporated into organizational SETA programs to protect the company. Exploiting vulnerabilities and poor practices related to physical security may introduce cyber attacks (Tam & Jones, 2018). Physical security is a component of an organization's defense strategy, and awareness of the subject is important in protecting the organization (Conteh & Schmick, 2016). Participants P3, P4, and P6 indicated the importance of training employees on proper physical security practices. Participant P6 described their goal of ensuring employees felt knowledgeable on various cybersecurity topics to include physical security and understanding defensive tactics against social engineering.

When examining Theme 2 through the lens of SCT, awareness and training programs based on threats, vulnerabilities, and risk will promote desired employee behavior to appropriately interact with information systems and data. The agentic framework of SCT applies to Theme 2. Agents practice intentionality and forethought. Intentionality is an individual's ability to deliberately make decisions and select action (Bandura, 2006), but does not always result in a positive outcome (Bandura, 2001a). Intentionality does not occur in a vacuum but may be influenced by external entities and support activities (Bandura, 2006). Organizational leaders and education programs may serve as external entities to influence human behavior and intentionality. All participants of all organizations indicated that they implemented SETA strategies to promote positive desired security practices. Participant P4 indicated that the goal of the organization was to avoid being exploited from vulnerabilities by ensuring employees took appropriate actions with respect to physical security and proper password management to protect financial data.

The agentic framework of SCT also consists of the properties of forethought and self-reactiveness. Forethought is the development of future actions and plans based on individual goals and self-assessing outcomes of performing a forecasted action (Bandura, 2006). Forethought shares a relationship with the triadic reciprocal determinism model that provides an individual with the opportunity to will a desired outcome within their present situation (Bandura, 2018). Self-reactiveness operates within the framework of forethought because an individual will plan and select an action based on constant evaluation of a perceived outcome at a particular moment (Bandura, 2001a). Self-reactiveness is influenced by utilizing prior knowledge and inferencing outcomes based off prior knowledge (Bandura, 2001a).

Self-regulation is a component of SCT that applies to Theme 2. Self-regulation is a pillar of SCT that incorporates the constructs of forethought and self-reflectiveness. Self-regulation refers to an individual being able to self-assess their actions (Benight et al., 2018). Self-regulation is a dynamic internal process made up of the self-monitoring, self-diagnostic, self-motivating, judgmental, and reactive systems (Bandura, 1991). The human aspects of an information security model describe the relationships between individuals, organizations, and intervention factors with the behaviors, education, and awareness related to information security (McCormac et al., 2017). All participants indicated the presentation of threats, risks, and vulnerabilities to positively manipulate the security behavior of employees.

These desired actions incorporate the concepts of forethought and self-reactiveness, and the collected training material also supported this finding. The delineation of vulnerabilities, threats, and risks in the training material serves as learned and prior knowledge to support the forethought and self-reactiveness constructs. Participant P3 indicated that risks to the organization are constantly changing, and our training alters based on the risks at that moment. All participants indicated that the SETA strategy and training material presented threats, vulnerabilities, and risks so that employees were aware and understood what they needed to look out for to protect information systems and data. P5 indicated that external devices might be found, and the desired action of employees is to handle the external devices appropriately and limit exposure to information systems. Participants P1, P2, P3, P4, P5, and P6 all indicated training based on the risk of phishing and SETA program success is related to the percentage of employees that reported real-world or test phishing attempts or appropriately handled phishing attempts.

Insider threats and inappropriate security behavior are an organizational risk, which is significantly influenced by poor cybersecurity awareness (Muhirwe & White, 2016). Cybersecurity behavior is influenced by user characteristics and cyber threats, risks, and vulnerabilities (Yan et al., 2018). Successful self-regulation is strongly correlated with appropriate behavior (Dohle, Diel, & Hofmann, 2018). When viewed through the lens of SCT, an organization with a SETA strategy that is based on threats, vulnerabilities, and risks, and informs users of these concepts may improve self-regulation. By improving the self-regulation of employees, organizations may promote better security behaviors to protect the organization, its users, and customers. Based on the findings of this study, a successful SETA program will incorporate threats, vulnerabilities, and risks in developing an awareness and training strategy for employees. To accomplish this requirement, organizational IT leaders must examine current threats and risks, and delineate training based on these results.

Theme 3: Consequences and Disclosed Expectations

The third theme of consequences and disclosed expectations emerged through the data analysis phase. The third theme that emerged from this study confirmed the findings in the literature. Businesses of small-to-medium stature must implement cybersecurity awareness and training programs that align with delineated policies and guidance from leaders (Bada & Nurse, 2019). Five themes of risk associated with physical and digital, economic, psychological, reputational, and social and societal encompass the potential harm an organization may encounter within the cyber domain and should be presented to stakeholders, including employees (Agrafiotis et al., 2018).

The findings of this study did not confirm the categories of psychological and social and societal harms. Psychological risks and harms include confusion, discomfort, frustration, guilt, worry, and other negative psychological sensations (Agrafiotis et al., 2018). Social and societal harms include changes in societal perceptions, decreased employee morale, negative national impacts, and disruptions to daily activities (Agrafiotis et al., 2018). None of the participants, nor collected documents indicated potential psychological risks as a focus within their respective SETA programs. Further, none of the participants and collected documents indicated that social and societal harms were delineated in their SETA programs. Although participant P2 and P6 indicated that repeat offenses were likely limited due to employees feeling embarrassed after a first offense, this psychological outcome was not a deliberately desired one from the organization. Further, none of the participants nor documents collected indicated the presence of social and societal harms as a result of inappropriate cybersecurity behavior within the examined SETA programs.

Inappropriate cyber behavior, such as sharing passwords or opening inappropriate emails, should result in consequences to the employee (Evans, Maglaras, He, & Janicke, 2016). Three organizations have implemented an information security awareness and training program that incorporates employee consequences as indicated by participants and collected documents. The participants from Organizations O1, O2, and O3 indicated that consequences due to inappropriate cyber behavior are a philosophy of their organization's SETA program (see Table 3). Participant P2 indicated that the organization examines violations on a case-by-case basis depending on severity, but they have not had anyone perform multiple information assurance events or a situation that resulted in termination. Participant P2 and P6 indicated that repeat offenses did not occur because they believed that offenders were embarrassed after the first offense. This was confirmed through the triangulation of current literature and the secondary data collected across the four organizations that documented the use of escalation and consequences for inappropriate behavior. The use of escalation and consequences was essential and necessary to promote desired behavior to protect organizational information systems and data. Organizational IT leader, P5, indicated that there is very much a possibility of termination based on employee cybersecurity behavior.

Consequences not only include termination, but restricted network access as a result of inappropriate cyber behavior. All participants from organizations O1, O2, and O3 indicated the disabling of user accounts to protect the organization's information systems and data in the case an information assurance event occurred due to employee actions. Participant P2 indicated that they disable network access when an employee performs an inappropriate action on the network, and it would not be re-enabled until security training was completed again. This finding is in alignment with the literature that inappropriate cyber behavior may disrupt daily activity and encompasses social harm.

Table 3

Frequency of Third Major Theme in Participant Responses and Documentation.

	Participant		Document	
Major Theme	Count	References	Count	References
Consequences and Disclosed Expectations	6	31	23	67

The other component of this theme that emerged was disclosing expectations. SETA programs should utilize an effective framing strategy to effectively present expectations and importance. Effective framing strategies for an organizational SETA program include demonstrating the importance of cybersecurity to society and connecting the meaning of cybersecurity to other facets of life (de Bruijn & Janssen, 2017). All four organizations indicated that their SETA programs disclosed that failure to adhere to appropriate use policy would result in personal consequences. Participant P4 indicated that the training within the organization made it known that their cyber behavior has an impact. Participant P6 indicated that guidance on the appropriate use of information systems and consequences are disclosed in the human resources handbook and disclosed during onboarding. The SETA strategies across the organizations incorporated training that disclosed how inappropriate actions impact customers, employees, and the organization.

The findings of this study also indicated that punishment due to the inappropriate use of information systems was not the only form of consequence. Participants P1, P2, P3, P5, and P6 indicated that there was a mechanism that informed employees about security training that required completion. All participants from organizations O1, O2, and O3 indicated that management would also be made aware of incomplete training, and account access would be disabled if the training was not completed by the delineated due date. Participant P1 indicated that employees would be notified via email that they had training due with the required completion date, and if it was not completed, they would lose network access. Participant P2 indicated that not only are employees made aware of training requirements, but the associate's manager would be informed of employees that were delinquent in training.

When examining this theme through the lens of SCT, an organization that utilizes outcomes and disclosed expectations would promote the desired employee behavior. Social learning is one of the pillars of SCT. Social learning refers to the persuasions incurred from negative and positive social influences that impact an individual's learning (Lowry et al., 2017). Human behavior and learning are influenced by social learning (Lowry et al., 2017). The participants at all the organizations indicated that they implemented and adhered to cybersecurity and awareness training programs that informed users of the potential impacts of the actions. According to participant P3, they indicated that their SETA program focused on informing employees on how their actions can impact customer privacy and satisfaction. Organizational IT leaders should select effective SETA strategies that inform users of the impact their actions have on themselves, fellow employees, customers, the organization, and society as a whole. By informing users of these facts, organizations may be able to change human behavior accordingly and promote the desired cybersecurity culture.

Furthermore, from the context of SCT, this emerging theme also aligned with outcome expectation. Outcome expectation is another pillar of SCT. Outcome expectation refers to an individual's assessment of the positive and negative implications of an action or decision (Bandura, 2006). Outcome expectation can be generalized into one of three categories, which are physical effects, social effects, and self-evaluation effects (Bandura, as cited by Lin & Chang, 2018). The findings of this study indicated that physical effects, social effects, and self-evaluation effects were addressed in their SETA strategies. Physical effects refer to physiological pleasure and discomfort (Lin & Chang, 2018). Participant P3 indicated that not completing training results in a loss of network access and enforces accountability. Participant P3 also disclosed that losing network access greatly impacts their ability to do their job, which may incur physiological stress due to falling behind in work. Participant P4 indicated that a sense of stress could be felt due to opening the wrong email. Furthermore, in the case of termination, an employee would lose the ability to earn an income, which would incur physiological discomfort.

The two remaining categories that are incorporated into outcome expectation are social effects and self-evaluative effects. Social effects refer to positive and negative social recognition, and self-evaluative effects refer to personal levels of satisfaction (Lin & Chang, 2018). Organizations O1, O2, and O3 indicated that not completing training and inappropriate use of information systems would result in other levels of management being informed of employee lack of compliance. This mechanism creates an environment that not adhering to policy will result in negative recognition. Further, organizations O1, O2, O3, and O4 indicated that training material disclosed outcomes of inappropriate behavior that has impacts on other entities. This creates an environment in which employees understand that organizational reputations may be damaged based on internal actions. For example, a compromise from a PCI DSS standpoint would require notification outside the organization, which may result in further social recognition. Last, organizations O1, O2, and O3 indicated that inappropriate behavior and failure to complete training would result in disabled network access, which reduces an employee's ability to complete their work. Job satisfaction in hospitality is influenced by their perception of significance (Kong, Jiang, Chan, & Zhou, 2018). Creating an environment that reduces the capability to perform job tasks based off negative actions may promote better behaviors to maintain individual work satisfaction.

The factors of the triadic reciprocal determinism model and relationships between each other are influenced by social learning or modeling, and outcome expectancy (Lowry et al., 2017). Social learning is a mechanism to deter the misuse of information systems by emphasizing the consequences of inappropriate actions (D'Arcy et al., 2009). Delineation of outcome expectations to employees has positively impacted the learning outcomes of information assurance principles and is enhanced by incorporating the monitoring of network activity (Ahmad et al., 2019). When viewed through the lens of SCT, an organization with a SETA program that leverages social learning and outcome expectance will improve employee cybersecurity behavior. Based on the findings of this study, a successful SETA program will take into consideration the need to disclose consequences of inappropriate behavior, failure to accomplish training, and inform users of the full impact of their actions. To accomplish this requirement, organizational IT leaders must implement effective strategies to inform employees of outcome expectation and leverage social learning, which are two of the pillars of SCT.

Applications to Professional Practice

The specific IT problem investigated with this research was the perception that some corporate hospitality IT leaders lacked the strategies to implement cybersecurity awareness and training programs to protect organizational information systems and data. Current literature suggests that many organizations do not possess effective cybersecurity awareness and training programs to protect organizational information systems and data. The hospitality organizations involved in this study incorporated an effective SETA strategy to protect organizational information systems and data. All four organizations operate in heavily regulated industries, and the responses of the participants indicated the importance of satisfying federal and state laws, as well as industry regulations in developing and implementing an effective SETA strategy. The SETA strategies presented by all the participants of this study indicated the need for incorporating consistent, persistent, and relevant cybersecurity awareness and training. Participants also indicated awareness and training based on threats, vulnerabilities, and risks, as well as disclosing outcomes and expectations. Organizational IT leaders within regulated and unregulated sectors and industry domains may utilize the results of this study as a guide on developing and implementing an information security awareness and training strategy within their organization.

Components of SCT were demonstrated to be important concepts for the participating organizations in the design and implementation of their cybersecurity awareness and training strategies to protect organizational information systems and data. The use of SCT by organizations across industry domains that are concerned with promoting specific cybersecurity behaviors may benefit by leveraging the constructs of SCT. By assuming that employees are agentic, and their behavior and learning are directed by the triadic reciprocal determinism model, organizational IT leaders can incorporate SETA strategies and foster environments that promote desired behavior. Hospitality organizations demonstrated the value of self-efficacy, self-regulation, social learning, and outcome expectation in promoting employee behaviors that protect organizational information systems and data.

The findings of this study may contribute to the reduction of inappropriate cybersecurity behavior, more effective SETA programs, and strengthening of the human factor. It is commonly understood that the weakest layer in an organization's defense strategy is related to the user's unawareness of cybersecurity best practices, threats, and vulnerabilities (de Bruijn & Janssen, 2017). Inappropriate cybersecurity behavior has resulted in grave damage to national security (Gootman, 2016), significant financial penalties (Plachkinova & Maurer, 2018), and reputational damage (Jeong et al., 2019). The hospitality industry is a highly regulated industry that must adhere to federal and state laws, industry regulations such as PCI DSS, and additions requirements such as GDPR. Hospitality organizations must be concerned with GDPR requirements because of the significant penalties incurred, in addition to other costs of a data breach (Wilson, 2018). In addition to financial penalties, the degradation of reputation and loss of customer trust may decrease revenue due to a data breach. Not only does a significant cyber event pose potential harm to the individual organization, but it may also result in wider spread impacts to a localized hospitality industry. These findings are relevant to improved IT practices because effective SETA programs in the hospitality industry impact local and state economies, individual professions, and protect customers.

Implementing a SETA program requires that training material be presented consistently and persistently to employees while ensuring the training is relevant. The use of consistent, persistent, and relevant training was evident from all organizational IT leaders for this study. Examples of relevant training by participants P1, P2, P3, P4, P5, and P6 was demonstrated by incorporating training materials that contained hands-on, problem-based scenarios. Further, participants P1, P2, P3, P5, and P6, indicated the use of test phishing emails to validate training and improve awareness. Analysis of the study’s findings was performed through the lens of SCT. Appropriate behavior can be promoted by improving self-efficacy in respect to SCT. When an organization consistently provides relevant training, with scenario-based problems designed to improve knowledge transference will improve cybersecurity self-efficacy. Stronger employee beliefs to respond appropriately in the face of cyber risks may lead to more confident and appropriate behavior.

The next characteristic that was apparent from the participating organizations was self-regulation. The organizations utilized SETA strategies that promoted the development of employee self-regulation. Organizational training materials, documents and practices that emphasized threats, vulnerabilities, and risks influenced self-regulation. The organizations strived to inform employees of the vulnerabilities, risks, and threats they were likely to encounter in their environment and daily functions. The participating organizations performed risk assessments of their organization and selected training materials that presented appropriate risks, threats, and vulnerabilities. Self-regulation was improved by informing employees what to be wary of and how to respond when faced with potentially malicious activity. These training focal points were advantageous in developing self-monitoring, self-diagnostic, and personal reactive systems to ultimately behave appropriately to protect sensitive assets.

The final aspect of SCT that had an impact on the participating organization's SETA strategies was the emphasis of outcome expectation, and social learning from the SCT construct. The participating organizations disclosed expected personal, customer, and organizational outcomes for inappropriate behavior. Furthermore, participating organizations enforced consequences for inappropriate behavior in order to ensure repeat offenses did not occur in the future. The most relevant aspect of developing outcome expectation was enforcing consequences, whether it included disabling network access, requiring additional training, or termination. Participating organizations also disclosed outcomes and expectations to leverage social learning throughout the organization to promote positive cyber behaviors. Employees' awareness of harm and consequences due to behavior throughout the work environment enforces the practice of social learning.

The research findings in this study revealed the participating organization's strategies when implementing SETA programs. The study also delineates the advantages of utilizing SCT as a guide in implementing SETA strategies to protect sensitive data and assets. Ultimately, the findings of this study may benefit organizational IT leaders nationally and internationally by providing them with strategies revealed in this study. These discovered strategies may be used to guide SETA program implementation and improve organizational cybersecurity programs. The strategies discovered from this study may support SETA programs across various industries, in addition to the hospitality industry.

Implications for Social Change

The implications for social change are related to the effects resulting from effective cybersecurity awareness and training strategies that hospitality organizations utilized. Improving the level of cybersecurity education in employees may translate into improved behaviors at home. The cyber environment is unsafe for children, and cybersecurity awareness is necessary to inform them of risks and how to appropriately act (Rahim, Hamid, & Kiah, 2019). Cybersecurity awareness and understanding is a critical requirement to protect families from cyber threats (Hermogeno, 2019). The lessons acquired from organizational SETA programs can be transferred to families and children, which may result in less harm to families.

Improved levels of cybersecurity awareness from effective SETA programs may result in fewer compromises due to inappropriate behavior, which results in protecting customers, employees, and societal programs. Small-to-medium sized businesses reduce the risk of falling victim to cybercrime by properly implementing SETA programs (Bada & Nurse, 2019). The proper function and availability of healthcare equipment due to a reduction in cyber incidents may be enhanced through SETA programs, which avoids patient harm, further injury, or even death (Schwartz et al., 2018). The effective implementation of cybersecurity awareness and training programs have promoted stronger organizational stock prices (Berkman et al., 2018). Improving SETA programs better protects private personal information from potential compromise (Hermogeno, 2019). Social benefits to customers, employees, and protection of societal programs may be incurred by better implemented SETA strategies.

The findings of this study may also improve understanding of the social cyber sub-domain. The cyber domain is comprised of the physical, logical, information, and social layers (Zeleke, 2019). The social sub-domain encompasses humans, behavior, and cognitive function (Eggenschwiler, 2018). The importance of examining and educating social and organizational factors in the domain of cyber is undervalued (Dawson & Thomson, 2018). By improving understanding of the social sub-domain of cyber across organizations, employees, and customers, better protection of information systems and data may be achieved due to a better understanding of the whole cyber domain.

The findings from this study add to the existing cybersecurity awareness and training body of knowledge by delineating strategies from four hospitality organizations and may be of value to society by providing improved SETA program strategies. The information in this study describes how four different hospitality organizations develop and implement effective SETA strategies to promote appropriate cybersecurity behavior, reduce information assurance events, and improve overall compliance. This study may also help raise awareness of the challenges of creating and implementing SETA programs and demonstrate how four hospitality organizations are navigating through various challenges.

Recommendations for Action

The findings of this study may benefit organizational IT leaders around the world by providing them with strategies that could be utilized with respect to SETA programs. This study explored the strategies that hospitality IT leaders used to develop and implement an effective SETA program. This study revealed how a SETA program could be implemented through three key strategies to protect organizational information systems and data. First was consistent, persistent, and relevant cybersecurity awareness and training. The second was security training based on threats, vulnerabilities, and risks. The third was disclosing outcomes and expectations.

The first recommendation calls for organizational IT leaders to conduct a strategic, operational, and tactical level examination with all required stakeholders to review existing SETA program implementation. Cybersecurity is a shared responsibility, and every member of the organization has an obligation to protect organizational information systems and data. Key stakeholders should examine current trends and threats within cyberspace in order to implement an effective SETA strategy that addresses the concerns of the current threat landscape. Organizational IT leaders within hospitality should enroll in a service that provides threat intelligence, or they should conduct organic threat intelligence. Hospitality organizational IT leaders should consistently assess the findings of cyber threat intelligence to effectively focus on security awareness and training strategies. Additionally, any organization that has not implemented a SETA program should review this study and determine if any of the findings may support their organizational requirements.

The second recommendation is for organizational IT leaders to closely examine the current measures they are utilizing in implementing their SETA program. Organizational IT leaders should also perform an inventory of employee's level of information security knowledge. This study demonstrated the importance of implementing consistent, persistent, and relevant cybersecurity awareness and training to promote desired behavior. Organizational IT leaders should collaborate with one another, across various industry domains to share effective SETA strategies. Collaboration creates an opportunity for organizational IT leaders to support each other against committed and well-resourced malicious actors. Additionally, collaboration and sharing of strategies may rapidly transmit effective SETA strategies to promote desired behavior and decrease negative events due to unintentional insider threats.

The third recommendation is for organizational IT leaders to examine existing policies and human resources onboarding processes in relation to the inappropriate use of information systems. This review of policy should also examine education compliance and remediation training processes. Organizational IT leaders should strive to create an environment in which outcomes and expectations are known throughout an employee's tenure at the organization. This study demonstrated the importance of disclosing outcomes and expectations to employees in order to ensure compliance and appropriate behavior.

The fourth and final recommendation is for organizational IT leaders to examine the social cyber sub-domain to leverage the findings of psychology, sociology, and human behavior to support their SETA programs. Cybersecurity awareness and training is predominately a social concern and heavily reliant on the human factor. Therefore, organizational IT leaders should strive to understand human behavior and implement strategies that promote appropriate behavior. Organizational IT leaders should also consider performing psychological assessments on employees to better understand their tendencies to promote desired behavior. Organizations are a social environment and organizational IT leaders should examine principles of sociology and social psychology to implement effective cybersecurity cultures and an environment that is conducive to appropriate cyber behavior.

Dissemination of the findings of this study will be accomplished through multiple approaches. Once I have received approval from the Chief Academic Officer, every participant of the participating hospitality organizations will be provided with an executive summary of my findings. The study will also be available in the ProQuest database, which has active partnerships with over 9,000 publishers worldwide. Furthermore, I intend to pursue publication in scholarly journals, industry publications, magazines, and conferences, which will widen the dissemination of these findings to a larger target audience of information security professionals across multiple industries.

Recommendations for Further Study

Several recommendations for further study exist. One of the delineated limitations noted at the beginning of this study was the number of examined organizations. Further research could expand on the number of more hospitality organizations and include examining more participants. Although a small number of organizations were examined, this study benefited significantly from having organizational IT leaders within the hospitality industry who were able to provide detailed information that aligned with current literature. Of note, it is possible that examining additional organizations and interviewing additional participants may reveal additional items of interest not discovered in this study, which would contribute further to the current literature.

Another limitation noted in this study was the geographic region of examination. Different locations are subject to different laws and regulations. The hospitality industry in different geographic locations within the same country may operate differently. Furthermore, hospitality industries may differ significantly when compared to different nations. It is possible that examining hospitality organizations in different areas of the United States and in other nations may reveal additional areas not exposed in this study.

Bias introduced by the participants by not responding truthfully or not fully disclosing information for various reasons was another limitation delineated in this study. I assess that the participants answered truthfully and disclosed when they were not able to discuss an issue or provide internal documents. Concerns with open disclosure within the subject of organizational cybersecurity practices is not unusual, but in the future, anonymous surveys to collect information may overcome this challenge.

An area of future research that would be interesting and potentially add to the body of knowledge would be the examination of SETA programs from the standpoint of employees. Interviews or anonymous surveys of the effectiveness of their organization’s

SETA program and the translation of cybersecurity education to home life would be interesting. Also, examining the concepts that they believed to be most important to bring into their personal lives would be interesting.

Another area of study that may add value to existing information security literature would be further examination of cybersecurity from the perspective of industrial/organizational, social, and behavioral psychology. Understanding how organizations implement effective cybersecurity cultures and promote behavior through artifacts, beliefs, and values would be of interest. Further, understanding why employees behave and respond to information security policies, regulations, and consequences within the work environment would also be an interesting addition to the body of research. Another area of interest would be an examination of cybersecurity behavior to the big-five personality traits of openness, conscientiousness, extraversion, agreeableness, and neuroticism. Understanding which traits better explain and influence cybersecurity behavior may contribute to more effective organizational cybersecurity programs.

Reflections

This doctoral study was a true test of grit, resiliency, and patience. From the moment I entered the third year of my bachelor program, I knew I wanted to earn a doctoral degree and become a professor, but I had not reached a time in my life where I was prepared for the demands of a doctoral program. Not only was I unprepared to pursue a doctoral program, but there were also other endeavors that I believed I needed to pursue first. Over the past twelve years of active duty military service, I have developed, matured, and changed. In 2016, I realized that I was ready to pursue a doctoral degree.

Before beginning my doctoral journey, I did not fully grasp the benefit of continuous development and the power of compounding progress. The process of defining a research problem, constructing a rigorous academic piece, and collecting data have significantly contributed to my development as a person, professional, and academic.

The process of completing a doctoral program has significantly improved my technical ability, research capability, and writing skills. Additionally, I my level of grit, resiliency, and patience have developed even further. Continuing to push forward and not quit has been a considerable challenge that I had to overcome several times throughout this process. I was so fortunate to have a supportive partner in my wife. Her continued support, encouragement, and belief in me are one of the major reasons I have been able to finish. I was so close to quitting after I received my master's degree along the way, but pushing through and being open with someone trustworthy throughout has brought me to this point. To all that follow and decide to pursue a doctoral degree, I cannot emphasize the importance of support, grit, patience, and resiliency to complete this challenge.

Summary and Study Conclusions

Organizational IT leaders are implementing strategies, policies, and procedures within their organizations to protect employees and customers from the constant threat in cyberspace. There may be cases in which strategies being implemented may or may not have full support across all organizational executives or may not be effectively incorporated within an organized cybersecurity awareness and training program. It may also be possible that organizations have not even implemented a SETA program to protect information systems and data. This study may assist organizational IT leaders plan, develop, and implement a SETA strategy the promotes the protection of organizational information systems and data through awareness and training. By utilizing established security frameworks and principles from industrial/organizational, social, and behavioral psychology, IT leaders may create a comprehensive security strategy.

References

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33*(3), 236-248. doi:10.1080/0144929X.2012.708787

Abdalla, M. M., Oliveira, L. G. L., Azevedo, C. E. F., & Gonzalez, R. K. (2018). Quality in qualitative organizational research: Types of triangulation as a methodological alternative. *Administração: Ensino e Pesquisa, 19*(1), 66-98. doi:10.13058/raep.2018.v19n1.578

Abrahamson, D., & Kapur, M. (2018). Reinventing discovery learning: A field-wide research program. *Instructional Science, 46*(1), 1-10. doi:10.1007/s11251-017-9444-y

Agnew, D., Marks, A., Henderson, P., & Woods, C. (2018). Deselection from elite Australian football as the catalyst for a return to sub-elite competitions: When elite players feel there is ‘still more to give.’ *Qualitative Research in Sport, Exercise and Health, 10*(1), 117-136. doi:10.1080/2159676X.2017.1380074

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity, 4*(1), 1-15. doi:10.1093/cybsec/tyy006

Ahmad, Z., Ong, T. S., Liew, T. H., & Norhashim, M. (2019). Security monitoring and information security assurance behaviour among employees: An empirical analysis. *Information & Computer Security, 27*(2), 165-188. doi:10.1108/ICS-10-2017-0073

Alahmad, G. (2018). Informed consent in pediatric oncology: A systematic review of qualitative literature. *Cancer Control, 25*(1), 1-8. doi:10.1177/1073274818773720

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet, 11*(3), 73. doi:10.3390/fi11030073

Alohali, M., Clarke, N., & Furnell, S. (2018). The design and evaluation of a user-centric information security risk assessment and response framework. *International Journal of Advanced Computer Science and Applications, 9*(10), 148-163. doi:10.14569/IJACSA.2018.091018

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

Amico, K. R., Mugavero, M., Krousel-Wood, M. A., Bosworth, H. B., & Merlin, J. S. (2018). Advantages to using social-behavioral models of medication adherence in research and practice. *Journal of General Internal Medicine, 33*(2), 207-215. doi:10.1007/s11606-017-4197-5

Amundsen, D., Msoroka, M., & Findsen, B. (2017). “It’s a case of access.” The problematics of accessing research participants. *Waikato Journal of Education, 22*(4), 5-17. doi:10.15663/wje.v22i4.425

Anaya-Reig, N. (2018). Cajal: Key psychological Factors in the self-construction of a genius. *Social Epistemology, 32*(5), 311-324. doi:10.1080/02691728.2018.1522555

Anderson, R. C., Graham, M., Kennedy, P., Nelson, N., Stoolmiller, M., Baker, S. K., & Fien, H. (2019). Student agency at the crux: Mitigating disengagement in middle and high school. *Contemporary Educational Psychology, 56*, 205-217. doi:10.1016/j.cedpsych.2018.12.005

Angstmann, J. L., Rollings, A. J., Fore, G. A., & Sorge, B. H. (2019). A pedagogical framework for the design and utilization of place-based experiential learning curriculum on a campus farm. *Journal of Sustainability Education, 20*, 1-14. Retrieved from http://www.susted.com/wordpress/content/a-pedagogical-framework-for-the-design-and-utilization-of-place-based-experiential-learning-curriculum-on-a-campus-farm_2019_04/

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35. doi:10.1108/JIST-02-2018-0028

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

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security, 27*(3), 393-410. doi:10.1108/ICS-07-2018-0080

Bagdonienė, L., & Zemblytė, J. (2005). Service research: Advantages and limitations of quantitative and qualitative approaches. *Socialiniai Mokslai, 50*(4), 26-37. Retrieved from https://etalpykla.lituanistikadb.lt/object/LT-LDB-0001:J.04~2005~1367157369344/J.04~2005~1367157369344.pdf

Bai, Y., Lin, L., & Liu, J. T. (2019). Leveraging the employee voice: A multi-level social learning perspective of ethical leadership. *The International Journal of Human Resource Management, 30*(12), 1869-1901. doi:10.1080/09585192.2017.1308414

Bakker, A. (2018). Discovery learning: Zombie, phoenix, or elephant?. *Instructional Science, 46*(1), 169-183. doi:10.1007/s11251-018-9450-8

Balhara, Y. P. S., Harshwardhan, M., Kumar, R., & Singh, S. (2018). Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness programme. *Asian Journal of Psychiatry, 34*, 38-42. doi:10.1016/j.ajp.2018.04.010

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory.* Englewood Cliffs, N.J: Prentice-Hall.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes, 50*(2), 248-287. doi:10.1016/0749-5978(91)90022-L

Bandura, A. (2001a). Social cognitive theory: An agentic perspective. *Annual Review of Psychology, 52*(1), 1-26. doi:10.1146/annurev.psych.52.1.1

Bandura, A. (2001b). Social cognitive theory of mass communication. *Media Psychology, 3*(3), 265-299. doi:10.1207/S1532785XMEP0303_03

Bandura, A. (2004). Health promotion by social cognitive means. *Health Education & Behavior, 31*, 143-164. doi:10.1177/1090198104263660

Bandura, A. (2006). Toward a psychology of human agency. *Perspectives on Psychological Science*, 1(2), 164-180. doi:10.1111/j.1745-6916.2006.00011.x

Bandura, A. (2012). On the functional properties of perceived self-efficacy revisited. *Journal of Management, 38*(1), 9-44. doi:10.1177/0149206311410606

Bandura, A. (2018). Toward a psychology of human agency: Pathways and reflections. *Perspectives on Psychological Science, 13*(2), 130-136. doi:10.1177/1745691617699280

Bandura, A. (2019). Applying theory for human betterment. *Perspectives on Psychological Science, 14*(1), 12-15. doi:10.1177/1745691618815165

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal, 61*(4), 1189-1195. doi:10.5465/amj.2018.4004

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

Bauer, S., Bernroider, E. W. N., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159. doi:10.1016/j.cose.2017.04.009

Baumeister, R. F., Tice, D. M., & Vohs, K. D. (2018). The strength model of self-regulation: Conclusions from the second decade of willpower research. *Perspectives on Psychological Science, 13*(2), 141-145. doi:10.1177/1745691617716946

Bayne, H. B., & Branco, S. F. (2018). A phenomenological inquiry into counselor of color broaching experiences. *Journal of Counseling and Development, 96*(1), 75-85. doi:10.1002/jcad.12179

Beauchamp, M. R., Crawford, K. L., & Jackson, B. (2019). Social cognitive theory and physical activity: Mechanisms of behavior change, critique, and legacy. *Psychology of Sport & Exercise, 42*, 110-117. doi:10.1016/j.psychsport.2018.11.009

Beccaria, L., Kek, M. Y., & Huijser, H. (2018). Exploring nursing educators' use of theory and methods in search for evidence based credibility in nursing education. *Nurse Education Today, 65*, 60-66. doi:10.1016/j.nedt.2018.02.032

Benight, C. C., Harwell, A., & Shoji, K. (2018). Self-regulation shift theory: A dynamic personal agency approach to recovery capital and methodological suggestions. *Frontiers in Psychology, 9*(1738), 1-8. doi:10.3389/fpsyg.2018.01738

Bennett, B., Sharma, M., Bennett, R., Mawson, A. R., Buxbaum, S. G., & Sung J. H. (2018). Using social cognitive theory to predict medication compliance behavior in patients with depression in southern United States in 2016 in a cross-sectional study. *Journal of Caring Sciences, 7*(1), 1-8. doi:10.15171/jcs.2018.001

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508–526. doi:10.1016/j.jaccpubpol.2018.10.003

Beuran, R., Pham, C., Tang, D., Chinen, K. I., Tan, Y., & Shinoda, Y. (2018a). Cybersecurity education and training support system: CyRIS. *IEICE TRANSACTIONS on Information and Systems, 101*(3), 740-749. doi:10.1587/transinf.2017EDP7207

Beuran, R., Tang, D., Pham, C., Chinen, K., Tan, Y., & Shinoda, Y. (2018b). Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security, 78,* 43-59. doi: 10.1016/j.cose.2018.06.001

Bingöl, T. Y. (2018). Determining the Predictors of Self-Efficacy and Cyber Bullying. *International Journal of Higher Education, 7*(2), 138-143. doi:10.5430/ijhe.v7n2p138

Blaikie, N. (2018). Confounding Issues Related to Determining Sample Size in Qualitative Research. *International Journal of Social Research Methodology, 21*(5), 635-641. doi:10.1080/13645579.2018.1454644

Blewitt, J. C., Blewitt, J. M., & Ryan, J. (2018). Business forums pave the way to ethical decision making: The mediating role of self-efficacy and awareness of a value-based educational institution. *Journal of Business Ethics, 149*(1), 235-244. doi:10.1007/s10551-016-3103-0

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior, 87*, 87-97. doi:10.1016/j.chb.2018.05.023

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

Bolkan, S., Pedersen, W. C., Stormes, K. N., & Manke, B. (2018). Predicting 4-Year Graduation: Using Social Cognitive Career Theory to Model the Impact of Prescriptive Advising, Unit Load, and Students' Self-Efficacy. *Journal of College Student Retention: Research, Theory & Practice, 0*(0), 1-21. doi:10.1177/1521025118783485

Bosley, H., Appleton, J., Henshall, C., & Jackson, D. (2019). Using local communities to establish geographical boundaries for case studies. Nurse Researcher, 27(1), 41-44. doi:10.7748/nr.2019.e1623

Bozkus Kahyaoglu, S., & Caliyurt, K. (2018). Cyber security assurance process from the internal audit perspective. *Managerial Auditing Journal*, *33*(4), 360-376. doi:10.1108/MAJ-02-2018-1804

Broman, K. W., & Woo, K. H. (2018). Data organization in spreadsheets. *American Statistician, 72*(1), 2-10. doi:10.1080/00031305.2017.1375989

Brooks, A. T., Krumlauf, M., Beck, K. H., Fryer, C. S., Yang, L., Ramchandani, V. A., & Wallen, G. R. (2019). A mixed methods examination of sleep throughout the alcohol recovery process grounded in the social cognitive theory: The role of self-efficacy and craving. *Health Education & Behavior, 46*(1), 126-136. doi:10.1177/1090198118757820

Brown, C., Willett, J., Goldfine, R., & Goldfine, B. (2018). Sport management internships: Recommendations for improving upon experiential learning. *Journal of Hospitality, Leisure, Sport & Tourism Education, 22*, 75-81. doi:10.1016/j.jhlste.2018.02.001

Bush, A., Persky, A., & Amechi, M. (2019). An Exploration of Pharmacy Education Researchers' Perceptions of and Experiences Conducting Qualitative Research: Challenges and Benefits. *American Journal of Pharmaceutical Education, 1*, 1-21. Retrieved from https://www.ajpe.org/doi/abs/10.5688/ajpe7129

Butler, A. E., Copnell, B., & Hall, H. (2019). Researching people who are bereaved: Managing risks to participants and researchers. *Nursing Ethics, 26*(1), 224-234. doi:10.1177/0969733017695656

Capous-Desyllas, M., & Barron, C. (2017). Identifying and navigating social and institutional challenges of transgender children and families. *Child & Adolescent Social Work Journal, 34*(6), 527-542. doi:10.1007/s10560-017-0491-7

Carcea, I., & Froemke, R. C. (2019). Biological mechanisms for observational learning. *Current Opinion in Neurobiology, 54*, 178-185. doi:10.1016/j.conb.2018.11.008

Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. *Information & Computer Security, 27*(1), 101-121. doi:10.1108/ICS-11-2016-0088

Carminati, L. (2018). Generalizability in qualitative research: A tale of two traditions. *Qualitative Health Research, 28*(13), 2094-2101. doi:10.1177/1049732318788379

Carr, L. T. (1994). The strengths and weaknesses of quantitative and qualitative research: What method for nursing?. *Journal of Advanced Nursing, 20*(4), 716-721. doi:10.1046/j.1365-2648.1994.20040716.x

Carroll, J. A., Sankupellay, M., Rodgers, J., Newcomb, M., & Cook, R. (2018). GoSoapBox in public health tertiary education: A student response system for improving learning experiences and outcomes. *Australasian Journal of Educational Technology, 34*(5), 58-71. doi:10.14742/ajet.3743

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *The Qualitative Report, 21*(5), 811-831. Retrieved from https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2337&context=tqr

Castka, P., & Balzarova, M. A. (2018). An exploration of interventions in ISO 9001 and ISO 14001 certification context–A multiple case study approach. *Journal of Cleaner Production, 174*, 1642-1652. doi:10.1016/j.jclepro.2017.11.096

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity, 5*(1), 1-19. doi:10.1093/cybsec/tyz001

Chauvette, A., Schick-Makaroff, K., & Molzahn, A. E. (2019). Open data in qualitative research. *International Journal of Qualitative Methods, 18*, 1-6. doi:10.1177/1609406918823863

Chen, C. X., Draucker, C. B., & Carpenter, J. S. (2018). What women say about their dysmenorrhea: A qualitative thematic analysis. *BMC Women's Health, 18*(1), 47-54. doi:10.1186/s12905-018-0538-8

Chen, H., & Li, W. (2017). Mobile device users' privacy security assurance behavior: A technology threat avoidance perspective. *Information & Computer Security, 25*(3), 330-344. doi:10.1108/ICS-04-2016-0027

Chen, H. S., & Jai, T.-M. (2019). Cyber alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management, 82*, 326-334. doi:10.1016/j.ijhm.2018.10.002

Clark, K. R., & Vealé, B. L. (2018). Strategies to enhance data collection and analysis in qualitative research. *Radiologic Technology, 89*(5), 482-485. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/29793921

Clarke, V., & Braun, V. (2018). Using thematic analysis in counselling and psychotherapy research: A critical reflection. *Counselling & Psychotherapy Research, 18*(2), 107-110. doi:10.1002/capr.12165

Cleary, M., Horsfall, J., & Hayter, M. (2014). Data collection and sampling in qualitative research: Does size matter? *Journal of Advanced Nursing, 70*(3), 473-475. doi:10.1111/jan.12163

Connolly, L. Y., Lang, M., & Wall, D. S. (2019). Information security behavior: A cross-cultural comparison of Irish and US employees. *Information Systems Management, 36*(4), 1-17. doi:10.1080/10580530.2019.1651113

Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research, 6*(23), 31-38. doi:10.19101/IJACR.2016.623006

Cope, D. G. (2014). Methods and meanings: Credibility and trustworthiness of qualitative research. Oncology Nursing Forum, 41(1), 89-91. doi:10.1188/14.ONF.89-91

Coulson, T., Mason, M., & Nestler, V. (2018). Cyber capability planning and the need for an expanded cybersecurity workforce. *Communications of the IIMA, 16*(2), 1-11. Retrieved from https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=1401&context=ciima

Cuganesan, S., Steele, C., & Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. *Behaviour & Information Technology, 37*(1), 50-65. doi:10.1080/0144929X.2017.1397193

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

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79-98. doi:10.1287/isre.1070.0160

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology, 9*(744), 1-12. doi:10.3389/fpsyg.2018.00744

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

DeCapua, A., Marshall, H. W., & Frydland, N. (2018). The transformational learning journey of a novice ESL teacher of low-literate adults. *Journal of Transformative Education, 16*(1), 17-38. doi:10.1177/1541344617704645

Deighton-Smith, N., & Bell, B. T. (2018). Objectifying fitness: A content and thematic analysis of #fitspiration images on social media. *Psychology of Popular Media Culture, 7*(4), 467-483. doi:10.1037/ppm0000143

DeJonckheere, M., & Vaughn, L. M. (2019). Semistructured interviewing in primary care research: A balance of relationship and rigour. *Family Medicine and Community Health, 7*(2), 1-8. doi:10.1136/fmch-2018-000057

Dohle, S., Diel, K., & Hofmann, W. (2018). Executive functions and the self-regulation of eating behavior: A review. *Appetite, 124*, 4-9. doi:10.1016/j.appet.2017.05.041

Ebneyamini, S., & Moghadam, M. R. S. (2018). Toward developing a framework for conducting case study research. *International Journal of Qualitative Methods, 17*(1), 1-11. doi:10.1177/1609406918817954

Edwards, S., Nolan, A., Henderson, M., Mantilla, A., Plowman, L., & Skouteris, H. (2018). Young children’s everyday concepts of the internet: A platform for cyber-safety education in the early years. *British Journal of Educational Technology*, 49(1), 45-55. doi:10.1111/bjet.12529

Eggenschwiler, J. (2018). A typology of cybersecurity governance models. *St Antony's International Review, 13*(2), 64-78. Retrieved from https://www.ingentaconnect.com/content/stair/stair/2018/00000013/00000002/art00006

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal, 50*(1), 25-32. doi:10.5465/AMJ.2007.24160888

Elias, J., Hendlin, Y. H., & Ling, P. M. (2018). Public versus internal conceptions of addiction: An analysis of internal Philip Morris documents. *PLOS Medicine, 15*(5), 1-18. doi:10.1371/journal.pmed.1002562

Ellis, P. (2019). The language of research (part 20): Understanding the quality of a qualitative paper (2). *Wounds UK, 15*(1), 110-111. Retrieved from https://www.wounds-uk.com/download/wuk_article/7843

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks, 9*(17), 4667-4679. doi:10.1002/sec.1657

Fàbregues, S., & Fetters, M. D. (2019). Fundamentals of case study research in family medicine and community health. Family Medicine and Community Health, 7(2), 1-8. doi:10.1136/fmch-2018-000074

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

Falco, G., Noriega, A., & Susskind, L. (2019). Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. Journal of Cyber Policy, 4(1), 90-116. doi:10.1080/23738871.2019.1586969

Flacking, R., & Dykes, F. (2017). Perceptions and experiences of using a nipple shield among parents and staff – An ethnographic study in neonatal units. *BMC Pregnancy and Childbirth, 17*(1), 1-8. doi:10.1186/s12884-016-1183-6

Fletcher, J. A., & Friedel, J. N. (2018). Interrelationships between funding and state community college governance systems. *Journal of Applied Research in the Community College, 25*(1), 1-15. Retrieved from https://www.researchgate.net/profile/Jeffrey_Fletcher6/publication/324482093_Interrelationships_between_Funding_and_State_Community_College_Governance_Systems/links/5acf5cd60f7e9b18965b1933/Interrelationships-between-Funding-and-State-Community-College-Governance-Systems.pdf

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59*, 26-44. doi:10.1016/j.cose.2016.01.004

Flynn, S. V., & Korcuska, J. S. (2018). Credible phenomenological research: A mixed-methods study. *Counselor Education and Supervision, 57*(1), 34-50. doi:10.1002/ceas.12092

Fomby, P., & Sastry, N. (2019). Data Collection on Sensitive Topics with Adolescents Using Interactive Voice Response Technology. *Methods, Data, Analyses, 13*(1), 91-110. doi:0.12758/mda.2018.05

Font, X., Garay, L., & Jones, S. (2016). A social cognitive theory of sustainability empathy. *Annals of Tourism Research, 58*, 65-80. doi:10.1016/j.annals.2016.02.004

Forero, R., Nahidi, S., Costa, J., Mohsin, M., Fitzgerald, G., Gibson, N., McCarth, S., & Aboagye-Sarfo, P. (2018). Application of four-dimension criteria to assess rigour of qualitative research in emergency medicine. *BMC Health Services Research, 18*(120), 1-13. doi:10.1186/s12913-018-2915-2.

Fu, G., & Clarke, A. (2019). Individual and collective agencies in China's curriculum reform: A case of physics teachers. *Journal of Research in Science Teaching, 56*(1), 45-63. doi:10.1002/tea.21467

Fusch, P. I., & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report, 20*(9), 1408-1416. Retrieved from https://search-proquest-com.ezp.waldenulibrary.org/docview/1721368991?accountid=14872

Geoffroy, P. A., Hoertel, N., Etain, B., Bellivier, F., Delorme, R., Limosin, F., & Peyre, H. (2018). Insomnia and hypersomnia in major depressive episode: Prevalence, sociodemographic characteristics and psychiatric comorbidity in a population-based study. *Journal of Affective Disorders, 226*, 132-141. doi:10.1016/j.jad.2017.09.032

George, G., & Selimos, E. D. (2018). Using narrative research to explore the welcoming of newcomer immigrants: A methodological reflection on a community-based research project. *Forum: Qualitative Social Research, 19*(2), 119-138. doi:10.17169/fqs-19.2.2907

Ghaffari, K., & Lagzian, M. (2018). Exploring users' experiences of using personal cloud storage services: A phenomenological study. *Behaviour & Information Technology, 37*(3), 295–309. doi:10.1080/0144929X.2018.1435722

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing, 74*(10), 4986-5002. doi:10.1007/s11227-018-2337-2

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

Goertzen, M. J. (2017). Introduction to quantitative research and data. *Library Technology Reports, 53*(4), 12-18. doi:10.5860/ltr.53n4

González-Manzano, L., & de Fuentes, J. M. (2019). Design recommendations for online cybersecurity courses. *Computers & Security, 80*, 238–256. doi:10.1016/j.cose.2018.09.009

Goodman, D., Johnson, C. O., Bowen, D., Smith, M., Wenzel, L., & Edwards, K. (2017). De-identified genomic data sharing: The research participant perspective. *Journal of Community Genetics, 8*(3), 173-181. doi:10.1007/s12687-017-0300-1

Goodrich, A. (2019). Spending their leisure time: Adult amateur musicians in a community band. *Music Education Research, 21*(2), 174-184. doi:10.1080/14613808.2018.1563057

Gootman, S. (2016). OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research, 11*(4), 517-525. doi:10.1080/19361610.2016.1211876

Graham, J. D., Li, Y. C., Bray, S. R., & Cairney, J. (2018). Effects of cognitive control exertion and motor coordination on task self-efficacy and muscular endurance performance in children. *Frontiers in Human Neuroscience, 12*(379), 1-14. doi:10.3389/fnhum.2018.00379

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. doi:10.1016/j.cose.2017.11.015

Guo, J., Tang, Y., Wiley, J., Whittemore, R., & Chen, J. L. (2018). Effectiveness of a diabetes prevention program for rural women with prior gestational diabetes mellitus: Study protocol of a multi-site randomized clinical trial. *BMC Public Health, 18*(1), 809-819. doi:10.1186/s12889-018-5725-x

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

Hadlington, L. (2018). Employees attitude towards cyber security and risky online behaviours: An empirical assessment in the United Kingdom. *International Journal of Cyber Criminology, 12*(1), 269-281. doi:10.5281/zenodo.1467909

Halcomb, E. J. (2019). Mixed methods research: The issues beyond combining methods. *Journal of Advanced Nursing, 75*(3), 499-501. doi:10.1111/jan.13877

Hall, J., & Martin, B. R. (2019). Towards a taxonomy of research misconduct: The case of business school research. *Research Policy, 48*, 414-427. doi:10.1016/j.respol.2018.03.006

Hart-Johnson, A. M. (2017). Gaining Access to Socially Stigmatized Samples. *The Qualitative Report, 22*(6), 1550-1564. Retrieved from https://nsuworks.nova.edu/tqr/vol22/iss6/5/

Haydon, G., Browne, G., & van der Riet, P. (2018). Narrative inquiry as a research methodology exploring person centered care in nursing. *Collegian, 25*(1), 125-129. doi:10.1016/j.colegn.2017.03.001

He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce*, 1-9. doi:10.1080/10919392.2019.1611528

Heale, R., & Twycross, A. (2018). What is a case study?. *Evidence-Based Nursing, 21*(1), 7-8. doi:10.1136/eb-2017-102845

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2016). Code saturation versus meaning saturation: How many interviews are enough? *Qualitative Health Research, 27*(4), 591-608. doi:10.1177/1049732316665344

Herath, T., Yim, M. S., D'Arcy, J., Nam, K., & Rao, H. R. (2018). Examining employee security violations: Moral disengagement and its environmental influences. *Information Technology & People, 31*(6), 1135-1162. doi:10.1108/ITP-10-2017-0322

Hermogeno, M. S. (2019). Assessment on the cybersecurity awareness in academic institutions. *International Journal of Engineering Science, 9*(3), 20543-20547. Retrieved from https://pdfs.semanticscholar.org/d94b/11ddcbfcb523a020588e286e072755613731.pdf

Hess, M. F., & Cottrell, J. H. (2016). Fraud risk management: A small business perspective. *Business Horizons, 59*(1), 13-18. doi:10.1016/j.bushor.2015.09.005

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

Ho, M. H. R., Uy, M. A., Kang, B. N., & Chan, K. Y. (2018). Impact of entrepreneurship training on entrepreneurial efficacy and alertness among adolescent youth. *Frontiers in Education, 3*(13), 1-10. doi:10.3389/feduc.2018.00013

Hoch, E., Scheiter, K., & Schüler, A. (2019). Implementation intentions for improving self-regulation in multimedia learning: Why don't they work?. *The Journal of Experimental Education*, 1-23. doi:10.1080/00220973.2019.1628693

Hodhod, R., Wang, S., & Khan, S. (2018). Cybersecurity curriculum development using AI and decision support expert system. *International Journal of Computer Theory and Engineering, 10*(4), 111-115. doi:10.7763/IJCTE.2018.V10.1209

Hovey, R., Jordan, S., Bedos, C., Rodriguez, C., & Apelian, N. (2018). Reflective practice and the role of transformational learning in healthcare. *International Journal of Whole Person Care, 5*(1), 21-22. doi:10.26443/ijwpc.v5i1.144

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A Survey. *ACM Computing Surveys, 51*(4), 1-36. doi:10.1145/3199674

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

Ikeda, E., Hinckson, E., Witten, K., & Smith, M. (2018). Associations of children's active school travel with perceptions of the physical environment and characteristics of the social environment: A systematic review. *Health & Place, 54*, 118-131. doi:10.1016/j.healthplace.2018.09.009

Irani, E. (2019). The use of videoconferencing for qualitative interviewing: Opportunities, challenges, and considerations. *Clinical Nursing Research, 28*(1), 3-8. doi:10.1177/1054773818803170

Ivanova-Gongne, M., Koporcic, N., Dziubaniuk, O., & Mandják, T. (2018). Collecting rich qualitative data on business relationships and networks in CEE countries:

Challenges and plausible solutions. *Industrial Marketing Management, 70*, 193-204. doi:10.1016/j.indmarman.2017.07.007

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems, 28*(1), 66-82. doi:10.1016/j.jsis.2018.09.003

Jentoft, N., & Olsen, T. S. (2019). Against the flow in data collection: How data triangulation combined with a “slow” interview technique enriches data. *Qualitative Social Work, 18*(2), 179-193. doi:10.1177/1473325017712581

Jeong, C. Y., Lee, S. Y. T., & Lim, J. H. (2019). Information security breaches and IT security investments: Impacts on competitors. *Information & Management, 56*(5), 681-695. doi:10.1016/j.im.2018.11.003

Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning, 12*(1), 150-158. doi:10.11591/edulearn.v12i1.7736

Johnson, J. L., Adkins, D., & Chauvin, S. (2019). Quality indicators of rigor in qualitative research. *American Journal of Pharmaceutical Education*, 1-22. Retrieved from https://www.ajpe.org/doi/abs/10.5688/ajpe7120.

Jones, J., & Smith, J. (2017). Ethnography: Challenges and opportunities. *Evidence-Based Nursing, 20*(4), 98-100. doi:10.1136/eb-2017-102786

Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce, 28*(3), 269-282. doi:10.1080/10919392.2018.1484598

Kahan, S., Wilson, D. K., & Sweeney, A. M. (2018). The role of behavioral medicine in the treatment of obesity in primary care. *Medical Clinics, 102*(1), 125-133. doi:10.1016/j.mcna.2017.09.002

Kappelman, L., Johnson, V., Maurer, C., McLean, E., Torres, R., David, A., & Nguyen, Q. (2018). The 2017 SIM IT issues and trends study. *MIS Quarterly Executive, 17*(1), 53-88. doi:10.17705/2msqe.00008

Karanja, E. (2017). The role of the chief information security officer in the management of IT security. *Information & Computer Security, 25*(3), 300-329. doi:10.1108/ICS-02-2016-0013

Kelle, U., Kühberger, C., & Bernhard, R. (2019). How to use mixed-methods and triangulation designs: An introduction to history education research. *History Education Research Journal, 16*(1), 5-23. doi:10.18546/HERJ.16.1.02

Kentischer, F., Kleinknecht, D. M., Spirig, R., Frei, I. A., & Huber, E. (2018). Patient-related complexity of care: A challenge or overwhelming burden for nurses – A qualitative study. *Scandinavian Journal of Caring Sciences, 32*(1), 204–212. doi:10.1111/scs.12449

Khorakian, A., & Sharifirad, M. S. (2019). Integrating implicit leadership theories, leader–member exchange, self-efficacy, and attachment theory to predict job performance. *Psychological Reports, 122*(3), 1117-1144. doi:10.1177/0033294118773400

Kim, L. (2017). Cybersecurity awareness: Protecting data and patients. *Nursing management, 48*(4), 16-19. doi:10.1097/01.NUMA.0000514066.30572.f3

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. *Frontiers in Psychology, 9*(39), 1-19. doi:10.3389/fpsyg.2018.00039

Kolkowska, E., Karlsson, F., & Hedström, K. (2017). Towards analysing the rationale of information security non-compliance: Devising a value-based compliance analysis method. *Journal of Strategic Information Systems, 26*, 39-57. doi:10.1016/j.jsis.2016.08.005

Kong, H., Jiang, X., Chan, W., & Zhou, X. (2018). Job satisfaction research in the field of hospitality and tourism. *International Journal of Contemporary Hospitality Management, 30*(5), 2178-2194. doi:10.1108/IJCHM-09-2016-0525

Kongsholm, N. C. H., & Kappel, K. (2017). Is consent based on trust morally inferior to consent based on information?. *Bioethics, 31*(6), 432-442. doi:10.1111/bioe.12342

Kortjan, N., & Von Solms, R. (2014). A conceptual framework for cyber-security awareness and education in SA. *South African Computer Journal, 52*(1), 29-41. Retrieved from http://sacj.cs.uct.ac.za/index.php/sacj/article/download/201/95

Koyuncu, M., & Pusatli, T. (2019). Security awareness level of smartphone users: An exploratory case study. *Mobile Information Systems*, 1-11. doi:10.1155/2019/2786913

Krasznay, C., & Hámornik, B. P. (2019). Human factors approach to cybersecurity teamwork - The military perspective. *Advances in Military Technology, 14*(2), 291-305. doi:10.3849/aimt.01296

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25*(1), 1-10. doi:10.3233/THC-161263

Kulasegaram, K., Axelrod, D., Ringsted, C., & Brydges, R. (2018). Do one then see one: Sequencing discovery learning and direct instruction for simulation-based technical skills training. *Academic Medicine, 93*(11), 37-44. doi:10.1097/ACM.0000000000002378

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

Lau, C., Kitsantas, A., Miller, A. D., & Rodgers, E. B. D. (2018). Perceived responsibility for learning, self-efficacy, and sources of self-efficacy in mathematics: A study of international baccalaureate primary years programme students. *Social Psychology of Education, 21*(3), 603-620. doi:10.1007/s11218-018-9431-4

Leggett, A. (2018). Environmentalist protection: Feminist methodology and participant risk for research with Chinese NGOs. *Contemporary Social Science, 13*(3/4), 354-371. doi:10.1080/21582041.2017.1418522

Levitt, H. M., Bamberg, M., Frost, D. M., Creswell, J. W., Josselson, R., & Suarez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA publications and communications board task force report. *The American Psychologist, 73*(1), 26-46. doi:10.1037/amp0000151

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45*, 13-24. doi:10.1016/j.ijinfomgt.2018.10.017

Lin, F. L. Y. (2019). Using Thematic Analysis to Facilitate Meaning-Making in Practice-Led Art and Design Research. *International Journal of Art & Design Education, 38*(1), 153-167. doi:10.1111/jade.12177

Lin, H. C., & Chang, C. M. (2018). What motivates health information exchange in social media? The roles of the social cognitive theory and perceived interactivity. *Information & Management, 55*(6), 771-780. doi:10.1016/j.im.2018.03.006

Lin, L. (2009). Data management and security in qualitative research. *Dimensions of Critical Care Nursing, 28*(3), 132-137. doi:10.1097/DCC.0b013e31819aeff6

Liu, C. H., Tang, W. R., Wang, H. M., & Lee, K. C. (2013). How cancer patients build trust in traditional Chinese medicine. *European Journal of Integrative Medicine, 5*(6), 495-500. doi:10.1016/j.eujim.2013.08.003

Locke, E. A. (1987). Social foundations of thought and action: A social-cognitive view. *Academy of Management Review, 12*(1), 169-171. https://doi.org/10.5465/amr.1987.4306538

Lo Schiavo, M., Prinari, B., Saito, I., Shoji, K., & Benight, C. C. (2018). A dynamical systems approach to triadic reciprocal determinism of social cognitive theory. *Mathematics & Computers in Simulation, 159*, 18-38. doi:10.1016/j.matcom.2018.10.006

Lowry, P. B., Zhang, J., & Wu, T. (2017). Nature or nurture? A meta-analysis of the factors that maximize the prediction of digital piracy by using social cognitive theory as a framework. *Computers in Human Behavior*, *68*, 104-120. doi:10.1016/j.chb.2016.11.015

Lucero, J., Wallerstein, N., Duran, B., Alegria, M., Greene-Moton, E., Israel, B., Kastelic, S., Magarati, M., Oetzel, J., Pearson, C., Schulz, A., Villegas, M., & White Hat, E. R. (2018). Development of a mixed methods investigation of process and outcomes of community-based participatory research. *Journal of Mixed Methods Research, 12*(1), 55-74.

Lund, R., Panda, S. M., & Dhal, M. P. (2016). Narrating spaces of inclusion and exclusion in research collaboration - researcher-gatekeeper dialogue. *Qualitative Research, 16*(3), 280-292. doi:10.1177/1468794115611208

Magny-Normilus, C., Mawn, B., & Dalton, J. (2019). Self-management of type 2 diabetes in adult Haitian immigrants: A qualitative study. *Journal of Transcultural Nursing*, 1-8. doi:10.1177/1043659619841586

Maher, C., Hadfield, M., Hutchings, M., & de Eyto, A. (2018). Ensuring rigor in qualitative data analysis: A design research approach to coding combining NVivo with traditional material methods. *International Journal of Qualitative Methods, 17*(1), 1-13. doi:10.1177/1609406918786362

Manton, K. J., Gauld, C. S., White, K. M., Griffin, P. M., & Elliott, S. L. (2019). Qualitative study investigating the underlying motivations of healthy participants in phase I clinical trials. *BMJ Open, 9*(1), 1-9. doi:10.1136/bmjopen-2018-024224

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

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

Mavhandu-Mudzusi, A. H. (2018). The couple interview as a method of collecting data in interpretative phenomenological analysis studies. *International Journal of Qualitative Methods, 17*(1), 1-9. doi:10.1177/1609406917750994

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

McGonagle, K. A., & Freedman, V. A. (2017). The effects of a delayed incentive on response rates, response mode, data quality, and sample bias in a nationally representative mixed mode study. *Field Methods, 29*(3), 221-237. doi:10.1177/1525822X16671701

McGrath, C., Palmgren, P. J., & Liljedahl, M. (2018). Twelve tips for conducting qualitative research interviews. *Medical Teacher, 41*(9), 1002-1006. doi:10.1080/0142159X.2018.1497149

McHugh, T. L. F., Deal, C. J., Blye, C.J., Dimler, A. J., Halpenny, E. A., Sivak, A., & Holt, N. L. (2019). A meta-study of qualitative research examining sport and recreation experiences of indigenous youth. *Qualitative Health Research, 29*(1), 42-54. doi:10.1177/1049732318759668

McLaughlin, M. D., & Gogan, J. (2018). Challenges and best practices in information security management. *MIS Quarterly Executive, 17*(3), 237-262. Retrieved from https://aisel.aisnet.org/misqe/vol17/iss3/6

Mei, X. Y., & Lantai, T. (2018). Understanding travel constraints: An exploratory study of Mainland Chinese International Students (MCIS) in Norway. *Tourism Management Perspectives, 28*, 1-9. doi:10.1016/j.tmp.2018.07.003

Meijers, M. H., Remmelswaal, P., & Wonneberger, A. (2018). Using visual impact metaphors to stimulate environmentally friendly behavior: The roles of response efficacy and evaluative persuasion knowledge. *Environmental Communication*, 1-14. doi:10.1080/17524032.2018.1544160

Melin, U., & Axelsson, K. (2016). Action in action research: Elaborating the concepts of action, roles and dilemmas in a public e-service development project. *Journal of Systems and Information Technology, 18*(2), 118-147. doi:10.1108/JSIT-10-2015-0074

Merlin, J. S., Young, S. R., Johnson, M. O., Saag, M., Demonte, W., Kerns, R., Bair, M. J., Kertesz, S., Turan, J. M., Kilgore, M., Clay, O. J., Pekmezi, D., & Davies, S. (2018). Intervention mapping to develop a social cognitive theory-based intervention for chronic pain tailored to individuals with HIV. *Contemporary Clinical Trials Communications, 10*, 9-16. doi:10.1016/j.conctc.2018.02.004

Miraglia, M., Cenciotti, R., Alessandri, G., & Borgogni, L. (2017). Translating self-efficacy in job performance over time: The role of job crafting. *Human Performance, 30*(5), 254-271. doi:10.1080/08959285.2017.1373115

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. *International Management Review, 14*(2), 5-10. Retrieved from http://www.imrjournal.org/uploads/1/4/2/8/14286482/imr-v14n2art1.pdf

Moen, T. (2006). Reflections on the narrative research approach. *International Journal of Qualitative Methods, 5*(4), 56-69. doi:10.1177/160940690600500405

Mohajan, H. K. (2018). Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People, 7*(1), 23-48. doi:10.26458/jedep.v7i1.571

Molley, S., Derochie, A., Teicher, J., Bhatt, V., Nauth, S., Cockburn, L., & Langlois, S. (2018). Patient experience in health professions curriculum development. *Journal of Patient Experience, 5*(4), 303-309. doi:10.1177/2374373518765795

Molok, N. N. A., Ahmad, A., & Chang, S. (2018). A case analysis of securing organisations against information leakage through online social networking. *International Journal of Information Management, 43*, 351-356. doi:10.1016/j.ijinfomgt.2018.08.013

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods, 1*(2), 13-22. doi:10.1177/160940690200100202

Moser, A., & Korstjens, I. (2017a). Series: Practical guidance to qualitative research. Part 1: Introduction. *European Journal of General Practice, 23*(1), 271-273. doi:10.1080/13814788.2017.1375093

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

Moser, A., & Korstjens, I. (2018). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice, 24*(1), 9-18.10.1080/13814788.2017.1375091

Motl, R. W., Pekmezi, D., & Wingo, B. C. (2018). Promotion of physical activity and exercise in multiple sclerosis: Importance of behavioral science and theory. *Multiple Sclerosis Journal - Experimental, Translational and Clinical, 4*(3), 1-8. doi:10.1177/2055217318786745

Moustakas, C. E. (1994). *Phenomenological research methods*. Thousand Oaks, CA: Sage Publications.

Muhirwe, J., & White, N. (2016). Cybersecurity awareness and practice of next generation corporate technology users. *Issues in Information Systems, 17*(2), 183-192. Retrieved from http://iacis.org/iis/2016/2_iis_2016_183-192.pdf

Mulyaningsih, I., Suwandi, S., Setiawan, B., & Rohmadi, M. (2018). PARMI (Production, Attention, Retention, Motivation, and Innovation): An alternative to improving scientific writing skills. *Lingua Cultura, 12*(4), 317-321. doi:10.21512/lc.v12i4.4159

Murray, P. D., Bierer, B. E., Hirschfeld, S., Klein, A. K., & Davis, J. M. (2018). Assessment of a shortened informed consent form for pediatric research: A pilot study. *Pediatric Research, 84*(4), 516-519. https://doi.org/10.1038/s41390-018-0043-7

Myneni, S., Patel, V. L., Bova, G. S., Wang, J., Ackerman, C. F., Berlinicke, C. A., Chen, S. H., Lindvall, M., & Zack, D. J. (2016). Resolving complex research data management issues in biomedical laboratories: Qualitative study of an industry–academia collaboration. *Computer Methods and Programs in Biomedicine, 126*, 160-170. doi:10.1016/j.cmpb.2015.11.001

Na, O., Park, L. W., Yu, H., Kim, Y., & Chang, H. (2019). The rating model of corporate information for economic security activities. *Security Journal*, 1-22. doi:10.1057/s41284-019-00171-z

Nakabayashi, K. (2018). Course design investigation and trial on the subject of self-regulated learning using video content and online report submission. *Interactive Technology and Smart Education, 15*(2), 104-118. doi:10.1108/ITSE-10-2017-0050

Namey, E., Guest, G., McKenna, K., & Chen, M. (2016). Evaluating bang for the buck: A cost-effectiveness comparison between individual interviews and focus groups based on thematic saturation levels. *American Journal of Evaluation, 37*(3), 425-440. doi:10.1177/1098214016630406

Nasir, A., Arshah, R. A., Hamid, M. R. A., & Fahmy, S. (2019). An analysis on the dimensions of information security culture concept: A review. *Journal of Information Security and Applications, 44*, 12-22. doi:10.1016/j.jisa.2018.11.003

National Institutes of Health. (1979). National commission for the protection of human subjects of biomedical and behavioral research. *The Belmont Report. Ethical Principles and Guidelines for the Protection of Human Subjects of Research.*

Neale, J. (2016). Iterative categorization (IC): A systematic technique for analysing qualitative data. *Addiction, 111*(6), 1096-1106. doi:10.1111/add.13314

Nolan, S., Hendricks, J., Williamson, M., & Ferguson, S. (2017). Using narrative inquiry to listen to the voices of adolescent mothers in relation to their use of social networking sites (SNS). *Journal of Advanced Nursing, 74*(3), 743-751. doi:10.1111/jan.13458

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods, 16*(1), 1-13. doi:10.1177/1609406917733847

Nusbaum, L., Douglas, B., Damus, K., Paasche-Orlow, M., & Estrella-Luna, N. (2017). Communicating risks and benefits in informed consent for research: A qualitative study. *Global Qualitative Nursing Research, 4*, 1-13. doi:10.1177/2333393617732017

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

O'Halloran, L., Littlewood, M., Richardson, D., Tod, D., & Nesti, M. (2018). Doing descriptive phenomenological data collection in sport psychology research. *Sport in Society, 21*(2), 302-313. doi:10.1080/17430437.2016.1159199

Okumus, F., Altinay, L., & Roper, A. (2007). Gaining access for research: Reflections from experience. *Annals of Tourism Research, 34*(1), 7-26. doi:10.1016/j.annals.2006.07.006

Oltmann, S. (2016). Qualitative interviews: A methodological discussion of the interviewer and respondent contexts. *Forum: Qualitative Social Research, 2*(15), 1-16. doi:10.17169/fqs-17.2.2551

O’Sullivan, K., & Howden-Chapman, P. (2017). Mixing methods, maximising results: Use of mixed methods research to investigate policy solutions for fuel poverty and energy vulnerability. *Indoor and Built Environment, 26*(7), 1009-1017. doi:10.1177/1420326X17707327

Palos-Sanchez, P., Saura, J. R., Reyes-Menendez, A., & Esquivel, I. V. (2018). Users acceptance of location-based marketing apps in tourism sector: An exploratory analysis. *Journal of Spatial and Organizational Dynamics, 6*(3), 258-270. Retrieved from https://www.jsod-cieo.net/journal/index.php/jsod/article/download/144/129

Pandey, A. (2018). Non-adherence to lifestyle (diet and exercise) modification recommendations among the type 2 diabetes mellitus patients in a tertiary level hospital. *Journal of Institute of Medicine, 40*(1), 37-45. Retrieved from http://jiom.com.np/index.php/jiomjournal/article/download/975/925

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

Park, E. H., Kim, J., Wiles, L. L., & Park, Y. S. (2018). Factors affecting intention to disclose patients’ health information. *Computers & Security, 8*(1), 1-14. doi:10.1016/j.cose.2018.05.003

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security, 66*, 40-51. doi:10.1016/j.cose.2017.01.004

Patino, C. M., & Ferreira, J. C. (2018). Inclusion and exclusion criteria in research studies: definitions and why they matter. *Jornal Brasileiro De Pneumologia, 44*(2), 84. doi:10.1590/s1806-37562018000000088

Patton, S. K., & Henry, L. J. (2019). Nursing students' experience with fall risk assessment in older adults. *Nursing & Health Sciences, 21*(1), 21-27. doi:10.1111/nhs.12427

Pendley, J. A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance, 29*(1), 53-58. doi:10.1002/jcaf.22291

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

Phillippi, J., & Lauderdale, J. (2018). A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research, 28*(3), 381-388. doi:10.1177/1049732317697102

Phillips, M., & Lu, J. (2018). A quick look at NVivo. *Journal of Electronic Resources Librarianship, 30*(2), 104-106. doi:10.1080/1941126X.2018.1465535

Phillips, R., & Tanner, B. (2019). Breaking down silos between business continuity and cyber security. *Journal of Business Continuity & Emergency Planning, 12*(3), 224-232. Retrieved from https://eds-a-ebscohost-com.ezp.waldenulibrary.org/eds/Citations/FullTextLinkClick?sid=5340134a-f676-45b8-ab4d-6d24a3a72c0d@sessionmgr4008&vid=2&id=pdfFullText

Phoenix, M., Nguyen, T., Gentles, S. J., VanderKaay, S., Cross, A., & Nguyen, L. (2018). Using qualitative research perspectives to inform patient engagement in research. *Research involvement and engagement, 4*(1), 20-24. doi:10.1186/s40900-018-0107-1

Pierre, M. (2018). WASP (Write a Scientific Paper): Informed consent in research. *Early Human Development, 124*, 54-57. doi:10.1016/j.earlhumdev.2018.04.025

Pinnell, M., Franco, M. S., Petry, L., Mian, A., Doudican, B., & Srinivasan, R. (2018). Leveraging regional strengths for STEM teacher professional development: Results from an NSF RET program focused on advanced manufacturing and materials. *Research in the Schools, 25*(1), 20-34. Retrieved from https://eds-b-ebscohost-com.ezp.waldenulibrary.org/eds/Citations/FullTextLinkClick?sid=b05fee87-e838-4215-a2cf-8ed4c6d9d642@sessionmgr101&vid=1&id=pdfFullText

Plachkinova, M., & Maurer, C. (2018). Teaching case: Security breach at Target. *Journal of Information Systems Education, 29*(1), 11-20. Retrieved from https://eds-b-ebscohost-com.ezp.waldenulibrary.org/eds/Citations/FullTextLinkClick?sid=2d066237-c0f7-436e-9938-0bb453d7f6a0@pdc-v-sessmgr01&vid=1&id=pdfFullText

Polkinghorne, D. E. (2005). Language and meaning: Data collection in qualitative research. *Journal of Counseling Psychology, 52*(2), 137-145. doi:10.1037/0022-0167.52.2.137

Queiros, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies, 3*(9), 369-387. doi:10.5281/zenodo.887089.

Qutoshi, S. B. (2018). Phenomenology: A philosophy and method of inquiry. *Journal of Education and Educational Development, 5*(1), 215-222. doi:10.22555/joeed.v5i1.2154

Råheim, M., Magnussen, L. H., Sekse, R. J., Lunde, Å., Jacobsen, T., & Blystad, A. (2016). Researcher-researched relationship in qualitative research: Shifts in positions and researcher vulnerability. *International Journal of Qualitative Studies on Health and Well-Being, 11*, 1-12. doi:10.3402/qhw.v11.30996

Rahim, N. H. A., Hamid, S., & Kiah, L. M. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. *Malaysian Journal of Computer Science, 32*(3), 221-245. doi:10.22452/mjcs.vol32no3.4

Rahman, M. S. (2017). The advantages and disadvantages of using qualitative and quantitative approaches and methods in language "testing and assessment" research: A literature review. *Journal of Education and Learning, 6*(1), 102-112. doi:10.5539/jel.v6n1p102

Regnault, A., Willgoss, T., & Barbic, S. (2018). Towards the use of mixed methods inquiry as best practice in health outcomes research. *Journal of Patient-Reported Outcomes, 2*(1), 19-22. doi:10.1186/s41687-018-0043-8

Rettke, H., Pretto, M., Spichiger, E., Frei, I. A., & Spirig, R. (2018). Using reflexive thinking to establish rigor in qualitative research. *Nursing Research, 67*(6), 490-497. doi:10.1097/NNR.0000000000000307

Ricci, J., Breitinger, F., & Baggili, I. (2018). Survey results on adults and cybersecurity education. *Education and Information Technologies*, 1-19. doi:10.1007/s10639-018-9765-8

Ridder, H. G. (2017). The theory contribution of case study research designs. *Business Research, 10*(2), 281-305. doi:10.1007/s40685-017-0045-z

Rivard, J. R., Fisher, R. P., Robertson, B., & Mueller, D. H. (2014). Testing the cognitive interview with professional interviewers: Enhancing recall of specific details of recurring events. *Applied Cognitive Psychology, 28*(6), 917-925. doi:10.1002/acp.3026

Robertson, A. E., Stanfield, A. C., Watt, J., Barry, F., Day, M., Cormack, M., & Melville, C. (2018). The experience and impact of anxiety in autistic adults: A thematic analysis. *Research in Autism Spectrum Disorders, 46*, 8-18. doi:10.1016/j.rasd.2017.11.006

Roloff, J., & Zyphur, M. J. (2018). Null findings, replications and preregistered studies in business ethics research. *Journal of Business Ethics*, 1-11. https://doi.org/10.1007/s10551-018-3864-8

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

Roulston, K. (2018). Qualitative interviewing and epistemics. *Qualitative Research, 18*(3), 322-341. doi:10.1177/1468794117721738

Rubenstein, L. D., Ridgley, L. M., Callan, G. L., Karami, S., & Ehlinger, J. (2018). How teachers perceive factors that influence creativity development: Applying a Social Cognitive Theory perspective. *Teaching and Teacher Education, 70*, 100-110. doi:10.1016/j.tate.2017.11.012

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A case study in Canada. *Journal of Cases on Information Technology (JCIT), 21*(3), 26-39. doi:10.4018/JCIT.2019070102

Sanders, S., Stensland, M., & Juraco, K. (2018). Agency behind bars: Advance care planning with aging and dying offenders. *Death Studies, 42*(1), 45-51. doi:10.1080/07481187.2017.1303552

Sarstedt, M., Bengart, P., Shaltoni, A. M., & Lehmann, S. (2018). The use of sampling methods in advertising research: A gap between theory and practice. *International Journal of Advertising, 37*(4), 650-663. doi:10.1080/02650487.2017.1348329

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: Exploring its conceptualization and operationalization. *Quality & Quantity, 52*(4), 1893-1907. doi:10.1007/s11135-017-0574-8

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the human: The prevalence paradox in cybersecurity. *Human Factors, 5*, 597-609. doi:10.1177/0018720818780472

Scharp, K. M., & Sanders, M. L. (2019). What is a theme? Teaching thematic analysis in qualitative communication research methods. *Communication Teacher, 33*(2), 117-121. doi:10.1080/17404622.2018.1536794

Schoenfeld, J., Segal, G., & Borgia, D. (2017). Social cognitive career theory and the goal of becoming a certified public accountant. *Accounting Education*, *26*(2), 109-126. doi:10.1080/09639284.2016.1274909

Schoon, I., & Heckhausen, J. (2019). Conceptualizing individual agency in the transition from school to work: A social-ecological developmental perspective. *Adolescent Research Review*, 1-14. doi:10.1016/j.jvb.2010.06.006

Schwartz, S., Ross, A., Carmody, S., Chase, P., Coley, S. C., Connolly, J., Petrozzino, C., & Zuk, M. (2018). The evolving state of medical device cybersecurity. *Biomedical Instrumentation & Technology, 52*(2), 103-111. doi:10.2345/0899-8205-52.2.103

Seo, J. H., Bruner, M., Payne, A., Gober, N., McMullen, D., & Chakravorty, D. K. (2019). Using Virtual Reality to Enforce Principles of Cybersecurity. *Journal of Computational Science, 10*(1), 81-87. doi:10.22369/issn.2153-4136/10/1/13

Sessford, J. D., Brawley, L. R., Cary, M. A., Flora, P. K., Blouin, J. E., Strachan, S. M., & Gyurcsik, N. C. (2019). Facing multiple barriers to exercise: Does stronger efficacy help individuals with arthritis?. *Applied Psychology: Health and Well-Being, 11*(1), 59-79. doi:10.1111/aphw.12144

Shabani, M., & Borry, P. (2018). Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation. *European Journal of Human Genetics, 26*(2), 149–156. doi:10.1038/s41431-017-0045-7

Shamir, B., & Eilam, G. (2005). “What’s your story?” A life-stories approach to authentic leadership development. *The Leadership Quarterly, 16*(3), 395-417. doi:10.1016/j.leaqua.2005.03.005

Shappie, A. T., Dawson, C. A., & Debb, S. M. (2019). Personality as a predictor of cybersecurity behavior. *Psychology of Popular Media Culture, 2019*, 1-6. doi:10.1037/ppm0000247

Sheehan, B., Murphy, F., Mullins, M., & Ryan, C. (2018). Connected and autonomous vehicles: A cyber-risk classification framework. *Transportation Research Part A, 124*, 523-536. doi:10.1016/j.tra.2018.06.033

Shelly, M., & Jackson, M. (2018). Research data management compliance: Is there a bigger role for university libraries? *Journal of the Australian Library & Information Association, 67*(4), 394-410. doi:10.1080/24750158.2018.1536690

Shepherd, L., & Macklin, R. (2018). Erosion of informed consent in U.S. research. *Bioethics, 33*(1), 4-12. doi:10.1111/bioe.12532

Sherif, V. (2018). Evaluating preexisting qualitative research data for secondary analysis. *Forum: Qualitative Social Research, 19*(2), 26-42. doi:10.17169/fqs-19.2.2821

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

Sil, A., & Das, N. K. (2017). Informed consent process: Foundation of the researcher-participant bond. *Indian Journal of Dermatology, 62*(4), 380-386. doi:10.4103/ijd.IJD_272_17

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018). Can sample size in qualitative research be determined a priori? *International Journal of Social Research Methodology, 21*(5), 619-634. doi:10.1080/13645579.2018.1454643

Sim, J., Saunders, B., Waterfield, J., & Kingstone, T. (2018b). The sample size debate: Response to Norman Blaikie. *International Journal of Social Research Methodology, 21*(5), 643-646. doi:10.1080/13645579.2018.1454642

Singer, J. N., Shaw, S., Hoeber, L., Walker, N., Agyemang, K. J. A., & Rich, K. (2019). Critical conversations about qualitative research in sport management. *Journal of Sport Management, 33*(1), 50-63. doi:10.1123/jsm.2018-0085

Sitzmann, T., & Weinhardt, J. M. (2018). Training engagement theory: A multilevel perspective on the effectiveness of work-related training. *Journal of Management, 44*(2), 732-756. doi:10.1177/0149206315574596

Smith, D. T., & Ali, A. I. (2019). You've been hacked: A technique for raising cyber security awareness. *Issues in Information Systems, 20*(1), 186-194. Retrieved from https://iacis.org/iis/2019/1_iis_2019_186-194.pdf

Smith, B., & McGannon, K. R. (2018). Developing rigor in qualitative research: Problems and opportunities within sport and exercise psychology. *International Review of Sport and Exercise Psychology, 11*(1), 101-121. doi:10.1080/1750984X.2017.1317357

Spiers, J., Morse, J. M., Olson, K., Mayan, M., & Barrett, M. (2018). Reflection/commentary on a past article: "Verification strategies for establishing reliability and validity in qualitative research." *International Journal of Qualitative Methods, 17*, 1-2. doi:10.1177/1609406918788237

Squires, A., & Dorsen, C. (2018). Qualitative research in nursing and health professions regulation. *Journal of Nursing Regulation, 9*(3), 15-26. doi:10.1016/S2155-8256(18)30150-9

Stajkovic, A. D., Bandura, A., Locke, E. A., Lee, D., & Sergent, K. (2018). Test of three conceptual models of influence of the big five personality traits and self-efficacy on academic performance: A meta-analytic path-analysis. *Personality and Individual Differences, 120*, 238-245. doi:10.1016/j.paid.2017.08.014

Sugihara, T., Fujinami, T., Jones, R., Kadowaki, K., & Ando, M. (2015). Enhancing care homes with assistive video technology for distributed caregiving. *AI & Society, 30*(4), 509-518. doi:10.1007/s00146-014-0560-9

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

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian Journal of Hospital Pharmacy, 68*(3), 226-231. doi:10.1080/08870449608400256

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *Journal of Cyber Policy, 3*(2), 147-164. doi:10.1080/23738871.2018.1513053

Tambo, E., & Adama, K. (2017). Promoting cybersecurity awareness and resilience approaches, capabilities and actions plans against cybercrimes and frauds in Africa. *International Journal of Cyber-Security and Digital Forensics, 6*(3), 126-138. doi:10.17781/P002278

Terlizzi, M. A., Meirelles, F. D. S., & Viegas Cortez da Cunha, M. A. (2017). Behavior of Brazilian banks employees on Facebook and the cybersecurity governance. *Journal of Applied Security Research, 12*(2), 224-252. doi:10.1080/19361610.2017.1277886

Timms, K. (2017). BYOD must be met with a wider appreciation of the cyber-security threat. *Computer Fraud & Security, 2017*(7), 5-8. doi:10.1016/S1361-3723(17)30058-1

Tur-Porcar, A., Roig-Tierno, N., & Llorca Mestre, A. (2018). Factors affecting entrepreneurship and business sustainability. *Sustainability, 10*(2), 1-12. doi:10.3390/su10020452

Uprichard, E., & Dawney, L. (2019). Data diffraction: Challenging data integration in mixed methods research. *Journal of Mixed Methods Research, 13*(1), 19-32. doi:10.1177/1558689816674650

Usman, L. M. (2018). Terrorism and female teacher leadership in girls' secondary school. *International Journal of Educational Management, 32*(4), 669-688. doi:10.1108/IJEM-04-2017-0084

Uszynski, M. K., Casey, B., Hayes, S., Gallagher, S., Purtill, H., Motl, R. W., & Coote, S. (2018). Social cognitive theory correlates of physical activity in inactive adults with multiple sclerosis. *International Journal of MS Care*, *20*(3), 129-135. doi:10.7224/1537-2073.2016-111

Van Horne, S., & Murniati, C. T. (2016). Faculty adoption of active learning classrooms. *Journal of Computing in Higher Education, 28*(1), 72-93. doi:10.1007/s12528-016-9107-z

Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. *Communication Research, 45*(8), 1146-1166. doi:10.1177/0093650215627483

Wadams, M., & Park, T. (2018). Qualitative research in correctional settings: Researcher bias, western ideological influences, and social justice. *Journal of Forensic Nursing, 14*(2), 72-79. doi:10.1097/JFN.0000000000000199

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems, 19*(3), 150-159. Retrieved from http://www.iacis.org/iis/2018/3_iis_2018_150-159.pdf

Wang, S., Hung, K., & Huang, W. J. (2019). Motivations for entrepreneurship in the tourism and hospitality sector: A social cognitive theory perspective. *International Journal of Hospitality Management, 78*, 78-88. doi:10.1016/j.ijhm.2018.11.018

Ward, D, & Webster, A. (2018). Understanding the lived experiences of university students with autism spectrum disorder (ASD): A phenomenological study. *International Journal of Disability, Development, and Education, 65*(4), 373-392. doi:10.1080/1034912X.2017.1403573

Wilk, V., Soutar, G. N., & Harrigan, P. (2019). Tackling social media data analysis: Comparing and contrasting QSR NVivo and Leximancer. *Qualitative Market Research: An International Journal, 22*(2), 94-113. doi:10.1108/QMR-01-2017-0021

Wilson, S. (2018). A framework for security technology cohesion in the era of the GDPR. *Computer Fraud & Security, 2018*(12), 8-11. doi:10.1016/S1361-3723(18)30119-2

Wixted, J. T., Mickes, L., & Fisher, R. P. (2018). Rethinking the reliability of eyewitness memory. *Perspectives on Psychological Science, 13*(3), 324-335. doi:10.1177/1745691617734878

Wood, R., & Bandura, A. (1989). Social cognitive theory of organizational management. *Academy of Management Review, 14*(3), 361-384. doi:10.5465/AMR.1989.4279067

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382. doi:10.1016/j.chb.2018.02.019

Yeong, M. L., Ismail, R., Ismail, N. H., & Hamzah, M. I. (2018). Interview protocol refinement: Fine-tuning qualitative research interview questions for multi-racial populations in malaysia. *The Qualitative Report, 23*(11), 2700-2713. Retrieved from https://nsuworks.nova.edu/tqr/vol23/iss11/7/

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*, 107-118. doi:10.1016/j.dss.2018.02.009

Zach, L. (2006). Using a multiple-case studies design to investigate the information-seeking behavior of arts administrators. *Library Trends, 55*(1), 4-21. doi:10.1353/lib.2006.0055

Zeleke, T. A. (2019). The quandary of cyber governance in Ethiopia. *Journal of Public Policy and Administration, 3*(1), 1-7. doi:10.11648/j.jppa.20190301.11

Zhang, Y., Zhang, M., Luo, N., Wang, Y., & Niu, T. (2019). Understanding the formation mechanism of high-quality knowledge in social question and answer communities: A knowledge co-creation perspective. *International Journal of Information Management, 48*, 72–84. doi:10.1016/j.ijinfomgt.2019.01.022

Zhou, Q. (2018). Academic libraries in research data management service: Perceptions and practices. *Open Access Library Journal, 5*, 1-12. doi:10.4236/oalib.1104693

Zimmermann, S., Rentrop, C., & Felden, C. (2017). A multiple case study on the nature and management of shadow information technology. *Journal of Information Systems, 31*(1), 79-101. doi:10.2308/isys-51579

Zinette, B., Manfred, M. B., & Andrew, T. (2019). Agency and Bandura's model of triadic reciprocal causation: An exploratory mobility study among metrorail commuters in the Western Cape, South Africa. *Frontiers in Psychology, 10*, 1-14. doi:10.3389/fpsyg.2019.00411

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1-16. doi:10.1080/08874417.2020.1712269

Appendix A: Interview Protocol

Interview: Cybersecurity Awareness and Training Strategies to Protect Organizational Information Systems and Data?

Participant ID: _______________ Date:________________ Starting Time:_________

A. The interview will begin with introductions and an overview of the topic.
B. I will thank the participant for agreeing to participate in the study.
C. I will remind the participant that the interview is being recorded and that all information will remain strictly confidential.
D. I will begin the recording, announce the participants alphanumeric code, and the date and time.
E. Each interview will last approximately 45 – 60 minutes, or until all of the interview questions and any follow-up questions have been answered.
F. At the conclusion of the interview, I will explain the concept and plan for member checking.
G. Once answers have been confirmed to the satisfaction of the participant, the interview will conclude with thanking the participant for participating.

Introductory Protocol

To facilitate our note-taking, I would like to audio record our conversations today. For your information, only researchers on the project will be privy to the recordings which will be eventually destroyed after they are transcribed. In addition, you must sign a form devised to meet our human subject requirements. Essentially, this document states that: (1) all information will be held confidential, (2) your participation *is voluntary and you may stop at any time if you feel uncomfortable, and (3) we do not intend to inflict any harm. Thank you for your agreeing to participate. I have planned this interview to last between 45 to 60 minutes. During this time, I will have several questions that I would like to cover. May I have your permission to start the recording and proceed with the interview.*

Interviewing:

Each response from the participant will be paraphrased to ensure accuracy (i.e. in essence you mean; from what I heard).

1. What aspects of cybersecurity interest you most?

   Comments:

2. What are the components of your cybersecurity program?

   Comments:

3. What cybersecurity awareness strategies have you used to promote the protection of organizational information systems and data?

   Comments:

4. How do you determine which cybersecurity awareness strategies are used to promote the protection of organizational information systems and data?

   Comments:

5. How do you determine what cybersecurity concepts are most important in your organization’s cybersecurity awareness and training program?

   Comments:

6. How do you determine that employees have been adequately trained through cybersecurity awareness strategies to protect organizational information systems and data?

   Comments:

7. What methods worked best in cybersecurity awareness strategies to promote the protection of organizational information systems and data?

   Comments:

8. How do you enforce cybersecurity compliance and conduct remediation training?

   Comments:

9. How do you measure success of your cybersecurity awareness and training program?

   Comments:

Appendix B: Interview Questions

1. What aspects of cybersecurity interest you most?
2. What are the components of your cybersecurity program?
3. What cybersecurity awareness strategies have you used to promote the protection of organizational information systems and data?
4. How do you determine which cybersecurity awareness strategies are used to promote the protection of organizational information systems and data?
5. How do you determine what cybersecurity concepts are most important in your organization’s cybersecurity awareness and training program?
6. How do you determine that employees have been adequately trained through cybersecurity awareness strategies to protect organizational information systems and data?
7. What methods worked best in cybersecurity awareness strategies to promote the protection of organizational information systems and data?
8. How do you enforce cybersecurity compliance and conduct remediation training?
9. How do you measure success of your cybersecurity awareness and training program?

Appendix C: Letter of Invitation

Dear Participant:

My name is Michael Hanna. I am currently pursuing a Doctorate of Information Technology (DIT) through Walden University in Minneapolis. My doctoral study is to explore the strategies used in implementing cybersecurity awareness and training programs to protect organizational information systems and data within the hospitality industry. Your participation will not incentivize or affect your standing at your company.

I am interested in studying the strategies that leaders use to educate and train their employees to protect information systems and data. Your hospitality organization has granted permission to conduct interviews with willing participants and was selected as potential partner organization in this study based on satisfying the following requirements:

1. Your organization within Hampton Roads, Virginia, United States maintains and uses sensitive information.
2. Your organization has a managed cybersecurity awareness and training program.
3. You possess basic information security training and are involved in the implementation of information security education, training, and awareness strategies.

The interview process will last approximately 45-60 minutes during a time and date that is convenient with you. Your protection in your participation and information will be consistent with Walden University's confidentiality guidelines. The consent form describes your rights during the process and the purpose of the doctoral study. At the end of this doctoral research study, I will share the results and findings with participants, scholars, and other stakeholders. Interview participation will be voluntary.

If you are interested in participating in this research study or have any questions, please contact me at michael.hanna@waldenu.edu. Your participation in the study may help other communities understand the strategies used to implement cybersecurity awareness and training programs to protect technical systems and data.

Thank you for your time and consideration.

Very respectfully,

Michael M. Hanna
Walden University
Doctoral Candidate

Appendix D: Informed Consent Form

You are invited to participate in a research study about strategies you utilize to implement cybersecurity awareness and training programs to protect organizational information systems and data. The purpose of this study is to explore strategies used by corporate hospitality IT leaders to implement cybersecurity awareness and training programs to protect organizational information systems and data. The researcher is inviting organizational IT leaders that operate within hospitality organizations that maintain and use sensitive data within Hampton Roads, Virginia, United States. The participants must possess basic information security training and be involved in the implementation of information SETA strategies. This form is part of a process called "informed consent" to allow you to understand this study before deciding whether to participate.

This study is being conducted by a researcher named Michael Hanna, who is a doctoral student at Walden University.

Procedures:

If you agree to participate in this study, you will be asked to:

- Participate in a 45 to 60-minute audio interview at your convenience. The interview can be performed with the use of video teleconference software, such as Skype. Any video teleconference software that is convenient to you may be used. Please note that the interview will be recorded for transcription.

- Review the transcribed interview for accuracy and your consent to use the information in the study.
- Participate in a follow-up interview, if additional information is needed.
- Provide me with pertinent documents that portray the implementation of your information SETA program. Copies of these documents would be preferred, but if you are unable to provide copies, then eyes only viewing will suffice.

Voluntary Nature of the Study:

This study is voluntary. You are free to accept or decline this invitation. No one at your organization will treat you differently if you decide not to participate in the study. If you decide to participate in the study now, you can still change your mind later, and your decision will not impact any past relationships you may have had with me or any other employee at your organization.

Risks and benefits of being in the Study:

Being in this type of study involves some risk of the minor discomforts that may be encountered in daily life, such as taking time out of your day to support this study or discussing the implementation of your cybersecurity awareness and training program. Being in this study would not pose risk to your safety or well-being.

There may be no direct benefits to you, but the identified strategies can be used in coordination of information SETA programs with this knowledge.

Payment:

There will be no compensation for participation in this study.

Privacy:

Reports and publications resulting from this study will not show the identities of individual participants, nor the name of the organization. Details that might identify participants, such as the location of the participant will not be shared. The researcher will not use your personal information for any purpose outside of this research project. Data will be kept secure by replacing participant names with codes, data files of the participants will be encrypted, and password protected, and the location of the participant will not be disclosed in the report. You will not be asked and are not obliged to answer any sensitive/confidential information concerning your organization. If any sensitive/confidential information is inadvertently divulged, the information will be deleted from the transcript, or replaced with a code to mask that information or identity. Data will be kept for a period of at least five years, the deleted/destroyed, as required by the university. Identifying participant and organizational details will remain confidential.

Contacts and Questions:

You may ask any questions you have now, or if questions arise later, you may contact the researcher via michael.hanna@waldenu.edu. If you want to speak privately regarding your rights as a participant, you may contact the Research Participant Advocate at

Walden University at +1 612-312-1210. Walden University's approval number for this study is XXXXXXXXXXXX and it expires on XXXXXXX.

Please print or save this consent form for your records.

Obtaining your Consent:

If you feel you understand the study well enough to make an informed decision about it, please indicate your consent by replying to this email with the words, "I consent.".