2020

Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals

Vivian Lyon
Walden University

Walden University

College of Management and Technology

This is to certify that the doctoral study by

Vivian Lyon

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. Nicholas Harkiolakis, Committee Chairperson, Information Technology Faculty
Dr. Bob Duhainy, Committee Member, Information Technology Faculty
Dr. Steven Case, University Reviewer, Information Technology Faculty

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

Walden University
2020

Abstract

Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals

by

Vivian Lyon

MS, Walden University, USA, 2018

MSc, University of East London, UK, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

January 2020

Abstract

The cyber threat landscape has led some cybersecurity leaders to focus on a holistic approach encompassing people, processes, and technology to make their government agencies and organizations more responsive to a more diverse and inclusive cyber workforce to protect critical infrastructure from hackers or cybercriminals intent on causing harm. This qualitative multiple case study used Schein's organizational culture theory to explore strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive systems from rising cyber threats. The study's population consisted of cybersecurity leaders from 3 government agencies and 9 organizations in small, medium, and large enterprises in the Atlanta, Georgia, metropolitan area in the United States. The data collection process included semistructured interviews of cybersecurity leaders (N = 12) and the analysis of publicly available documents and presentations (n = 20). Data triangulation and member checking produced major and minor themes to increase the study findings' validity. Thematic analysis was used to identify 5 prominent themes: maintain a diverse and inclusive approach to recruitment; continuous training and development; maintain a culture of openness and teamwork; top leadership support; and overcoming challenges to cyber talent attraction, recruitment, and retention. The study findings showed that valuing all diversity may enable cyber teams to execute cybersecurity functions and missions promptly with a variation of thought and lenses. The study findings may contribute to positive social change by improving diversity, inclusion, work-life balance, morale, stress-levels, and opportunities for women and minorities in the cyber workforce.

Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals

by

Vivian Lyon

MS, Walden University, USA, 2018

MSc, University of East London, UK, 1998

Doctoral Study Submitted in Partial Fulfillment

of the Requirements for the Degree of

Doctor of Information Technology

Walden University

January 2020

Dedication

I dedicate this study to my Almighty God and Savior, Jesus Christ. You are my pillar and source of inspiration. Thank you for the strength, wisdom, knowledge, understanding, and divine mercies to embark on this journey. I'm forever indebted to the love and grace you have bestowed upon me. I also dedicate this study to my children (Carnell, Nicole, and Olivia). Your words of encouragement, patience, understanding, support, and prayers helped me fulfill this dream. You can attain any heights through hard work and devotion. My love for you all can never be quantified. Thank you, and God bless you.

Acknowledgments

First and foremost, I would like to thank God for making this doctoral journey possible and fruitful. I thank my family for their love, continued support, and encouragement in my pursuit of the highest academic degree in Information Technology. I want to thank my committee chair, Dr. Nicholas Harkiolakis, who provided tremendous guidance, support, and encouragement throughout the sleepless nights during my doctoral journey. Thank you for your patience, motivation, understanding, and support. Thank you, Dr. Bob Duhainy, my second committee member, for your valuable feedback and inspiration, which helped me better solidify my affinity for my research topic. I want to thank my university research reviewer (URR), Dr. Steven Case, for taking the time to review my work to help me improve the overall quality of my work and better understand the research process. I want to thank the participants in my study who took time out of their busy schedules to generously share valuable information. Your participation in my research is much appreciated.

Table of Contents

List of Tables

List of Figures

Section 1: Foundation of the Study

Protecting sensitive information from rising cyber threats, new scalable attacks, and vulnerabilities is a challenging task in part due to attracting, recruiting, and retaining diverse cybersecurity talent. Consequently, effective and efficient cybersecurity experts and network security specialists are essential to the defense against the increasing cybercrimes. A diverse cyber talent deficit exists, resulting in government agencies and businesses struggling to defend themselves against data breaches, denial of service attacks, ransomware, and threats. Differences in perspectives and thinking could lead to the innovation of new ideology, the discovery of new vectors, and new practice to help solve problems. For this reason, attracting, recruiting, and retaining diverse cybersecurity professionals could help protect mission-critical systems through effective collaboration of diverse cyber talent.

The purpose of this qualitative exploratory multiple case study was to explore strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. Section 1 contains the foundation of the study, background of the problem, problem and purpose statement, nature of the study, research question, interview questions, conceptual framework, definitions of terms, assumptions, limitations, and delimitations, the significance of the study, contribution to information technology (IT) practice, implications for social change, and literature review. A review of the professional and academic literature covered five principal components of my research: the (a) challenges of cybersecurity talent deficit and the absence of diversity and

inclusion in the workplace, (b) use of organizational culture theory (OCT) as a conceptual framework in research and as a means of increasing workforce diversity to improve the effectiveness of cybersecurity teams, (c) effect of culture on cybersecurity teams' performance, (d) role of leadership in a culture of diversity and inclusion in the cyber workforce, and (e) use of case study research design in exploring strategies used by cybersecurity leaders in the attraction, recruitment, and retention of cyber talent. Following the literature review is a conclusion and transitions to Sections 2 and 3 of the study.

Background of the Problem

Cybersecurity, although a rapidly growing segment of IT, is a significant concern for many security professionals in government and private sectors (Dunn Cavelty, 2014; White, 2016). Outsider threats due to cyber attacks and compromised credentials account for 92% of most investigated incidents (Kappelman et al., 2018). Cybersecurity experts expect an upward trend toward advanced cyber attacks (Andriole, 2015). However, the cyber challenges go beyond rising cyber threats, because there is a widespread shortage of qualified and diverse cybersecurity talent to fill the available cybersecurity roles to effectively and efficiently protect sensitive information. Cybersecurity professionals protect confidentiality, integrity, availability of data, information systems, and provide security awareness (Chabinsky, 2017). Cybersecurity leaders seek strategies to attract, recruit, and retain diverse cybersecurity talent to protect sensitive information (Pretorius et al., 2015). This research reinforces the critical need for diversity in cybersecurity and alignment of security objectives with strategic goals ("Global Information," 2017).

Qualified women and minority cybersecurity talent are underrepresented in the cybersecurity workforce (Peacock & Irons, 2017; Ritchey, 2016; "The 2017 (ISC)2 Global," 2017). Women account for only 11% of the information security workforce ("Global Information," 2017); 24% of science and engineering workers (Beard, 2014); and 34 percentage points lower than the U.S. average of women in the workforce (PWC, 2017). Women possess unique and essential character traits that enable them to succeed in cybersecurity, governance, risk, and compliance (CGRC) roles, with 58% having either a master's or doctorate versus 47% of men having such academic degrees (Ritchey, 2016). The risks of a lack of diversity in cybersecurity results in a deficit of cybersecurity talent to secure systems (Ritchey, 2016).

Problem Statement

The lack of a more inclusive information security workforce and diversity of thought is a contributing factor to past intelligence failures and critical missions ("Overcoming Barriers," 2015), data loss, network disruptions, target by hackers, and catastrophic performance failures (Cowley et al., 2015; Steinke et al., 2015; White, 2016). Women and minorities represent only 11% of the cybersecurity workforce, compared with the national workforce ("U.S. Department of Labor," 2018; U.S. House Committee on Homeland Security, 2017), despite the urgent need for skilled cyber talent and apparent lack of diversity which severely affects the sufficiency of the cybersecurity workforce (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018). The general IT problem that I addressed in this study is the lack of a more inclusive cybersecurity workforce with the necessary skills, attributes, and knowledge to protect

sensitive information from rising cyber threats. The specific IT problem that I addressed in this study is that some cybersecurity leaders lack strategies to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats.

Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. The population for this study comprised cybersecurity leaders within three government agencies and nine IT organizations in small, medium, and large enterprises in the Atlanta, Georgia, metropolitan area in the United States with strategies to attract, recruit, and retain diverse cybersecurity professionals. The implication for positive social change resulting from my study might improve diversity in the workplace, work-life balance, morale, stress levels, and opportunities for women who have experienced institutional and social barriers in the course of their cybersecurity careers as well as ensure better protection of protected health information and personally identifiable information.

Nature of the Study

Qualitative, quantitative, and mixed methods are the primary approaches used in scholarly research. In this study, I used a qualitative methodology approach to explore and fully understand the strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive

information from rising cyber threats. The qualitative approach is an in-depth strategy to explore and fully understand a particularly complex phenomenon or topic within its real-world context (Cronin, 2014). My research involved collecting and analyzing data from interviews and organizational artifacts pertaining to strategies to attract, recruit and, retain diverse cybersecurity professionals to develop a comprehensive understanding of the phenomenon under study from the perspectives of experienced cybersecurity leaders. When a researcher cannot definitively identify variables and elements for evaluation, or they want to study and understand a phenomenon fully, qualitative designs provide the conceptual frameworks for analysis (Fallahpour & Zoughi, 2015). Therefore, there were no dependent nor independent variables, no hypotheses nor theory testing, and no collection of numeric data for statistical testing. I used the conceptual framework to create a deeper understanding of strategies that cybersecurity leaders use to attract, recruit, and retain cybersecurity professionals as opposed to showing a correlation between cybersecurity leaders and attraction, recruitment, and retention strategies. Quantitative methods emphasize objective measurements and the mathematical, statistical, or numerical analysis of data collected through questionnaires, surveys, and polls, or by manipulating pre-existing statistical data using computational techniques (Barczak, 2015). The quantitative methodology was not appropriate for my research because I did not intend to examine differences or relationships among variables nor formulate and test hypotheses. A mixed-methods approach to research uses a qualitative and quantitative portion within the same study (McCusker & Gunaydin, 2015). I did not

use the mixed methods approach because only the qualitative methodology applied to the study.

The case study, ethnography, and phenomenology are the standard designs in qualitative applied research (Yilmaz, 2013). The qualitative case study design is used by researchers when studying complex phenomena to understand and describe the phenomena in detail (Hyett, Kenny, & Dickson-Swift, 2014; Yin, 1981). The qualitative multiple case study design through the use of various sources of data and multiple sites was the appropriate design for my research, because I sought to explore and fully understand the strategies cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. Ethnography focuses on studying distinct cultures or cultural groups (Kruth, 2015; Petty, Thomson & Stew, 2012) to better understand the social behaviors of the participants within their natural environment (Cruz & Higginbottom, 2013). As such, ethnography was not appropriate for my research as the study was not concerned with a distinct culture or cultural group, nor did it focus on the cultural or social behaviors of participants. Phenomenology is used to explore and deeply understand lived experiences of individuals from their perspectives (Kruth, 2015; Petty et al., 2012). Further, the phenomenological design focuses on describing and clarifying the typical qualities of the individuals that experienced an unusual phenomenon (Sloan & Bowe, 2015). This focus on lived experiences was not relevant to my study, thus making a phenomenological design inappropriate for my research.

Research Question

What strategies do cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats?

Demographic Questions

1. Without including your name or your organization's name, what is your current role and how long have you been in similar roles?

2. What is your background in cybersecurity education/training and/or recruiting cybersecurity personnel?

Interview Questions

1. What strategies do you have for ensuring the highest possible attraction, recruitment, and retention of diverse cybersecurity professionals to protect sensitive systems?

Probe: Do you differentiate between attract, recruit, and retain in your strategy?

2. What strategies have you found to be the most effective and efficient for attracting, recruiting, and retaining diverse cybersecurity professionals?

3. What strategies have you found to be least effective and efficient?

4. What is your perception of the impact of the culture of your organization on your strategies to attract, recruit, and retain diverse cybersecurity professionals? Please explain.

5. What is your perception of consideration of diversity in the workplace? Please explain.

6. What, if any, challenges do you face regarding the application of attraction, recruitment, and retention best practices for diverse cybersecurity professionals? Please elaborate.

7. How would you describe the effects of your strategies to attract, recruit, and retain diverse cybersecurity professionals on the team's performance to protect sensitive systems.

8. Is there anything else you would like to add in relation to your cybersecurity attraction, recruitment, and retention strategies that we have not addressed already?

Conceptual Framework

I used OCT as the conceptual framework for this study to assist me in data interpretation and evaluation as well as theme identification. In 1980, Schein (2010) developed an organizational culture model to make culture more visible within an organization and provided guidelines to follow to influence an organization's effectiveness and bring about cultural change within organizations. Schein (2010) explains organizational culture as a formal environment and norms that characterize a specific organization's problem-solving abilities, and informal behaviors that are considered valid and correct among individuals in the organization. Organizational culture is divided into three effective levels or elements: artifacts, espoused values, and basic underlying assumptions and beliefs (Schein, 2010). OCT highlights three barriers to the successful sharing and transference of strategies within an organization: ignorance on both ends (the receiver and giver), unavailability of resources, and lack of relationship between the giver and receiver (O'Dell & Grayson, 1998; Szulanski, 2017).

OCT is used to address different strategic issues in the organization and serves as the conceptual framework in exploratory studies of an organization's attraction, recruitment, and retention strategies (Lehman, 2017). In this study, I explored strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity talent to effectively and efficiently protect sensitive information. OCT provides the lens and connections needed (literature, methodology, and results) to explore and understand the adoption of organizational strategies (Carter-Sowell & Zimmerman, 2015). OCT has three elements, but only the cultural factors of espoused values and beliefs of OCT aligned with this study and identified the elements of the research that are crucial when exploring the strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity talent. Espoused values are seen in the organization's stated vision, strategies, mission, objectives, philosophies, and goals, and beliefs are seen in individual principles and personal aspirations (McDermott & O'Dell, 2001; Schein, 2010). Organizational culture influences the environment, work habits, performance, productivity, and profitability of motivated talent, which in turn affects an organization's performance (Zhu, Gardner, & Chin, 2018).

Definition of Terms

The following are unique operational definitions that I used in this study to enable the reader to understand some terms related to cybersecurity:

Availability: Property of being accessible and usable upon demand by an authorized entity (National Institute of Standards and Technology [NIST], 2015).

Confidentiality: Property that information is not made available or disclosed to unauthorized (NIST, 2015).

Cyber attack: The deliberate exploitation of computer systems using malicious tools and techniques (Samtani, Chinn, Chen & Nunamaker, 2017).

Cybersecurity: Cybersecurity encompasses measures that monitor, protect, maintain data, computers, electronic communications systems and services, electronic communications, and wired communications by ensuring their confidentiality, availability, authentication, integrity, and non-repudiation ("Joint Publication 3-0," 2017; Von Solms & Van Niekerk, 2013).

Cyberspace: All the systems for collection, processing, and distribution of information to support decision making at the time and to provide command and control operations (International Organization for Standardization [ISO], 2016).

Cybercriminals: Individuals with illicit cyber intent that leverage dangerous cyber tools or assets to conduct destructive cyberattacks against technologically driven organizations (Samtan et al., 2017).

Information security: Preservation of confidentiality, integrity, and availability of information, individuals, entities, or processes (NIST, 2015).

Integrity: Property of accuracy and completeness (NIST, 2015).

Risk: Effect of uncertainty on objectives (ISO, 2016).

Security incident: A violation or imminent threat of breach of computer security policies, acceptable use policies, or standard security practices (NIST, 2015).

Vulnerability: The weakness of an asset or control that can be exploited by one or more threats (ISO, 2016).

Assumptions, Limitations, and Delimitations

Several internal or external phenomena influence research and outcomes. Recognizing, acknowledging, and documenting these phenomena is part of establishing integrity and credibility. The three categories of phenomena that occur in research are assumptions, limitations, and delimitations.

Assumptions

Assumptions are beliefs and opinions that are accepted as truths by a researcher without measurable proof and can introduce bias (Kirkwood & Price, 2013; Walsh, 2015). I made certain assumptions in this study. My first assumption was that the cybersecurity leaders understood the semistructured interview questions and answered them honestly and truthfully. My second assumption was that the cybersecurity leaders were qualified (domain wise) and considered as experts in the areas relevant to the study to provide information regarding strategies to recruit and retain cybersecurity professionals to protect sensitive information from cyber threats. My third assumption was that the use of a qualitative research methodology would be effective in providing the data needed to answer the research question. The results of a multiple case study are derived from personal communications allowing bias to interfere and influence the research process and the study's results (Yin, 2014). As such, the fourth assumption was that individual interpretations of the data could mold the path of the research. To address this assumption, the interview questions were framed in a way to minimize bias and

prevent the interviewer's influence on the interviewee. Open-ended questions rather than yes-or-no questions are used for the study.

Limitations

Limitations are inevitable in every study, despite the researcher's best efforts to limit the theoretical or methodological constraints, shortcomings, restrictions, or defects (Busse, Kach, & Wagner, 2016). The qualitative nature of this research was the primary limitation of this study. Theme artifacts and dialogue interpretation is a subjective process that could result in possible validity issues that could introduce bias into the research (Yin, 2014). A second limitation was that the data sources consisted of responses to interview questions and policy documents, which may limit the findings of the research. *Transferability*, or *external validity*, in qualitative research, refers to the extent to which researchers can generalize the study findings or use them in other settings or contexts (Aravamudhan & Krishnaveni, 2015; Marshall & Rossman, 2016; Yilmaz, 2013; Yin, 2015). An additional limitation was that the maturity level of cybersecurity attraction, recruitment, and retention practices at the case organization are different from the maturity level of these practices or policies implemented in other organizations, so the responses to interview questions were representative solely of the organizations used in this study.

Delimitations

Delimitations are boundaries that a researcher foists on a study to narrow or control the scope of the research (Svensson & Doumas, 2013). There were six primary delimitations in my research. First, I considered only organizations and government

agencies that have strategies to attract, recruit, and retain cybersecurity professionals to effectively and efficiently protect sensitive information. Second, I considered only cybersecurity leaders who have the authority to attract, recruit, and retain cybersecurity professionals within their organization or government agency. Third, I considered only cybersecurity leaders who had been involved in attraction, recruitment, and retention activities within the same organization or government agency or at any other organization or government agency for a minimum of 5 years. Fourth, I considered only cybersecurity leaders who have conducted or been involved in recruitment campaigns within their organization or government agency. Fifth, I included only cybersecurity leaders who work in the metropolitan area of Atlanta, Georgia. Sixth, I considered cybersecurity leaders who have been employed at the case organization as full-time employees of their organization or government agency at the time of the study.

Significance of the Study

The strategies to attract, recruit, and retain diverse cybersecurity professionals might help increase the cybersecurity workforce to efficiently and effectively protect sensitive information from rising cyber threats. Given the gap in the literature, this research might contribute to the body of academic knowledge and practice in this area. I expect that this study might provide a foundation for further research on this topic.

Contribution to Information Technology Practice

This research might contribute to IT practice as it provides detailed descriptions of strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive information.

My study findings might allow me to provide cybersecurity leaders a broader understanding of the best strategies, attributes, skills, and qualifications to increase diversity in cybersecurity teams and enhance their effectiveness to protect sensitive information from rising cyber threats (Cowley, Nauer, & Anderson, 2015). The value created by including women in cyber warfare and risk management might translate into more secure and safer information systems (Bagchi-Sen, Rao, Upadhyaya & Chai, 2010; Dunn Cavelty, 2014). Addressing the shortage of women and minorities in cybersecurity teams requires connecting with them as they enter high school, investing in training, mentoring, advancement, and sponsorship programs, as well as creating more inclusive workplaces (Lemos, 2017; Liu & Murphy, 2016; Pusey, Gondree, & Peterson, 2016).

Implications for Social Change

The implications for positive social change might include improved diversity in the workplace, work-life balance, morale, and opportunities for women who have experienced institutional and social barriers in the course of their cybersecurity careers. Approaching issues through different lenses and variations of thought might enhance the efficiency and effectiveness of the cybersecurity professionals who protect sensitive information and those that benefit from the protection. Increased productivity might indicate that cybersecurity professionals and beneficiaries accomplish their work tasks in less time, decreasing the stress levels of both cybersecurity professionals and owners of sensitive information. Diminished work stress levels might subsequently improve employee morale and productivity. The results of the study might also contribute to social change by helping to bridge the gap in the recruitment and retention of female

cybersecurity professionals. The findings from this study might also guide effective intervention programs for gender equity in the cybersecurity workforce and science, technology, engineering, and mathematics (STEM) fields as a whole (Wilson, Broughan, & Hillier, 2017). The study might enlighten middle schools, high schools, colleges, and universities regarding the need to hire a more diverse team of STEM-oriented instructors and teachers as role models for the students who might pursue a career in cybersecurity.

A Review of the Professional and Academic Literature

The purpose of this qualitative exploratory multiple case study was to explore strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals in their efforts to efficiently and effectively protect sensitive information from rising cyber threats. In this literature review, I cover five principal components of my research: the (a) challenges of cybersecurity talent deficit and the absence of diversity and inclusion in the workplace, (b) use of OCT as a conceptual framework in research and as a means of increasing workforce diversity to improve the effectiveness of cybersecurity teams, (c) effect of culture on cybersecurity teams' performance, (d) role of leadership in a culture of diversity and inclusion in the cyber workforce, and (e) use of case study research design in exploring strategies used by cybersecurity leaders in the attraction, recruitment, and retention of cyber talent.

A research literature review forms a systematic, explicit, and reproducible method for identifying, evaluating, and synthesizing the existing body of work produced by researchers (Fink, 2013). I used the literature review as the foundation for this research as well as a means of establishing expectations of outcomes based on the findings of prior

scholars regarding the research question of my study. Booth, Sutton, and Papaioannou (2016) emphasized that conducting a good integrative literature review helps in identifying gaps in the literature and provides reliable and trustworthy answers to the research questions. Booth et al. noted that the literature review enables the researcher to show the readers the quality of the studies that form part of the research and the level of confidence they should expect in the results of the study.

I conducted numerous searches of sources of academic and professional journals and articles to uncover relevant and useful materials relating to the research topic. I used Google Scholar for initial searches and followed up with, ProQuest Electronic Databases, ProQuest Central, EBSCO Host, Science Direct, Research Gate, Academic Search Complete, IEEE Computer Society Digital Library, IEEE Explore, ACM Digital Library, government-issued reports relevant to the study, and scholarly books available from Walden Library as the primary search locations for peer-reviewed literature pertinent to the study.

While conducting the web and library searches, I focused on reviewing seminal and other relevant journal articles from 2014 and later to ensure that the information and topics discussed are current. The search terms or keywords that I used to retrieve information represented as themes in my literature review are detalied in the following text. For OCT, the search terms included the following: *organizational culture theory, organizational culture, the evolution of organizational culture, models of organizational culture theory, supporting models of organizational culture theory,* and *contrasting models of organizational culture theory.* For cybersecurity, the search terms included the

following: *shortage of cybersecurity professionals, cyber talent deficit, diverse cyber workforce, cybersecurity talent deficit,* and *cybersecurity team effectiveness.* For diversity and inclusion, the search terms included the following: *benefits of cybersecurity workforce diversity, barriers to cybersecurity workforce diversity, cyber workforce diversity,* and *inclusion.* For performance, the search terms included the following: *organizational performance, diverse cybersecurity teams,* and *performance, effects of organizational culture on teams performance.* For leadership, the search terms included the following: *organizational culture and leadership* and *the effects of leadership in workforce diversity.* For attraction, recruitment, and retention strategies, the search terms included the following: *barriers to attraction, recruitment, and retention, strategies for attraction, recruitment,* and *retention.* The literature retrieved for OCT, diverse cybersecurity talent attraction, recruitment, and retention strategies, and performance provided a foundation for the use of case study as a research design.

I conducted a critical analysis and review of the references for this study, which included 256 journals articles published within the last 5 years (2014 and newer) with 249 (97% of journals articles published within the previous 5 years) being peer-reviewed journal articles, 23 government-issued reports, 10 scholarly books, and seven doctoral dissertations or thesis. I began this literature review with an analysis of the literature regarding organizational culture, followed by the various definitions of organizational culture, and then an analysis of literature regarding OCT, which was the conceptual framework for this study. I evaluated Schein's organizational culture model carefully as a part of this research to explore and understand the relationship between organizational

culture and the strategies for the attraction, recruitment, and retention of diverse cybersecurity professionals by cybersecurity leaders. Prior studies have indicated that cyber attacks are on the rise with catastrophic effects reported across many organizations and that the potential cybersecurity talent to help prevent these attacks are underrepresented in the public and private sectors (Castro, 2018; Cowley et al., 2015; Liu & Murphy, 2016). In this literature review, I discuss past studies on the effect of organizational culture, leadership, and diversity and inclusion on the performance of cybersecurity teams to effectively and efficiently mitigate cyberattacks to prevent data breaches.

Conceptual Framework

The review of the literature on organizational culture was critical to this research because the fundamental dynamic element of the conceptual framework of OCT that I used to guide my research was organizational culture (Campbell & Göritz, 2014). The concept of organizational culture originated from cultural anthropology (Schein, 1996), and as researchers began engaging in organizational analysis in the late 1970s, the term *organizational culture* became more widely used and recognized (Alvesson & Sveningsson, 2015). Between 1980 and 1990, researchers believed that organizational culture was the central element of success in organizations; however, that idea has since been dispelled by other researchers (Alvesson & Sveningsson, 2015). Nevertheless, organizational culture remains an essential factor in the analysis of organizations, and it influences an organization's performance and competitive advantage (Beugelsdijk et al., 2014). Organizational culture binds together members of an organization and allows

leaders to align the culture of their organization with its vision and strategic objectives (Chatman, Caldwell, O'Reilly, & Doerr, 2014). Wei, Samiee, and Lee (2014) highlighted that enterprises regard organizational culture as a strategic resource that significantly affects a plethora of internal organizational activities such as hiring, retention, and development of new talents. However, Trompenaars and Hampden-Turner (1998) emphasized the complexity of organizational culture by noting that culture is not verbalized, yet it provides the roots of action by offering individuals a meaningful context to face the outer world, think about themselves, and meet personal goals.

Schein's Organizational Culture Theory and Model

OCT comprises numerous theories that researchers have used to attempt to explain and predict how organizations and their members will behave in varying organizational circumstances, cultures, and structures (Shafritz, Ott, & Jang, 2015). The physical attributes of an organization include founders, leaders, employees, products, and services, which are all easy to change compared with a culture, which is the most challenging attribute to change (Schein, 1985). Cao, Huo, Li, and Zhao (2015) noted many definitions of organizational culture in the literature, which has resulted in a wide variation of definitions of *organizational culture* (Nikpour, 2017). Essentially, no consistent definition of *organizational culture* exists in the literature. Büschgens et al. (2013) defined *organizational culture* as a complex set of beliefs, assumptions, values, and symbols that represent the way enterprises conduct their business. Organizational culture involves the values and beliefs that are deep-rooted in an organization, its employees, and their work values, which influence their behavior and attitudes.

Trompenaars (1994) defined *culture* as a shared system of meanings that dictates what one values, how one acts, and what one pays attention to. Schein (1996) described *organizational culture* as a social force that is powerful yet mostly invisible. In a seminal work, Schein (1985, p. 9) defined *culture* as a model of fundamental assumptions developed, discovered, or invented by a designated group of individuals to enable them to manage challenges with internal integration and external adaptation that has been accepted as valid and passed on to new members as the best way to view problems.

Schein et al. (2015) observed organizational norms and values and described an organizational culture with three interrelated cognitive levels: (a) artifacts, (b) espoused values, and (c) basic underlying assumptions.

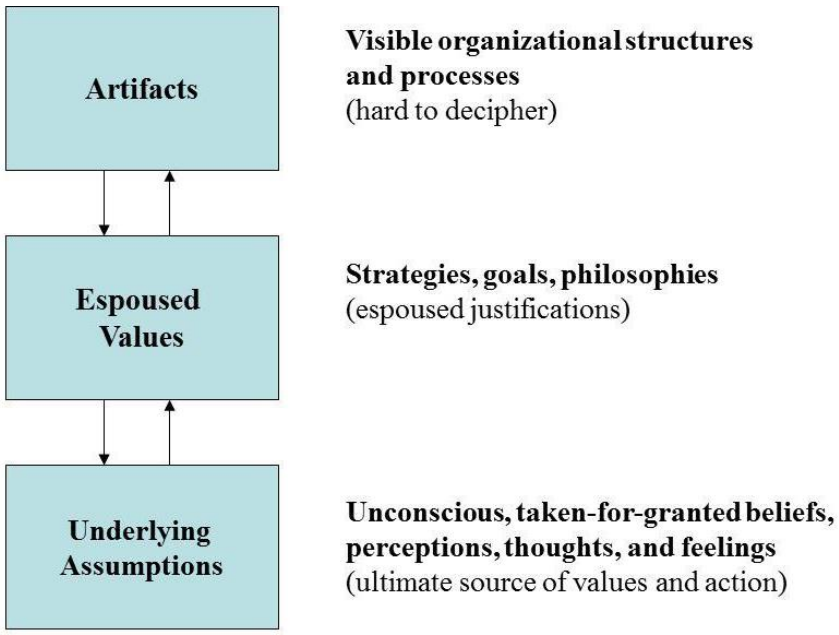

Figure 1. Dimensions of diversity. Adapted from *Organizational Culture and Leadership by Schein,* 2004, p. 26. Copyright E. H. Schein.

Artifacts. Schein (1996) described *artifacts*, the first cognitive level, as organizational features, processes, structures, including behavior patterns, innovations, and manner of visible interactions among members that a person sees, feels, and hears upon entry into the organization.

Espoused Values. The second cognitive level, espoused values, involves the organization members' perception of culture. Schein observed that at the espoused values level, mission statement, company policies, and operational creeds are observed and expressed, unlike norms and values that cannot be observed, leading to disconnects between the artifacts and espoused values. Norms are closely aligned with values, and they are rules in unwritten form that guide the expectations of members of a culture in various situations. Organizational members, therefore, conform to norms and hold values based on their underlying assumptions of the norms (Schein, 1985). Norms and values promote activities that produce the artifacts. At this espoused value level, organizational behavior can be observed through questionnaires and interviews of organizational members.

Basic Underlying Assumptions. The third cognitive level, the organization's basic underlying assumptions, constitutes the elements of culture that are often ignored and taken for granted in daily interactions among organizational members. These elements of culture are off-limits for discussions within many organizations (Alvesson & Sveningsson, 2015). Organizational members become accustomed to these rules and view them as attributes through time, thus making them invisible and deep-rooted within the organization. Casual interviews and surveys cannot expose these attributes; instead, more

in-depth data collection procedures are required to identify and understand this level of organizational culture (Schein, 1985). Organizational behaviorists often miss this level of culture, which include the underlying assumptions and driving elements that guide actions and everyday interactions in organizations (Alvesson & Sveningsson, 2015).

The various levels of Schein's cultural model are intertwined and, therefore, influence each other. The governing, or underlying, assumptions expressed in norms influence behavior. With Schein's model, researchers can analyze the interconnected beliefs and deep assumptions about organizational artifacts and values (Alvesson & Sveningsson, 2015). Researchers can also gain an understanding of the challenges of changing an organizational culture that requires the exposure of customarily hidden assumptions. Schein (1999), however, offered useful strategies for effecting cultural change in organizations: (a) creating motivation for change by discarding any legacy culture, (b) learning from past deficiencies and embracing new opportunities, and potential solutions, (c) providing clear and concise targets for change, (d) providing comprehensive formal and informal training of teams and groups, (e) providing role models and mentors, (f) promoting continuous employee involvement, (g) providing opportunities to offer input and feedback, (h) making available support groups to share ideas and address any concerns, (i) creating, choosing, and editing suitable cultural artifacts, behaviors, forms, and collaboration approaches, (j) building charismatic leaders, (k) creating a feasible and reasonable migration plan, and (l) addressing risks, benefits, and remediation strategies.

Using Schein's OCT as a lens enabled me to explore the strategies used by cybersecurity leaders to recruit and retain diverse cyber talents. Schein (1992) stressed that for organizations to attain sustainable success their culture must consider the following in conjunction with the critical components of culture (values, behavioral norms, patterns, artifacts, and symbols): the (a) organization should not only be reactive, instead must be proactive. (b) organization should not only adapt to the environment, instead must manage and influence it. (c) organization should not only be idealistic, instead must be pragmatic. (d) organization should not only be past/present-oriented, instead must be future-oriented. (e) organization should not only conform to uniformity, instead must embrace diversity and inclusion. (f) organization should not only be task-oriented, instead must be relationship-oriented. (g) organization should not only promote internal integration but instead must also embrace external connectivity.

Previous researchers of organizational culture have focused on the link between organizational culture and numerous activities of the organizations, including, but not limited to, the relation to attraction, recruitment, and retention as well as performance. For example, Leithy (2017) discussed the link between organizational culture and performance, Fattah (2017) examined the effects of organizational culture, leader behavior, self-efficacy, and job satisfaction on the job performance of employees, and Alhadid (2016) examined the relationship between organizational performance and leadership practices.

Supporting Conceptual Models

Systems Theory. Systems theory is one supporting theory of organizational culture that is used to analyze all kinds of cultures, including national and corporate cultures, and presume that cultures can be understood and explained by looking at their assumptions and core values. In the 1940s, Von Bertalanffy (1968) developed the general systems theory (GST) from which modern systems theory emerged. Systems theory is a way to analyze and understand complex adaptive systems, which are collections of many different components (agents) interacting in nonlinear ways (Sturmberg, Martin, & Katerndahl, 2014, p. 66). Although understanding current situations and seeking to explain the behaviors of systems through axioms and propositions, Von Bertalanffy (1968) argued that open systems are self-correcting and self-regulating. Whitney, Bradley, Baugh, and Jr (2015) pointed out that some systems theory axioms include achieving desired outcomes through certain behaviors and the use and manipulation of information. Katina (2015) indicated that systems theory was an approach to understanding current situations and seek to explain the behaviors of systems through axioms and propositions, linking systems theory to organizational culture. Adams, Hester, Bradley, Meyers, and Keating (2014) expanded the definition of systems theory as a unified group of propositions that work together with the objective of understanding systems. Montgomery and Oladapo (2014) noted that systems theory was more suitable for qualitative studies, even though some researchers have applied the theory to quantitative studies.

Total Quality Mangement. Total quality management (TQM) is another supporting theory of organizational culture. In the mid-1980s, Deming and Juran began the TQM movement in the United States after a decline in the U.S. economy during the 1970s and 1980s (Hill, 2008; Joyce, 2015). TQM is defined as an organization's culture, structure, and attitude toward providing customers with satisfactory outcomes (Hill, 2008). TQM is a collection of components, procedures, and policies that directly influence organizational performance (Choi & Eboch, 1998). Deming (1982) defined TQM with three primary focuses: continuous improvement, customer satisfaction, and involving everyone. Valmohammadi and Roshanzamir (2015) described TQM as a holistic management concept that aims for constant improvement in all organizational functions, and it can only be realized with the utilization of the total quality concept. Organizations apply TQM to increase profitability, market share, competitiveness, teamwork, productivity, product quality, and customer satisfaction (Valmohammadi & Roshanzamir, 2015). The authors conducted a quantitative study to compare organizational culture models and TQM to explain the relationships among culture, TQM and performance using the Competing Values Framework (CVF) developed by Cameron and Quinn (2011) to diagnose organizational culture and measure organizational performance. The results of the study showed that there are positive direct effects of culture and TQM on performance. Prior studies by Gimenez-Espin et al. (2013) and Haffar et al. (2013) also revealed significant relationships of different types of culture and the success of TQM as well as the same relations between different dimensions of organizational culture and TQM (Kaluarachchi, 2010).

Mehralian, Nazari, Nooriparto, and Rasekh (2017) recognized that quality improvement was a critical issue in organizations that apply TQM to increase profitability, market share, teamwork, competitiveness, productivity, product quality, and customer satisfaction to reach their strategic objectives. Mehralian et al. (2017) examined the relationship between the implementation of TQM and various dimensions of organizational performance, using the balanced scorecard (BSC) approach. The results of the study revealed that TQM implementation could positively and significantly influence the BSC and its four perspectives of organizational performance (financial, customer, internal process, and learning and growth). The study findings provided substantial evidence to support the implementation of TQM in the pharmaceutical industry. Mehralian et al. (2017) concluded that the implementation of TQM encourages and motivates organizations to identify the measures that answer the question of what internal processes should be improved.

Alghamdi (2018) reported that organizational culture, in combination with TQM, has been widely investigated to understand its contributions to organizational performance in public and private organizations. Alghamdi (2018) noted that TQM facilitates a culture of continuous improvement to enable successful organizations or teams to strive for quality and boost organizational performance and customer satisfaction. Alghamdi (2018) explained that organizational performance and effectiveness are multidimensional constructs that evaluate the position of an organization regarding its internal or external standards. Alghamdi (2018) examined the relationship between TQM and organizational performance and its effect on

organizational culture using the Competing Value Framework (CVF), which is a combination of organizational theories (Cameron & Quinn, 2011). The first dimension is the degree to which an organization pays closer attention to controlling organizational processes via centralization. The second dimension is the degree to which an organization is oriented to its inside environment and relationships with outside entities. The results of the study indicated that an inclusive organizational culture significantly improved organizational performance with an effective TQM program implementation because it empowered employees to contribute new ideas and take risks as a part of the process of continuous improvement, which is a significant component of TQM. Iqbal, Shabbir, Zameer, Tufail, Sandhu, and Ali (2017) explored the critical factors of TQM and their impact on organizational performance and found that the critical factors of TQM that affects an organizations performance in the service sector include top management commitment (TMC), human resource focus (HRF), strategic alignment (SA), and customer-oriented process management (COPM).

Contrasting Conceptual Model

Denison's Model. Denison's model is in contrast to Schein's culture model, which considers organizational culture as a multidimensional concept that required a multi-layered analysis (Denison, Nieminen, & Kotrba, 2014). Denison's model is used to explain four cultural elements based on two viewpoints: internal (consistency and involvement) and external (mission and adaptability) (Denison et al., 2014; Shehadeh, Al-Zu'bi, Abdallah, & Maqableh, 2016). The internal viewpoints are linked to the organization's internal strategic goals and objectives while the external views are related

to the organization's worldwide objectives to meet the stakeholders' and customers' needs while balancing the lessons learned, change creation, and client focus (Denison et al., 2014). Shehadeh et al. (2016) emphasized that the inability of an organization to focus on the need of the customers implies that the organization is challenged with the application of the lessons learned to their client base. Denison et al. (2014) posited that organizational success lies with their stability and definition of organizational goals and strategic objectives. Ali and Zhang (2015) and Cheng, Lee, and Shevlin (2016) agree with Denison et al. (2014) that for an organization to meet its stated mission, it must balance its goals, objectives, vision, and strategic direction. Denison's model of organizational culture suggested that adaptation and involvement are indicative of flexibility, responsiveness and, openness. Figure 2 shows Denison's model of culture.

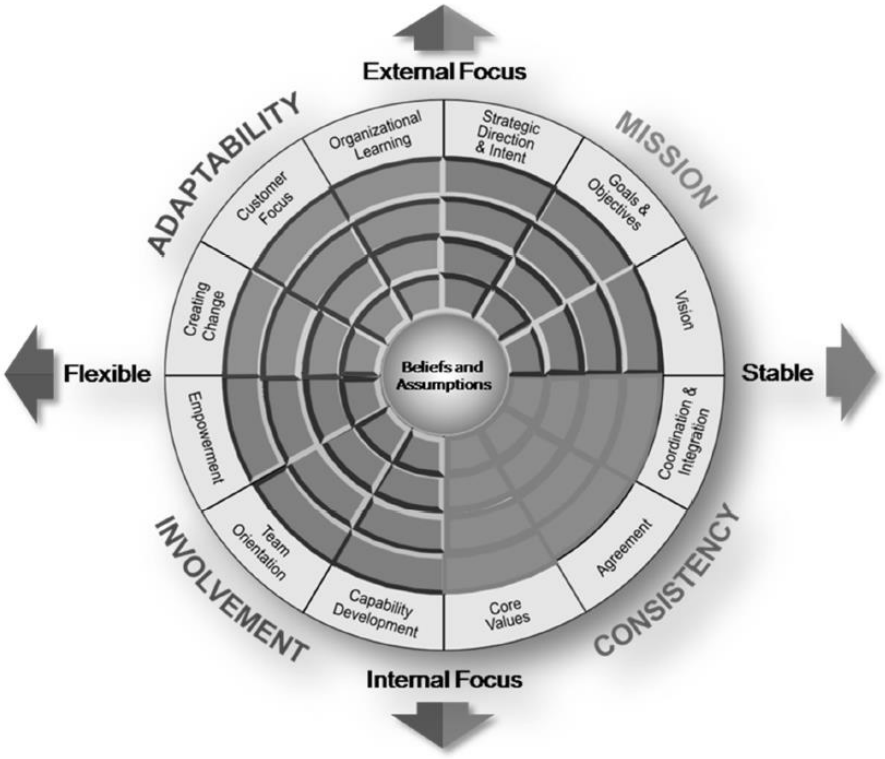

Figure 2. Denison's model of culture. Adapted from Kokina and Ostrovska (2014). Reprinted with permission.

Kokina and Ostrovska's (2014) analysis of Denison's model indicated that stable organizations are differentiated from flexible organizations by the vertical dimension. In stable organizations, consistency and mission point to the ability of the organization to sustain its stability and direction based on core values, vision, goals, and objectives, while, for flexible organizations, involvement, and adaptability highlight the strength of the organization to adopt changes. Denison's model also denoted that organizations that embrace culture geared toward consistency and mission tend to be stable, under control, and more content with the way they operate. Conversely, organizations that embrace culture geared toward adaptability and involvement tend to introduce different views and support diverse solutions to their problem (Kokina & Ostrovska, 2014).

Usage of Organizational Culture Theory

Hogan and Coote (2014) highlighted the importance of innovation to organizational survival and developed an empirical model based on Schein's multi-layered model of organizational culture, which provides a useful framework for viewing processes that foster innovation. Hogan and Coote (2014) assumed that Schein's model with artifacts and behaviors, and values and norms as its characteristics explain the cultural processes that support organizational innovation. Hogan and Coote (2014) reported a positive relationship between organizational culture layers, particularly artifacts, innovative behaviors, and norms and performance, and innovative values. Murphy, Cooke, and Lopez (2013) used OCT as the conceptual framework to clarify

distinct aspects of a firm's culture on performance and structural equation modeling to show that culture relates positively to cooperation, coordination, and performance. Murphy et al. (2013) found that organizations that embrace cultures and shared values with higher intensity enhanced their outcomes and performance by driving collaboration and coordination.

Yilmaz (2014) noted that Schein's model of organizational culture offers a practical heuristic that examines different elements of organizational culture on three integrated levels, resembling the structure of an onion. The first level of Schein's model, which is the most visible element in this level, includes the artifacts that are displayed or created by organizational members and the explicit communication behaviors of those organizational members. The second level refers to the espoused values to which the organization is expected to adhere. Underlying assumptions are the third level, and it relates to how individuals in the organization perceive the world and core principles underlying their worldview. Yilmaz (2014) organized an activity to stimulate an organizational context to analyze, critique, and present a cultural analysis of an organization applying Schein's model. The exercise involved a group of four or five diverse students that discussed their group's application of the model and explained artifacts, values, and underlying assumptions by answering open-ended questions that elaborate cultural markers and different levels of organizational culture. The results of the activity indicated that the students benefited from the diverse group activity by working interactively, cooperatively, and productively.

Ovidiu-Iliuta (2014) examined the relationship between performance management and organizational culture based on the notion that the culture of an organization could influence its short and long-term performance and highlighted Schein's definition of culture namely its basic assumptions, values, or shared beliefs. The results of the study showed that strongly proactive cultures helped organizations enhance and support effective and efficient performance as well as anticipate and adapt to changes in the environment. All four traits of organizational culture (mission, involvement, consistency, adaptability) had positive influences on performance management practices, with consistency being the most significant influencer. Ovidiu-Iliuta (2014) noted that it is critical to retain key employees that are adequately integrated, highly coordinated, and aware of the organizational goals, core values, norms, and behavior while implementing practices that enhance career development and job security. Morcos (2018) also noted that organizational culture is a significant driver of organizational excellence and the long-term effectiveness and performance of an organization. Morcos (2018) explored effective cultural-oriented strategies that senior business leaders use to align the organization's culture with different national cultures to improve organizational performance. The author found that an effective organizational culture that portrays the same set of beliefs, norms, and values as other national cultures affects the employees' sense of belonging, motivation, satisfaction, and commitment, which in turn increased performance, profits, and organizational effectiveness.

Culture and knowledge are an essential aspect of any institution as well as the most valuable resource in any organization (Gracia, & Tomas, 2014). Lehman (2017)

emphasized that the successful management of knowledge in any organization is highly influenced by culture. As such, the author applied OCT to the research administration knowledge management and explored shared artifacts, espoused beliefs and values, and basic underlying assumptions. The findings of the study revealed opportunities for creating knowledge-sharing, knowledge management initiatives, and common barriers to knowledge management. Lehman (2017) noted that creating and sustaining a knowledge-sharing community requires organizational leaders to establish knowledge that exhibits the beliefs, ideals, and principles of the profession, utilizing dynamic information systems, allocating opportunities for research administration professionals to share and communicate, and establishing metrics for knowledge management initiatives. A critical component of knowledge management within an organization is to create new knowledge, thus promoting its value and continued existence to stakeholders (Nonaka, 1994). Davenport and Prusak (1998, p. 5) defined knowledge management as the systematic process of identifying, capturing, and transferring the experience, know-how, and intellectual capital of people within organizations. O'Dell and Grayson (1998) noted that knowledge could be characterized as having either an explicit and tacit forms which are not mutually exclusive, although they coexist within an institution at the organizational, individual, and group levels. Gao, Meng, and Clarke (2008) noted that explicit knowledge is found in an organization’s policies, procedure manuals, and institutional documents such as the mission, vision, and value statements and is easily, stored, codified, and transferred. Tacit knowledge, on the other hand, is individualized and personal such that it is influenced by personal values, created and validated by

personal experience, contextualized in specific situations, and cannot be easily transferred or communicated (Cardoso, Meireles, & Ferreira Peralta, 2012). An organization's culture can be divided into three levels: artifacts, espoused beliefs and values, and basic underlying assumptions (Schein, 2010). Artifacts, which are easily observed in prominent places in the organization, the behavior of employees, and the organization and work processes can be aligned with the explicit knowledge within an organization (McDermott & O'Dell, 2001; Schein, 2010). Espoused beliefs and values which can be found in the organization's missions, stated vision, and goals as well as in individual principles, ideals, and personal aspirations are expressed as explicit knowledge and tacit knowledge (McDermott & O'Dell, 2001; Schein, 2010). The cultural level of basic underlying assumptions which represents perceptions, feelings, and the unexpressed or unstated thoughts that influence employee behavior and decision-making actions (Schein, 2010) relates to tacit knowledge that is the invisible dimension of an organization not readily or easily communicated (McDermott & O'Dell, 2001).

Schein (2010) noted that four barriers that are directly related to an institution's culture hinders the successful sharing and transferring of knowledge of strategies within an organization. The first barrier is ignorance on both ends of the transfer of knowledge where knowledgeable individuals realize their values to others while others seeking knowledge don't know where to find it (Serban & Luan, 2002; Szulanski, 2017). The second barrier is the unavailability of resources such as internal processes to acquire the necessary knowledge (O'Dell & Grayson, 1998; Szulanski, 2017). The third barrier is the lack of relationship between the knowledge receiver and a knowledge holder through

shared experiences and storytelling, which is hindered by the organization's values and structure (Serban & Luan, 2002; Szulanski, 207). The fourth barrier which is caused by the lack of motivation within the organization is the slow rate of adoption of new knowledge (Davenport & Prusak, 1998; O'Dell & Grayson, 1998; Szulanski, 2017). These four barriers must be successfully overcome to promote a learning organization (Lehman, 2017). Zheng, Yang, and McLean (2010) examined the mediating role of knowledge management in the relationship between organizational culture, organizational effectiveness, strategy, and structure. The authors attempted to detect and explain one of the mechanisms through which organizational contextual and strategic factors could be mobilized to achieve higher levels of organizational effectiveness. The authors emphasized that the practice of knowledge management is context-specific, and therefore, could influence the effectiveness of an organization. The results of the study suggested that knowledge management fully mediated the impact of organizational culture on organizational effectiveness, and partially mediated the effects of organizational structure and strategy on organizational effectiveness. The results support the knowledge-based view of the firm that knowledge management is not only an independent managerial practice, but also a central mechanism that leverages organizational cultural, structural, and strategic influence on organizational effectiveness. Prado-Gascó, Pardo, and Pérez-Campos (2017) analyzed knowledge management levels and organizational culture, as well as the relationship between organizational culture and knowledge management at a Spanish software development enterprise. Schein's OCT was the conceptual framework used for this study, which consisted of 196 employees between

21 and 45 years old. The findings of the study indicated that the organization was oriented towards a constructive organizational culture. Further, the results showed that the company emphasizes efficient knowledge management practices, particularly regarding teamwork. The authors noted that the results of the study showed a positive link between organizational culture and knowledge management performance as hypothesized and which is also in alignment with the studies in the literature that have explored these questions at the empirical level.

Xiao and Dasgupta (2005) examined the impact of organizational culture on IT practices and performance based on the literature that shows that researchers and practitioners acknowledge that organizational culture plays a significant role in IT implementation and influences organizational and IT performance. Xiao and Dasgupta (2005) noted that there had been little research in this area and aimed to address this gap in the information systems (IS) literature using Schein's' conceptualization of organizational culture as the framework for the study. The authors analyzed culture on three levels: artifacts, espoused beliefs and values, and underlying assumptions. Artifacts are visible organizational structures and processes. Espoused beliefs and values are the espoused justifications including strategies, goals, and philosophies. Underlying assumptions refer to the unconscious and taken-for-granted beliefs, perceptions, thoughts, and feelings that members of the organization share. Xiao and Dasgupta (2005) proposed a research model that relates the culture of innovation and espoused values to IT practices, IT Management, and IT performance using a survey method to test the relationships among the constructs. The authors noted that organizational culture is

essential for understanding practices that characterize organizations and for predicting their success, particularly in a complex and competitive environment. Further, it is crucial that leaders create a culture that facilitates innovation and IT management practices to improve IT performance. Xiao and Dasgupta (2005) highlighted that theoretically, their study would contribute to the body of knowledge in two folds: first, by addressing a gap in Information Systems (IS) literature by examining the relationship between organizational culture and IT. Secondly, the study would identify values and assumptions shared among organizational members that are more conducive than others to IT success and improvement of organizational performance. However, Xiao and Dasgupta (2005) noted that practically, the findings of this study would help leaders create constructive organizational culture to improve IT success rate and organizational performance. Furthermore, the results of this study showed a positive step in the conceptualization and empirical support of culture of innovation that promotes IT and performance.

Cybersecurity

Cybersecurity is a growing concern that poses severe challenges for communities in the United States and abroad due to rapidly changing advancements in technology. White (2016) identified the need for diverse teams and the importance of establishing effective and efficient cybersecurity teams that understand the growth of cyber threats, security controls, and measures to adapt to prevent future cyberattacks and tackle the rapidly changing threat landscape. McCollum (2015) discussed the top causes of cybersecurity breaches, including cybercriminals, malicious and non-malicious insiders, and hackers, as well as the need to recruit diverse cybersecurity talent with advanced

cybersecurity knowledge, training, and certifications. McCollum (2015) suggested an organization-wide approach to cybersecurity in a more diverse operating environment, a tailor marketed-appropriate to cybersecurity solutions for businesses, and a framework that enables all organizational members to be on the same page regarding cyber risk. McCollum (2015) further suggested collaborations with key stakeholders throughout the organization to promote the need to recruit and retain diverse cybersecurity talent to prevent rising cyber attacks.

Hawthorne (2013) acknowledged that the urgent need to secure the nation's cyberspace has called for a diverse cybersecurity workforce and recognized that an insufficient number of cybersecurity talents exist to protect and defend the US government and private sectors. The author argued that the current cybersecurity training and education programs are limited in focus and lack unity of effort. Therefore, cybersecurity awareness to build the workforce are needed urgently. Dunn Cavelty (2014) examined cyber threats and the measures necessary to counter their sophisticated and organized nature in government-led and private-led cyber-security initiatives and argued that the neglect of the human element or the lack of consideration for “the human” in resolving cyber threats is a direct consequence of a focus on technology-based countermeasures in cyber-security. Dunn Cavelty (2014) indicated that the current approaches to cybersecurity are not working due to a lesser inclusion of humans in solving cyber issues.

Prager and Prager (2016) noted that with the growing use of mobile technology, cloud computing, and data centers, no organization is immune to cyber attacks, not even

the NSA who work under the assumption that they have already been breached. Prager and Prager (2016) recognized the need for cybersecurity in top industry targets as well as the need for a skilled, technically trained, sophisticated talent pool for business defense. However, cybersecurity positions take one-third longer to fill than the average IT job due to the growing requirement for industry certifications, which take long to obtain. Prager and Prager (2016) suggested that diversifying the cybersecurity workforce by bridging the education gaps with diplomas, internships, and apprentices to provide job exposure and cultivate experience could help attract more talent to protect sensitive information.

Cybersecurity Defined and Explained

Cybersecurity experts and network security specialists are an organization's first line of defense against the increasing cyber-crimes (Rick Van der, Geert, & Heather, 2017). Their duties include not only the selection, setup, and maintenance of networks, but also network and systems monitoring and viewing network logs and intrusion alerts for suspicious or unusual activity (Rick Van der et al., 2017). The members of the cybersecurity workforce are individuals with roles and responsibilities that have an impact on an organization's (public and private) ability to protect its data, operations, and systems (NICE, 2018). The vital assets of many individuals, organizations, and governments are exposed to new scalable attacks and vulnerabilities that are emerging faster than cyber professionals are coming up with improved defenses (Goodman, 2014). Goodman (2014) called for the Centers of Academic Excellence (CAE) to help close the gaps between the supply and demand of cybersecurity talent. Goodman (2014) suggested

that organizations need diverse cyber talent to respond to these security incidents proactively.

Cybersecurity Talent Deficit as an Applied IT Problem

Government agencies and businesses are struggling to defend themselves against data breaches, denial of service attacks, ransomware, etc. due to cyber talent deficit. Cyber attacks are growing in frequency and sophistication, based on an estimate that in 2014, $1 billion of personally identifiable information (PII) was stolen from cyber attacks, and the average cost of a data breach is projected to rise to $150 million by 2020. Unfortunately, qualified cyber talent to handle these challenges are not available (NIST, 2017). Castro (2018) emphasized that persistent talent shortages have contributed to organizations failing to implement many essential cybersecurity controls, including network and endpoint forensics, multifactor authentication, biometrics, access controls, intrusion prevention systems, etc. Castro (2018) suggested that certification programs, degree programs, and cyber workforce development programs should be established to attract diverse cybersecurity talent to tackle the growing cyber threat landscape. Abel (2017) suggested that giving women more cyber opportunities and involving them more could help reduce the shortage of cybersecurity talent. These opportunities could lead to an increase in ideas, creativity, profitability, and introduction to various viewpoints and solutions.

Hwee-Joo and Pairin (2014) examined the effect of integrating cultural, social, and political dimensions into the approaches to tackle cyber attacks since the increasing numbers of cyberterrorism and hacktivism suggest that cybersecurity exerts political,

religious, and cultural influence. Hwee-Joo and Pairin (2014) agreed that cyberattacks today are not only limited to website defacements but also involve targeting specific organizations or industries to destroy infrastructure, ruin a reputation, steal intellectual property, or disrupt the economy motivated by political agenda. Hwee-Joo and Pairin (2014) suggested diversifying and understanding the nontechnical aspects of cybersecurity - the people - to protect public and private infrastructures.

Mansfield-Devine (2017) reported that the shortage of skilled information security personnel in Europe reached a crisis point just as the EU's General Data Protection Regulation (GDPR) threatened crippling fines for any organization that encounters a security breach due to non-compliance. Mansfield-Devine (2017) revealed that the global research by the Information System Security Certification Consortium (ISC)² showed that 40% of organizations plan to address the security issue by growing their cybersecurity teams by 15% over the coming year if they can find cyber talents. The author pointed out that the “Global Information Security Workforce Study” (GISWS), which is conducted every two years by the Centre for Cyber Safety and Education and (ISC)², predicted that by 2022, there would be a global shortfall of 350,000 information security practitioners. The author suggested having a layered defense including cybersecurity training and increasing the numbers of women and minorities in cybersecurity to prevent security breaches from becoming the norm for government and businesses. The Homeland Security Advisory Council (2017) highlighted that not only is there a shortage of diverse cybersecurity professionals needed to operate and support systems, there is also an even more desperate need for cyber talent who can design and

develop secure systems and sophisticated tools necessary to prevent, detect, mitigate, and rebuild systems after a cyber-attack.

Oltsik and Alexander (2016) pointed out that the shortage of cybersecurity skills contributed to the increase in data breaches, zero-day vulnerabilities, and malicious internet protocol addresses. South (2015) noted that the lack of security expertise and diverse teams contributed to the increase in data breaches in the United States. South (2015) suggested that acquiring degrees in cybersecurity and certificates like the Certified Information Systems Security Professional (CISSP) could help individuals gain useful cybersecurity knowledge and get a cybersecurity job. Kerner (2016) investigated the impact of the security skills shortage on hacking activities and found that the lack of cybersecurity skills makes organizations more vulnerable and greater hacker targets. Coppel (2016) reported on the 'Hacking the Skills Shortage' study by Intel Security and the Center for Strategic and International Studies (CSIS) which found that the continued cybersecurity skills shortage and workforce gap has already created substantial risks and resulted in damages to organizations by making them vulnerable to hacking. Coppel (2016) indicated that 82% of organizations revealed that they had been breached and lost their proprietary data due to the demand for cyber experts surpassing the supply of experienced workers. Coppel (2016) suggested diversifying the cybersecurity workforce with skilled women and minorities to increase the cybersecurity workforce to prevent cyber attacks.

The Senate Homeland Security and Governmental Affairs Committee discussed the need to improve the bureaucratic federal hiring process and lengthy security clearance

process to address the severe cybersecurity talent deficit to protect information systems in the U.S. federal government and private organizations (Congress.gov, 2018). Congress enacted into law H.R. 3210, the "Securely Expediting Clearances Through Reporting Transparency Act of 2018" or the "SECRET Act of 2018" which was signed by President Trump on May 22nd, 2018 (WhiteHouse.gov, 2018). The Senate Homeland Security and Governmental Affairs Committee also suggested diversifying talent pools by recruiting specialists from various backgrounds as well as training the existing workforce to protect sensitive information (Congress.gov, 2018). Shumba et al. (2013) also acknowledged the cybersecurity talent deficit to defend the country from digital intrusions and noted that the lack of women and minorities progressing through a full career in cybersecurity could be a contributing factor to the cyber talent shortage.

Cybersecurity Talent Attraction, Recruitment, and Retention Strategies

The Overcoming Barriers to Advancement - CIA Diversity in Leadership Study (2015) [CDL] examined the lack or absence of inclusivity, equal opportunity, and accountability in promoting diversity, integrating talent, and enhancing the recruitment process of cybersecurity professionals by senior leadership across organizations. The findings of the CDL study indicated that the lack of a more inclusive cybersecurity workforce, particularly females, has been identified as a contributing factor to past intelligence failures and critical missions.

The GWIS (2017) discussed the statistically low percentage of female cybersecurity professionals to tackle rising cyber threats. The GISWS draws upon data that showed that women account for only 11% of the information security workforce.

GIWS noted that there is a likelihood of a cybersecurity workforce gap of 1.8 million by 2022, which is a 20% increase over the forecast made in 2015. The U.S. Department of Labor, Bureau of Labor Statistics (2018) reported the growing demand for cybersecurity professionals by 13 percent. This growth is faster than the average for all occupations, and yet women remain significantly underrepresented in the cyber workforce. The GIWS showed that two-thirds of the 20,000 respondents indicated that their organizations lacked a sufficient number of cyber talent to combat the cyber risks in today's ever-evolving threat landscape. The GIWS suggested that organizations should differ their scope of potential cyber talent-hiring practices by including talented, innovative, and motivated women and minorities to working within a team to help prevent loss of data, reputational damage, disruption of networks, and target by hackers.

Ghosh (2015) also recognized the underrepresentation of women in the cybersecurity workforce and attributed the stigma attached to cybersecurity professionals as being male-dominated. Ghosh (2015) suggested tapping into the growing field of Healthcare Informatics as a way of introducing and engaging women in cybersecurity concepts. Cabaj, Domingos, Kotulski, and Respício (2018) examined the impact of the growing cyber attacks in governmental and non-governmental organizations and the insufficient cyber workforce to satisfy the increasing demand for cybersecurity experts. Cabaj et al. (2018) suggested that academic institutions offer cybersecurity topics such as information assurance that help increase qualified cybersecurity professionals. Abdul-Alim (2017) suggested that organizations recruit and retain diverse talent from universities and colleges that include diverse populations as opposed to non-diverse

populations. These cyber talents should have intellectual curiosity and possess today's cyber skills to mitigate cyber attacks. Liu and Murphy (2016) examined the cybersecurity concerns due to significant data breaches and acknowledged that there is a cybersecurity talent deficit, notably the limited number of women in the workforce to protect our digital world. Liu and Murphy (2016) suggested the concept of "cybersecurity for all" which emphasizes personal responsibility for security and privacy and a more inclusive cyber workforce. Further, cybersecurity should be taught at all ages (from K through Gray) using the scientific method, the experiential learning model, and the constructivist theory to help attract, inspire, and engage students (especially females) in cybersecurity. The authors noted that the scientific method contains five essential elements: (a) formulating a question from previous observations, measurement, or experiments. (b) induction and formulation of hypotheses. (c) making predictions from the hypotheses. (d) experimental testing of the predictions. (e) analysis and modification of the hypotheses. The authors explained that experiential learning involves "learning through reflection" to gain genuine knowledge from experience. Lastly, the constructivist theory of learning enables students to master the most powerful and modern technology by acquiring in-depth ideas from mathematics, the art of intellectual model building, and science.

Burrell and Nobles (2018) noted that recruiting and retaining diverse cybersecurity workforce requires having cybersecurity leaders that are adequately trained in diversity, inclusion, and employee engagement in ways that can constructively influence positive organizational and employee behavioral change. Burrell and Nobles (2018) suggested that having competent and empowered leaders that leverage diversity

and inclusion (D&I) strategies are one the most critical aspects of attracting, developing, and retaining women and minority cyber talents. Burrell and Nobles (2018) emphasized that diversity promotes differences in thinking and perspectives, enabling organizations to discover new practices, new vectors, and innovate ideology to solve problems and ensure operational successes. Furthermore, a socially diverse cyber workforce with various core capabilities and specialties are more strategically advantageous than a homogeneous group at approaching and solving complex, emergent problems with holistic viewpoints such as critical cultural and gender-based perspectives on technical issues. Burrell and Nobles (2018) further suggested that diversity could broaden knowledge, incite new practices by adding to an organization's intellectual capacity and innovative ideology and provide organizations with a core strategic advantage by approaching projects, challenges, problems, and strategies from clear vantage points. Burrell, Aridi, and Nobles (2018) argued that IT managers lack adequate leadership experience, skills, and preparation, particularly in the delegation, communication, and business savviness to drive information security practices forward. Burrell et al. (2018) emphasized that the failure of some organizations to regard cybersecurity as a fundamental business strategy is detrimental to the health of the organization's information security practices, critical data, and systems. Burrell et al. (2018) suggested the use of leadership development interventions that focus on building diverse teams and individual competence to protect mission-critical systems through the effective collaboration of diverse cyber talent.

Crosman (2017) pointed out that the demand for cybersecurity talent is outgrowing the supply, as three big banks (USAA, Wells Fargo, and U.S. Bank) discussed their challenges with being top hacker targets. Crosman (2017) suggested recruiting a diversified cyber workforce and establishing recruitment programs to increase the cyber interests of high school and college students. The bank security chiefs agreed that a diverse pool of talents with cybersecurity training and experience in dealing with attackers was a rich source of cybersecurity talent. Dahlberg (2012) pointed out the significance of broad participation (BP) in the cybersecurity field for continued innovation due to the increasing demand for diversity that drives creativity. Dahlberg (2012) suggested a multipoint focus that includes research, sharing best practices, professional development, and raising awareness. For example, Computing in the Core (CIC) and Coalition to Diversify Computing (CDC) encourages underrepresented undergraduates to obtain a graduate degree to promote ethnic and gender diversity in IT classrooms.

Bagchi-Sen et al. (2010) suggested that women should thoroughly evaluate the required skills and the existing barriers (social, institutional, and personal challenges) to advance to executive levels in cybersecurity. Also, women and men alike must possess soft skills and a strong background in hardware and software systems with the ability to transform their knowledge into government policy and external regulations to progress in the cyber field. Lemos (2017) indicated that addressing the shortage of women in cybersecurity requires valuing their opinions, making the workplace more equitable, encouraging cybersecurity leaders to create more inclusive workplaces, closing the wage

gap, cybersecurity leaders connecting with women as they enter high school, investing in training, mentoring, advancement, and sponsorship programs. Pretorius et al. (2015) suggested the promotion of a family-supportive philosophy that allows telecommuting and collaboration through secure interconnectivity as well as good wages, job security, flexible-worktimes, flexible work environments, and job satisfaction to attract women to a career in cybersecurity.

Abel (2017) pointed out that diversity reports revealed that 85% of Uber staff, 83% of Facebook staff, and 77% of Apple staff are male. Abel (2017) suggested creating cybersecurity career awareness programs, breaking the barriers and stereotypes that prevent women and minorities from pursuing a career in cyber and making tech feel more inclusive through sponsorship opportunities for women and minorities. Janeja et al. (2018) suggested that individuals who received peer mentoring showed more interest in cybersecurity issues and made more informed decisions to help mitigate cyber attacks. McCandless (2017) noted that cybersecurity is a top priority for state and local IT leaders, yet the Center for Digital Government reported that 93% of states indicated a current cybersecurity workforce gap. McCandless (2017) suggested an investment in a diverse team of cyber professionals to bridge the cyber talent gap. NICE (2017) suggested that cultural change is much needed to recruit more women and minorities in the cyber workforce. Kappelman, Johnson, Maurer, McLean, Torres, David, and Quynh (2018) indicated that cybersecurity is the most important and most challenging IT workforce skill and remains the highest-ranked concern in many organizations, thus,

suggesting that organizations increase their cybersecurity talent attraction, recruitment, and retention budget to help protect their systems.

Cybersecurity Team Effectiveness and Workforce Diversity

Diversity is the key to cybersecurity teams in overcoming security challenges, and it is uniquely critical to the work in the intelligence community (Innovation and diversity in the cyber fight, 2015). The lack of diversity has contributed to past intelligence failures and mistakes because of the absence of individuals with a diversity of thought, perspectives, experience, culture, and upbringing to ask the ‘what if ‘questions (Innovation and diversity in the cyber fight, 2015). An essential element to help keep pace with diverse threats is to be as diverse as the threats itself, raise the cyber literacy level, and empower people who are innovative to push themselves to the fullest extent (Innovation and diversity in the cyber fight, 2015). Cyber experts need to think differently, have a unique cultural background, different thought patterns or processes, have diverse expertise, understand different programming languages, and have a diverse understanding of global communities if they are to bring value to the cybersecurity and intelligence community (Innovation and diversity in the cyber fight, 2015). The foundation for successfully protecting U.S. national security and economic prosperity to maintain a competitive advantage relies on the nation’s private and public sector cybersecurity workforce (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018). Thus, the nations’ successful cybersecurity workforce strategy should incorporate and focus on the values of diversity and inclusion (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018). Further, sustaining and

fostering a diverse workforce supports the ability to find new cyber talent to perform cybersecurity functions and uncover innovative ways of solving problems (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018).

Cowley, Nauer, and Anderson (2015) suggested closing the gap between the workforce and expertise in cybersecurity teams by selecting diverse individuals with diverse capabilities to address a wide variety of cyber threats. Cowley et al. (2015) explored the relationship between interpersonal style, team performance, and the degree of interpersonal maladjustment (the mean interpersonal style vector lengths). The author explained that certain personality traits predict certain behaviors, and these trait-behavior patterns are called interpersonal styles. Further, interpersonal styles are said to be complimentary if a behavioral style responds the way it is predicted to respond. The author used four theories of complementarity to evaluate the number of complementary interpersonal styles. The psychometric test revealed that top-performing cybersecurity teams possess different characteristics and involve a wide array of human factors that play significant roles in team selection and enhances the team's performance.

The computer security incident response teams (CSIRTs) in organizations need to respond quickly and effectively to computer security incidents on an ad hoc basis, in close collaboration with diverse teams, and in time-constrained environments to help organizations to minimize the impact of breaches and improve creativity, productivity, adaptability, information processing capacity, and performance. Rick Van der et al. (2017) noted that the failure of these CSIRTs could have far-reaching effects and catastrophic consequences for national security and the economy, given the growing

threat landscape. The authors suggested that the focus should be on identifying areas for team improvements and on potential solutions by increasing team members' skills level, knowledge, technical resources, participation, and cooperation to close the gaps between current and desired incident handling practices.

Chen, Shore, Zaccaro, Dalal, Tetrick, and Gorab (2014b) examined the cognitive abilities and processes involved in a cybersecurity job in collaboration with organizational psychologists to ascertain how diverse team members interact with one another when responding to security events. Chen et al. (2014b) suggested that CSIRT managers use the cognitive task analysis technique to gain a deeper understanding of the individual, team, and team system tasks in which their employees engage to facilitate the hiring of qualified employees. Steinke et al. (2015) also noted that CSIRTs protect the security of the technological infrastructure of both government and private organizations and are often required to work collaboratively to mitigate cybersecurity threats. Despite the significance of the role of CSIRTs, finding talents to fill the positions is challenging because they need a blend of technical and interpersonal skills. Chen et al. (2014b) suggested the collaboration of a diverse team of cybersecurity talents with different cultures, demographics, domain expertise, structure, and temporal dynamics to accomplish a shared goal as diverse teams are successful and productive when they collaborate and share information to solve complex problems and manage information systems collectively.

Steinke, Bolunmez, Fletcher, Wang, Tomassetti, Repchick., and Tetrick (2015) also suggested that diverse team members function better, communicate better, and

interpret information and situational contingencies in similar ways due to shared mental models which significantly impacts team effectiveness. Steinke et al. (2015) emphasized that having a diverse cybersecurity team increases information sharing, increases trust, promotes cooperation, reduces conflict, and drives successful team performance. The authors also noted that diverse cybersecurity teams boost staff morale, improves work-life balance, and lower stress levels because they rely on each other in risky situations to quickly resolve problems. DHS (2015) also emphasized the need to have diverse CSIRTs that share physical security and cyber information to enhance the effectiveness and efficiency of the U.S. government's efforts to make critical infrastructure more resilient and secure. DHS (2015) suggested that a diverse CSIRT assists operators of critical systems by responding to incidents, restoring services, analyzing potentially broader cyber or physical impacts to critical infrastructure, locating cyber threats, and determining the best prevention mechanisms.

Champion, Rajivan, Cooke, and Jariwala (2012) examined the impact of situational awareness (SA) in teams of security analysts using a cyber defense simulation environment known as CyberCog. The results of the study revealed that the absence of team diversity among the cyber analysts proved to be a substantial obstacle that resulted in nondiverse teams experiencing communication breakdowns, information overload, and feelings of being overwhelmed, which led to cognitive fatigue and frustration. The diverse teams, on the other hand, were more adaptive, maintained awareness, and responded to the situations seamlessly. Granåsen and Andersson (2016) investigated the role of behavioral assessment techniques as a complement to task-based performance

measurement. Using a combination of behavioral assessment techniques and technical performance measurements to assess team effectiveness revealed that implementing diverse teams of cyber talent improved team effectiveness and performance. Similarly, Carlin, Manson, and Zhu (2010) noted that the National Security Agency (NSA) determined that a diverse cybersecurity team was able to maintain its network services while detecting, analyzing, and responding to potential intrusions, leading to effective and efficient team performance.

Buchler, Rajivan, Marusich, Lightner, and Gonzalez (2018) examined how high-performing diverse cybersecurity teams respond to and mitigate live cyberdefense tasks or attacks. The authors recognized that humans are behind many cybersecurity challenges as both the problem and the solution. Thus the human dimension in a diverse team structure must be able to cooperate, adapt, anticipate, reason, and orchestrate an effective strategy to respond to ongoing threats effectively. Pusey et al. (2016) noted that engaging females, gifted students, low-income, and high-risk groups in cybersecurity through competitions guided ethical standards, fostered a shared understanding of diverse tasks, and created a developmental pathway that aid the growth of cybersecurity skills. Pusey at al. (2016) suggested that diverse skill levels enable differentiated learning, enriched experiences, build confidence, improve career awareness, and support the development of soft skills such as teamwork, communication, and critical thinking required for cybersecurity teams to effectively and efficiently resolve problems.

Barriers to Diversity in Cybersecurity

Bagchi-Sen et al. (2010) examined the existing barriers, the required skills, and the critical success factors necessary for the career advancement of women in the cybersecurity field. The authors blamed IT's "hacker culture," IT's "old boys' network," social expectations, security concerns, and work-life-balance for the underrepresentation of women in cybersecurity. The authors suggested that perceived self-efficacy, the lack of interest in math and science, and the historical discouragement of girls from pursuing computer science could be blamed for the lack of female career advancements in cybersecurity. The authors further noted that the shortage of female IT faculty and female science and math teachers as role models in middle schools, high schools, colleges, and universities could be another contributing factor to the underrepresentation of women in cybersecurity.

Pretorius, Mawela, Strydom, de Villiers, and Johnson (2015) also highlighted the worldwide decline in the participation of women in cybersecurity and examined the impact of domestic influences on women in cybersecurity. Pretorius et al. (2015) found that women with families struggled to find enough time to keep up with the demands of the IT industry. Dahlberg (2012) also pointed out that the continued existence of disparities in the participation of women, underrepresented minorities, and persons with disabilities in cybersecurity. Abel (2017) and Dahlberg (2012) noted that while studies showed that women make up approximately 25% of the computing workforce, women of color make up less than 10 percent, according to the National Center for Women and Information Technology. Wilson, Broughan, and Hillier (2017) also examined the gender

disparities in STEM-oriented disciplines like cybersecurity and found that lack of leadership, inadequate mentoring, limited education, and the responses to life transitions negatively impacted the careers of women. The authors also found that intrapersonal influences, work influences, financial influences, social influences, and expectations significantly impacted the careers of women. Master, Cheryan, and Meltzoff (2016) also examined the gender disparities in STEM and found that high school girls' avoided computer science courses due to the persistent stereotypes that signaled to them that they do not belong. Master et al. (2016) suggested educational environments that are stereotypes free to help reduce gender disparities in STEM disciplines like cybersecurity.

In a study published by the Center for Cyber Safety and Education, Risk Management and Privacy, and the Executive Women's Forum in conjunction with the International Information System Security Certification Consortium, (ISC)2, Lemos (2017) found that skilled women struggled to join the workforce to address cyber threats, amidst the estimates of a shortfall in the cyber-security workforce. Similarly, a report by Women, Minorities, and Persons with Disabilities in Science and Engineering (2013) (WMPD) found that women, people with disabilities and minorities from three racial and ethnic groups - black, Hispanic and American Indian or Alaska Native - are accounted for in disproportionately smaller percentages in science and engineering. Ritchey (2016) examined the careers of several women who have excelled in cybersecurity, and they expressed concerns about the underrepresentation of qualified women and minority cyber talent in the cybersecurity segments of government and businesses. Similarly, Peacock

and Irons (2017) also expressed substantial concerns about the low numbers of qualified female cyber talent who can address the increasing threat landscape.

Abdul-Alim (2017) examined the job profiles of security analysts and the shortage of female and minority talent in the emerging cybersecurity sector and pointed out that the demand for security analyst is expected to grow by 18% between 2014 and 2024 - "much faster than average," based on the projections from the U.S. Bureau of Labor Statistics. However, there is an insufficient cyber talent to fulfill the demand, and women and minorities do not have access to these jobs at the same rate as their other colleagues based on a report from the Business-Higher Education Forum (Abdul-Alim, 2017). The report indicated that African Americans and Hispanics represented only 6% and 7% of the STEM employment, with men outnumbering women by three to one (Abdul-Alim, 2017). Similarly, Urrico (2016) pointed out the challenges due to the shortage of information security professionals is failing to meet increasing market demand and suggested that there is an opportunity for women to fill this workforce gap to help secure their systems and increase the talent pool. According to the Homeland Security Advisory Council (2017), the size of the cyber skills gap in the United States was estimated to be over 200,000 in 2015, and it is expected to grow to about 265,000 in North America by 2022. Further, the national average ratio of existing cybersecurity workers to cybersecurity job openings is only 2.5, while the national average for all jobs is 5.6 (Homeland Security Advisory Council, 2017).

Burrell and Nobles (2018) highlighted that for the past 30 years, researchers, educators, government, industry, and academia have struggled to understand the

underrepresentation of women and minorities in STEM fields. Burrell and Nobles (2018) noted that the unrelenting cyber attacks and the deficiency in the strategic initiative to recruit and retain women and minority cyber talent begs for a diversity of thinking and perspectives to enable organizations to discover new ways to solve problems efficiently. Burrell and Nobles (2018) suggested that the lack of role models and mentors, non-female friendly teaching practices and curricula, rigorous STEM environments, inadequate academic preparation, societal stereotypes about who can be scientists, and educational and social factors affect the participation of women in the cyber workforce. Burrell, Aridi, and Nobles (2018) also examined the perceptions of the career advancements of women in cybersecurity who experienced social and institutional barriers in both IT and cybersecurity careers. The results of their study suggested that a lack of technical skills, cybersecurity knowledge, job experience, practical experience, confidence, social skills, management opportunities, wages, etc. could deter women from joining the cyber workforce.

Cybersecurity Workforce Gaps and U.S. Congressional Concerns

The persistent difficulties facing the government as it seeks to increase its cybersecurity workforce have aroused the interest of members of Congress. Chalfant (2017) suggested better attraction, recruitment, and retention practices such as offering security personnel competitive salaries and training comparable to the private sector to fill vital federal and private sector to defend the nation from the now more pervasive cyber attacks. The author noted that statistics showed that the global cybersecurity workforce who respond to security breaches, is expected to be short in both the public

and private sectors. The White House recognized the need to bolster the cyber workforce due to the shortage of cybersecurity professionals to secure the nation's infrastructure; to that effect, the administration signed an executive order in May 2019 on America's Cybersecurity Workforce to help address the gaps in the cyber workforce to strengthen the nation's security (WhiteHouse.gov, 2019). The Department of Homeland Security (DHS) is severely short of cybersecurity talent, and the Senate Homeland Security and Government Affairs Committee recognized the extremely rigorous cyber talent recruiting process as a significant barrier to attracting top cyber talents (Congress.gov, 2018). The lawmakers on the panel put forward a bill known as the "Securely Expediting Clearances Through Reporting Transparency Act of 2018" or the "SECRET Act of 2018" to relax the bureaucracy involved in hiring cyber talent to protect sensitive information (Congress.gov, 2018). Francis and Ginsberg (2016a) noted that the law requires DHS to provide details of its plans to recruit and retain employees in cyber positions and also measure its progress. However, the statutes governing flexibilities for DHS and DOD cyber positions at the U.S. Cyber Command do not include provisions that make it mandatory for human resources staff to obtain training on the operation, structure, and availability of cybersecurity pay and recruiting flexibilities (Francis & Ginsberg, 2016a). The laws also do not mandate DHS and DOD to determine the effect of the recruitment and pay flexibilities on the departments' ability to attract and retain qualified cybersecurity talent.

Francis and Ginsberg (2016b) pointed out that the excepted service designations which are not typically available to all federal employees could increase an agency's

ability to attract and retain cybersecurity professionals. The service allows agencies to fill specialized jobs or any position in unusual or exceptional circumstances. The cyber talents that meet minimum qualification requirements and excepted service position's eligibility do not have to compete with other DOD and DHS applicants. Also, additional performance or non-performance based monetary compensation could be offered. Francis and Ginsberg (2016c) also acknowledged that the federal cybersecurity workforce, DOD, and DHS, who are responsible for protecting the U.S. government networks and systems against cyber threats and attacks, have also expressed difficulties with finding qualified cyber talent to fulfill their departments' cyber missions. Francis and Ginsberg (2016c) revealed that Congress authorized hiring and pay flexibilities to expedite the federal hiring process for cyber talent.

The Hastings' bipartisan amendment (2018) to H.R.6237 in collaboration with the heads of other intelligence community agencies, directed the DNI (Director of National Intelligence) to create and implement a plan that expands the recruitment efforts of all intelligence community (IC) agencies such that minorities including women, African-Americans, Hispanics, and Native Americans are fully included and represented in recruitment efforts across the nation. The Hastings' bipartisan amendment (2018) supported the significance of protecting the cyberspace with diverse teams of cyber talents that have strong vision and leadership. Similarly, the House of Commons Science and Technology Committee recommended a series of initiatives to encourage an inclusive workplace culture, values, demands, and work-life balance (Wilson et al., 2017). The efforts proposed included bias prevention, diversity and equality training,

identifying suitably qualified female candidates for senior roles, realizing gender equity in STEM academia, and mentoring schemes to encourage women to apply for such positions.

Computer science is no longer ‘an optional skill’ in the modern economy because, in 2016, President Obama proposed the ‘Computer Science for All’ initiative geared toward diversifying the cybersecurity workforce. Fisher (2016) noted that the strategic objective of the initiative was not to isolate females but to create a diverse gender-neutral environment as opposed to a male-dominated cybersecurity workplace. Fisher (2016) suggested that aligning the 'Computer Science for All' initiative with universities could create an overarching platform to guide cybersecurity curriculum development in K-12, undergraduate, master, doctoral levels, and senior citizens outreach programs.

Workplace Diversity and Inclusion

Kundu and Mor (2017) noted that the pervading influence of diversity in organizations could no longer be ignored as diversity has transformed from being a governmental or legal obligation to a strategic priority. Kundu and Mor (2017) emphasized that the goal of attaining sustainable competitive advantage has instigated organizations to embrace the concept of diversity. However, embracing diversity as a concept alone does not guarantee success as organizations need to effectively manage diversity by celebrating, valuing, integrating, supporting, and actively encouraging workforce diversity through fair employment practices. Kundu and Mor (2017) defined a diverse workforce as the co-existence of people from various social, cultural, and ethnic backgrounds within an organization. Leaders and managers argue that diversity

management should go much further than just complying with existing regulations or reacting to changes in the labor market (Kundu & Mor, 2017). Mazur (2014) emphasized that diversity is a cultural question of norms, values, beliefs, and expectations. The author described diversity as being focused on a "culture of inclusion," which means an organizational environment that allows people with different ways of thinking, multiple backgrounds, and mindsets to work effectively together while performing to their highest potential to achieve organizational objectives based on solid principles.

Diversity Management

The lack of workplace diversity is framed as a problem that needs to be controlled (managed) by managers in organizations. Bouten-Pinto (2016) noted that workplace diversity should be inclusive of all aspects of diversity that matter to the employees and not just those mandated by or sanctioned through organizational directives or legislation. The author established reflexivity, which positions the development of relationships between employees and managers as a key ingredient in controlling and managing diversity rather than focusing on compliance only. The author also highlighted that diversity management is fundamental to harnessing the skills, knowledge, and abilities of diverse employees and creates competitive advantage focused on increasing the capacity of employees' to appreciate, negotiate, and overcome barriers to effective interactions based on their current perceptions of difference.

Diversity and Inclusion Best Practices

There is an urgent need for organizational leaders to ensure a diverse workforce in the science, technology, engineering, and mathematics (STEM) fields because it has

become increasingly vital to the competitiveness of industries in a global market. Cohen (2017) explored the strategies for a robust, diversified STEM field workforce to ensure companies are integrating their talent pool with diverse individuals to meet future innovative demands. Mazur (2014) argued that the challenges of creating an inclusive corporate culture by demanding innovation, creativity, and flexibility within competitive, dynamic, and increasingly global markets are best achieved by an expanded pool of knowledge and experience that exists in an effectively managed diverse workforce. Mazur (2014) further emphasized that the creative and innovative potential inherent in a diverse workforce as it relates to cultural background, ethnic origin, gender, age, way of thinking, religion, working style, nationality, education, lifestyle, etc. could be used to bridge cultural boundaries, innovate product ideas, and search for solutions to problems. Although many organizations have employment policies that include initiatives geared toward diversity, their culture does not embrace the creation of a conducive atmosphere for diversity. Mazur (2014) noted that the studied organization, Cisco corporation, employs engineers from various cultural backgrounds by building an inclusive and diverse organization with trust and mutual respect as a business imperative.

Lambert (2016) noted that diversity and diversity management (DM) could create a fertile environment for innovation to flourish in the organization either explicitly using formal policies and guidelines directly tied to cultural diversity or implicit through the behavior of leaders. Lambert (2016) also found that the strategic and sustained outcome of embracing diversity could lead to a more significant number of women and minorities who are empowered to influence process and product innovation effectively and

efficiently based on the extent to which policies or practices embraced diversity. Organizations that value diversity tends to attract a wide variety of talent because they draw from a larger talent pool to create a competitive advantage in finding individuals with varied cognitive skills that support innovation and problem-solving (Lambert, 2016). Amegashie (2018) suggested that implementing workforce DM practices and policies at the strategic, tactical, and operational levels of the organizational structure positively affect an inclusive change in culture and workplace performance growth that outpaces homogeneous workgroups.

Sustainability of Workforce Diversity and Inclusion

Organizational leaders struggle when creating a sustainable culture of diversity and inclusion (D&I) regardless of turnover, restructuring, downsizing, or market trends. Farmer (2014) explored the role of chief diversity officers (CDOs) in promoting and sustaining D&I in organizations and found that CDOs play a significant role in uniting employees, providing awareness, education, and training programs, and creating the business case that aligns with core business goals and objectives but struggles with creating a work environment where everyone feels included and valued. Farmer (2014) explored Schein's concept of leaders as shapers of organizational culture as well as Schein's culture model, which highlights culture from an observer's perspective, described by three cognitive levels of organizational culture: artifacts, espoused values, and basic underlying assumptions. Age, ethnicity, gender, race and sexual orientation, and mental/physical abilities and characteristics represent the core of diverse identities (Farmer, 2014).

Organizational Performance

Diversity and inclusion, as well as culture and leadership, could significantly impact the performance of an organization, as discussed below. Ardakani, Abzari, Shaemi, and Fathi (2016) and Kundu and Mor (2017) examined the effects of diversity and inclusion on organizational performance. Ilieş and Metz (2017), Ruygrok (2016), etc. examined the effects of culture on organizational performance. Alhadid (2016) and Erkutlu (2012) examined the effects of leadership on organizational performance.

The Effects of Diversity and Inclusion on Organizational Performance

Kundu and Mor (2017) evaluated employee perceptions of diversity based on their receptivity to diversity and its management, equal representation and developmental opportunities for all employees, hiring and retaining diverse employees, and promoting gender diversity. The results of the study indicated that employees' perceived organizational performance was directly related to their perception of promotion of gender diversity and equal representation and developmental opportunities. Also, the male respondents did not value their employer hiring and retaining diverse employees' practices, whereas minority and socially disadvantaged respondents supported the attraction, recruitment, and retention efforts of diverse employees to remain effective and efficient.

Ardakani et al. (2016) described workforce diversity as all the differences that comprise the individual like, for example, culture, ethnicity, nationality, age, religion, disability, gender, education, beliefs. Ardakani et al. (2016) analyzed the effects of DM and its approaches on human resource productivity (HRP) and confirmed that perceived

organizational justice, perceived organizational attractiveness, and perceived social identity served as gatekeepers. The authors suggested that Managers need to understand demographic diversity variables; establish performance evaluation programs based on merit; conduct diversity awareness training programs to increase competitive advantage, improve team creativity, increases job commitment, increase organizational outcomes, improve job satisfaction, decreases operational cost, increase productivity, reduce discrimination lawsuits, promote organizational attractiveness, justice, and social identity, and include different cultures, sexes, and ages in their diversity efforts. Lambert (2016) argued that empirical evidence demonstrated that cultural diversity impacts organizational creativity and performance. Therefore, it should logically follow that diversity plays a role in how firms become innovative while embracing and valuing the diversity that is linked to creativity.

The Effects of Culture on Organizational Performance

Innovation is regarded as a significant contributing factor to the long-term success of an organization in competitive markets today. Naranjo-Valencia, Jimenez-Jimenez, and Sanz-Valle (2016) examined the influence of organizational culture on behavior and people and found that adhocratic culture could foster innovation and improve an organization's performance based on the values promoted. Lawson, Hatch, and Desroches (2013) examined the need for a progressive organization to formulate its strategy, implement processes that support operations, provide performance evaluation and operational control, and learn and change with the use of a management system. The authors noted that methodologies, metrics, processes, and systems make up corporate

performance management (CPM) systems used to manage performance at the corporate level. They also suggested the use of maturity modeling, which is a tool designed to help organizations manage change, prioritize actions, and foster a performance-directed culture. The use of maturity modeling helps improve the effectiveness of a CPM system, which could provide organizations with a wide variety of operational and strategic benefits. These benefits include (a) increased employee efficiency and adaptability. (b) increased employee accountability and visibility. (c) critical decisions based on timely information. (d) delivery of targeted best practices and methodologies. (e) more capable and motivated workforce. (f) enhanced ability to respond to changes in the operating environment.

Jacobs, Mannion, Davies, Harrison, Konteh, and Walshe (2013) examined the associations between organizational culture and performance using the Competing Values Framework (CVF) to measure senior management team culture. The authors found that a stronger blend of cultures would move the organization towards better and more competitive outcomes. The findings also indicated that single dominant cultures became less prominent. Jacobs et al. (2013) defined culture as a set of beliefs, attitudes, customs, practices, and values which are shared by a group (ethnicity, geography, politics, religion) whose core values help shape its members' preference patterns, decision-making, and performance. Organizations strive for excellence in practice through the development of a strong team culture, which Ruygrok (2016) defined as a set of shared norms, values, and beliefs that drive performance and behavior. Ruygrok (2016) suggested that leaders foster a cohesive, high-performance culture with clearly

defined values, principles, and beliefs to sustain an efficient and effective team in an environment that understands the critical need to groom teams. Ruygrok (2016) further suggested identifying the performance expectations of each team member and defining expected behaviors while restating the core values during communications, team briefings, and during the interview for potential hires. Ilieş and Metz (2017) explored the relationship between culture and organizational performance and found that organizations recognize that a strong culture is a source of sustained competitive advantage in achieving short and long-term strategic business objectives. Ilieş and Metz (2017) noted the consensus that organizational culture is a set of sharable values, beliefs, and understandings that are transmitted to new members as the correct way of thinking, feeling, and behaving. Past research on this topic by Saffold III (1988) and Zheng, Yang, and McLean (2010) supports the idea that "adaptive cultures" are the key to good organizational performance as people are willing to take risks, trust each other, be proactive, and work together to identify and solve problems.

Croitoru and Robescu (2014) highlighted that the success or failure of an organization or team lies in the leader's beliefs in constraints and opportunities the company faces. Croitoru and Robescu (2014) explained that culture and management are intertwined as culture affects management the same way management affects culture affecting the “personality” of the organization. Thus, management needs to pay attention to detail, value everyone, and be innovative while recognizing the importance of economic growth. Leithy (2017) defined culture as a collection of beliefs, work styles, relationships, and values that are passed from manager to employee, and from employee

to employee in the form of work-life decisions. Leithy (2017) found that there is a positive linear relationship between work behavior and organizational performance as observed from the behavioral component of the three components of attitudes: the cognitive component, the effective component, and the behavioral component.

The Effects of Leadership on Organizational Performance

Alhadid (2016) considered leadership as the critical factor that influences the success of strategies for creating competitive advantages in a dynamic environment and examined the effect of leadership practices in both its transactional and transformational styles on organizational performance. Alhadid (2016) found that leadership practices positively influenced organizational performance as well as transactional and transformational styles. Fattah (2017) examined the effect of organizational culture, leader behavior, job satisfaction, and self-efficacy on the job performance of the employees and noted that organizational culture is an invisible force that could influence the actions, feelings, thoughts, and performance of people who work in an organization. Fattah (2017) found that organizational culture, the behavior of leaders, and self-efficacy positively affect job satisfaction and performance.

Erkutlu (2012) examined the relationship between organizational culture, proactive team behavior, and shared leadership and found that shared leadership within a work team positively influenced proactive team behavior with support for diverse cultures, which improves team effectiveness. Para-González, Jiménez-Jiménez, and Martínez-Lorente (2018) examined the relationship between organizational performance and transformational leadership and found that transformational leaders promote

employees' collective interest by helping them to reach mutual goals, enhance their performance through knowledge and learning; and be innovative with problem-solving tools through organizational culture and competitive strategies.

Transition and Summary

In this section, I introduced my research, including a brief background of the study, problem and purpose statements, research question, an introduction to the chosen conceptual framework, and a literature review of the framework and study topic. The purpose of this study was to explore strategies cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. Cybersecurity challenges are growing at an exponential rate, but there is insufficient cyber talent to protect organizations from data breaches and cyber threats. According to Schein's organizational culture model as a conceptual framework, organizational culture is a set of sharable values, beliefs, and understandings that are transmitted to new members as the correct way of thinking, feeling, and behaving. In this context, organizational culture binds members of an organization and allows leaders to align the culture of their organization with its vision and strategic objectives. I summarized the issues associated with workplace diversity and inclusion in organizations as being a strategic priority as opposed to a governmental or legal obligation. The conceptual framework provided the lens through which I conducted my research and evaluated data including the effects of organizational culture, leadership, diversity, and inclusion on performance. The framework also helped provide a

perspective on why some cybersecurity leaders lack strategies to attract, recruit, and retain diverse cybersecurity professionals.

In Section 2, I provide details and explanations of the planned execution of the study. In the section, I expand the chosen research methodology and design; the population and sampling method that I used to select participants; how I collected, organized, and analyzed the data; and the ethical, reliability, and validity considerations that I implemented. In Section 3, I present the results of the executed research and analyzed data, drawn conclusions, and report on the implications of the research findings to the target population and society.

Section 2: The Project

In this section, I restate the purpose of this study and discuss the research and the main reasons for pursuing a qualitative case study. In Section 2, I provide further details about my role as the researcher and the procedures for participant selection and access with a defined set of criteria as well as an explanation for the population. I provide detailed description and justification for the chosen method and design for the research as well as my rationale for using the method and design, descriptions of data collection tools or instrumentation, and the process of seeking consent for the research. I also present the technique to analyze the data that I gathered from responses to the research questions and information about the reliability and validity of the study.

Purpose Statement

The purpose of this qualitative exploratory multiple case study was to explore strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. The population for this study comprised cybersecurity leaders within three government agencies and nine IT organizations in small, medium, and large enterprises in the Atlanta, Georgia, metropolitan area in the United States with strategies to attract, recruit, and retain diverse cybersecurity professionals. The implications for positive social change resulting from my study might improve diversity in the workplace, work-life balance, morale, stress-levels, and opportunities for women who have experienced institutional and social barriers in the course of their cybersecurity careers as well as to

ensure better protection of protected health information and personally identifiable information.

Role of the Researcher

As the sole researcher in my study, I was the primary data collection instrument. The nature of qualitative research demands that the researcher is the primary data collection instrument (Yin, 1981). As such, I played the role of the data collector from all sources that informed the study, interviewer, data analyzer, and author of the final report. During data collection and analysis, I sought to mitigate any personal bias so that the data collection was not skewed or hampered in any way.

I am familiar with the topic of this research because I have served in various roles as a cybersecurity professional working in multiple teams and as a software engineer, solutions architect, and technical architect since 1997. I have lived in the target geographic area (metropolitan Atlanta, Georgia, area) for more than a decade and have worked at several major organizations in the area. Thus, my personal and professional experience with the study topic was my rationale for conducting this study. I do not have any personal or professional relationships with the participants. Ahrens and Khalifa (2013) noted that it is critical that the researcher is clear and concise about their location and familiarity with the field to show how the study may influence them.

I reviewed the *Belmont Report* provided by the U.S. Department of Health and Human Services. Ethical research, as stipulated by the *Belmont Report* and related protocols, requires a balance between justice, beneficence, and respect for human subjects while conducting research, which are partly obtained through the use of

informed consent (Bromley, Mikesell, Jones & Khodyakov, 2015; Faden et al., 2013; Lantos & Spertus, 2015; Ryan et al., 2014; U. S. Department of Health & Human Services, 2015). The principles of ethical research ensure that the researcher considers all of the following: (a) the balance between benefit and risk, (b) that the same participants taking the risk are the ones who realize the benefit, and (c) that potential participants are free to decide on whether to participate in the study (Faden et al., 2013; Lantos & Spertus, 2015; Ryan et al., 2014).

I achieved this balance by treating all human participants equally, fairly, without harm, with respect during, and after, conducting my study within the parameters of the *Belmont Report*, and by following the processes I described in the ethical research section. Having completed the National Institute of Health (NIH) Office of Extramural Research web-based training course on protecting human research participants (certificate located in Appendix C), I ensured that all participants were made aware that their names would not be divulged and identities would be anonymous. I ensured that all participants signed the informed consent form and were reminded not to disclose any information from the interviews to anyone in efforts toward maintaining participant confidentiality and protect their identities.

Bias is a significant part of ethical research as it could influence the outcome of the study (De Massis & Kotlar, 2014; Hyett et al., 2014; Yin, 1981). Bias is a deviation from the truth in data collection, analysis, interpretation, or publication, which may lead to false conclusions (Šimundić, 2013). In qualitative research, bias is mitigated through conducting interviews with more than one interviewee, following an interview protocol,

implementing member checking, and the use of multiple types of data sources (De Massis & Kotlar, 2014; Hyett et al., 2014; Yin, 1981). The acceptable data sources used to minimize bias include interviews, documentation, historical records, and direct observation (De Massis & Kotlar, 2014; Hyett et al., 2014; Yin, 1981). To mitigate bias in this study, with permission from the study participants, I collected data from multiple sources, including interview data and organizational documents such as recruitment and retention policy and procedure manuals. I used open-ended interview questions, which my committee reviewed to ensure the questions themselves were devoid of bias. I transcribed the interviews, conducted member checking, and provided details of the data collection procedures used in the data collection section to ensure that I did not injected any bias. Further, I ensured that my participants were selected without bias by strictly following the set of criteria outlined in the participant's section that defines who qualifies to participate in the study. Interview questions need to be considered with care to ensure that the sample is as closely matched to the population as possible (Šimundić, 2013). I used the OCT as the conceptual framework for this study. Conceptual frameworks help researchers navigate multiple relationships between the case study and theory (Rule & John, 2015). Another critical component of a study is how the researcher addresses and mitigates their worldview during data collection and analysis (Fusch & Ness, 2015). I took the necessary steps to ensure that bias was avoided and mitigated throughout my multiple case study.

I used an interview protocol presented in Appendix A to guide the open-ended in-depth-interviews with participating cybersecurity leaders. Case study research designs

require documenting and following protocols to establish and maintain rigor (Cronin, 2014). An interview protocol that assures trustworthiness and reliability as a research instrument could be used to guide an inquiry-based conversation (Castillo-Montoya, 2016). Interview protocols guide inquiry-based conversations with questions that are organized in the following order: beginning, transitional, key, and closing questions (Castillo-Montoya, 2016). The interview protocol enables the researcher to have a prepared list of questions to focus on the participant responses rather than memorizing and trying to remember the interview questions (Rivard, Fisher, Robertson, & Mueller, 2014). Furthermore, Rivard et al. (2014) recommended a five-step interview process that includes building rapport, allowing for long pauses, avoiding leading questions, asking follow-up questions to fill in gaps, and avoiding interrupting the interviewee. Fusch and Ness (2015) noted that qualitative researchers use an interview protocol to guarantee consistency and dependability of the research.

Participants

In qualitative research, researchers preferably select participants for their ability to provide comprehensive descriptions of the phenomenon under investigation (Draper, 2015; Petty, Thomson, & Stew, 2012; Wahyuni, 2012). The individuals for my multiple case study were at three government agencies and nine IT organizations in small, medium, and large enterprises within the Atlanta, Georgia, metropolitan area that have formal or informal strategies to attract, recruit, and retain cybersecurity professionals to effectively and efficiently protect sensitive information. Eligibility criteria are the guidelines for who can and cannot participate in a study. The criteria I used for

participation include the following: (a) cybersecurity leaders who have the authority to attract, recruit, and retain cybersecurity professionals within their organization or government agency; (b) cybersecurity leaders who have conducted or been involved in attraction, recruitment, and retention activities and campaigns within the same organizations or government agency or at any other organizations or government agency for a minimum of 5 years; (c) cybersecurity leaders who have prior or current knowledge and extensive experience in cybersecurity strategic planning/implementation, cyber threat mitigation, remediation, training, auditing, compliance, technical and nontechnical controls within the organizations or government agency; (d) cybersecurity leaders who work in the metropolitan area of Atlanta, Georgia; and (e) cybersecurity leaders I have never had a recurring working relationship. These selection criteria maximized the benefits of the research while minimizing risk to participants in the study. The exclusion criteria for participants in the study included withdrawing from the study.

Hoyland, Hollund, and Olsen (2015) noted that strategies for gaining access to participants might involve sending potential participants a brief introduction of the study, its potential benefits, confidentiality, and anticipated interview process. I gained access to potential research participants who met my eligibility criteria via LinkedIn. I obtained their contact information directly from LinkedIn. These participants were cybersecurity leaders with designations such as the chief information security officer (CISO), chief information officer (CIO), director of security operations, director of cybersecurity strategy, and cybersecurity governance risk compliance leader. Peticca-Harris, deGama, and Elias (2016) developed a nonlinear, dynamics four-part process for gaining access to

participants, including study design and planning, identifying participants, contacting participants, and interacting with participants during the data collection procedure. I explained the purpose of this study to the participants, and I vetted the participants using the eligibility criteria and demographics to determine their titles, roles, and amount of experience with cybersecurity attraction, recruitment, and retention practices. I sent the potential participants an email using the invitation to participate email template as presented in Appendix B to gain access to the participants. Before recruiting the potential participants in a study, researchers must gain institutional review board (IRB) approval to ensure proper protections are in place for human participants, including the use of an informed consent process for potential participants (Faden et al., 2013; Lantos & Spertus, 2015; Ryan et al., 2014). I obtained IRB approval (approval number 10-04-19-0671273) from Walden University's Center for Research Quality before recruiting the study participants.

In research based on a qualitative methodology, it is critical to establish trust and rapport with the study participants before interviewing them for effective and efficient data collection (Shah, 2014). As part of building trust and rapport, it is critical to develop an understanding that portrays the researcher as a member of the participant's community to establish a basis for empathy with the participant (Chou & Chiang, 2013; Shah, 2014). Goode et al. (2015) suggested being attentive to the participants' needs. I built trust and rapport with the study participants in various ways. First, I learned about the culture of the case organization. Ruetzler, Taylor, Reynolds, Baker, and Killen (2012) noted that a researcher's prior knowledge of the organization's culture could influence the decisions

and impressions during an interview. Second, I worked with each study participant to select a suitable and convenient date and time for the interviews to ensure I met their comfort and privacy requirements without imposing on their work schedules and responsibilities. As noted by Yin (2014), a comfortable environment enables participants to provide in-depth responses to research questions, which was unlikely in an environment with privacy and confidentiality concerns. Third, I informed the study participants that I am familiar with the topic, the concept of cybersecurity, and the terminologies, although I sought an explanation of any unfamiliar terms. Ahrens and Khalifa (2013) noted that it is critical that the researcher is clear and concise about their familiarity with the field to show how the study may influence them. Fourth, I ensured that participants were aware of my goal in the interviews, which was to explore their input, views, and opinions, not mine. Doody and Noonan (2013) pointed out that researchers can help participants prepare for interviews by going over the interview protocol to ensure the participants are aware of what to expect during the interview.

Research Method and Design

Throughout the literature, the terms *methodology* and *method* are used interchangeably when, in fact, the two have different meanings (Wahyuni, 2012). A *methodology* provides researchers the foundation for selecting a design that best aligns with their beliefs, whereas a method is a way of data analysis (Wahyuni, 2012). Interpretivism, positivism, pragmatism, and postpositivism are true paradigms with different views on the nature of reality (ontology), nature of knowledge and truth (epistemology), and the role of ethics and values (axiology) (Patton, 2015, pp. 105-106;

Wahyuni, 2012). Thus, a paradigm helps researchers to determine the appropriate approaches to systematic inquiry (methodology) to investigate and answer the research questions. For instance, a constructivist or interpretative paradigm typically assumes a qualitative methodology, whereas a positivistic paradigm typically uses a quantitative methodology (Wahyuni, 2012). Pragmatism assumes both quantitative and qualitative (i.e., mixed methodologies), whereas postpositivism could assume either (Wahyuni, 2012).

Method

I used the qualitative approach as a viable research method for conducting my study. The qualitative research methodology enables researchers to explore and understand phenomena under investigation without definitively identifying variables and elements for evaluation (De Massis & Kotlar, 2014; Yin, 2014). I used qualitative research to explore each participant's experiences and personal viewpoints to answer the primary research question. Grossoehme (2014) noted that researchers might use qualitative research to provide insight into each participants' experience. I chose qualitative research because it allowed the participants and I to have open discussions while sharing their personal experiences and perspectives on responses to open-ended questions regarding strategies to attract, recruit, and retain diverse cybersecurity professionals. Frels and Onwuegbuzie (2013) highlighted that qualitative research provides an opportunity for researchers to use interview questions to acquire in-depth responses to interview questions. Thus, if a participant's response requires further clarification or information, the researcher could ask probing questions. Imran and

Yusoff (2015) noted that researchers use qualitative research to explore new phenomena with less information available on such phenomena. By conducting a qualitative research study, I was able to gather data based on the knowledge and experiences of cybersecurity leaders with strategies to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. I used the exploratory nature of this study to justify the selection of a qualitative methodology. I used the conceptual framework (OCT) and the perceptions and thoughts of the cybersecurity leaders to interpret the data that I collected using the techniques and procedures described in the data collection section. The combination of the interpretive nature of the data analysis and the explorative nature of this research informed the use of a qualitative methodology.

I considered using a quantitative research method for this study but did not select it. The quantitative research methodology is about objective measurements, mathematical, statistical, or numerical data analysis, and examining differences or relationships among variables (De Massis & Kotlar, 2014; McCusker & Gunaydin, 2015). Thus, a quantitative researcher builds on the positivist epistemological stance that requires the use of theoretical framework to formulate and test hypotheses (Everett, Neu, Rahaman, & Maharaj, 2015). Numerical data would not provide insight into the participant's experiences about strategies to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive systems. Hence, I did not use numerical data to explain the phenomenon. Quantitative research is intended to generalize and predict data through deductive reasoning and fails to provide

insight into the participants' knowledge and experiences (Yilmaz, 2013). In this study, I provide insight into participants' knowledge and experiences about strategies that cybersecurity leaders use to attract, recruit, and retain diverse cyber talent to protect sensitive information. Barnham (2015) pointed out that quantitative researchers assume that their participants interpret the meanings of the survey questions they are asked the same way they analyze their data. My study adds to the body of knowledge regarding my topic rather than focusing on testing hypotheses with statistics or using measurements.

I considered mixed-method research, but I did not select it. Mixed-methods research combines qualitative and quantitative methods in the same study by including the collection, analysis, and interpretation of both narrative and numerical (Halcomb & Hickman, 2015). The mixed-method approach explores an issue from both an open-ended and closed-ended approach (Purohit & Singh, 2013). However, my study consisted of only the open approach, which did not include the use of surveys; rather, I used semistructured interviews. Mixed-method researchers design, build, and test theories as well as complete inductive and deductive analysis within the same study (Spillman, 2014). In my research, I focused solely on participants' experiences and not theory building, hypotheses testing, or studying relationships between variables. Charman, Petersen, Piper, Liedeman, and Legg (2015) noted that a mixed-methods approach might be used when neither a qualitative nor a quantitative approach is enough on its own to serve as the research method for the research topic. My research did not require quantification of data to answer the research question of this study, and neither mixed methods nor quantitative research applied to this study. In comparison to using a single

research method, mixed methods are time consuming, and the quantitative aspect was not required for my research. Hence, a mixed methods approach was not appropriate for this study.

Research Design

I used an exploratory multiple case study design for this qualitative research study. The case study, ethnography, phenomenology, and narrative are the standard designs in qualitative applied research (Palinkas, 2014). I used an exploratory multiple case study design to conduct a thorough inquiry into the strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to protect sensitive information. Researchers use the case study design when the focus of the research is on studying, understanding, and describing complex phenomena in detail in a real-world setting, asking what or how type questions (Cronin, 2014; Hyett et al., 2014; Yin, 2014). The fundamental tenet of a case study design is to explore a phenomenon in-depth in its natural setting and understand the context of one or more decisions, the implementation of those decisions, and the results of those decisions (Cronin, 2014). Thus, interviewing the participants about their experiences regarding attraction, recruitment, and retention strategies for diverse cybersecurity professionals allowed me to acquire a holistic understanding of the phenomenon under study. A case study's strength is that it can include multiple sites and various sources of data, including interviews, observations, artifacts, and documents in its analysis (Hyett et al., 2014; Wohlin & Aurum, 2015). My analysis of the organization's documents helped enhance my understanding of the strategies used by cybersecurity leaders to attract, recruit, and

retain diverse cybersecurity professionals to protect sensitive information. The case study is one of the most flexible study designs (Stake, 2013). A case study differs from other research designs because the focus of the research is on the case itself which is unique, and the units of analysis (Kruth, 2015). Wynn and Williams (2012) noted that case studies might focus on a specific phenomenon, individuals, groups, interactions, relationships, activities, or anything else the researcher deems necessary. Tsang (2014) surmised that the case study design supports the exploration of a phenomenon under investigation through multiple lenses without manipulating the relevant behaviors of the participants, thus enabling the discovery and understanding of multiple facets of the phenomenon under study. My research focus was on the exploration and understanding of a phenomenon with multiple cases and several sources of data.

I considered the phenomenology research design for my study. Phenomenological research originates from philosophy and psychology with the aim of exploring and understanding the lived experiences of individuals from their perspectives (Kruth, 2015; Sloan & Bowe, 2014). Grossoehme (2014) added that phenomenology research focuses on participant experiences and their meanings. Although participant experiences will be essential to inform my study, using a phenomenology research design would not allow me to collect company documents to gain more insight from an organization's perspective. Marshall and Rossman (2016) highlighted that the phenomenological research design does not allow for the gathering of information from publicly available documents. The significance of phenomenology is that the researcher studies self-awareness and human consciousness (Sloan & Bowe, 2014). My research was not about

how cybersecurity leaders experience strategies. Instead, I focused on just what strategies they use, making phenomenology inappropriate for this research.

I considered ethnographic research design for my study but did not select it. Ethnographic research focuses on studying the beliefs, behaviors, and languages of individuals in distinct cultures or cultural group (Draper, 2015). The focus of my research was not on investigating the cybersecurity leaders themselves, their beliefs, and behaviors. Instead, I explored strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive information. Ethnographic research enables data collection through the personal observation of members of a cultural group in their natural setting over a specified period (Schober, Gerrish, & McDonnell, 2016). I did not intend to directly observe how the participants interacted within their workspace nor did I intend to study members of a cultural group over a specified period. Ethnography originates from anthropology, and ethnographic research is time-consuming due to the in-depth study of the cultures (Baskerville & Myers, 2015), which leads to rich descriptive conclusions necessary for qualitative research (Lewis, 2015). Thus, making ethnography inappropriate for this research.

I considered a narrative research design for my study but did not select it. A narrative research design is used to explore the life experiences of an individual (Wolgemuth, 2014). I focused on collaborating with multiple individuals as opposed to studying a single individual which would not yield the appropriate data to answer my research questions. The narrative design involves gathering data about the participant's

experience with an event and how they view themselves (Berry, 2016), including recounted interviews, stories as recalled, diaries, and photos to form meaning (Grbich, 2015). Although gathering data about a participant's experience will inform this study, I did not focus on how humans experience the world; Rather, I focused on the strategies cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals. The greatest strength of the narrative approach is the use of the allegorical account (Lewis, 2015) as it fully captures all the useful information about the issues the researcher and participant discuss. Thus, chronologically giving account of the situation. Lewis (2015) described the narrative inquiry as unanalyzed stories and accounts using conversations, interviews, letters, and notes put together by a researcher. Focusing my research on collaboration between multiple participants will require my understanding of their perceptions and not their stories. The disadvantage of using a narrative inquiry is that it changes its explanations and frames of orientation (Lewis, 2015), which was counterproductive to the goals of this study. I did not use the narrative research design in this study as it was not appropriate since it explores the life of an individual and not a collaboration between multiple individuals.

Data saturation is crucial to the rigor of case study research. A researcher can achieve data saturation by spending adequate amount of time in the field collecting data until the researcher uncovers no more new data (Fusch & Ness, 2015) or where any new data does not continue to address the research question and other researchers are able to replicate the findings (Gentles et al., 2015; Kruth, 2014). I collected data until I no longer uncovered new information to inform my study. Malterud, Siersma, and Guassora (2015)

suggested that interviewing participants with significant knowledge and experience with the phenomenon under study enables a study to achieve data saturation. Therefore, I interviewed participants who have substantial knowledge and experience about strategies to attract, recruit, and retain diverse cybersecurity professionals to aid in achieving data saturation. Fusch and Ness (2015) further pointed out that face-to-face interviews facilitate a study reaching data saturation by asking multiple participants the same set of probing questions to ensure richness and depth of the data collected. Thus, I asked all participants the same probing questions to ensure the depth and richness of data I gathered to help reach data saturation.

Population and Sampling

This qualitative case study's population comprised cybersecurity leaders within three government agencies and nine IT organizations in small, medium, and large enterprises in the Atlanta, Georgia metropolitan area in the United States. The cybersecurity leaders included positions such as the chief information security officer (CISO), chief information officer (CIO), director of cybersecurity strategy, and cybersecurity governance risk compliance leader. The qualitative research population characteristics of interest are attributed to the participants' subjective experience with the phenomenon of interest (Stern, Jordan, & McArthur, 2014). The population for the study included cybersecurity leaders' experience with implementing and utilizing strategies to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats, which is the phenomenon under study. The study population included cybersecurity leaders who have knowledge or

perceptions of attraction, recruitment, and retention strategies for diverse cybersecurity leaders. The initial step towards the process of data collection is to define the population of the study with the use of the inclusion and exclusion criteria (Robinson, 2014). An eligibility criterion is critical to focus on a specific population for this study. It is essential to apply the participant selection criteria to the sampling process to ensure robust and accurate sampling that focuses on a specific study population to achieve data saturation (Elo et al., 2014). I applied the eligibility and exclusion criteria set above to the sample selection procedure as they provided the most valuable and detailed information on the phenomenon of interest while minimizing the possibility of the appearance of bias.

I used a purposive sampling approach for this study to collect data from the population that met the eligibility criteria. Purposive sampling is used to identify prospective participants from their population who could contribute to addressing the research question based on their expected abilities and qualifications (Barratt, Ferris, & Lenton, 2015; Petty et al., 2012; Walker, 2012). Using a purposive sampling technique for this study ensured that the selected participants in the study had specific experience and knowledge regarding the research topic and thus experts in the field of cybersecurity and the recruitment and retention of cybersecurity professionals. This type of purposive sampling technique where researchers draw their sample from experts in the field of study to capture knowledge rooted in a particular form of expertise is referred to as expert sampling (Barratt et al., 2015). Gentles et al. (2015) stressed that the main strength of expert sampling is that the selected participants are experienced and knowledgeable about a subject area and, therefore, are willing to share their knowledge. The participants

chosen for my study were in their current role for at least five years, willing to provide articulate and expressive information necessary to answer the research questions based on their proficiency level, experience, and knowledge about the strategies to attract, recruit, and retain diverse cybersecurity professionals.

Purposive sampling is a cost-effective and time-effective technique that is appropriate for research with only limited and small populations available, which can contribute to the study (Barratt et al. 2015). Further, purposive sampling generates a small sample size (Barratt et al. 2015). However, Robinson (2014), highlighted that the researcher should conduct as much data collection as necessary to reach the theoretical point of data saturation. O'Reilly and Parker (2013), further added that in qualitative research, sampling should focus more on the adequacy of the data collected as opposed to the amount of data collected. A purposive sample is a non-probability sample that is selected based on the objective of the study and the characteristics of a population (Barratt et al., 2015). Hence, my focus was on gathering detailed and thorough data to answer my research question and inform my study based on the characteristics of the population. Simou and Koutsogeorgou (2014) indicated that the inclusion criteria should capture all participants of interest in the study population. However, given the limited number of samples that may be gathered in the study, it is critical to use only experts in the field to provide a complete and detailed understanding of the phenomenon under investigation (Barratt et al., 2014).

Although purposive sampling is cost-effective and time-effective, it could be vulnerable to errors in judgment by the researcher, susceptible to bias, and the findings of

the research may not be generalizable (Barratt et al., 2015). Therefore, to help minimize these shortcomings, for each of my cases, I selected highly knowledgeable and experienced participants from my identified population and continued recruiting participants until I achieved the point of data saturation. Ebersole et al. (2016) stated that researchers could minimize bias in the study by the nonrandom selection of participants. Etikan, Musa, and Alkassim (2016) added that this shortfall of purposive sampling could be mitigated by strictly including those participants that will provide useful responses to inform the research. Therefore, by including only the participants with expert knowledge and experience in attracting, recruiting, and retaining cybersecurity talent, I was able to gather enough in-depth and thorough responses to my research question to increase the reliability of my study, reduce errors in judgement, eliminate the perception of bias, and subsequently achieve data saturation quickly. Convenience sampling was considered but not chosen. Etikan et al. (2016) highlighted that convenience sampling is appropriate where members of the target population are only selected because they meet certain eligibility criteria such as willingness to participate, easy accessibility, availability at a given time, and geographical proximity, in spite of the fact that more suitable participants may otherwise fit the purpose. Costanza et al. (2015) added that using convenience sampling, a researcher draws participants that may be familiar with, or maybe local, or may be willing to work with their schedule. Malterud, Siersma, & Guassora (2016) pointed out that convenience samples are, therefore, less representative of the study population than other sampling methods and may lead to an increase in the number of in-depth interviews necessary for a researcher to achieve the point of theoretical data

saturation. Homogeneous sampling was also considered but not chosen. Etikan et al. (2016) stated that homogeneous sampling focuses on potential participants who share specific characteristics or similar traits such as cultures, jobs, and age or life experiences, ages, jobs, or cultures. Homogeneous sampling was not appropriate for my research as the study did not need cybersecurity leaders age or life experiences to be the same, even though the participants would need to have worked in cybersecurity field for at least five years and have experience, knowledge, and authority to recruit and retain cybersecurity professionals. The objective of homogeneous sampling is to focus on the precise characteristics or similarities and their relationship with the phenomenon understudy (Etikan et al., 2016).

The sample size for this study consisted of all participants who met the inclusive eligibility criteria. Robinson (2014) noted that practical and theoretical considerations influence the size of a sample used for a qualitative study. Therefore, Malterud et al. (2016) argued that the sample size needed to achieve data saturation depends on how well the sample for the study represents the population, the quality of the interviews, the structure of the interviews, and the study participants' experience and knowledge of the phenomenon under investigation. Patton (2015, p. 311) explained that researchers select sample sizes based on specific factors concerning the research including the goals, credibility, usefulness, resources, and time. The purpose of selecting a suitable sample is to gather as much information as possible with the least number of study participants (Malterud et al., 2016). Further, interviewing research participants who have direct experience and knowledge of the phenomenon under study might lower the sample size

necessary to achieve data saturation (Malterud et al. 2016). However, Marshall et al. (2013) noted that a suitable sample size for a study is closely related to the study reaching the point of data saturation. Guest, Bunce, and Johnson (2006) conducted a study on the number of interviews required to achieve data saturation. The study concluded that researchers could potentially achieve data saturation with six to twelve in-depth interviews as the data collection method (Guest et al., 2006). Palinkas et al. (2015) emphasized that with purposive sampling researchers can achieve data saturation by continuing to sample until no new information is uncovered. Therefore, I initially aimed at recruiting ten cybersecurity leaders in the study that met the eligibility criteria and continue until saturation was achieved. However, I reached saturation by collecting interview data, and organizational documents from twelve cybersecurity leaders I recruited based on their extensive background, knowledge, and experience of attracting, recruiting, and retaining cybersecurity professionals to protect sensitive systems from cyberattacks.

I used the data I collected from multiple sources to facilitate triangulation and achieve data saturation. Researchers reach saturation through continuous data sampling until no new information is uncovered from other sources of information (Fusch & Ness, 2015). Carman et al. (2015) explained that in qualitative research the concept of data saturation involves interviewing participants until no new data are uncovered in the data collected, thus achieving saturation. Methodological triangulation in qualitative research refers to the collection of data from more than one source to understand the phenomenon (Denzin, 1978) and to achieve saturation (Houghton et al., 2013; Yilmaz, 2013).

Therefore, I used multiple sources of data, including semi-structured interviews of participants and organizational documents, policies, and artifacts focused on strategies to attract, recruit, and retain cyber talent to protect information systems to achieve saturation.

Member checking and triangulation were used to verify the reliability and accuracy which ensured the credibility of my study. Failure to reach saturation has an impact on the quality of the research conducted (Fusch & Ness, 2015), and saturation guarantees qualitative rigor (Morse, 2015). Saturation could be reached with member checking, giving the study participants the opportunity to crosscheck the researcher's interpretations of the data and make any necessary amendments or provide additional information until no new data emerges to increase the consistency and credibility of the study (De Massis & Kotlar, 2014; Denzin, 1978) as well as to establish validity (Morse, 2015). James (2017) added that member checking and data triangulation are used to ensure the authenticity of the data. I implemented member checking through followup interview sessions with the study participants to achieve overall saturation and ensure that my interpretation of the data closely reflected the information provided by the participants to inform the research question. Saturation has become broadly accepted as an indicator of sufficient data collection (Gentles et al., 2015). Therefore, I strived to collect adequate data until I reach the point where further data collection became 'counterproductive', and where the 'new information gathered' did not necessarily add anything to the overall study to achieve data saturation for this study.

The location of an interview could have a significant influence on the performance of an interview (Dempsey, Dowling, Larkin, & Murphy, 2016; Gagnon, Jacob, & McCabe, 2015; Rimando et al., 2015). Thus, the location of the interview should be convenient, and the environment should be comfortable to provide a sense of privacy/safety for open conversations with the study participant (Dempsey et al., 2016; Gagnon et al., 2015; Rimando et al., 2015). Seitz (2016) suggested a quiet room without distractions to ensure participants remain focused. I coordinated with the participants of the study to identify suitable meeting times and dates of their choice without imposing on their work schedules and responsibilities.

Ethical Research

The three basic ethical principles and guidelines for the protection of human subjects of research in line with the Belmont Report include respect for persons, beneficence, and justice (Ryan et al., 2014). Beneficence addresses the balance between the risks and benefits of the research (Faden et al., 2013; Ryan et al., 2014) and justice ensures that the risk experienced by one group does not become the benefit of another group (Faden et al., 2013; Ryan et al., 2014). The risk encountered in everyday life is comparable to the risk associated with participation in this research. The participants in this research were the individuals that benefited from this study. Thus, addressing the basic principles of justice and beneficence. Respect for persons is addressed through the informed consent process by allowing the individuals to control the bounds of their participation in the research (Lantos & Spertus, 2015; Ryan et al., 2014; Yilmaz, 2013). Respecting the rights of the participants addresses the principles of respect for persons.

The accomplishment of empirical research requires adherence to several ethical considerations including informed consent, which is the ability of a study participant to withdraw from the research, confidentiality of the provided information, and the protection of participants from privacy violations (Dekking, Van der Graaf & Van Delden, 2014). The IRB validates every research to ensure it meets or exceeds ethical standards before the execution of the planned study (Faden et al., 2013; Lantos & Spertus, 2015; Ryan et al., 2014). Therefore, before communicating with the study participants, I obtained IRB approval from Walden University. Obtaining informed consent from the study participants is imperative to conduct ethical research (Ruiz-Palomino & Martínez-Cañas, 2014). Therefore, upon receipt of the IRB approval (approval number 10-04-19-0671273), I sent a consent form that required the identified participants to reply with the words “I consent’ to the participant's email address using an invitation template presented in Appendix B while making myself available to answer any questions the participants may have. This informed consent form included details of the criteria for participation, consent to participate, consent to withdraw at any time during the interview process, any monetary incentives for participation, data retention, data protection policies, and protection of personally identifiable information (PII) by withholding details regarding the participant's demographics. The participants should not provide any personal information such as name, address or other pertinent information, which may act as personal identifiers (Saunders, Kitzinger & Kitzinger, 2015). In my final report, to enhance anonymity, I used aliases to obfuscate the identity of the individuals and organizations mentioned in the interview.

To ensure alignment with ethical principles for protecting human subjects of research, participants should have the opportunity to withdraw from participation for any reason and at any time during the study without any consequence or penalty (Elo et al., 2014). I ensured that the participants know that they have this right to withdraw from participation at will through a formal request to me or let Walden University's research participant advocate know of their intentions to withdraw. The study participants had access to my contact cell phone number or email address to notify me of their intentions to proceed or not. The consent form included a statement indicating that the informants participated voluntarily without coercion and no incentives, reimbursement, or compensation whatsoever was available to the individuals for their participation, but I relied on their goodwill to participate in the interviews. I required the participants to show their consent by replying to the email invitation with the words 'I Consent,' indicating that they have read and understood the requirements and objectives of the research.

I stored all the data obtained for this research either in print form or digital form in Dropbox. The hard copy documents will be stored in a securely locked fireproof safe for five years from the final research approval date, after which the data will be deleted from Dropbox and any paper documents securely shredded. The permanent destruction of the data will protect the privacy of the study participants and ensure compliance with the ethical standards for research. Khan (2014) highlighted the significance of maintaining the confidentiality of the information provided by the study participants. Thus, the stored data will only be accessible to me.

Data Collection

Elo et al. (2014) defined data collection, which goes hand in hand with data analysis as the systematic process of gathering data on the meaning, concepts, and definitions of phenomena for a study. The information obtained in this data collection process answered my research questions and helped evaluate the outcomes of the study. Collins & Cooper (2014) noted that researchers focus on data collection, data organization, and data analysis in qualitative studies. I discussed how the data was collected and applied in detail in the following three subsections, which comprise the instruments, data collection techniques, and the technique used to organize the data.

Instruments

Qualitative research methods and designs, including the case study design regard the researcher as the primary data collection instrument and rely on the use of well-structured and well-defined interview protocols to guide the data collection (Bourke, 2014; De Massis & Kotlar, 2014). During the study, reflexive journals help provide a rationale for the thoughts, decisions, and challenges the researcher experiences (Sloan & Bowe, 2014); thus, increasing the authenticity of data collection (Shannon & Hambacher, 2014). I used a reflexive journal to track coding decisions. In addition to collecting data from the participants through semistructured interviews, De Massis and Kotlar (2014) noted that it is valuable for researchers to capture contextual information about the interview by documenting their observations. As pointed out in the Role of the Researcher section, I was the primary data collection instrument.

Yin (2014) suggested the collection of data from a minimum of two to six sources, including interviews, documents, direct observation, participant observation, physical artifacts, and archival records. Thomas (2015) noted that the primary data source in qualitative case studies includes original data collected from interviews. I used semi-structured interviews with open-ended questions as presented in the interview protocol in Appendix A and the Research Question section of the study to collect data from the research participants. Yin (2014) suggested that researchers use documents as a secondary data collection method to verify findings from the primary data source. In the course of the interview, I asked the study participants to make available for analysis any publicly available organizational documents, policies, historical documents, or multimedia sources that support the idea of increasing diversity in the cybersecurity workforce to protect sensitive information. Throughout my research, I kept a reflexive journal that provided the general rationale for the perceptions, thoughts, decisions, and challenges of the study.

Researchers use member checking, triangulation, and transcript review to enhance and maximize the reliability and validity of the study (De Massis & Kotlar, 2014). Member checking is a means of complementing saturation by relaying the researcher's interpretations to the study participants to check for accuracy and provide corrections or additional information to increase the overall credibility of the research (De Massis & Kotlar, 2014; Perrotta, 2015). Researchers use member checking to ensure the credibility and trustworthiness of the study findings (Bell, 2015). Thus, to further maximize the reliability and validity of my study, I used member checking (interviews and follow-up

questions when necessary during the interviews to get clarification on interviewees' responses) to review and verify the accuracy of my interpretations of the data until participant responses uncovered no new data. Triangulation is the use of several data sources to study a phenomenon (Hyett et al., 2014). I used data triangulation (semistructured interviews with organizational policies and documents) and methodological triangulation (through semistructured interviews with open-ended questions, and analysis of organizational documents and procedures related to cybersecurity talent recruitment and retention strategies) to verify my findings from the primary data collection methods. Hussein (2015) noted that methodological triangulation involves the use of at least two data collection methods to explore and analyze the phenomenon under study. Dikko (2016) noted that data collection instruments in every research design must pass the tests of reliability and validity to be considered a good measure. Therefore, I performed mock interviews on a small number of participants that have the same characteristics as those in the main study using the interview protocol presented in Appendix A to identify and rectify any flaws or issues upfront.

Data Collection Technique

After I obtained approval from Walden University's Institutional Review Board and the consent of the participants, I used a semistructured approach to interview the participants in over the phone. McIntosh and Morse (2015) emphasized that the aim of semistructured interviews is to gather the perspectives of participants' regarding their knowledge and experience about the phenomenon under study. An advantage of semistructured interviews is that all these participants are asked the same questions in the

same order using the interview protocol, thus making the data collected or participants' responses flexible and easier to compare and analyze (McIntosh & Morse, 2015). Another advantage of using semistructured interviews is that the study participants are free to respond to the posed open-ended questions at will, and the researcher can probe their responses to gain more insight into their answers to the research questions. The flexibility of the participants' responses and the degree of relevancy semistructured interviews provide to the phenomenon of interest while remaining responsive to the participant makes semistructured interviews unique among all other interview methods. Further, the use of the telephone to communicate with the study participants provides the advantage of enhanced accessibility, time and labor efficiency, and private auditory communication, which will be beneficial to participants who are unavailable for a face-to-face interview. McIntosh and Morse (2015) noted that even though semistructured interviews are widely used in qualitative research, one disadvantage is that not enough attention is paid to their applications, its construction, and assumptions made by the researcher. Further, poor telephone network or coverage, lack of access to a suitable phone, and long-distance charges could hamper the efforts of a semistructured interview (McIntosh and Morse, 2015). However, this disadvantage could be remediated with collect calls that are permitted during the period of data collection.

I gained access to potential research participants and obtained their contact details through their publicly available profiles on LinkedIn. These participants were cybersecurity leaders with designations such as the chief information security officer (CISO), chief information officer (CIO), director of security operations, director of

cybersecurity strategy, and cybersecurity governance risk compliance leader. Peticca-Harris, deGama, and Elias (2016) developed a nonlinear, dynamics four-part process for gaining access to participants, including: study design and planning, identifying participants, contacting participants, and interacting with participants during the data collection procedure. I explained the purpose of the study to the participants, and I vetted the participants using the eligibility criteria and demographics to determine their title, role, and amount of experience with cybersecurity attraction, recruitment, and retention practices. I sent the potential participants an email using the invitation to participate email template as presented in Appendix B to gain access to the participants. Before recruiting the potential participants in a study, researchers must gain Institutional Review Board (IRB) approval to ensure proper protections are in place for human Participants', including the use of an informed consent process for potential participants (Faden et al., 2013; Lantos & Spertus, 2015; Ryan et al., 2014). I obtained IRB approval from Walden University's Center for Research Quality before recruiting the study participants.

For participants that replied to the email invitation with the words 'I Consent,' I proceeded to schedule suitable times and dates with them for telephone semistructured interviews and collection of organizational documents that define their attraction, recruitment, and retention strategies. On the agreed-upon date and time, I conducted telephone interviews of the participants and followed the interview protocol presented in Appendix A to gather data from the study participants. O'Malley, Gourevitch, Draper, Bond, and Tirodkar (2015) emphasized that the interview protocol is a series of instructions that explain the procedures and methods for conducting the interview. The

interview protocol served as a guide during the interview and included an introduction to describe the study, instructions on what to expect, followed by demographic and open-ended questions with probes for clarity and justifications as reminders. Taylor et al. (2016) suggested that the use of open-ended questions encourage more in-depth discussion on the research topic, and probing questions promotes more detailed interpretation and clarity of the participants' responses. Morse (2015) noted that audio recorded interviews allow the researchers to listen to an interview multiple times to increase their understanding and enable subsequent interpretation of the interview responses based on their understanding. I obtained permission from each interview participant to record the sessions using a conference call recording feature for subsequent transcription into a text document, review, and analysis. I interpreted the transcriptions based on my understanding of the interview responses and the literature. After concluding the first interview portion of the meeting, I asked the interviewees if they had any organizational documents or multimedia presentations or other information that they would like to provide regarding the topic discussed during the interview. I gathered those documents for evaluation and preserved them following the data retention policy described in the informed consent form.

Member checking gives the study participants the opportunity to review the researcher's relayed interpretations of their responses to check for accuracy and provide comments, corrections, or additional information where necessary (De Massis & Kotlar, 2014; Perrotta, 2015). After the interviews and collection of any organizational documents, I thanked the participants for contributing to the study and then explained the

concept of member checking. I scheduled follow- up emails or sessions with each participant for member checking to ensure the accuracy of the data collected, data saturation, and the correct interpretation of the data. I provided the participants with copies of the interview transcription and report of my interpretation of the responses from the original open-ended questions to the follow-up interview for review with the study participant. I gave each participant the express opportunity to confirm, elaborate, or correct the information they provided. Caretta (2016) suggested that researchers continue the member checking process until the participants confirm all interpretations, provide no more new information, and additional clarifications no longer needed. Therefore, where necessary, I scheduled other member checking sessions with the participant to review my interpretations of the original and follow-up open-ended interviews. I repeated the member checking process until all participants confirmed all my interpretations and provided no new information. I recorded the audio of the follow-up sessions, updated the transcriptions with any new data uncovered, and kept a copy of the research data, also following the data retention policy described in the informed consent form.

Data Organization Techniques

Aleti et al. (2013), De Massis & Kotlar (2014), Elo et al. (2014), and Petty et al. (2012) suggested using a research database to improve the reliability and trustworthiness of the research by providing a chain of evidence, logging when and where data is collected (Cronin, 2014). I cataloged all data collected as part of the case study in NVivo 12, in a computer-aided qualitative data analysis software tool (CAQDAS). Edward-Jones (2014) noted that computer-aided software tools such as NVivo enables researchers

to visually analyze and code the data into themes while using reports, clusters, graphs, models, and maps to provide a visual representation of the data. Although NVivo software is a versatile, easy to use, and understand program, the software cannot automatically perform all the necessary work concerning data organization and coding (Castleberry, 2014). A researcher facilitates the labeling, sorting, and comparison of the data collected by selects concepts, codes, and categories (Vaismoradi, Jones, Turunen, & Snelgrove, 2016). Categorization involves analyzing the data for similarities and grouping the data that are alike (Plamondon, Bottorff, & Cole, 2015). NVivo enables the sorting, characterization, and composition of information in an easy to use format for data analysis until the researcher uncovers the answers to the research questions (Castleberry, 2014). Further, with NVivo, the researcher can collect, file, and break down several sources of data including Microsoft Word documents (.doc and .docx), Excel spreadsheets, rich text (.rtf), portable document format (.pdf), plain text (.txt), Access database, most forms of photos, video and audio files (Castleberry, 2014). I used Microsoft Excel to categorize all interview transcripts, member checking transcripts, organizational documents, and multimedia presentations collected from the participants of the study.

Fabian, Ermakova, and Junghanns (2015) stressed the importance of protecting the data collected to respect the participants' privacy and maintain data confidentiality. Therefore, I have locked the physical artifacts for five years in lockable file storage for review, easy retrieval by only myself, and subsequent permanent destruction. Every hard copy will be shredded, and electronic sources deleted after five years. All data sources,

including the physical artifacts, bear the date and participant ID to identify who provided the source and establish a chain of evidence. The forms of data stored in the NVivo database include the raw interview data in an audio format and transcriptions in an accessible and readable format, the digitized form of all collected organizational documents, and reflexive journals.

Data Analysis Technique

Inductive and deductive are two primary modalities used in research. Qualitative studies use inductive approaches (De Massis & Kotalar, 2014; Kruth, 2015), which rely on the collected data to provide themes while deductive approaches compare categories among studies (Kruth, 2015). Harrison and Kirkham (2014) described how the inductive approach could be used to gain a more in-depth understanding of individual interactions through the collection of qualitative data using fewer samples as opposed to larger research participants. Yilmaz (2013) also noted that qualitative researchers might follow inductive reasoning to gain a better understanding of the data or to interpret the data. Triangulation is the use of several data sources to study a phenomenon to add credibility to case study research and inductive approaches (Cronin, 2014; De Massis & Kotlar, 2014; Hyett et al., 2014).

In qualitative research, data, methodology, theory, and investigator are four primary types of triangulation (Fusch & Ness, 2015; Wilson, 2014). Gathering multiple sources of data at a time from more than one study participant enables a researcher to achieve data triangulation (Wilson, 2014). Methodological triangulation is the use of multiple methods to analyze and correlate data collected from numerous sources (Fusch

& Ness, 2015; Hussein, 2015). The methods used in methodological triangulation include removing organizational or personal identifiers from the data, transcribing audio sources and verifying the transcriptions, and data storage methods (Wahyuni, 2012). Theory triangulation is applicable when multiple theoretical strategies are used, and investigator triangulation applies when more than one researcher participates in the study (Fusch & Ness, 2015; Wilson, 2014). As I was the only investigator in my research, the investigator triangulation did not apply to my study. I used one conceptual framework (OCT) in my study; thus, theory triangulation did not apply to my research as well. I used both data and methodological triangulation. Using methodological triangulation, I reviewed and analyzed the semi-structured interview transcripts with follow-up member checking transcripts, organizational documents, and multimedia presentations related to best practices, standards, and policies for attraction, recruitment, and retention of cybersecurity professionals. I achieved data triangulation by conducting interviews and collecting organizational documents, and for methodological triangulation, I organized all gathered data as previously described in the data organization section.

The two conventional approaches for inductive analysis of qualitative data are thematic and content analysis (Petty et al., 2012; Vaismoradi et al., 2013; Wahyuni, 2012). Thematic analysis is the inductive process of identifying codes, analyzing, grouping, and reporting themes or patterns found within the collected qualitative data that describe the phenomenon (Cruzes, Dyba, Runeson, & Host, 2014; Petty et al., 2012; Vaismoradi et al., 2013; Wahyuni, 2012). Donaldson, Panesar, and Darzi (2014) noted that the thematic analysis examines patterns as themes within the collected non-numeric

qualitative data. Content analysis is the identification of categories of information within the data and the use of the categories to quantify the phenomenon (McCusker & Gunaydin, 2015; Vaismoradi et al., 2013; Wahyuni, 2012). Although content analysis and thematic analysis are used interchangeably, the boundaries between the two lies in the ability to quantify data such that measuring the frequency of different themes and categories is possible in content analysis (Vaismoradi et al., 2013). I did not use content analysis for this research. The use of a six-step thematic analysis allows a researcher to better comprehend the most impactful coding (Halverson, Graham, Spring, Drysdale, & Henrie, 2014). In this study, I employed the six-step thematic analysis technique to generate my data, code the data, analyze the data, search for the major themes within the data, define the major themes following a naming convention, and then present the findings. I did not insert my own opinions into data analysis and only used the member-checked versions of the transcribed data rather than the pre-member-checked versions of the collected data.

I used a third-party transcription software, Happy Scribe (happyscribe.co), to transcribe the audio recordings of the interviews and member-checking sessions in an audio format and validate the transcriptions using transcription software (InqScribe). I performed the transcriptions myself using the transcription software to ensure the confidentiality and privacy of participant information. I loaded all transcribed data, documents, and reflective journals into NVivo for coding and thematic analysis. Before starting the coding process, I read through the collected data several times for familiarity. I based the coding on phrases and words related to attraction, recruitment, and retention

of diverse cybersecurity professionals to protect sensitive information (e.g., diversity, retention, recruitment, protection, sensitive, professionals, etc.) and recorded the phrases and words that I grouped into codes for future verification and reference. After defining the codes, I analyzed and evaluated the codes and identified the themes. I continuously monitored the literature, member checking results, and follow-up interviews for any new information on the topic of strategies used by cybersecurity leaders to attract, recruit and retain diverse cybersecurity professionals to protect sensitive information from rising cyber threats. Whether new information was uncovered or not, I requested further member checking sessions to validate whether the identified themes accurately reflected the interpretation of the transcribed data.

Reliability and Validity

Qualitative research should be robust, dependable, credible, and trustworthy (Yilmaz, 2013). The trustworthiness of research is assessed by the dependability, credibility, confirmability, and transferability criteria, which are analogous to the quantitative principles of reliability, internal validity, objectivity, and external validity respectively (Houghton et al., 2013; Petty et al., 2012; Wahyuni, 2012). If other researchers can produce similar results for the study of the phenomenon using the same techniques and methods, qualitative research is said to be reliable (Leung, 2015). However, it can be challenging to replicate a qualitative study due to the subjective nature of the participants and researchers. Researchers' should instead focus on the consistency and dependability of the data rather than attempting to reproduce the results (Leung, 2015). The reliability of research data is necessary for the validity of the research

data (Stevens, Lyles, & Berke, 2014). The findings and results must be dependable and consistent to ensure reliability by providing detailed descriptions of the phenomena, all methods, techniques, and procedures used for the study to enable other researchers to hypothetically achieve similar outcomes (Stevens et al., 2014).

The validity of a qualitative research is a measure of how well the intentions or purpose of the research is studied (Kruth, 2015), and it requires that the study participants and researcher understand the phenomena and view the study findings as authentic, trustworthy, and credible (Merriam & Tisdell, 2015; Yilmaz, 2013). The credibility and trustworthiness of the study are established by the validity of the process of data collection, data analysis, and data interpretation (Elo et al., 2014). For most research designs, external validity, construct validity, reliability, and internal validity are classes of validity, although internal validity applies to quantitative research and not exploratory studies (Holweg & Helo, 2014; Leung, 2015; Martini et al., 2015). The credibility of the study measures the rigor of qualitative research, dependability of the findings, the confirmability of the data and analysis, and the transferability of their research (Houghton et al., 2013; Petty et al., 2012; Wahyuni, 2012; Yilmaz, 2013).

Credibility

Credibility indicates the acceptability or genuineness of the results of the collected research data from the participants' perspectives (Cope, 2014, Darawsheh, 2014; Leung, 2015). Researchers establish and enhance credibility through gathering rich descriptions, member checking, data triangulation, prolonged engagement to reach data saturation, participant transcript review, interview protocol, and direct observations

(Houghton et al., 2013; Marshall & Rossman, 2016; Petty et al., 2012). Member checking is the most crucial technique of all for establishing credibility by allowing the participants to verify the credibility and accuracy of the researchers' interpretation of their experiences (Houghton et al., 2013; Lincoln & Guba, 1985; Onwuegbuzie & Byers, 2014). A qualitative study is credible if the study participants find the result to be truthful, valid, and legitimate (Amankwaa, 2016; Vanclay, Baines, & Taylor, 2013; Yilmaz, 2013). Therefore, I relied on member checking and data triangulation through the collection of interview data and organizational documents to enhance the credibility of the study findings. Further, I employed methodological triangulation with multiple steps for data organization and analysis, and participant observations to boost the credibility of the findings of the research. Methodological triangulation is used to develop an in-depth understanding of the research phenomenon to provide rich data that contributes to affects accuracy, validity, and reliability (Denzin, 1978; Fusch & Ness, 2015; Hussein, 2015). Complementary data collection and analysis methods are used to increase the accuracy and credibility of a study using the within-method methodological triangulation (Hussein, 2015). I requested that the participants keep all aspects of their participation confidential until the conclusion of the research to further maintain the credibility of the study.

Data saturation is reached when a researcher collects data in the field until no new information is uncovered (Houghton et al., 2013) or until no new themes that continue to inform the research question emerge (Fusch & Ness, 2015; Gentles et al., 2015; Kruth, 2015). One means of achieving data saturation is data triangulation, which enhances the

reliability and validity of a study (Fusch & Ness, 2015; Lincoln & Guba, 1985; Petty et al., 2012). I reached data saturation by tracking emerging themes and data gathered from semi-structured interviews and organizational documents until no new themes or data emerged. I then followed-up with member checking to ensure accurate and complete interpretation of the data to reflect the participant's viewpoints and meanings. Lastly, I used methodological triangulation to analyze the data.

Dependability

In qualitative research, dependability emphasizes the need to account for the changing context within which the study takes place (Amankwaa, 2016; Darawsheh, 2014; Leung, 2015). Methods suggested in previous studies to improve the dependability of research include member checking, expert validation of the interview questions, transcript review, interview protocol, focus group protocol, and direct observations (Carter et al., 2014; Marshall & Rossman, 2016; Zohrabi, 2013). I relied on member checking to improve the dependability of the findings by allowing the participants to review my interpretations and revise or comment on any discrepancies between my descriptions of the data and their meanings. Cho & Lee (2014), Houghton et al. (2013), and Yilmaz (2013) suggested that the use of reflexive journals, chains of evidence, or audit trails are other methods of achieving dependability. I used a reflexive journal, chains of evidence, or audit trails to track coding decisions of the data stored in the NVivo database using the Participant ID as a unique identifier.

Confirmability

The confirmability, or construct validity of a study involves the ability of other researchers to review designs, methods, and reasoning of one study to see if it substantiates or corroborates the findings from other studies or to ensure the research makes sense with the logical interpretations using the methods and techniques the researcher describes (Hanson et al., 2011; Lincoln & Guba 1985; Yilmaz, 2013). In qualitative research, confirmability ensures that a study is free from bias, and therefore, trustworthy through the use of multiple interview participants to minimize the possibility of researcher bias and to maintain the neutrality of the collected data (Amankwaa, 2016; Houghton et al., 2013) and the objectivity of the researcher (Petty et al., 2012). Confirmability checks for researcher bias by the researcher performing member checking throughout the research process to receive participant feedback. This feedback ensures that the interpretation of the meanings are correct based on the ability of other researchers to corroborate that the study was conducted using the techniques and methods described by the researcher (Harding & Fox, 2015; Lincoln & Guba 1985; Schmidlein et al., 2014). Member checking involves (a) taking notes or keeping reflexive journals during or after the interview. (b) checking and rechecking the data collected throughout the study. (c) probing the respondents from different perspectives. (d) triangulation. (e) prolonged engagement with the interviews (Anney, 2014; Cope, 2014; Tong & Dew, 2016).

I relied on member checking, verifying the interviews with organizational documents, methodological triangulation, prolonged engagement, and probing the interviewees from different perspectives to ensure confirmability of the data and to

increase the trustworthiness of the results of the study. Cuthbert (2014), Gutmann (2014), and Zitomer and Goodwin (2014) suggested an audit trail was essential for confirmability because it provides a clear and concise map of a researcher's decision process. Gutmann (2014) further noted that an audit trail gives other researchers the opportunity to evaluate the methods, designs, plans, data collection processes, data records, results of the research, and conclusions, to apply them to their study to attain reliable results. I provided an audit trail and chains of evidence with recorded reflexive journals to show how I arrived at my conclusions and essentially used all the techniques above to acquire detailed descriptions of data that can be corroborated or substantiated by other studies.

Transferability

Transferability, or external validity, in qualitative research, refers to the extent to which researchers can generalize the study findings or use them in other settings or contexts (Aravamudhan & Krishnaveni, 2015; Marshall & Rossman, 2016; Yin, 2015). Transferability of the outcomes of the study to various settings or contexts requires the researcher to provide enough information and a clear understanding of the study for other researchers to transfer findings (Amankwaa, 2016; Barnes, 2015; Elo et al., 2014). Transferability could be enhanced or increased by thoroughly presenting the research findings and using the rich, detailed description of the background of the study, participants eligibility, data collection methods, data sources, the method of sampling, population size, and study findings (Connelly, 2016; Houghton et al., 2013; Yilmaz, 2013). The transferability of research is ascertained when another researcher decides to transfer the study findings (Hanson et al., 2011; Lincoln & Guba, 1985; Marshall &

Rossman, 2016). In this study, I enhanced transferability using in-depth descriptions of the research, data collection methods and techniques, accurately collected data, underlying assumptions considered in the research process, and the findings of the study.

Transition and Summary

In Section 2, I provided details of my study, indicating that the purpose was to explore the strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to protect sensitive information. I performed all data collection, acting as the primary data collection instrument. I followed all guidelines regarding the ethical responsibilities and treatment of participants as required by the IRB and as outlined in the *Belmont Report*, including informed consent. Although I did not target any protected groups as participants, cybersecurity leaders tasked with attracting, recruiting, and retaining diverse cybersecurity professionals were the intended participants. I used an exploratory qualitative multiple case study as the research method and design and purposive sampling to select participants to achieve data saturation. I collected data from cybersecurity leaders via semistructured interviews and organizational documents and organized, analyzed all gathered data, and kept a log of all decisions made during my research using NVivo as my research database. I used both data and methodological triangulation across multiple data sources to ensure saturation and completeness. I used member checking, reflexive journals, audit trail, and details of my experiences with the topic and study participants to address reliability and validity. In Section 3, I record and discuss the research findings as executed and interpreted, including conclusions, reflections, and recommendations for actions and further study.

Section 3: Application to Professional Practice and Implications for Change

My focus in this study was to explore strategies used by cybersecurity leaders in the Atlanta, Georgia, metropolitan area to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive systems from rising cyberattacks. In this section, I explore the use of these findings from experts in the field of cybersecurity. This section includes (a) an overview of the study, (b) presentation of findings, (c) application to professional practice, (d) implications for social change, (e) recommendations for action, (f) further study suggestions, and (g) personal reflections and the conclusion of the study.

Introduction

The purpose of this qualitative exploratory multiple case study was to explore strategies that cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. I gathered data from cybersecurity leaders at government agencies and IT organizations in the Atlanta, Georgia, metropolitan area in the United States, by conducting semistructured telephone interviews, performing member-checking sessions with 12 cybersecurity leaders, and collecting 15 organizational documents and five multimedia presentations. The cybersecurity leaders I interviewed had between 5 and 30 years of cybersecurity experience. I triangulated data from the semistructured interviews and interviewee member checking with the organizational documents and multimedia presentations to produce major and minor themes to increase the validity of the study findings. Thematic analysis was employed to identify five prominent themes, namely

maintain a diverse and inclusive approach to recruitment, continuous training and development, maintain a culture of openness and teamwork, top leadership support, avoid barriers to cyber talent recruitment and retention. My analysis of the data collected showed strategies, considerations, and methods used by cybersecurity leaders to attract, recruit, and retain diverse cyber talent to effectively and efficiently protect sensitive information from rising cyber threats.

Presentation of the Findings

In this section, I discuss the five major themes and corresponding minor themes that emerged during the analysis of the collected information. I sought to address the following overarching research question: What strategies do cybersecurity leaders use to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats? The answer to this research question may be used to help solve the specific IT problem that some cybersecurity leaders lack strategies to attract, recruit, and retain diverse cybersecurity professionals to efficiently and effectively protect sensitive information from rising cyber threats. I conducted semistructured interviews, member checking sessions, and collected organizational documents and multimedia presentations to gain an in-depth understanding of the strategies used by cybersecurity leaders to attract, recruit, and retain cybersecurity professionals. The access to company documents allowed for triangulation and validation of information obtained throughout the interview process, which I conducted on a distraction-free conference line and lasted no more than 60 minutes in total for each participant. There were 12 participants in total. To improve readability, I

referred to the participants as Participants 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Participants 1 and 12 were females, whereas the rest of the participants were males.

I used the six-step thematic analysis described in the data analysis technique section to approach the analysis of the data collected from all 12 participants. With the use of NVivo 12 software and Microsoft Excel, I was able to identify core emergent major and minor themes, which I categorized into five prominent themes based on commonalities. The development of the themes during the data analysis phase tied back to the review of existing literature and the conceptual framework. Following the data collection and analysis, five major themes emerged during my data analysis: maintain a diverse and inclusive approach to recruitment, continuous training and development, maintain a culture of openness and teamwork, top leadership support, overcoming challenges to cyber talent recruitment, and retention. These five themes exemplify potential strategies that cybersecurity leaders could use to facilitate the attraction, recruitment, and retention of diverse cyber talent to effectively and efficiently perform cybersecurity functions and missions. I compared these following five major themes and subsequent minor themes to the review of existing literature and tied back to Schein's OCT, which served as the conceptual framework for this study.

Theme 1: Maintain a Diverse and Inclusive Approach to Recruitment

Maintaining a diverse and inclusive approach was one of the prominent themes. Maintaining a diverse and inclusive approach to recruitment aligns with existing literature as well as Schein's (2010) culture model, which highlights culture from an observer's perspective, described by three cognitive levels of organizational culture:

artifacts, espoused values, and basic underlying assumptions. Age, ethnicity, gender, race and sexual orientation, and mental/physical abilities and characteristics represent the core of diverse identities (Farmer, 2014). The theme maintaining a diverse and inclusive approach demonstrates an alignment with Schein's (1992) concept, which stressed that for organizations to attain sustainable success, their cultures must not only conform to uniformity, but embrace diversity and inclusion. I leveraged all 12 participants' responses and 20 documents to facilitate the discussions in this maintain a diverse and inclusive approach to recruitment theme. Participant 1 emphasized the "extreme importance and high value of all diversity, including backgrounds, gender, age, perspective, personality, temperament, because it helps provide solutions to problems while recognizing and celebrating differences." The approach to attract, recruit, and retain diverse talent must be inclusive, diverse, supportive, and tolerant to enable employees to explore and innovate. Participant 2 emphasized that their "government agency makes an effort to recruit qualified candidates from very diverse backgrounds, including females, minorities, and particularly people who speak different languages fluently." Organizational documents that I collected from Participant 2 in the form of a recruitment and retention policy manual showed that in response to the globalization of technology-based threats, their government agency increased the need for employees with enough foreign language skills. The nations' successful cybersecurity workforce strategy should incorporate and focus on the values of diversity and inclusion (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018). Carlin, Manson, and Zhu (2010) reported that the National Security Agency (NSA) determined that a diverse cybersecurity team was able

to maintain its network services while detecting, analyzing, and responding to potential intrusions, leading to effective and efficient team performance. All the participants, except Participant 5, acknowledged that ethnic and racial diversity is fairly represented in their teams. Participant 5 shared that their "organization has overall about 15% of minorities, which to him, is a pretty low number that should change." Women, Minorities, and Persons with Disabilities in Science and Engineering (2013) (WMPD) found that women, people with disabilities and minorities from three racial and ethnic groups—Black, Hispanic, and American Indian or Alaska Native—are accounted for in disproportionately smaller percentages in science and engineering. Peacock and Irons (2017) also expressed substantial concerns about the low numbers of qualified female cyber talent who can address the increasing threat landscape. Abdul-Alim (2017) reported that African Americans and Hispanics represented only 6% and 7% of the STEM employment, with men outnumbering women by three to one. The GISWS (2017) found that there was a statistically low percentage of female cybersecurity professionals to tackle rising cyber threats. Participant 8 noted that although their organization makes some effort to recruit the right mix of diversity, they still find it challenging. Participant 8 indicated that there is a reasonably well representation of diversity based on ethnicity and race in their team, although their "cybersecurity team is all-male at the moment due to the difficulty in finding female workers." Participant 3 pointed out that "diversity and education in the workplace should be maintained as standards to follow to ensure the effectiveness and efficiency of the cybersecurity teams."

There was a consensus among the participants on the influence of diversity in the workplace as well as the shortage of cybersecurity professionals. Participant 7 firmly believed that their "strategies to attract, recruit, and retain diverse cybersecurity professionals significantly have a positive impact on their team's performance as they have helped their teams succeed and continue to thrive each day." Participant 7 pointed out that their "organization's success is based on their proactive use of different approaches, including a culture of internal cooperation, teamwork, performance recognition." In addition, Participant 7 highlighted that their "use of a multiplicity of sources to seek out qualified diverse cybersecurity talent that performs the cybersecurity functions necessary to protect sensitive systems from the cyber threats contribute to the success of their cyber teams." These findings align with Buchler et al. (2018) that emphasized that the human dimension in a diverse team structure must be able to cooperate, adapt, anticipate, reason, and orchestrate an effective strategy to respond to ongoing threats effectively. Participant 8 acknowledged that "diversity plays a role in the workplace, although they find it challenging to find a more diverse workforce with people that represent both diversity across different populations and have the necessary qualifications that could fill the seats that they have because of the shortage of cybersecurity professionals in general and the competitiveness of the cybersecurity field." Participant 8 noted that "when seeking candidates to fill available positions, their preference whenever possible, is to find a diverse mix of qualified candidates." Participant 10 further shared "that the lack of diversity in the workplace has a significant impact on their attraction, recruitment, and retention process because it does not allow

individuals to feel comfortable to perform their cybersecurity functions and tasks due to the impression that minorities do not have the necessary skill set to work in the cybersecurity field." Champion et al. (2012) found that the absence of team diversity among the cyber analysts proved to be a substantial obstacle that resulted in nondiverse teams experiencing communication breakdowns, information overload, and feelings of being overwhelmed, which led to cognitive fatigue and frustration. Champion et al. (2012) found that diverse teams, on the other hand, were more adaptive, maintained awareness, and responded to the situations seamlessly. Participant 3 highlighted that "the lack of availability of resources geared toward improving diversity in the workplace could negatively impact the application of best practices for the attraction, recruitment, and retention of diverse cybersecurity professionals." Burrell and Nobles (2018) emphasized that diversity promotes differences in thinking and perspectives, enabling organizations to discover new practices, new vectors, and innovate ideology to solve problems and ensure operational successes. Participant 6 noted that "diversity significantly affects the performance of cybersecurity professionals because a more diverse workforce can approach problems from different lenses, a variation of thought, understanding, and approach to solving the problems." Participant 6 emphasized that "if everybody in the team wears the same lens and has the same understanding, then the team will have the same solution rather than different solutions to the problem." Chen et al. (2014b) suggested the collaboration of a diverse team of cybersecurity talents with different cultures, demographics, domain expertise, structure, and temporal dynamics to accomplish a shared goal as diverse teams are successful and productive when they

collaborate and share information to solve complex problems and manage information systems collectively. Steinke et al. (2015) emphasized that having a diverse cybersecurity team increases information sharing, increases trust, promotes cooperation, reduces conflict, and drives successful team performance. Participant 6 indicated that "having people of varying backgrounds with different understandings, different education levels, and different thought processes contributes to the quick and comprehensive resolution to problems than having a single approach to the issues."

There was a consensus among the participants about the significance of diversity in the cyber teams. Participant 4 emphasized that "cybersecurity isn't just a technology issue rather risk management and business issue; thus, cybersecurity teams should be more diverse so that organizations can know what cybercriminals know to protect themselves against them." The Hasting's bipartisan amendment (2018) supported the significance of protecting the cyberspace with diverse teams of cyber talents that have strong vision and leadership. The House of Commons Science and Technology Committee also recommended a series of initiatives to encourage an inclusive workplace culture, values, demands, and work-life balance (Wilson et al., 2017). The efforts proposed included bias prevention, diversity and equality training, identifying suitably qualified female candidates for senior roles, realizing gender equity in STEM academia, and mentoring schemes to encourage women to apply for such positions (Wilson et al., 2017). Participant 2 strongly agreed that "the cybersecurity workforce should be inclusive and diversified with people from all ethnic backgrounds as everyone can offer something unique to the cyber team." Participant 2 suggested that "all government agencies should,

therefore, maintain a unique, diversified, and inclusive recruitment policy like theirs, to ensuring that the cyber teams enjoy their work and surroundings so that they can stay and not leave to go work for another company that might offer them a better employment package." Participant 3 pointed out that "cybersecurity threats are global; thus, the need to attract, recruit and retain diverse candidates from all cultures to ensure full and effective coverage to defend and protect assets." Participant 4 noted that "the effects of the strategies to attract, recruit, and retain diverse cybersecurity professionals are significant from a positive standpoint because in the past four years their organization has experienced a 50% to 90% increase in diversity which translated to higher performing, overachieving, and more driven cyber teams." Participant 7 further added that "the core intellectual reservoir of any company is as rich as its diversity because ideas can come from anywhere and do come from a multiplicity of direction," therefore emphasizing that "to eliminate diversity in the pursuit of protecting sensitive systems is counterproductive because it not only minimizes the organization's potential but also hurts it by being ineffective." Hence, Participant 7's belief that "diversity is critical to dealing with the threats that organizations face because those threats are global and diverse." An essential element to help keep pace with diverse threats is to be as diverse as the threats itself, raise the cyber literacy level, and empower people who are innovative to push themselves to the fullest extent (Innovation and diversity in the cyber fight, 2015). Participant 9 noted that "diversity plays a significant role in the workplace with a positive impact because people with different backgrounds and experiences contribute differently and bring unique ideas, different perspectives, and approaches into the operations and management

of cybersecurity functions and missions to solve cybersecurity-related problems." Sustaining and fostering a diverse workforce supports the ability to find new cyber talent to perform cybersecurity functions and uncover innovative ways of solving problems (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018). Participant 11 highlighted that their organization "partners with specialized cybersecurity recruiting organizations to ensure that the candidates they are seeking are qualified and therefore meet specific criteria to ensure that they have diversity within their organization that brings different backgrounds, different experiences, and different levels of education to their department." Participant 11 indicated that they are satisfied with the diversity of their workplace, although "some with mixed opinions might argue that their organization takes diversity in the workplace too seriously." Participant 11 strongly expressed that "diverse backgrounds do affect how their cybersecurity teams perform because diverse teams provide diverse solutions, give all members a different perspective on how to approach a problem, and how to come up with a solution." Whereas Participant 11 recognized that many of those solutions are based on experience, the participant believed that "diverse solutions are only achieved from having a diverse team instead of a team that represents one background." Steinke et al. (2015) suggested that diverse team members function better, communicate better, and interpret information and situational contingencies in similar ways due to shared mental models, which significantly affect team effectiveness. Participant 11 stressed that "diverse cyber teams think creatively, think outside the box, look at all angles, and all avenues to come up with different strategies toward solving problems as opposed to just coming out with one basic

approach to solving a particular problem." Participant 7 emphasized the importance of diversity in the workplace and pointed out that "a lot of organizations don't recognize that diversity is a tremendous asset to the success of any organization," including theirs. Participant 7 justified his statement by emphasizing that "as organizations move from environments that are non-global to global relationships, it becomes recognizable that cybercriminals and cyber-terrorists who are looking to cause harm and damage the industry are diverse." Participant 7 noted that, therefore," it becomes critical to mitigating their cyber threats from a diverse point of view." For instance, "it is better to have a Chinese cybersecurity professional try to counter a threat that is coming from China because they would understand how they think as well as their technical practices, more than, for instance, someone from another part of the world." Participant 7 strongly suggested "having a diverse workforce that goes well with the global threats that organizations face, which could come from anywhere."

The participants presented differing opinions about how to diversify the cybersecurity workforce and who to include in the cyber workforce. Participant 4 stressed that the "cybercriminals that organizations are up against are from different backgrounds, different nationalities, and different races; therefore, cyber teams have to be as diverse as the cybercriminals to be able to protect sensitive systems from the cyber-attacks otherwise, organizations stand no chance." The Overcoming Barriers to Advancement - CIA Diversity in Leadership Study (2015) [CDL] found that the lack of a more inclusive cybersecurity workforce, particularly females, has been identified as a contributing factor to the past intelligence failures and critical missions. Participant 4 noted that "the fact that

organizations are not winning the battle implies that we're all doing something wrong." Participant 4, therefore, suggested that "organizations should improve diversity based on gender, race, culture, and background by being more intentionally diverse and inclusive as anyone with the potential to learn, be developed and taught has a place in the cybersecurity industry." Coppel (2016) suggested diversifying the cybersecurity workforce with skilled women and minorities to increase the cybersecurity workforce to prevent cyber attacks. Mansfield-Devine (2017) suggested having a layered defense, including cybersecurity training and increasing the numbers of women and minorities in cybersecurity, to prevent security breaches from becoming the norm for government and businesses. Abel (2017) suggested that giving women more cyber opportunities and involving them more could help reduce the shortage of cybersecurity talent through the increase in ideas, creativity, and introduction to various viewpoints and solutions. Participant 10 stressed that "maintaining the status quo by not doing anything or doing more on diversity and inclusion by bringing everyone on board, including women and minorities, especially the young girls, might be detrimental to the cybersecurity industry." Participant 10's opinions demonstrate alignment with Schein's (1992) concept, which stressed that for organizations to attain sustainable success, their culture must not only adapt to the environment, instead must manage and influence it. Participant 10 highlighted that "young girls shouldn't only be thinking about being chefs or restaurant owners because they could join the cybersecurity workforce just like astronauts, doctors, or engineers." Crosman (2017) suggested recruiting a diversified cyber workforce and establishing recruitment programs to increase the cyber interests of high school and

college students. Participant 10 further emphasized that “if women and minorities chose to join the cyber field, then organizations and government agencies focused on cybersecurity need to offer the women and minorities a path into the cybersecurity world like they do in the military.”

Participants’ opinions aligned with Schein's (1992) concept, which stressed that for organizations to attain sustainable success, their culture must not only be reactive, instead must be proactive. Participant 8 shared that for their team, “the hardest challenge is finding the female workers who have the necessary background because qualified women often don't apply for the positions.” However, “women should be included in the cybersecurity workforce for their unique abilities.” Participant 10 also emphasized that “diversity certainly plays a significant role in the cyber teams, and as an African-American, he's seen a lack of diversity in the cybersecurity field, especially with women, although their organization always makes an effort to recruit minorities.” Participant 4 noted that their “strategy to attract, recruit, and retain diverse cybersecurity professionals is to find unconventional ways to include them in the industry, particularly individuals who wouldn't even think that they are qualified to be in the industry.” Participant 4 pointed out that “people from non-technical backgrounds, diverse cultures, and backgrounds, especially women and minorities, should be included in the cybersecurity industry because diverse cultures mean diverse perspectives, and they bring a unique skill set to the industry.” Participant 4 noted that “without a diverse culture, it is often difficult to attract people from diverse backgrounds.” Participant 6 pointed out that “the issue today is how to get women and minorities to fill all the positions available in

cybersecurity because diversity brings value for the organization." Participant 6 highlighted that "the most important strategy in their organization to attract, recruit, retain women and minorities in cybersecurity is maintaining diversity and inclusion because you can't have diversity without inclusion, and you can't have inclusion without diversity." Participant 4 highlighted that "people from Arts, non-technical backgrounds, and different cultures have different perspectives and opinions on how to tackle the problems and protect sensitive systems, thus if organizations had enough diverse professionals, they wouldn't have as many breaches as they have now." The Senate Homeland Security and Governmental Affairs Committee suggested diversifying talent pools by recruiting specialists from various backgrounds as well as training the existing workforce to protect sensitive information (Congress.gov, 2018). Ghosh (2015) suggested tapping into the growing field of Healthcare Informatics as a way of introducing and engaging women in cybersecurity concepts. Participant 7 pointed out that "part of their inclusion effort is to check for temperamental fit and functional fitness, as they would rather send a professional to an environment they are conversant as opposed to an entirely new domain to ensure the professional is happy." Participant 7 highlighted that "a good retention strategy would be to offer flexible compensation packages that allow the individual to choose whether they prefer to be direct W2 employees, especially for long term projects or 1099-C subcontract relationship employees." Participant 7 also shared that they "accommodate consultants to permanent employee relationships as well as flexibly increasing their compensation package by rolling over the cost of benefits." Participant 12 highlighted that their "government agency predominantly recruits via

LinkedIn and several cybersecurity recruiters, although the available positions are open to all types of people, regardless of race or gender, to ensure fair recruiting processes." Participant 8 noted that although their strategies to attract, recruit, and retain cyber talent have not been formalized due to constrained hiring practices in their organization, he found that "using an approved external recruiter has historically been the organization's best bet for finding the talent that they need." However, participant 12 emphasized that their "recruitment strategy is based on not only the knowledge that the candidates have in the cybersecurity space but also on their ability to work with others, as well as their interpersonal skills, which she considers to be the key skill for success." Participant 1 pointed out that "recruitment strategies must include recruiting people who are competent, talented, team-oriented, energetic, and passionate about their work." Participant 12 indicated that "the cybersecurity team in their government agency is very diverse, and as such, diversity is not an issue in their government agency." Abel (2017) pointed out that diversity reports revealed that 85% of Uber staff, 83% of Facebook staff, and 77% of Apple staff are male. Participant 12 indicated that her "team was made up of men and women from different backgrounds and nationalities, although she tends to focus on the individual." However, participant 12 expressed "concerns about the cybersecurity industry as a whole being more dominated by male cybersecurity professionals." Participant 12 highlighted that "although the cybersecurity industry is heading in that direction at the moment, she is beginning to see that women are becoming more recognized in the cyberspace." Table 1 below highlights the number of references related to the theme of Maintain a Diverse and Inclusive Approach to recruitment.

Table 1

Frequency of First Major Theme: Maintain a Diverse and Inclusive Approach to Recruitment

Major theme	Participant Count	Participant References	Documents Count	Documents References
Maintain a Diverse and Inclusive Approach to Recruitment	12	262	20	236
Minor themes				
Develop diversity and inclusion	12	18	16	17
Implement diversity and inclusion	12	20	20	21
Value all diversity	6	8	7	9
Diversity adds value to organizations	6	14	11	13
Diversity impacts team's performance	12	19	7	14
Embrace anyone with interest in cybersecurity	5	8	5	10
Women and minority cyber talent	12	25	8	13
Diversity in cyber teams	12	16	9	12
Diversified cyber workforce	12	19	11	15
Recruit from a diverse background	12	18	12	17
Variation of thought	5	8	4	9
Different lenses	5	9	6	7
Different perspectives	5	9	6	10
Different understanding	5	10	6	11
Different approach	5	12	6	11
Improve diversity based on gender, race, culture, and background	12	15	9	18
Be supportive and tolerant	4	5	2	6
Diverse culture, means diverse perspectives	2	5	2	4
Diverse culture brings unique skill set	3	8	4	7
Cybercriminals are from different backgrounds	3	6	3	6
Cyber talent should be diverse	5	10	6	9

Theme 2: Continuous Training and Development

Continuous training and development emerged as one of the prominent themes during the data analysis phase of the study. The findings of the study demonstrate how

the continuous training and development ties back to existing literature and Schein's (2010) OCT. Continuous training and development align with Schein's (1999) useful strategies for effecting cultural change in organizations, which include (a) providing comprehensive formal and informal training of teams and groups. (b) providing role models and mentors. (c) promoting continuous employee involvement. I leveraged all 12 participants' responses and 20 documents to synthesize the discussions in this continuous training and development theme. The findings of the study confirmed that cybersecurity professionals should be trained, developed, and nurtured continuously to ensure the retention of cyber talent. Rick Van der et al. (2017) noted that the failure of CSIRTs could have far-reaching effects and catastrophic consequences for national security and the economy, given the growing threat landscape. Rick Van der et al. (2017) suggested that cyber leaders should focus on identifying areas for team improvements and on potential solutions by increasing team members' skills level, knowledge, technical resources, participation, and cooperation to close the gaps between current and desired incident handling practices. Participant 1 noted that "organizations should continually grow and invest in cyber talent to increase participation and efficiency of performing the cybersecurity security tasks and missions." Participant 1's opinion aligns with Schein's (1999) useful strategies for effecting cultural change in organizations, which include promoting continuous employee involvement. Oltsik and Alexander (2016) pointed out that the shortage of cybersecurity skills contributed to the increase in data breaches, zero-day vulnerabilities, and malicious internet protocol addresses. McCollum (2015) noted that the top causes of cybersecurity breaches include cybercriminals, malicious and non-

malicious insiders, and hackers, as well as the need to recruit diverse cybersecurity talent with advanced cybersecurity knowledge, training, and certifications. Participant 2 reported that "combining diversified and inclusive recruitment and retention strategies with thorough and constant training and development at their agency's computer training institute makes the teams very proficient and well versed in protecting sensitive information systems." Thus emphasizing that "maintaining an upper hand with technology is essential for every cyber team because the Internet or the Computer scams of 5 to 10 years ago is obsolete, as criminals and organized crime figures are always trying to come up with very creative ways to infiltrate, compromise, and destabilize computer systems." As a result of the continually evolving cybercrimes, participant 2 noted that "the cyber teams in their government agency continuously undergo state of the art, very advanced training to keep up with the always emerging new threats due to the advances in computers." Participant 2 highlighted that "government agencies should invest in the training and development of their cyber teams while ensuring that they enjoy their work and surroundings to increase the retention rate due to the lack of a better employment package." Participant 3 emphasized that their "retention strategies involve investing in the resources by ensuring continuous training, discussing current threats in cybersecurity, learning new tools and solutions to mitigate cyber threats." Participant 3 pointed out that "growing, developing, and adequately compensating cyber talent makes them feel valued and encouraged to remain with the organization while continuing to do what they do best." Participant 10 pointed out that "cyber threats affect everyone in the world individually, and it's not about fighting with guns and machines and bombing

countries anymore; instead, it is happening over the internet." Thus, "organizations need to educate, train and develop young talent continuously to understand the future of cybersecurity." Participant 7 highlighted that part of their "robust retention strategy is to be proactive to the training needs of the existing employees or the potential cybersecurity professional they are looking to attract to avoid the risk of losing their valuable resource based on the shortage of cybersecurity professionals in the industry." Additionally, participant 7 noted that their "organization ensures that they offer effective compensation while trying to align the temperament, function, and experience of the individual with the vertical markets that they support." Participant 10 emphasized that "once professionals are recruited into their organization, they apply their retention strategies, which include knowing what they're looking for, what they are thinking, listening to them, and offering them continuous training, learning, growth, and development." Participant 6 suggested that "organizations should embrace, train, and develop anyone that has an understanding or interest in working in cybersecurity to be a part of the workforce." Lemos (2017), Liu and Murphy (2016), and Pusey et al. (2016) indicated that addressing the shortage of women in cybersecurity requires investing in training, mentoring, advancement, and sponsorship programs. The participant's opinions aligned with Schein's (1992) observation that for organizations to attain sustainable success, their culture must not only be task-oriented, instead must be relationship-oriented. Participant 12 stressed that "it is critical to help candidates understand what other benefits they can leverage by working for a government agency." For instance, "being committed to working with candidates to ensure their growth and development so that they can learn." However,

Participant 12 shared that she prides herself on “being very flexible at establishing a good rapport with your employees to offset the fact that they don't get paid as much as their counterparts in the private sector.” Participant 12 noted that “to make up for the low wages in the government sector, she engages in a lot of mentoring in the industry.” Participant 12 recommended “recruiting someone with limited experience in the cyberspace, and then training and developing them.” Burrell and Nobles (2018) suggested that the lack of role models and mentors, male-friendly teaching practices and curricula, rigorous STEM environments, societal stereotypes about who can be scientists, and educational and social factors affect the participation of women in the cyber workforce. The internal policy documents related to the recruitment and retention of cybersecurity professionals that I collected from the participants confirmed the need and importance of continuous training and development to ensure the retention of cyber talent that efficiently perform cybersecurity security missions and functions.

The participants shared different thoughts and opinions on the type and level of knowledge and training necessary to join the cybersecurity field. Participant 2 indicated that “candidates applying to get into the government agency's cybersecurity teams must have at least fundamental training and working knowledge of the language used in the world of cybersecurity. Some examples of the fundamental knowledge and training include firewalls, anti-malware, access controls, cryptographic software, antivirus software, social engineering, phishing scam, spoofing emails, etc.” Castro (2018) suggested that certification programs, degree programs, and cyber workforce development programs should be established to attract diverse cybersecurity talent to

tackle the growing cyber threat landscape. Participant 4 noted that “in addition to knowledge and practical experience, cybersecurity professionals should have a critical mindset and think like criminals to tackle rising cyber threats.” Pusey at al. (2016) suggested that diverse skill levels enable differentiated learning, enriched experiences, build confidence, improve career awareness, and support the development of soft skills such as critical thinking, teamwork, and communication required for cybersecurity teams to effectively and efficiently resolve problems. Participant 3 pointed out that “attracting high-quality cybersecurity professionals should involve considering their training, background, professional certifications such as CISSP to ensure that they qualify for the role they are seeking before putting them through an interview to vigorously protect data from cyber-attacks.” South (2015) suggested that acquiring degrees in cybersecurity and certificates like the CISSP could help individuals gain useful cybersecurity knowledge and get a cybersecurity job. Participants 1 and 10 stressed that “organizations should not ignore and shut down the training requests and ideas of their cyber professionals because they are the ones that figure out the problems, find ways to mitigate the cyber risks and solve the problems.” Participant 7 emphasized that “based on the dynamic nature of the industry with changing platforms, upgrades, and various threats, the strategy they deploy to attract, recruit, and retain diverse cybersecurity professionals follow that dynamism.” Participant 7, therefore, stressed that “an effective strategy for their organization is to attract, recruit, and retain cyber talent that is very conversant and current with the nature of emerging threats.” Prager and Prager (2016) suggested that diversifying the cybersecurity workforce by bridging the education gaps with diplomas, internships, and

apprentices to provide job exposure and cultivate experience could help attract more talent to protect sensitive information. Participant 7 highlighted that "to keep their professionals up to date with current trends in the cyber industry, they continuously offer training as well as tuition reimbursement to those professionals that decide to expand and strengthen their knowledge in cybersecurity."

There are various strategies for the recruitment of cybersecurity professionals, and the majority of the participants use similar strategies. Participant 10 pointed out that their "strategy for recruiting diverse cybersecurity professionals involve working with agencies that specialize in recruiting cybersecurity and technical personnel to interview individuals to understand their background, skill set, personalities, and their state of mind to qualify them for the potentials and responsibility to mitigate the cyber threats they face daily." Participant 7 also shared that they "try to seek and reach out to qualified, proven, and robust cybersecurity professionals through aggressive staff augmentation and word of mouth while incenting them by at least ensuring that they match some of the compensation sought." Participant 7 pointed out that they somewhat differentiate between their strategies to attract, recruit, and retain diverse cybersecurity professionals by highlighting that "the strategy to attract and recruit cyber talent is aligned and thus similar." Participant 7 noted that their organization "maintains a handy repository of information on cybersecurity professionals in the industry, which they tap into to search for cybersecurity professionals with the right skills and fit the nature of the threats and implementation of security remediation tasks when an opportunity arises." Participant 7 explained that "once they identify a potentially suitable cyber talent in the database with

fundamental skills and certifications, they reach out to them, find out their location, availability, and then interview them to see if they could be a potential fit to join their organization." However, Participant 7 noted that "if they are unable to find suitable candidates in their database due to the competitiveness of the industry, they engage the services of specialized cybersecurity consulting companies for specific vertical markets as a last resort after they've exhausted all options to find qualified cyber talent." Participant 7 noted that they either "hire consultants to do the work or train and develop potentially suitable candidates to meet the organization's cyber team's standards." Participant 7 also mentioned that "in addition to their internal database of cybersecurity professionals, they have access to several external databases, including Monster, a popular job posting site that was founded in 1999 to aid their search for suitable cyber talent." Participant 8 mentioned that although their "overall organization's policy is to select candidates with the right level of skills and education if they have them as opposed to a candidate who doesn't, they tend to recruit and train candidates with the potential to learn." Participant 9 noted that their "fundamental approach to attracting, recruiting, and retaining cybersecurity professionals is to consider the individual's background, skills, knowledge, and experience." Participant 9 cautioned that "attracting, recruiting, and retaining inexperienced cybersecurity professionals without offering them continuous training and development once they are on board would harm the industry and the company's operations." Participant 10 suggested "developing training and technical abilities in the inner cities to show women and minorities that they can believe in themselves to go out and find cybersecurity-related jobs." Participant 10 further

suggested that “instead of young individuals sitting around playing games, basketball, and football, they could change their mindset and grow by joining after school cybersecurity camps that organizations could develop to learn new skills and have unique opportunities to work in the cybersecurity field while being prepared to adapt as quickly as the threats emerge.”

The participants presented different opinions on the effects and benefits of training and the development of cyber teams. Participant 3 slightly distinguishes between strategies to attract, recruit, and retain cybersecurity professionals. Participant 3 summed that their “strategy to attract, recruit, and retain diverse cybersecurity professionals positively impacts the performance of the teams that protect sensitive systems in their organization because they continuously recruit qualified and diverse cybersecurity professionals and then continue to train them and keep them up to date with current trends in cybersecurity to defend and protect the organization's information systems.” Participant 3 further stressed that “continuous training and development goes a long way in ensuring the retention of cybersecurity professionals in the organization to protect and defend sensitive systems from cyber attacks. Organizations should, therefore, make itself attractive to potential diverse professionals.” Participant 5 highlighted the need to “ensure that individuals represent the right skills and education for the right level in a way that articulates the value of that individual that is trying to get into the organization.” Participant 5 recognized that “education and training significantly impact the cybersecurity teams’ performance because their cyber teams have been successful in the past and continue to be successful in solving cybersecurity issues because of vast and

continuous training, development, knowledge, hands-on experience in combination with a diversified team." Participant 6 noted that "organizations should give women and minorities the opportunity to ascend the ranks upon graduating from college or technical school with a certification that would enable them to join the cybersecurity workforce." Participant 6 stressed "the importance and benefits of the candidates attaining an advanced technical degree or certification to gain the necessary knowledge and then demonstrate that knowledge in a practical manner so that people can understand that they have the expertise and practical understanding." Participant 8 stressed that "candidates must have the necessary training and skills needed for the positions they seek because cybersecurity is a tough field to recruit for due to its competitiveness." The participant's opinions aligned with Schein's (1992) concept, which stressed that for organizations to attain sustainable success, their culture must not only be task-oriented, instead must be relationship-oriented. Participant 12 emphasized "the need for top cyber leaders to focus on developing individuals that have the right attitude, right interpersonal skills, and ability to get along and work with other people because it is a critical skill that top leadership often overlooks when attracting, recruiting, and retaining cyber talent." Table 2 below highlights the number of references related to the theme of Continuous Training and Development.

Table 2

Frequency of Second Major Theme: Continuous Training and Development

	Participant		Documents	
Major theme	Count	References	Count	References
Continuous training and development	12	246	20	216
Minor themes				

Grow and invest in talent	6	10	8	16
Invest more in people and processes	6	6	8	19
Attain an advanced degree	6	12	6	13
Attain a certification	6	14	6	15
Train to ensure cyber talent retention	12	40	20	46
Have a critical mind set	5	3	7	8
Think like a criminal	4	4	4	7
Increased training	12	24	10	22
Practical experience	12	44	12	29
Have a mentor	5	16	4	10
Keep up with emerging new threats	5	5	6	6
Recruit at lower levels	5	7	3	5
Have the right skills for the right level	5	8	3	4
Same opportunity and same mentorship	7	17	5	10
Benefits of training and development	5	9	5	7
Effects of training and development	6	9	6	8
Demonstrate competence and ability	3	6	5	5
Demonstrate teamwork and passion	5	5	5	6
Listen and respond to needs	5	7	6	9

Theme 3: Maintain a Culture of Openness and Teamwork

Maintaining a culture of openness and teamwork was another prominent theme. The findings of this study demonstrate how maintaining a culture of openness and teamwork aligns with existing literature and Schein's OCT. Organizations strive for excellence in practice through the development of a strong team culture, which Ruygrok (2016) defined as a set of shared norms, values, and beliefs that drive performance and behavior. I leveraged all 12 participants' responses and 20 documents to synthesize the discussions in this maintain a culture of openness and teamwork theme. Participant 1 highlighted that "organizations need to set the right tone on culture by attracting people who fit the culture, subscribe to it, practice it, and celebrate the unique perspectives of every cultural ethnicity. For instance, they celebrate Hindu festivals every season."

Participant 4 also noted that “Atlanta is unique because they celebrate and embrace different cultures and diversity, however, noting that as one travels out of Atlanta, Georgia, to other colder parts of the country, for instance, further north, less diversity is appreciated.” Participant 11 also shared that their organization and most of the other organizations he's worked for “celebrate every culture - for example, Black History Month, Cinco de Mayo, or any other cultural experiences and emphasized that it is essential during the onboarding process, to ensure that candidates are aware that the culture of the organization as a whole supports their heritage.” Morcos (2018) noted that organizational culture is a significant driver of organizational excellence and the long-term effectiveness and performance of an organization. Beugelsdijk et al. (2014) pointed out that organizational culture remains an essential factor in the analysis of organizations, and it influences an organization's performance and competitive advantage. Participant 1 noted that “culture speaks for itself, and with an organization's culture of inclusiveness, development, openness, and collaboration, people don't leave but rather stay because of the culture, the work, and mission.” Thus, participant 1 pointed out that “the positive culture and tone created in their organization is the main reason for their high employee retention rate.” However, participants 1 and 10 noted that “individuals who don't fit the culture of the organization often left the organization immediately, allowing them to attract and retain people that fit the culture of the organization.” Actively supporting “a strategy of first ensuring that the culture of the organization matches the beliefs and personality of the cybersecurity professional is crucial.” Mazur (2014) emphasized that diversity is a cultural question of norms, values, beliefs, and expectations. Some

participants differentiate in their attraction, recruitment, and retention strategies. Participant 1 pointed out they “attract people who will challenge the status quo and make it better.” Participant 1 also explained that her “retention strategy focuses on the culture of the organization as well as characteristics such as competency in the cybersecurity field, demonstration of excellence, teamwork, and ability to show a passion for the work done in the cybersecurity industry.” Participant 12 pointed out that “with the open-door culture of the government agency, ensuring regular communications with the team is vital to encouraging the team to bring any concerns or issues at any time so that they are addressed efficiently.” Participant 3 “considers cyber threats to be global and, therefore, attract, recruit, and retain diverse candidates from all cultures to ensure full and effective coverage to defend and protect assets.” NICE (2017) suggested that cultural change is much needed to recruit more women and minorities in the cyber workforce. Participant 1 emphasized that “with the use of proper communication, change management, and the right culture, organizations can execute the strategies for cyber talent recruitment and retention.” Participant 1 stressed that “creating the right culture and a suitable working environment for all roles makes people stay longer.” Participant 1 further noted that “a collaborative culture that includes everyone in the team including the CIO, head of security, peer leaders, and external IT teams is critical to implementing solutions and solving security problems together which are embedded in the data warehouse, infrastructure, application development, workflow, or implementation.” Therefore, “organizations can't just set and leave culture because it needs to be continuously nurtured like a relationship while constantly growing cyber talent, looking, listening, and

responding to any issues, concerns, needs, and desires rather than ignoring people in the organization." All the participant's contributions demonstrate alignment with Schein's (1999) useful strategies for effecting cultural change in organizations, which include (a) providing opportunities to offer input and feedback, and (b) making available support groups to share ideas and address any concerns. Ruygrok (2016) found that identifying the performance expectations of each team member and defining expected behaviors while restating the core values during communications, team briefings, and during the interview for potential hires is critical. Participant 1 noted that although "cybersecurity professionals are scarcer and harder to find, their open, collaborative, and friendly organizational culture significantly and positively boosts the performance of cybersecurity teams, making them stay longer, and it never gets in the way of high expectations." However, participant 1 further added that, "if an expectation is unmet, the expectations are reiterated to boost the teams' performance."

Participants discussed the significance of the culture of the organization on attracting new candidates and retaining existing candidates. Fattah (2017) found that organizational culture is an invisible force that could influence the actions, feelings, thoughts, and performance of people who work in an organization. Participant 5 reported that "the culture of the organization helps in attracting new candidates and keeping the existing employees around while maintaining an interest in the role." Participant 4 noted that "cybersecurity professionals should first be attracted to the culture of the organization, what they stand for, as well as getting them sold on the why." In other words, "why the role is important, and why they being in the role would serve a greater

good." Participant 10 mentioned that "candidates could be attracted to a welcoming culture with an open-door policy where they can share ideas, knowledge, trust, and belief in one community to solve problems with the same goals and state of mind because the shared ideas could be used to solve similar issues when they arise." Participant 10 pointed out that overall, their organization uses the same strategies to attract and recruit, however, noting that they "retain individuals in the organization by keeping the jobs and tasks challenging as well as ensuring that the organizational culture allows for a stress-free, flexible, and comfortable environment in combination with competitive salaries and excellent benefits such as paid vacation time." Participant 10 also emphasized that "in addition to setting the right tone on culture, offering higher wages, a pleasant work environment, friendly people, and flexible work environments could also help attract cyber talent to the organization." Lawson, Hatch, and Desroches (2013) examined the need for a progressive organization to formulate its strategy, implement processes that support operations, provide performance evaluation and operational control, and learn and change with the use of a management system. Participant 3 mentioned that "non-progressive or unfriendly cultures tend to discourage professionals from seeking cybersecurity roles within the organization." Participant 4 shared that "the culture of the organization should be inclusive and open because people want to go into an environment where they feel welcome rather than be the oddball." Participant 5 noted that "the culture of the organization significantly impacts the strategies to attract, recruit, and retain diverse cybersecurity professionals, and thus, organizations must make every effort or have some process to recruit and retain diverse cybersecurity professionals." Participant 7

stressed that “culture is a crucial element in their attraction, recruitment, and retention strategy and pointed out that their attraction strategy involves trying to ascend the resource at the point of entry by building a culture of teamwork, recognition, collective goal, and mission.” Naranjo-Valencia et al. (2016) found that organizational culture influences behavior and people and, therefore, could foster innovation and improve an organization's performance based on the values promoted. Participant 8 mentioned that although their organization isn't as flexible as other organizations and verticals who try different approaches to see what works, “the impact of the culture of the organization is significant to the candidates as it helps in attracting new candidates and keeping the existing employees around while maintaining an interest in the role.” Participant 9 emphasized that “the culture of the organization has a significant impact on their strategies to attract, recruit, and retain cybersecurity professionals depending on the operations of the sector in question.”

Many of the participants explained that their strategies to attract, recruit, and retain diverse cybersecurity professionals are interlinked and, therefore, go hand-in-hand with each other. While Participants 1 and 2 have not yet identified any ineffective and inefficient strategies, they “support strength-based leadership, by moving people currently in other areas who are interested in the cybersecurity field to the security field if the opportunity presents itself.” Participant 4 believes that “the best way to attract cybersecurity professionals is to give them some sense of mission as well as making them feel like they're part of something bigger than themselves.” Participant 7 emphasized that compared to other organizations, they “make it known to their employees that they are as

important as their clients by trying to create a robust culture of consciousness that they value their employees as much as they value their clients." Participant 7 noted that "it is a triangular relationship based on the principles that if the professional is happy, then the employees would do a good job." Likewise, "if the client is satisfied and content, then the organization would be rewarded repeatedly." Thus, participant 7 tries to "maintain a culture that recognizes the interrelationship between the client and the professional and the organization as the balance between the three relationships has served their organization well." Participant 8 highlighted that although they do not differentiate between their strategies or approaches to attract and recruit, "the retention of personnel is done slightly differently." Participant 8 shared that their organization has "lots of benefits and pros for cyber personnel within the organization, geared toward retention efforts, although the candidates have to either like the culture of the organization, the sort of environment, and benefits offered to enable their retention." Participant 8 pointed out that "the retention of professionals is usually based on getting the best fit for somebody who would appreciate and find appealing the organizational culture, benefits, and lifestyle, and if they do, they tend to stay a long time." Participant 12 indicated that their "government agency uses the same strategy to attract and recruit, but slightly different strategies to retain top talent." Participant 12 emphasized that "the culture of the government agency enables her to be an open manager that has built a solid foundation based on trust because she tends to allow her cybersecurity team to use their initiatives on any ongoing projects as long as she gets regular updates." Participant 12 highlighted that she was "not the sort of manager that shadows or micromanages her team; instead, she

creates opportunities to retain top talent." Table 3 below highlights the number of references related to the theme of Maintain a Culture of Openness and Teamwork.

Table 3

Frequency of Third Major Theme: Maintain a Culture of Openness and Teamwork

	Participant		Documents	
Major theme	Count	References	Count	References
Maintain a culture of openness and teamwork	12	148	20	108
Minor themes				
Set the right tone on culture	2	5	2	6
Have high perceptions of culture	2	2	2	2
Focus on inclusiveness	3	5	2	3
Focus on collaboration	5	5	3	5
Use proper communication	5	5	4	6
Nurture culture like a relationship	2	2	2	3
Shift from the male-dominated culture	6	6	6	6
Maintain a culture of openness	12	12	6	7
Maintain a friendly environment	12	12	6	6
Maintain a welcoming environment	12	12	6	9
Maintain a flexible work environment	12	12	6	8
Maintain a comfortable environment	6	6	4	6
Maintain an open-door policy	12	12	7	9
Maintain a culture of teamwork	12	12	20	20
Maintain a culture of recognition	12	12	7	7
Maintain a culture of collective goal	10	10	6	6
Build strong personal relationships	5	5	3	5
Cultivate accountability and trust	7	7	4	6
Champion change	4	4	6	9
Be the change you want to see	2	2	2	2

Theme 4: Top Leadership Support

Top Leadership Support was another prominent theme. Top leadership support aligns with Schein's (2010) concept of leaders as shapers of organizational culture as well as existing literature. Top leadership support demonstrates alignment with Schein (1999) useful strategies for effecting cultural change in organizations, which include

building charismatic leaders. Organizational culture binds together members of an organization and allows leaders to align the culture of their organization with its vision and strategic objectives (Chatman et al., 2014). I leveraged all 12 participants' responses and 20 documents to facilitate the discussions in this top leadership support theme. There was a consensus that top leadership should be wholeheartedly involved in the attraction, recruitment, and retention of diverse cybersecurity professionals. Participant 7 noted that "top leadership support is much needed to attract, recruit, and retain cybersecurity professionals." Burrell and Nobles (2018) indicated that recruiting and retaining diverse cybersecurity workforce requires having cybersecurity leaders that are adequately trained in diversity, inclusion, and employee engagement in ways that can constructively influence positive organizational and employee behavioral change. Organizational policies are relevant to the development and implementation of an organizational culture that supports diversity because they help to establish a recruitment and retention protocol for all to follow. Lambert (2016) noted that diversity and diversity management (DM) could create a fertile environment for innovation to flourish in the organization either explicitly using formal policies and guidelines directly tied to cultural diversity or implicit through the behavior of leaders. Participant 4 stressed that "organizations should drive a top-down diverse cyber talent policy-centric recruitment and retention approach from the highest level of executive leadership." Additionally, "executive leadership should sign off high-level all diverse cybersecurity recruitment and retention policies." Organizational documents and multimedia presentations collected from participant 4 confirmed that a top-down policy-centric approach is critical to recruiting and retaining

cyber talent. Farmer (2014) found that chief diversity officers (CDOs) that promote and sustain D&I in organizations play a significant role in uniting employees, providing awareness, education, and training programs, and creating the business case that aligns with core business goals and objectives while creating a work environment where everyone feels included and valued. Participant 5 noted that "to attract, recruit, and retain diverse individuals into the cybersecurity workforce; there is a need to have an advocate internally at the organization as well as an advocate on the outside in the form of top leadership helping the professional who is trying to get into the organization." Participant 5 emphasized that "the leadership within the organization should be an advocate for existing employees as well as potential employees to understand better that diversity can bring excellent quality work to the organization as well as add value to the organization." Participant 5 explained that "an advocate is a person within the top leadership who understands the challenges, the issues, and the need for all diversity on both ends to provide the necessary training and the strategies required to attract, recruit, and retain cyber talent." Participant 5 indicated that "the culture of the organization should include training the top leadership within the organization in diversity and the need to know the different backgrounds of professionals that are not part of their own culture."

Participants discussed why organizations need top leadership buy-in to facilitate the attraction, recruitment, and retention of diverse cybersecurity professionals. McCollum (2015) suggested collaborations with key stakeholders, including top leadership organization-wide, to promote the need to recruit and retain diverse cybersecurity talent to prevent rising cyber attacks. Participant 5 shared that "the low

percentage of diversity in their organization is systematically due to lack of top leadership support in the attraction, recruitment, and retention of diverse cybersecurity professionals." Participant 6 emphasized that "having a diverse workforce that includes not just non-management and middle management, but female executive-level positions bring value to the organization." Thus, "organizations need to have leaders' at the most senior level that are representative of the diverse workforce because without representation, it creates a perception that the organization does not care about diversity, whether ethnic, racial or gender diversity." Participant 6 pointed out that "CEO's, board of directors, and chief diversity and inclusion officers in organizations should be serious about having a diversity and inclusion program to attract, recruit, and retain women and minorities within the cyber workforce because with the shortage of diverse cybersecurity personnel, the teams cannot possibly execute all of the cybersecurity functions and missions as well as prevent vulnerabilities in systems which will not be addressed promptly without diverse cybersecurity teams." Burrell and Nobles (2018) suggested that having competent and empowered leaders that support and leverage diversity and inclusion strategies are one the most critical aspects of attracting, developing, and retaining women and minority cyber talents. Participant 7 suggested that "organizations support and partner with their chief information security officers by giving them the commensurate and budgetary authority to deal with the cyber threats by attracting, recruiting, and retaining qualified diverse cyber talent to tackle the rising cyberattacks." *P*articipant 11 stressed the importance of top management support for diversity efforts within organizations by sharing with candidates that the "senior leadership believe in

diversity and that they were not just selected based only on their qualifications for the job, instead because the top leadership in the organization genuinely wants to build a diverse and inclusive workforce that supports the advancement of diverse candidates and employees technically or toward managerial or director level promotions." Participant 6 stressed that "top leaders in organizations should give everyone the same opportunity, same mentorship, and same advocacy while having a strategic objective that is included in the strategic plan that makes sure that women and minorities are considered for executive-level positions, and have the opportunity to ascend and stay in those executive-level positions." Participant 7 shared that "the cybersecurity profession starts with the lowest levels of security professionals to the chief information security officers who face a multitude of issues such as inadequate budget to attract, recruit, and retain cyber talent."

The study findings showed how top leadership support plays an indispensable role in the attraction, recruitment, and retention efforts of diverse cybersecurity professionals. Alhadid (2016) found that leadership practices positively influence organizational performance and, therefore, considers leadership as a critical factor that influences the success of strategies for creating competitive advantages in a dynamic environment. Wilson, Broughan, and Hillier (2017) found that a lack of leadership, inadequate mentoring, limited education, and the responses to life transitions negatively impacted the careers of women. Participant 7 highlighted that often, "leadership in organizations that have never experienced any attacks or obstructions or negative impact, find it difficult to picture themselves as being victims of potential attacks until they are attacked." Therefore, participant 7 recommended that "top leaders in organizations should decouple

the relationship between CIO's and CISO's by having CISO's standalone with their budget in the industry to help with their attraction, recruitment, and retention efforts of diverse cybersecurity professionals." Participant 7 firmly believes that doing so would "help boost the confidence in those who seek to protect vital infrastructure from the threats that we face daily." Participant 12 reiterated that their "challenge with attracting, recruiting, and retaining top talent is mainly because, in the government sector, cybersecurity professionals are not paid as much as the security professionals in the private sector." Therefore, "top leadership, managers, and cybersecurity leaders in the government sectors should be willing to lower their standards and bring people with limited talent but with the potential to learn, train, and be developed in the cybersecurity space." Bagchi-Sen et al. (2010) suggested that women and men alike must possess soft skills and a strong background in hardware and software systems with the ability to transform their knowledge into government policy and external regulations to progress in the cyber field. Burrell et al. (2018) suggested the use of leadership development interventions that focus on building diverse teams and individual competence to protect mission-critical systems through the effective collaboration of diverse cyber talent. Participant 12 pointed out that "the top leadership's focus shouldn't only be on the technical side as that can be taught whereas you people cannot be taught how to work with others, get along with people, and deal with conflicts and various personalities." Erkutlu (2012) found that shared leadership within a work team positively influenced proactive team behavior with support for diverse cultures, which improves team effectiveness. Para-González et al. (2018) found that transformational leaders promote

employees' collective interest by helping them to reach mutual goals, enhance their performance through knowledge and learning; and be innovative with problem-solving tools through organizational culture and competitive strategies. Participant 12 mentioned that "being a hands-on leader helps motivate and positively affect the cyber team's performance and thus, recommends that due to the difficulties in attracting, recruiting, and retaining cyber talent in the public sector, government agencies should lower the standards for recruiting cybersecurity professionals so that they can train and develop them once they are in the government agency." Ilieş and Metz (2017) found that a strong culture is a source of sustained competitive advantage in achieving short and long-term strategic business objectives. Participant 12 suggested that "cyber leaders should be willing to support the individuals in getting to where they need to be as cyber professionals as well as teaching them how to communicate with non-technical staff so that they understand, and work together to meet the business objectives in a secure environment." Table 4 below highlights the number of references related to the theme of Top Leadership Support.

Table 4

Frequency of Fourth Major Theme: Top Leadership Support

	Participant		Documents	
Major theme	Count	References	Count	References
Top leadership support	12	49	20	73
Minor themes				
Have executive-level representation	12	12	10	11
Have an internal leadership advocate	3	5	4	4
Have an external leadership advocate	3	5	4	4
Be serious about diversity and inclusion	8	10	20	21
Be a mentor	10	12	12	14

Signed off high-level recruitment and Retention policies	3	3	6	9
Drive a top-down policy-centric Recruitment and retention approach	2	2	6	10

Theme 5: Overcoming Challenges to Cyber Talent Attraction, Recruitment, and Retention

Overcoming challenges to cyber talent recruitment and retention was another prominent theme. The findings of this study demonstrate how overcoming challenges to cyber talent attraction, recruitment, and retention aligns with the conceptual framework and existing literature. The theme overcoming challenges to cyber talent recruitment and retention aligns with Schein's (1999) conceptual framework which presents useful strategies for effecting cultural change in organizations, which include (a) creating motivation for change by discarding any legacy culture, and (b) learning from past deficiencies and embracing new opportunities and potential solutions. I leveraged all 12 participants' responses and 20 documents to synthesize the discussions in this overcoming challenges to cyber talent recruitment and retention theme. The participants discussed strategies that they found to be unsuccessful within their respective organizations and how other cybersecurity leaders could overcome those barriers to cyber talent attraction, recruitment, and retention. Schein's OCT highlights three barriers to the successful sharing and transfer of strategies within an organization: ignorance on both ends (the receiver and giver), unavailability of resources, and lack of relationship between the giver and receiver (O'Dell & Grayson, 1998; Szulanski, 2017). Participant 1 pointed out that "since security is always in demand, there is always the possibility that

after nurturing or training an individual, they could leave to another organization, although emphasizing that setting the right culture and tone will make it less challenging to find a replacement to fill the vacant role." Participant 1 noted that this "situation sometimes occurs with younger uncommitted professionals" and thus suggested "making them stay instead of preventing them from leaving." Participant 10 indicated that their "organization finds it challenging to recruit cybersecurity professionals through boot camps or college fairs because they don't have the necessary skill set." In contrast, participant 6 reported that their "organization goes out to different universities and different platforms to find candidates who have the opportunity to work in the cybersecurity field as it often works for their organization." However, participant 10 still "encourages organizations to take the risk to bring potential candidates in and then offer them training opportunities." Participant 10 explained that "the challenge of recruiting and retaining candidates coming straight out of college with a set of expectations, no industry certifications, no real-world experience, and academic knowledge versus hands-on experience is that they eventually leave and go somewhere else where they are offered better remuneration packages." Abdul-Alim (2017) suggested that organizations recruit and retain diverse talent from universities and colleges that include diverse populations as opposed to non-diverse populations. Participant 2 also expressed that their "government agency does experience the challenge of losing well-trained cybersecurity professionals to another organization that offers them a better employment package." Participant 2 explained that "once candidates are successfully recruited using the agencies very unique, diversified, and inclusive recruitment policy, the employees choose whether to work in

the cybersecurity division or not." Participant 2 pointed out that "the least effective and efficient recruitment and retention strategy would be to hire a candidate who has zero knowledge about cybersecurity as they may not be a good fit." However, those "employees who desire to work in cybersecurity are put through extensive training related to information security at their dedicated training facility, and if they are not happy with the job for one reason or another, the agency risks losing them although it did not happen very much at participant 2's agency." Participant 2 highlighted that their *government* "agency would do whatever it could to retain a cyber talent as it is challenging to invest so much money in training someone only to lose them to the corporate sector or fortune 500 companies where they may be offered a lot more than their government wage and benefits."

Participant 4 reported that their organization "avoids trying to get candidates to buy into the idea that they can make a lot of money in the cybersecurity industry because the approach of offering better monetary incentives to retain cyber talent typically does not work." Based on Participant 4's past experiences, "some other organization will always offer them a lot more money than you can offer, thus making retention very challenging." Participant 4, therefore, suggested that "organizations should avoid focusing on the monetary benefits because it is not enough to retain the cybersecurity professional." Participant 4 pointed out that "a challenge with the application of attraction, recruitment, and retention best practices for diverse cybersecurity professionals is getting the targeted individuals to see the opportunity as well as to see how their diverse backgrounds could be an advantage." Participant 4, therefore, noted

that “the potential cybersecurity professionals need to see and believe that the opportunity is for them to be attracted, recruited, and retained.” Participant 4 indicated that “the perception of who the hacker and the cybersecurity professional or practitioner is, needs to change because it could be anyone.” Participant 4 emphasized that “the image portrayed by the media of the hacker being Caucasian male, with a long ponytail and a hoodie is false and must be changed.” Participant 4 stressed that “those days are gone because the hacker could be, for instance, a male or female, Grandpa or Grandma, a twelve-year-old child with Asperger's syndrome or autism or someone from any part of the world.” Participant 4 believes that “it doesn't matter who it is because it could be anyone; Thus, stressing that since the underworld is diverse, the people protecting the systems from cyber-attacks should be diverse as well.” Bagchi-Sen et al. (2010) found that the critical success factors necessary for the career advancement of women in the cybersecurity field are to change the IT’s "hacker culture," IT’s "old boys' network," social expectations, and work-life-balance for the underrepresented women in cybersecurity. The participant’s responses aligned with Schein’s (1992) concept, which stressed that for organizations to attain sustainable success, their culture must not only be past/present-oriented, instead must be future-oriented. Participant 6 noted that “the organizational culture has to shift from a male-dominated culture to a culture that is open to attracting, recruiting, retaining, and advancing women to senior-level positions within the cyber workforce.”

Participant 5 noted that “a poor strategy would be for an organization to fail to realize and accept an individual's skills, education, background, and experience as well as

failing to expose the excellent characteristics of the particular individual." Participant 5, therefore, believes that "without the strategy that reveals the individuals' strengths, skills, education, and background, the organizations would not be effectively recruiting diverse cybersecurity professionals." Participant 6 noted that "a challenge to recruiting and retaining women and minorities to the cyber workforce is hiring at the lower levels because of lack of experience." Participant 6, therefore, suggested that "organizations ensure a healthy population of women and minorities at the lower level before advancing them to senior-level positions after thorough training to get the experience and maturity to advance within the organization." Bouten-Pinto (2016) noted that workplace diversity should be inclusive of all aspects of diversity that matter to the employees and not just those mandated by or sanctioned through organizational directives or legislation. Participant 6 emphasized that "it would be counterproductive not to have diversity and inclusion in the organization's cyber team and instead use a quota or token system to satisfy the diversity efforts." Participant 6, therefore, suggested that "cyber teams in organizations have diversity and inclusion programs in every aspect to ensure that the doors remain open for women and minorities to advance within the cyber team to overcome the challenge of using quota or token systems." Participant 6's suggestions demonstrate alignment with Schein's (1992) concept, which emphasized that "organizations must embrace diversity and inclusion to attain sustainable success instead of only conforming to uniformity." Participant 7 noted that "the utilization of consultants from consulting firms instead of directly recruiting cybersecurity professionals has been an unsuccessful strategy to recruit and retain cybersecurity professionals because it

involves seeking a level of control that they don't have as the consultants often have total control, thus making it challenging to implement and reinforce their retention strategies." Participant 7 indicated that "a significant threat to the application of their attraction, recruitment, and retention best practices is that organizations, small, medium, and large, face a scarcity of cybersecurity professionals." Participant 7 explained that "the supply of cybersecurity professionals and the ability to retain them is not at parity with the nature of the emerging cyber threats." Participant 7 further noted that "finding effective and robust cybersecurity talent is a tough and challenging undertaking at the moment as all organizations have to draw from the same reservoir at the end of the day, regardless of whether they are looking to protect their infrastructure or provide security as a service." Participant 7 pointed out that "the industry isn't meeting the demand for diverse cybersecurity professionals as fast as they should, thus making the scarcity of cyber talent the most significant challenge that their organization faces."

Participant 8 pointed out that "the effect of their strategies to attract, recruit, and retain diverse cybersecurity professionals on the cybersecurity teams' performance to protect sensitive systems is significant because they would like to see a more diverse workforce whenever possible." Participant 8 noted that they "encourage all candidates to apply but still try to find that one candidate that does represent different types of diversity." Participant 8 indicated that their "organization certainly wants to interview and recruit diverse candidates, particularly women, even though they find it challenging to increase the number of women who apply for the positions due to their organization's very rigid hiring practices, which they have to follow strictly." Participant 8 emphasized

that “they do not go to women's forums after they post a job to pitch the job because of the nature of their organization that mandates them to follow very stepwise rules in the recruitment process.” Participant 8, however, shared that “under their organization’s current hiring practices, more and more qualified women would have to apply for there to be a better chance of getting those qualified women into the positions.” Participant 8 further highlighted that “even though few women apply for the jobs in the first place, the ones that do apply often do not have the necessary skills for the positions.” Participant 8 stressed that “the cybersecurity field is a very competitive market, and their organization’s very structured and stringent rules on how you hire people in general, not just cybersecurity, makes it particularly difficult for people within cybersecurity to go through their hiring process as well as find qualified candidates to offer competitive remuneration that they'll accept.” Participant 8 highlighted that “the difficulties of making competitive offers from the financial point of view contribute to the challenges of hiring the right cyber talent.” However, participant 8 firmly believes that “given the highly competitive nature of the cybersecurity industry, organizations should offer excellent benefits and a good work-life balance that they could pitch to help attract, recruit, and retain diverse cyber talent in their organizations.” In other words, “pitching the working conditions to candidates versus the salary to attract, recruit, and retain cybersecurity professionals.” Participant 9 pointed out that their “day to day challenges with attracting, recruiting, and retaining cybersecurity professionals to meet the demands of intrusion and prevention of cyberattacks often emerge after the professional is recruited because if it turns out that the cybersecurity professional does not have enough

knowledge for the target area or environment, they would have to be trained in those areas where the operation is focused." Thus, once again cautioning that "it is challenging to recruit professionals who do not have the knowledge and experience in cybersecurity unless the organizations plan to train and develop the employee."

Participant 11 emphasized that while they do not differentiate between their strategies to attract, recruit, and retain cyber talent, their "organization and their recruiters always endeavor to attend different job fairs and college campus experiences in schools such as Morehouse, Gwinnett Tech, or Georgia Tech." Participant 11 noted that typically, "while they are at these job fairs, they share the job opportunities their organization has to offer and engage diverse individuals to get a sense of the talent that's out there to ensure they have a well-rounded team and a well-rounded organization." Participant 11 further noted that although they do not have formal recruitment strategies, they'll refer to as ineffective and inefficient, at times "when the need to fill a role arises, and they do not have a candidate that represents diversity with the necessary skill set, they tend to focus on only the individual's experience." Thus, *participant 11* "indicated that recruiting candidates without knowledge and experience would be an ineffective strategy for their organization unless training and development plans are in place." Participant 11 indicated that there are "some challenges with the application of their best practices to retain diverse cyber talent due to the intensely competitive nature of the cybersecurity workforce where there are more job opportunities than there are qualified candidates." Participant 11 pointed out that "retaining the right cyber talent has been the biggest challenge in part due to the slow upward mobility or advancement from, for instance, an

analyst to an engineer, an engineer to a manager, and a manager to a director position. In other words, retention efforts are negatively impacted when the opportunities to grow are not available." Participant 12 found "referring other people to advertised jobs to be their least effective and efficient strategy because, for some reason, they haven't had any successes with that approach." However, participant 12 emphasized that "everyone is given the same opportunity to apply for the roles, as they recruit through a wide range of avenues, including the use of LinkedIn and specialized cybersecurity recruiters." Participant 12 elaborated that "the culture of their organization, being a government agency, makes it challenging to attract top talent because the wages are a lot less than what the private sector pays their cybersecurity professionals." Participant 12 highlighted a scenario, where she recruited an employee with limited knowledge and experience from the help desk team and then mentored, trained, and developed that employee for three years to help her understand everything about cybersecurity since she already had some IT experience and knowledge but not the necessary skills for a role in cybersecurity. However, "the challenge was that she eventually left for the private sector," but while she was disappointed to see her go, she felt good about the relationship and her growth. Participant 12 shared that when the ex-team member was "recruited in the private sector, she had a wealth of impressive skills to offer above and beyond other candidates, thanks to her mentoring, training, and development efforts, which positively paid off." Participant 12 pointed out that "the skillset acquired included many different areas in cybersecurity as it relates to governance, incident response, and security awareness." Participant 12 cautioned that" although you eventually realize that there is always the

possibility that if you train up a cyber talent, they may leave to another position where they are offered better career growth, it should not deter any good cyber leader or good mentor from training and developing a cyber talent." Table 5 below highlights the number of references related to the theme of Overcoming Challenges to Cyber Talent Attraction, Recruitment, and Retention.

Table 5

Frequency of Fifth Major Theme: Overcoming Challenges to Cyber Talent Attraction, Recruitment, and Retention

	Participant		Documents	
Major theme	Count	References	Count	References
Overcoming challenges to cyber talent attraction, recruitment, and retention	12	58	20	61
Minor themes				
Avoid using a quota or token to Satisfy Diversity	2	2	2	5
Avoid using wages to attract Talent	12	15	8	12
Focus on leveraging other benefits	12	19	20	22
Avoid non-progressive cultures	5	9	7	13
Get individuals to see the opportunity	12	13	6	9

Applications to Professional Practice

The following discourse is meant to address the specific IT problem identified in the problem statement, namely that some cybersecurity leaders lack strategies to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive systems from rising threats. This research might contribute to IT practice as participants in the study provided detailed descriptions of strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive information from rising threats. The study

findings showed that highly valuing all diversity impacts the performance of cybersecurity teams significantly because people of varying backgrounds with different understandings, lenses, education levels, and thought processes contribute to the quick and comprehensive resolution of problems than having a single approach to it. Further, the findings of the study showed that a more diverse and inclusive team positively and significantly impacts the performance of cybersecurity professionals because a more varied cyber workforce can tackle cyber-related problems from different lenses, a variation of thought, understanding, and approach instead of having a single standard approach to solving the issues. The findings of this study aligned with Schein's (2010) concept of organizational culture that portrays the same set of beliefs, norms, and values as other national cultures which affects the employees' sense of belonging, motivation, satisfaction, and commitment, and in turn increases performance, profits, and organizational effectiveness.

Cybersecurity leaders might use the results of this study to assess the efficiency and effectiveness of their cyber teams in reducing the proliferation and vulnerability of sensitive systems and infrastructure, which increases as new threats emerge from diverse cybercriminals with new evolving techniques and creative ways to infiltrate and compromise computer systems. The foundation for successfully protecting U.S. national security and economic prosperity to maintain a competitive advantage relies on the nation's private and public sector cybersecurity workforce (U.S. Secretary of Commerce & U.S. Secretary of Homeland Security, 2018). The findings of the study revealed that it is imperative for cybersecurity leaders in both government agencies and organizations to

maintain a culture of teamwork, recognition, collaboration, collective goal, mission, internal cooperation, and trust which encourages participation and proactive knowledge sharing to enable the diverse cyber teams to solve complex problems and perform their cyber functions and missions unhindered to their highest potential. Rick Van der et al. (2017) suggested that the focus should be on identifying areas for team improvements and on potential solutions by increasing team members' skills level, knowledge, technical resources, participation, and cooperation to close the gaps between current and desired incident handling practices. The findings of the study showed that cybersecurity leaders promote open working environment that is highly adaptive and encourages the use of proper communication and interpersonal skills to enable diverse cyber teams to work together quickly, efficiently, and effectively to minimize potential misunderstandings, mainly when communicating with non-technical staff about the need for security awareness in organizations. Chen et al. (2014b) found that a blend of technical and interpersonal skills is critical for the role of CSIRTs, which makes finding talents to fill the positions challenging. Improved security awareness in the organization will help limit or prevent cyberattacks in the organization. An open, collaborative, and participatory culture might facilitate and accelerate the rate of identification of malware and security loopholes through different lenses, thoughts, and approaches. DHS (2015) suggested that a diverse CSIRT assists operators of critical systems by responding to incidents, restoring services, analyzing potentially broader cyber or physical impacts to critical infrastructure, locating cyber threats, and determining the best prevention mechanisms. Cybersecurity leaders might change their perception of who the hacker is and who the cybersecurity

since the study findings indicated that the image portrayed by the media of the hacker being Caucasian male with a long ponytail and a hoodie is false. Since the hacker or cybercriminal could be anyone, cybersecurity leaders might increase their understanding of the need to have diverse cybersecurity teams to tackle the diverse nature of the unrelenting cyberattacks.

Cybersecurity is not just a technical issue rather a business and risk management issue. Therefore, the value created by including women and minorities in cyber warfare and risk management might translate into more secure and safer information systems (Bagchi-Sen et al., 2010; Dunn Cavelty, 2014). The findings of the study indicated that cybersecurity leaders might enhance business value through the effects of the strategies to attract, recruit, and retain diverse cybersecurity professionals that showed significant impact based on a 50% to 90% increase in diversity which translated to higher performing, overachieving, and more driven cyber teams. The findings of the study also indicated that top leadership support for more competitive benefit and remuneration packages and increased budgetary authority for CISO's to help with the attraction, recruitment, and retention efforts of diverse cybersecurity professionals might significantly and positively boost the performance and confidence of diverse cybersecurity teams.

This study might give cybersecurity leaders a broader understanding of the best strategies, attributes, skills, and qualifications to increase diversity in cybersecurity teams and enhance their effectiveness to protect sensitive information from rising cyber threats. The findings of the study showed that cybersecurity leaders should continuously train and

develop their cybersecurity teams to ensure that they are conversant with the latest tools and skills to tackle cyber threats. These tools and skills include incident planning, handling and response, intrusion detection, intrusion prevention, vulnerability analysis, malware analysis, penetration testing, scanning and management, governance, security awareness, and so on. Addressing the shortage of women and minorities in cybersecurity teams requires connecting with them as they enter elementary, middle, and high schools, investing in training, mentoring, advancement, and sponsorship programs, as well as creating more inclusive workplaces (Lemos, 2017; Liu & Murphy, 2016; Pusey et al., 2016) to kept them up-to-date with trends in cybersecurity to better protect sensitive systems. The findings of the study showed that having a centralized database of qualified diverse cyber talent might facilitate access to skilled cyber teams when the need arises to urgently tackle a cyberattack successfully. Given the gap in the literature, this research might contribute to the body of academic knowledge and practice in this area. The findings of this study aligned with Schein's (1999) concepts of OCT on (a) creating motivation for change by discarding any legacy culture. (b) learning from past deficiencies and embracing new opportunities and potential solutions. (c) providing clear and concise targets for change. (d) providing comprehensive formal and informal training of teams and groups. (e) providing role models and mentors. (f) promoting continuous employee involvement. (g) providing opportunities to offer input and feedback. (h) making available support groups to share ideas and address any concerns. (i) creating, choosing, and editing suitable cultural artifacts, behaviors, forms, and collaboration approaches. (j) building charismatic leaders. (k) creating a feasible and reasonable

migration plan. (l) addressing risks, benefits, and remediation strategies. The findings of this study might provide the foundation for further research on this topic.

Implications for Social Change

The strategies to attract, recruit, and retain diverse cybersecurity professionals might help increase the cybersecurity workforce to efficiently and effectively protect sensitive information from rising cyber threats. The findings of this may provide societal value by improving diversity and inclusion, work-life balance, morale, and stress-levels in the cyber workforce to enable cyber teams to execute cybersecurity functions and missions promptly with a variation of thought and lenses to ensure better protection of protected health information and personally identifiable information. Approaching cybersecurity issues through different lenses and a variation of thought might enhance the efficiency and effectiveness of the cybersecurity professionals that protect sensitive information and those that benefit from the protection through the reduction in the fraudulent use of personal health information and personally identifiable information. Increased productivity might indicate that cybersecurity professionals and beneficiaries accomplish their work tasks in less time, decreasing the stress levels of both cybersecurity professionals and owners of sensitive information. Diminished work stress levels might subsequently improve employee morale and productivity.

The results of the study might also contribute to social change by improving diversity and inclusion to help cybersecurity leaders to create opportunities and bridge the gap in the attraction, recruitment, retention, and advancement of women and minority cybersecurity professionals. The findings from this study might guide effective

intervention programs for gender equity in the cybersecurity workforce and STEM fields as a whole. The study might enlighten middle schools, high schools, colleges, and universities on the need to hire a more diverse team of STEM-oriented instructors and teachers as role models and mentors for the students who might pursue a career in cybersecurity. The society might benefit by the cybersecurity leaders in both government agencies and the private sector helping to grow and change the mindset of the younger candidates in elementary, middle, and high schools, by setting up after school cybersecurity boot camps to nurture, engage, teach new skills, and capture their interests in the cybersecurity field at a tender age while ensuring and creating unique opportunities for them in the cybersecurity field once they graduate.

The study findings showed that individuals could be taught the technical aspect but not how to collaborate, communicate, work with others, get along with people, and deal with conflicts and various personalities. Diversity and inclusion naturally promote, builds, and encourages interpersonal skills, which the study participants consider to be a crucial often-overlooked skill to successfully communicate with non-technical staff in lay terms so that they understand and work together to meet the business objectives in a secure environment. Cybersecurity leaders will benefit from learning how to attract individuals to a collaborative and welcoming culture with an open-door policy to enable cyber teams to share ideas, knowledge, information, trust, respect, and belief in one community to solve complex problems with the same goals and state of mind. The society cannot function without interpersonal skills and will benefit from people's improved ability to get along and work together for the common good.

Recommendations for Action

I explored strategies used by cybersecurity leaders to attract, recruit, and retain cybersecurity professionals to effectively and efficiently protect sensitive systems from rising cyber threats. The study findings showed that valuing all diversity, setting the right tone on culture, and top leadership support and continuous training and development may enable cyber teams to execute cybersecurity functions and missions promptly with a variation of thought, lenses, approach, and understanding. The cybersecurity leaders from the case organizations that participated in this research all aligned with the concepts of OCT, the conceptual framework for this study.

Cybersecurity leaders should proactively and formally make it mandatory to continuously train, develop, and grow cybersecurity professionals within the organization to make the teams very proficient and well versed in minimizing cyber threats and protecting sensitive systems from cyberattacks while increasing the retention rate of cyber talent and keeping them up to date with the current trends in cybersecurity. Cybersecurity leaders should also consider mentoring potential candidates who show an affinity to join the cyber workforce to increase the attraction and recruitment rate and get them up to speed to quickly adapt to the fast-paced world of mitigating evolving cyber threats while creating opportunities to work in the cybersecurity field. Potential cybersecurity candidates applying to join the cyber workforce should have at least a fundamental training and knowledge of the language used in the world of cybersecurity whenever possible, although they could be recruited with limited knowledge in cybersecurity and then undergo advanced training once they successfully join the cyber

workforce. The fundamental cybersecurity knowledge should include firewalls, anti-malware, access controls, cryptographic software, antivirus software, social engineering, phishing scam, spoofing emails, etc. The advanced training, once the candidates are recruited, should include topics such as incident planning, handling and response, intrusion detection, intrusion prevention, vulnerability analysis, malware analysis, penetration testing, scanning and management, governance, security awareness, and so on. Organizations should also offer tuition reimbursement to those professionals that decide to expand and strengthen their knowledge in cybersecurity while working for the organization as part of the benefits package to increase the rate of retention of cybersecurity professionals, particularly in government agencies where the pay is significantly less than the private sector.

Cybersecurity leaders must maintain an inclusive, diverse, supportive, and tolerant approach to attracting, recruiting, and retaining cyber talent to enable them to innovate, grow, explore and effectively and efficiently provide solutions to cybersecurity issues. It is evident that highly valuing all diversity, including backgrounds, gender, age, perspective, personality, temperament, significantly impacts cyber talent attraction, recruitment, and retention process. Organizations should improve diversity based on gender, race, culture, and background by being more intentionally diverse and inclusive. It is imperative for the cybersecurity workforce in government agencies and the private sector to maintain a unique, diversified, and inclusive recruitment policy that embraces cyber teams from all ethnic backgrounds as everyone offers something unique. A diversified cyber workforce is critical to dealing with the threats that organizations face

because those cyber threats are global and diverse hence the need to attract, recruit, and retain diverse candidates from all backgrounds and cultures to ensure full and effective coverage to defend and protect the organization's assets. Cybercriminals are from different backgrounds, nationalities, races, and genders; therefore, cybersecurity teams must be as diverse as the cybercriminals to be able to understand their plots to protect sensitive systems from the cyber attacks. The findings of the study showed that a more diverse and inclusive team positively and significantly impacts the performance of cybersecurity professionals because a more diverse cyber workforce can tackle cyber-related problems from different lenses, a variation of thought, understanding, and approach instead of having a single standard approach to solving the issues. Organizations should not minimize or eliminate their pursuit of diversity and inclusion toward protecting sensitive systems as it would be counterproductive to the organization and its cybersecurity team’s efforts to effectively and efficiently mitigate and protect systems against cyberattacks. Therefore, maintaining the status quo on diversity and inclusion in the cyber workforce by not bringing everyone on board, including women and minorities, especially the young girls, might be detrimental to the cybersecurity industry. There was a consensus among the majority of the participants that the perception of who the hacker is and who the cybersecurity is should change because of the false image portrayed by the media of the hacker being Caucasian male, with a long ponytail and a hoodie. The study findings show that the hacker could be anyone, and therefore, the cybersecurity professionals should be diverse to tackle the diverse nature of the cyberattacks.

The findings of the study showed that it is critical to ensure that the culture of the organization aligns with the beliefs and personality of cyber talent. Therefore, it is crucial for organizations to set the right tone on culture to attract and recruit potential candidates who fit the culture, subscribe to it, practice it, and celebrate it. Cybersecurity leaders should also attract cyber talent to the culture of the organization and what they stand for while getting them sold on why they are a good fit for the role and why the position is important instead of focusing on the benefits package, which can be matched by any other organization. Cybersecurity professionals who are attracted to the excellent organizational culture, lifestyle, and promising benefits tend to stay with the organization for a long time while protecting the organization's infrastructure from cyber threats. It is evident that a work environment that is inclusive, friendly, pleasant, collaborative, stress-free, welcoming, flexible, comfortable, and open significantly and positively encourages participation, increases interest in the role, promotes and boosts the performance of cybersecurity teams, and increases retention rate without negatively impacting high expectations within the cyber team. It is also imperative that organizations maintain a culture of teamwork, recognition, collective goal, mission, and internal cooperation while celebrating every culture, including Black History Month, Divali, and so on. An organizational culture that promotes regular communications with the cyber leaders is vital to encouraging the team to bring any concerns, issues, desires at any time so that they are addressed efficiently while increasing trust among the team and facilitating the sharing of ideas to solve cybersecurity problems with the same goals and state of mind. Therefore, cybersecurity leaders should continuously nurture the culture of their

organization like a relationship to attract, recruit, and retain cyber talent to mitigate continually evolving cyber threats rather than just setting the culture and ignoring it.

Top leadership support is critical to implementing diversity and inclusion programs in the public and private sectors to successfully attract, recruit, and retain cybersecurity professionals. Kundu and Mor (2017) emphasized that for leaders and managers, diversity management should go much further than just complying with existing regulations or reacting to changes in the labor market. Therefore, it is crucial for top leadership to facilitate buy-in by sharing with potential candidates and existing employees that the organization genuinely believes in diversity and wants to build a diverse and inclusive workforce that supports their growth and advancement. Organizations need to drive a top-down diverse cyber talent policy-centric recruitment and retention approach from the highest level of executive leadership while signing off high-level diverse cybersecurity recruitment and retention policies. It is essential for every organization to have an internal and external advocate in the form of top leadership who understands that diversity can bring excellent quality work to the organization and help cybersecurity professionals who are trying to get into the organization while adding value to the organization. Due to the shortage of diverse cybersecurity personnel, organizations should consider decoupling the relationship between CIO's and CISO's by allowing CISO's to have their budgets towards the attraction, recruitment, and retention efforts of diverse cybersecurity professionals as doing so would help boost the confidence of the cybersecurity professionals who protect vital infrastructure from aggressive cyber threats. The cybersecurity leaders in the government agencies, in particular, should be

willing to lower the standards for cyber talent recruitment by bringing in individuals with limited talent but with the potential to learn, train, and be developed in the cybersecurity space to compensate for the low wages compared to those paid to the cybersecurity professionals in the private sector.

The findings of the study showed that there were mixed opinions about the best approach to attract, recruit, and retain diverse cyber talent to the cybersecurity workforce. Majority of the participants expressed concerns with recruiting inexperienced and qualified candidates, noting that they may not perform their tasks efficiently and effectively, and even if they are trained and developed internally, after being hired, there is a high probability that the cybersecurity professionals may eventually leave the organization or government agency for better career prospects since security is always in demand. However, due to the shortage of qualified cybersecurity professionals and the competitive nature of the cyber workforce, cybersecurity leaders should consider recruiting potential candidates at the lower levels and then grow and develop the cyber talent to improve recruitment and retention efforts to protect their sensitive systems from cyberattacks. In the government sector, where wages are predominantly low compared to the private sector, increasing the salaries to match those of the private sector might be beneficial in attracting, recruiting, and retaining diverse cybersecurity security professionals to protect sensitive systems. If the wages of cybersecurity professionals, particularly in the government agencies, continue to remain stagnant, cybersecurity leaders in those agencies should focus on the individual by promoting excellent working conditions and investing in training and development. In the private sector, where there is

more aggressive competition for cybersecurity professionals, monetary incentives are not enough to retain existing cybersecurity talent. Ovidiu-Iliuta (2014) noted that it is critical to retain key employees that are adequately integrated, highly coordinated, and aware of the organizational goals, core values, norms, and behavior while implementing practices that enhance career development and job security. Therefore, cybersecurity leaders should consider a combination of better wages, training, development, and excellent organizational culture to attract, recruit, and retain diverse cyber talent. Some participants were adamant about mainly using monetary incentives to attract, recruit, and retain cyber talent while some embraced the idea of combining competitive wages with the organizational culture and lifestyle to promote attraction, recruitment, and retention of cyber talent. There were also mixed opinions among participants about whether to attract and recruit potential candidates straight from college, through job fairs in colleges and boot camps. Some cybersecurity leaders found it to be successful and therefore recommend attracting and recruiting talent via those channels. Some other participants expressed their sentiments of training them only to let them go after they are trained to better job prospects. However, most of the participants suggested recruiting via LinkedIn and working with specialized cybersecurity recruiters to find potential diverse cyber talent. Cybersecurity leaders in both government agencies and the private sector should also target the younger candidates at the elementary, middle, and high school levels, by setting up cybersecurity boot camps to nurture and capture their interests in the cybersecurity field at a tender age while ensuring that they will have opportunities for them in the cyber workforce once they graduate.

Recommendations for Further Study

My multiple recommendations for further research stem from the limitations of the study and the findings associated with this research. The limitations of this study include the qualitative nature of this research, the subjective process of theme artifacts and dialogue interpretation that could introduce bias into the research, and the lack of qualitative research findings generalizability. During this qualitative collective case study, I interviewed 12 cybersecurity leaders in three government agencies and nine IT organizations that work in the Atlanta Metropolitan Area of Georgia, USA, with extensive backgrounds in cybersecurity education, training, and recruitment of cybersecurity professionals.

The first set of recommendations is for researchers to conduct additional qualitative studies of similar study design and varying participant sizes with cybersecurity leaders in East, West, North, and South regions of the United States to compare their findings with this study's findings to help address the generalizability and potential bias concerns. Two participants of this study pointed out that Atlanta, Georgia, USA was unique because they celebrate and embrace diversity compared to other parts of the country, for instance, further north, where it is apparent that diversity isn't embraced as much.

The second set of recommendations focuses on further exploration, and a more in-depth examination of the identified themes in this study as this would help reveal and introduce additional perspectives not represented in this study. I used Schein's OCT as the conceptual framework for this study. Researchers could conduct further studies using

either OCT again or a combination of both OCT and the leadership pipeline model (LPM) as the conceptual frameworks for the study to compare findings. The LPM creates opportunities for new knowledge on multidimensional levels for leaders within various organizations to gain an understanding of the importance of developing talents within the organization to become leaders (Charan, Drotter, & Noel, 2011). The combination of these two conceptual frameworks might be necessary to further explore the research problem in an in-depth manner and assist in the data interpretation. Insights gained from the recommended further study would be invaluable toward creating a comprehensive set of strategies that cybersecurity leaders could use all over the United States to attract, recruit, and retain cybersecurity professionals to effectively and efficiently protect sensitive systems from cyberattacks.

Conversely, as a counter to the above recommendations and because of the maturity level of the responses to interview questions in this study which were representative solely of the organizations used in the study, researchers could conduct a quantitative study to measure the extent to which organizational culture and diversity and inclusion influences the strategies that cybersecurity leaders use to attract, recruit, and retain cybersecurity professionals to protect sensitive systems from cyberattacks.

Reflections

Having been in the IT and security field for over two decades, I wrongly assumed that pursuing a doctoral degree in IT would be a straightforward and smooth journey. The pursuit of obtaining a doctoral degree is demanding and requires time, effort, sacrifices, patience, perseverance, and maintaining focus. The passion for my research topic

motivated and made me determined to push forward, overcome all obstacles, and complete the program. During this process, I quickly learned the art of scholarly writing, conducting research, and critical and analytical thinking. These skills have had a significant positive impact on my professional career far more than I envisioned, and they have been an invaluable addition to my skillset. Overall, I enjoyed learning, conducting research, discussing research, and collaborating with instructors and fellow DIT students during my DIT journey.

This qualitative case study explored strategies used by cybersecurity leaders to attract, recruit and retain cybersecurity professionals. I learned a lot of valuable information from the participants about the need to have a more diverse and inclusive cybersecurity workforce to better protect sensitive systems from rising cyberattacks. The data collection and analysis were exciting, enlightening, and rewarding. I did face some challenges with scheduling interview times with some participants due to the busy schedules of the cybersecurity leaders. As a result, the data collect and member checking of the data from the participants took five weeks. However, once the participants were onboard, they embraced the process with an attitude of wanting to contribute and share their knowledge, experiences, and thoughts regarding the phenomenon under study. I appreciate their participation very much.

Due to the semi-structured nature of the interview questions and being a consultant in the IT and cybersecurity field, I may have unintentionally or unknowingly introduced some bias to the study. However, I made every effort to remain objective and not inject any potential personal bias or preconceived notions into my data collection,

analysis, and results throughout the research study. To ensure the reliability and credibility of this study, the findings presented are directly traceable to triangulated evidence, thus attempting to proactively mitigate any potential data skewing during collection, analysis, and reporting.

Summary and Study Conclusions

Cyber threats are global and diverse; therefore, it is critical for cybersecurity professionals who mitigate and prevent these threats to be diverse. Diversity brings value to the organization, and the diverse cybersecurity teams with unique backgrounds, lenses, ideas, thoughts, understanding, perspectives, and approaches contribute differently to the comprehensive resolution of complex cybersecurity functions and missions to protect sensitive systems from continuously evolving and rising cyberattacks.

Cybersecurity leaders should set the right tone on culture and continuously nurture it like a relationship while ensuring that the culture of the organization and work environment is inclusive, friendly, pleasant, collaborative, stress-free, welcoming, flexible, comfortable, tolerant, and open to significantly and positively encourage participation, boost cyber team performance, and increase the attraction, recruitment, and retention rate. Organizations must maintain a culture of teamwork, recognition, collective goal, proper communication, and cooperation while celebrating every culture to facilitate the sharing of ideas to effectively and efficiently solve cybersecurity problems. The use of OCT helps cybersecurity leaders in government agencies and IT organizations to maintain a culture of openness and teamwork.

Given the shortage of cybersecurity professionals and underrepresentation of women and minorities in the cyber workforce, top leadership in the public and private sectors must be engaged to genuinely implement and maintain diversity and inclusion programs that support growth and advancement to successfully attract, recruit, and retain cybersecurity professionals. Organizations must drive a top-down diverse cyber talent policy-centric recruitment and retention approach to facilitate buy-in.

Cybersecurity leaders should proactively and continuously train, develop, and grow cybersecurity professionals within the organization and attract and recruit qualified cybersecurity professionals whenever possible as well as candidates at the lower levels who show affinity to join the cyber workforce and have the potential to be mentored, trained and developed into highly proficient cybersecurity professionals to prevent and protect sensitive systems from cyberattacks.

References

Abdul-Alim, J. (2017). Expert: Diversifying cybersecurity starts with ‘targeted recruiting.’ *Diverse: Issues in Higher Education, 34*(16), 8-9. Retrieved from http://diverseeducation.com/article/100254/

Abel, R. (2017). Priming the pipeline: Early education efforts are key to filling cybersecurity talent and gender gaps. *For IT Security Professionals (15476693), 28*(4), 24-27.

Adams, K. M., Hester, P. T., Bradley, J. M., Meyers, T. J., & Keating, C. B. (2014). Systems theory as the foundation for understanding systems. *Systems Engineering, 17*(1), 112-123. Retrieved from https://digitalcommons.odu.edu/emse_fac_pubs/32/

Ahmed, A., & Othman, I. (2017). Relationship between organizational resources and organizational performance: A conceptualize mediation study. *European Online Journal of Natural and Social Sciences, 6*(1), pp. 10-27. Retrieved from https://www.researchgate.net/publication/313915413_Relationship_between_Organizational_Resources_and_Organizational_Performance_A_Conceptualize_Mediation_Study

Ahrens, T., & Khalifa, R. (2013). Researching the lived experience of corporate governance. *Qualitative Research in Accounting and Management, 10*(1), 4-30. doi:10.1108/11766091311316176

Alejandro, A. T. (2017). National security implications of cyber threats. *Política Y Estrategia, 0*(125), 83-96. doi:10.26797/rpye.v0i125.44

Aleti, A., Buhnova, B., Grunske, L., Koziolek, A., & Meedeniya, I. (2013). Software architecture optimization methods: A systematic literature review. *IEEE Transactions on Software Engineering*, 39, 658-683. doi:10.1109/TSE.2012.64

Alghamdi, F. (2018). Total quality management and organizational performance: A possible role of organizational culture. *International Journal of Business Administration, 9*(4), 186. doi:10.5430/ijba.v9n4p186

Alhadid, A. Y. (2016). The relationship between leadership practices and organizational performance. *International Journal of Business Administration, 7*(3). doi:10.5430/ijba.v7n3p57

Ali, A., & Zhang, W. N. (2015). CEO tenure and earnings management. *Journal of Accounting & Economics*, 59, 60-79. doi:10.1016/j.jacceco.2014.11.004

Alvesson, M., & Sveningsson, S. (2015). *Changing organizational culture: Cultural change work in progress.* New York, NY: Routledge.

Amankwaa, L. (2016). Creating protocols for trustworthiness in qualitative research. *Journal of Cultural Diversity*, *23*(3), 121-127. Retrieved from http://tuckerpub.com/jcd.htm

Amegashie, A. R. (2018). *Diversity management program strategies to support competitive advantage and sustainable growth* (Order No. 10822480). Available from ProQuest Dissertations & Theses Global. (2046948194).

Andriole, S. J. (2015). The need for new business-technology relationships. *IT Professional, 17*(4), 4-6. doi:10.1109/MITP.2015.60

Anney, V. (2014). Ensuring the quality of the findings of qualitative research: Looking at

trustworthiness criteria. *Journal of Emerging Trends in Educational Research and Policy Studies,* 5, 272-281. Retrieved from http://jeteraps.scholarlinkresearch.com/index.php

Ardakani, M. S., Abzari, M., Shaemi, A., & Fathi, S. (2016). Diversity management and human resources productivity: Mediating effects of perceived attractiveness, organizational justice, and social identity in Isfahan's steel industry. *Iranian Journal of Management Studies, 9*(2), 407-432. doi:10.22059/ijms.2016.56412

Aravamudhan, N. R., & Krishnaveni, R. (2015). Establishing and reporting content validity evidence of training and development capacity building scale (TDCBS). *Management Journal of Contemporary Management Issues, 20*(1), 131-158. Retrieved from https://www.researchgate.net/publication/282301599_Establishing_and_reporting_content_validity_evidence_of_new_training_and_development_capacity_building_scale_TDCBS

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT Professional, 12*(1), 24-31. https://doi.org/10.1109/MITP.2010.39

Barczak, G. (2015). Publishing qualitative versus quantitative research. *Journal of Product Innovation Management, 32*(5), 658. doi:10.1111/jpim.12277

Barnes, J. (2015). Qualitative research from start to finish (2nd ed.). *Neuropsychological Rehabilitation,* 1-3. doi:10.1080/09602011.2015.1126911

Barnham, C. (2015). Quantitative and qualitative research: Perceptual foundations.

International Journal of Market Research, 57(6), 837-854. doi:10.2501/IJMR-2015-070

Barratt, M. J., Ferris, J. A., & Lenton, S. (2015). Hidden populations, online purposive sampling, and external validity: Taking off the blindfold. *Field Methods,* 27, 1-19. doi:10.1177/1525822X14526838

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

Beard, K. (2014). Million women mentors *launched* to fill the gap of women in STEM fields. Retrieved from https://www.usnews.com/news/stem-solutions/articles/2014/01/09/million-women-mentors-launched-to-fill-the-gap-of-women-in-stem-fields

Beidel, E., & Magnuson, S. (2011). Government, military face severe shortage of cybersecurity experts. *National Defense, 96*(693), 32-34. Retrieved from http://www.nationaldefensemagazine.org/archive/2011/August/Pages/Government,MilitaryFaceSevereShortageOfCybersecurityExperts.aspx

Bell, E. E. (2015). Understanding African American males' schooling experiences: A qualitative inquiry. *The Qualitative Report, 20*(8), 1260-1269. Retrieved from http://www.nova.edu/ssss/QR/QR20/8/bell6.pdf

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

Berry, L. E. (2016). The research relationship in narrative enquiry. *Nurse Researcher,*

24(1), 10-14. doi:10.7748/nr.2016.e1430

Beugelsdijk, S., Slangen, A., Maseland, R., & Onrust, M. (2014). The impact of home-host cultural distance on foreign affiliate sales: The moderating role of cultural variation within host countries. *Journal of Business Research,* 67, 1638-1646. doi:10.1016/j.jbusres.2013.09.004

Booth, A., Sutton, A., & Papaioannou, D. (2016). *Systematic approaches to a successful literature review.* Sage.

Bourke, B. (2014). Positionality: Reflecting on the research process. *Qualitative Report, 19*(33), 1-9. Retrieved from http://www.nova.edu/ssss/QR/QR19/bourke18.pdf

Bouten-Pinto, C. (2016). Reflexivity in managing diversity: A pracademic perspective. *Equality, Diversity, and Inclusion: An International Journal, 35*(2), 136-153. doi:10.1108/edi-10-2013-0087

Briody, E. K., & Ferraro, G. P. (2017). *The Cultural Dimension of Global Business.* Routledge.

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

Buchler, N., Rajivan, P., Marusich, L. R., Lightner, L., & Gonzalez, C. (2018). Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition. *Computers & Security, 7*(3), 114-136. doi:10.1016/j.cose.2017.10.013

Burrell, D. N., & Nobles, C. (2018). Recommendations to develop and hire more highly qualified women and minorities cybersecurity professionals. *Proceedings Of The International Conference On Cyber Warfare & Security*, 75-81.

Burrell, D. N., Aridi, A. S., & Nobles, C. (2018). The critical need for formal leadership development programs for cybersecurity and information technology professionals. *Proceedings Of The International Conference On Cyber Warfare & Security*, 82-91. Retrieved from https://search.proquest.com/openview/12cbf1c24ddb996f0f01a81fd12f4a4d/1?pq-origsite=gscholar&cbl=396500

Büschgens, T., Bausch, A., & Balkin, D. B. (2013). Organizational culture and innovation: A meta-analytic review. *Journal of Product Innovation Management,* 30, 763-781. doi:10.1111/jpim.12021

Busse, C., Kach, A., & Wagner, S. (2016). Boundary conditions: What they are, how to explore them, why we need them, and when to consider them. *Organizational Research Methods,* 1-36. doi: 10.1177/1094428116641191

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security, 7*(5), 24-35. doi:10.1016/j.cose.2018.01.015

Caine, V., Estefan, A., & Clandinin, D. J. (2013). A return to methodological commitment: Reflections on narrative inquiry. *Scandinavian Journal of Educational Research, 57*(6), 574–586. doi:10.1080/00313831.2013.798833

Cameron, K. S., & Quinn, R. E. (2011). *Diagnosing and changing organizational*

culture: Based on the competing values framework. John Wiley & Sons.

Campbell, J., & Göritz, A. (2014). Culture corrupts! A qualitative study of organizational culture in corrupt organizations. *Journal of Business Ethics,* 120, 291–311. doi:10.1007/s10551-013-1665-7

Cao, Z., Huo, B., Li, Y., & Zhao, X. (2015). The impact of organizational culture on supply chain integration: A contingency and configuration approach. *Supply Chain Management: An International Journal,* 20, 24-41. doi:10.1108/ SCM-11-2013-0426

Cardoso, L., Meireles, A., & Ferreira Peralta, C. (2012). Knowledge management and its critical success factors in a social economy organizations. *Journal of Knowledge Management, 16* (2), 267-284.

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

Carlin, A., Manson, D. P., & Zhu, J. (2010). Developing the cyber defenders of tomorrow with regional collegiate cyber defense competitions (CCDC). *Information Systems Education Journal, 8*(14). Retrieved from https://eric.ed.gov/?id=EJ1146949

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

Carter, N., Bryant-Lukosius, D., DiCenso, A., Blythe, J., & Neville, A. (2014). The use of triangulation in qualitative research. *Oncology Nursing Forum, 41*(5), 545-7.

doi:10.1188/14.ONF.545-547

Carter-Sowell, A. R., & Zimmerman, C. A. (2015). Hidden in plain sight: Locating, validating, and advocating the stigma experiences of women of color. *Sex Roles. 73*(9), 399-407. doi:10.1007/s11199-015-0529-2

Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. *Qualitative Report, 21*(5), 811-831. Retrieved from http://nsuworks.nova.edu/tqr/

Castleberry, A. (2014). NVivo 10 [software program]. Version 10. QSR International; 2012. *American Journal of Pharmaceutical Education, 78*(1), 25. doi:10.5688/ajpe78125

Castro, D. (2018). Boosting the cyberworkforce: Amid persistent shortages in cybersecurity positions, what can states do to strengthen their numbers? *Government Technology, 31*(3), 48. Retrieved from http://www.govtech.com/data/Boosting-the- Cyberworkforce.html

Chabinsky, S. (2017). Understanding the distinct and dependent roles of data, privacy, and cybersecurity professionals. *Security: Solutions For Enterprise Security Leaders, 54*(10), 34. Retrieved from https://www.securitymagazine.com/articles/88343-understanding-the-distinct-and-dependent-roles-of-data-privacy-and-cybersecurity-professionals

Chalfant, M. (2017, September 7). Congress wrestles with gaps in cyber workforce. *Hill.* p. 15. doi: 10.1038/363104a0

Champion, M. A., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-based cyber

defense analysis. *2012 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support, Cognitive Methods in Situation Awareness and Decision Support (CogSIMA),* 218. doi:10.1109/CogSIMA.2012.6188386

Charan, R., Drotter, S., & Noel, J. (2011). *The leadership pipeline: How to build the leadership powered company?* (2nd e.d.). San Francisco, CA: Wiley & Sons.

Chatman, J. A., Caldwell, D. F., O'Reilly, C. A., & Doerr, B. (2014a). Parsing organizational culture: How the norm for adaptability influences the relationship between culture consensus and financial performance in high-technology firms. *Journal of Organizational Behavior,* 35, 785-808. doi:10.1002/job.1928

Chen, C., Liao, J., & Wen, P. (2014b). Why does formal mentoring matter? The mediating role of psychological safety and the moderating role of power distance orientation in the Chinese context. *The International Journal of Human Resource Management,* 25, 1112-1130. doi:10.1080/09585192.2013.816861

Cheng, Q., Lee, J., & Shevlin, T. (2016). Internal Governance and Real Earnings Management. *The Accounting Review,* 91, 1051-1085. doi:10.2308/accr-51275

Cho, J. Y., & Lee, E.-H. (2014). Reducing confusion about grounded theory and qualitative content analysis: Similarities and differences. *Qualitative Report, 19*(32), 1-20. Retrieved from http://nsuworks.nova.edu/tqr/

Choi, T.Y., & Eboch, K. (1998). The TQM paradox: Relations among TQM practices, plant performance, and customer satisfaction. *J. Oper. Manag. 17*(1), 59–75. doi:10.1016/S0272-6963(98)00031-X

Chou, S.-W., & Chiang, C.-H. (2013). Understanding the formation of software-as-a-service (SaaS) satisfaction from the perspective of service quality. *Decision Support Systems,* 56, 148–155. doi:10.1016/j.dss.2013.05.013

Cohen, W. J. (2017). *Exploring the strategies needed to increase diversity in the STEM field workforce* (Doctoral dissertation). Retrieved from ProQuest Dissertations and Theses (Order No. 10639399, Colorado Technical University).

Collins, C. S., & Cooper, J. E. (2014). Emotional intelligence and the qualitative researcher. *International Journal of Qualitative Methods, 13*(1), 88–103. Retrieved from http://ejournals.library.ualberta.ca/index.php/IJQM/index

Congress.gov (2018). H.R.3210 - Securely expediting clearances through reporting transparency act of 2018. Retrieved from https://www.congress.gov/bill/115th-/house-bill/3210/text

Connelly, L. M. (2016). Understanding research. Trustworthiness in qualitative research. *MedSurg Nursing Journal, 25*(6), 435-436. Retrieved from https://www.amsn.org/

Costanza, D. P., Blacksmith, N., & Coats, M. (2015). Convenience samples and teaching organizational research methods. *The Industrial-Organizational Psychologist, 53*(1), 137-140. Retrieved from http://my.siop.org/tipdefault

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

Coppel, C. (2016). The cybersecurity crisis. *TD: Talent Development, 70*(11), 14. Retrieved from https://www.td.org/magazines/td-magazine/the-cybersecurity-crisis

Cowley, J. A., Nauer, K. S., & Anderson, B. R. (2015). Emergent relationships between team member interpersonal styles and cybersecurity team performance. *Procedia Manufacturing,* 3, 5110–5117. doi: 10.1016/j.promfg.2015.07.526

Croitoru, G., & Robescu, O. (2014). The impact of organizational culture on management performance for companies in Dambovita. *Revista Economica, 66*(4). Retrieved from http://economice.ulbsibiu.ro/revista.economica/archive/66402croitoru.pdf

Cronin, C. (2014). Using case study research as a rigorous form of inquiry. *Nurse Researcher*, *21*(5), 19–27. doi:10.7748/nr.21.5.19.e1240

Crosman, P. (2017). The secret to reeling in cybersecurity talent at three big banks. *American Banker, 183*(227), 1. Retrieved from https://www.ntsc.org/resources/ntsc-blog/ntsc-board-member-and-us-bank-ciso-jason-witty-featured-in-american-banker-article.html

Cruz, E. V., & Higginbottom, G. (2013). The use of focused ethnography in nursing research. *Nurse Researcher, 20*(4), 36–43. doi:10.7748/nr2013.03.20.4.36.e305

Cruzes, D. S., Dyba, T., Runeson, P., & Host, M. (2014). Case studies synthesis: A thematic, cross-case, and narrative synthesis worked example. *Empirical Software Engineering,* 20, 1634-1665. doi:10.1007/s10664-014-9326-8

Cuthbert, C., & Moules, N. (2014). The application of qualitative research findings to oncology nursing practice. *Oncology Nursing Forum*, *41*(6), 683-5. doi:http://dx.doi.org/10.1188/14.ONF.683-685

Dahlberg, T. A. (2012). Why we need an ACM special interest group for broadening

participation. *Communications of the ACM,* (12). 36. Retrieved from https://www.researchgate.net/publication/262209573_Broadening_Participation_Why_We_Need_an_ACM_Special_Interest_Group_for_Broadening_Participation

Darawsheh, W. (2014). Reflexivity in research: Promoting rigor, reliability, and validity in qualitative research. *International Journal of Therapy & Rehabilitation,* 21, 560-568. doi:10.12968/ijtr.2014.21.12.560

Davenport, T. H., & Prusak, L. (1998). *Working knowledge: How organizations manage what they know*. Boston, MA: Harvard Business School Press.

Dekking, S. A., Van der Graaf, R., & Van Delden, J. J. (2014). Strengths and weaknesses of guideline approaches to safeguard voluntary informed consent of patients within a dependent relationship. *BMC Medicine, 12*(1). doi:10.1186/1741-7015-12-52

De Massis, A., & Kotlar, J. (2014). The case study method in family business research: Guidelines for qualitative scholarship. *Journal of Family Business Strategy, 5*(1), 15-29. doi:10.1016/j.jfbs.2014.01.007

Deming, W. E. (1982). *Out of the crisis.* Cambridge, MA: Massachusetts Institute of Technology, Center for Advanced Engineering Study.

Deming, W. E. (1985). Transformation of western style of management. *Interfaces, 15*(3), 6-11. Retrieved from http://pubsonline.informs.org/journal/inte

Denison, D., Nieminen, L., & Kotrba, L. (2014). Diagnosing organizational cultures: A

conceptual and empirical review of culture effectiveness surveys. *European Journal of Work and Organizational Psychology,* 23, 145-161. doi:10.1080/1359432X.2012.713173

Denzin, N.K. (1978). *Sociological methods: A sourcebook.* New York, NY: McGraw-Hill.

DHS. (2015, September 22). Department of Homeland Security. From Cyber Security Overview. Retrieved from http://www.dhs.gov/cybersecurity-overview

Dikko, M. (2016). Establishing construct validity and reliability: Pilot testing of a qualitative interview for research in Takaful (Islamic insurance). *The Qualitative Report, 21*(3), 521-528. Retrieved from http://nsuworks.nova.edu/tqr/vol21/iss3/6

Doody, O., & Doody, C. M. (2015). Conducting a pilot study: Case study of a novice researcher. *British Journal of Nursing,* 24, 1074-1078. doi:10.12968/bjon.2015.24.21.1074

Donaldson, L. J., Panesar, S. S., & Darzi, A. (2014). Patient-safety-related hospital deaths in England: Thematic analysis of incidents reported to a national database, 2010-2012.*PLoS Med, 11*(6). doi:10.1371/journal.pmed.1001667

Draper, J. (2015). Ethnography: Principles, practice, and potential. *Nursing Standard, 29*(36), 36-41. doi:10.7748/ns.29.36.36.e8937

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics, 20*(3), 701–715. doi:10.1007/s11948-014-9551-y

Ebersole, C. R., Atherton, O. E., Belanger, A. L., Skulborstad, H. M., Allen, J. M.,

Banks, J. B., ... & Brown, E. R. (2016). Many labs 3: Evaluating participant pool quality across the academic semester via replication. *Journal of Experimental Social Psychology*, 67, 68-82.

Edward-Jones, A. (2014). Qualitative data analysis with NVIVO. *Journal of Education for Teaching, 40*(2) 193-195. doi:10.1080/02607476.2013.866724

Elo, S., Kaariainen, M., Kanste, O., Polkki, T., Utriainen, K., & Kyngas, H. (2014). Qualitative content analysis: A focus on trustworthiness. *SAGE Open*, *4*(1), 1–10. doi:10.1177/2158244014522633

Enkh-Amgalan, R. (2016). *The indulgence and restraint cultural dimension: A crosscultural study of Mongolia and the United States* (Undergraduate honors theses). Retrieved from http://dc.etsu.edu/cgi/viewcontent.cgi?article=1354&context=honors

Erkutlu, H. (2012). The impact of organizational culture on the relationship between shared leadership and team proactivity. *Team Performance Management: An International Journal, 18*(1/2), 102–119. doi: 10.1108/13527591211207734

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1-4. Retrieved from http://www.sciencepublishinggroup.com/j/ajtas

Fabian, B., Ermakova, T., & Junghanns, P. (2015). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems,* 48, 132-150. doi:10.1016/j.is.2014.05.004

Faden, R. R., Kass, N. E., Goodman, S. N., Pronovost, P., Tunis, S., & Beauchamp, T. L.

(2013). An ethics framework for a learning health care system: A departure from traditional research ethics and clinical ethics. *Hastings Center Report, 43*(s1), S16–S27. doi:10.1002/hast.134

Fallahpour, M., & Zoughi, R. (2015). Fast 3-D qualitative method for through-wall imaging and structural health monitoring. *IEEE Geoscience and Remote Sensing Letters*, 12, 2463–2467. doi:10.1109/lgrs.2015.2484260

Farmer, J. L. (2014). *Creating the kaleidoscope: An exploratory study of chief diversity officers' role in promoting and sustaining diversity and inclusion in organizations* [Doctoral dissertation]. Available from ProQuest Dissertation and Theses Database. (UMI No. 3617165).

Fattah, A. H. (2017). The effect of organizational culture, leader behavior, self-efficacy, and job satisfaction on job performance of the employees. *Jurnal Terapan Manajemen Dan Bisnis, 3*(2), 102-110. doi: 10.26737/jtmb.v3i2.212

Fink, A. (2013). *Conducting research literature reviews: From the Internet to paper.* Thousand Oaks, CA: Sage.

Fisher, L. M. (2016). A decade of ACM efforts contribute to computer science for all. *Communications of the ACM,* (4). 25. Retrieved from https://cacm.acm.org/magazines/2016/4/200155-a-decade-of-acm-efforts-contribute-to-computer-science-for-all/abstract

Francis, K. A., & Ginsberg, W. (2016a). Oversight policy options. *Congressional Research Service: Report,* 19-22. Retrieved from http://www.loc.gov/

Francis, K. A., & Ginsberg, W. (2016b). Selected hiring and pay flexibilities applicable

to DOD and DHS cybersecurity positions. *Congressional Research Service: Report*, 9-16. Retrieved from http://www.loc.gov/

Francis, K. A., & Ginsberg, W. (2016c). The federal cybersecurity workforce: Background and congressional oversight issues for the hepartments of defense and homeland security. *Congressional Research Service: Report,* 1-26. Retrieved from https://fas.org/sgp/crs/natsec/R44338.pdf

Frels, R. K., & Onwuegbuzie, A. J. (2013). Administering quantitative instruments with qualitative interviews: A mixed research approach. *Journal of Counseling and Development, 91*(2), 184-194. doi:10.1002/j.1556-6676.2013.00085.x

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

Fusch, P. I., Fusch, G. E., & Ness, L. R. (2017). How to conduct a mini-ethnographic case study: A guide for novice researchers. *Qualitative Report, 22*(3), 923-941. Retrieved from http://nsuworks.nova.edu/tqr/vol22/iss3/16

Gao, F., Meng, L., & Clarke, S. (2008). Knowledge, management, and knowledge management in business operations. *Journal of Knowledge Management, 12*(2), 3-17. Retrieved from http://j.pelet.free.fr/publications/km/Knowledge_management_and_knowledge_management_in_business_operations.pdf

Garrett, J., Hoitash, R., & Prawitt, D. F. (2014). Trust and financial reporting quality.

Journal of Accounting Research, 52(5), 1087-1125. doi: 10.1111/1475-679X.12063

Gebauer, H., Paiola, M., & Saccani, N. (2013). Characterizing service networks for moving from products to solutions. *Industrial Marketing Management, 42*(1), 31-46. doi:10.1016/j.indmarman.2012.11.002

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

Ghosh, K. (2015). Healthcare security: A course engaging females in cybersecurity education. *2015 IEEE Frontiers In Education Conference (FIE),* 1. doi:10.1109/FIE.2015.7344156

Gimenez-Esplin, J. A., Jiménez-Jiménez, D., & Martínez-Costa, M. (2013). Organizational culture for total quality management. *Total Quality Management & Business Excellence,* 24, 678–692. doi:10.1080/14783363.2012.707409

Global Information Security Workforce Study: Women in Cybersecurity (2017). Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

Goode, S., Lin, C., Tsai, J. C., & Jiang, J. J. (2015). Rethinking the role of security in client satisfaction with Software-as-a-Service (SaaS) providers. *Decision Support Systems,* 70, 73–85. doi:10.1016/j.dss.2014.12.005

Goodman, S. E. (2014). Building the nation's cyber security workforce: Contributions

from the CAE colleges and universities. *ACM Transactions on Management Information Systems (TMIS), 5*(2), 6. doi:10.1145/2629636

Granåsen, M., & Andersson, D. (2016). Measuring team effectiveness in cyber-defense exercises: A cross-disciplinary case study. *Cognition, Technology & Work, 18*(1), 121-143. doi:10.1007/s10111-015-0350-2

Grbich, C. (2015) Narrative analysis: The socio-cultural approach to analyzing short participant stories. *Sage Research Methods Datasets.* Sage Publications Ltd. doi:10.4135/9781473947498

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

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? An experiment with data saturation and variability. *Field methods, 18*(1), 59-82. doi:10.1177/1525822X05279903

Gutmann, J. (2014). Qualitative research practice: A guide for social science students and researchers (2nd e.d.). *International Journal of Market Research,* 56, 407. doi:10.2501/ijmr-2014

Haffar, M., Al-Karaghouli, W., & Ghoneim, A. (2013). The mediating effect of individual readiness for change in the relationship between organizational culture and TQM implementation. *Total Quality Management & Business Excellence, 24*(5-6), 693-706. doi: 10.1080/14783363.2013.791112

Halcomb, E., & Hickman, L. (2015). Mixed methods research. *Nursing Standard, 29*(32), 41-47. Retrieved from http://ro.uow.edu.au/smhpapers/2656

Halverson, L. R., Graham, C. R., Spring, K. J., Drysdale, J. S., & Henrie, C. R. (2014). A thematic analysis of the most highly cited scholarship in the first decade of blended learning research. *The Internet and Higher Education,* 20, 20-34. doi:10.1016/j.iheduc.2013.09.004

Hanson, J. L., Balmer, D. F., & Giardino, A. P. (2011). Qualitative research methods for medical educators. *Academic Pediatrics,* 11(5), 375–386. doi:10.1016/j.acap.2011.05.001

Harding, C., & Fox, C. (2015). It's not about "Freudian couches and personality changing drugs": An investigation into men's mental health help-seeking enablers. *American Journal of Men's Health, 9*(6), 451-463. doi: 10.1177/1557988314550194

Harrison, N., & Kirkham, J. (2014). The application of reflexivity in small business research and implications for the business practitioner. *Industry and Higher Education,* 28, 439-447. doi:10.5367/ihe.2014.0232

Hassan, H. M., Reza, D. M., & Farkhad, M. A.-A. (2015). An experimental study of influential elements on cyberloafing from general deterrence theory perspective Case study: Tehran subway organization. *International Business Research,* 8. doi:10.5539/ibr.v8n3p91

Hastings' bipartisan amendment (2018). Hastings' amendment on diversity in cybersecurity industry overwhelmingly passes house. (2018, July 12). *States News Service. Retrieved from https://fas.org/irp/congress/2017_cr/h-072817.html*

Hawthorne, E. K. (2013). Multifarious initiatives in cybersecurity education. *ACM*

Inroads, 4(3), 46. doi:10.1145/2505990.2505999

Hill, D. A. (2008). *What makes total quality management work: A study of obstacles and outcomes* (Doctoral dissertation, Capella University). Retrieved from http://search.proquest.com/docview/304832602

Hogan, S. J., & Coote, L. V. (2014). Organizational culture, innovation, and performance: A test of Schein's model. *Journal of Business Research,* 67, 1609-1621. doi:10.1016/j.jbusres.2013.09.007

Holweg, M., & Helo, P. (2014). Defining value chain architectures: Linking strategic value creation to operational supply chain design. *International Journal of Production Economics,* 147, 230–238. doi:10.1016/j.ijpe.2013.06.015

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

Hoyland, S., Hollund, J. G., & Olsen, O. E. (2015). Gaining access to a research site and participants in medical and nursing research: A synthesis of accounts. *Medical Education, 49*(2), 224–232. doi:10.1111/medu.12622

Hussein, A. (2015). The use of triangulation in social sciences research: Can qualitative and quantitative methods be combined? *Journal of Comparative Social Work, 4*(1), 1-12. Retrieved from https://doaj.org/article/a76dfb64227a46d3b7878af4c5b2d52e?

Hwee-Joo, K., & Pairin, K. (2014). Diversifying cybersecurity education: A non-

technical approach to technical studies. *2014 IEEE Frontiers in Education Conference (FIE Proceedings, Frontiers in Education Conference (FIE), 2014 IEEE,* 1. doi:10.1109/FIE.2014.7044197

Hyett, N., Kenny, A., & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International Journal of Qualitative Studies on Health and Well-Being, 9,* 1–12. doi:10.3402/qhw.v9.23606

Ilieş, L., & Metz, D. (2017). The link between organizational culture and organizational performance - A literature review. *Managerial Challenges of the Contemporary Society, 10*(1), 35–40.

Iqbal, J., Shabbir, M. S., Zameer, H., Tufail, M. S., Sandhu, M. A., & Ali, W. (2017). *TQM practices and firm performance of Pakistani service sector firms. Paradigms,* (1). doi:10.24312/paradigms110114

Imran, A., & Yusoff, R. M. (2015). Empirical validation of qualitative data: A mixed-method approach. *International Journal of Economics and Financial Issues, 5*(1). Retrieved from http://www.econjournals.com/index.php/ijefi/article/viewFile/1511/pdf

Innovation and diversity in the cyber fight. (2015). *Vital Speeches of the Day, 81*(12), 383-385. Retrieved from http://connection.ebscohost.com/c/speeches/111314611/innovation-diversity-cyber-fight

International Organization for Standardization [ISO]. (2016). "ISO/IEC 27000:2016(en)". Retrieved from https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Jacobs, R., Mannion, R., Davies, H. T. O., Harrison, S., Kone, F., & Walshe, K. (2013). The relationship between organizational culture and performance in acute hospitals. *Social Science & Medicine,* 76, 115–125. doi: 10.1016/j.socscimed.2012.10.014

James, N. (2017). Using narrative inquiry to explore the experience of one ethnically diverse ESL nursing student. *Teaching and Learning in Nursing*, 1-6. doi:10.1016/j.teln.2017.08.002

Janeja, V. P., Faridee, A. Z. M., Gangopadhyay, A., Seaman, C., & Everhart, A. (2018). Enhancing Interest in cybersecurity careers. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education - SIGCSE '18.* doi:10.1145/3159450.3159563

Joint Publication 3-0, Joint Operations. (2017). Retrieved from http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0_20170117.pdf

Joyce, S. A. (2015). Outstanding quality using team management. *International Journal of Metalcasting, 9*(3), 7–13. Retrieved from http://www.afsinc.org/technical/IJM.cfm

Kaluarachchi, K. A. S. P. (2010). Organizational culture and total quality management practices: A Sri Lankan case. *The TQM Journal, 22*(1), 41-55. doi:10.1108/17542731011009612

Kappelman, L., Johnson, V., Maurer, C., McLean, E., Torres, R., David, A., & Quynh, N. (2018). The 2017 SIM IT Issues and Trends Study. *MIS Quarterly Executive, 17*(1), 53-88. Retrieved from https://aisel.aisnet.org/misqe/vol17/iss1/6/

Karin Andreassi, J., Lawter, L., Brockerhoff, M., & J. Rutigliano, P. (2014). Cultural impact of human resource practices on job satisfaction: A global study across 48 countries. *Cross cultural management, 21*(1), 55-77. Retrieved from https://www.researchgate.net/publication/275110250_Cultural_impact_of_human_resource_practices_on_job_satisfaction_A_global_study_across_48_countries

Katina, P. F. (2015). Emerging systems theory-based pathologies for governance of complex systems. *International Journal of System of Systems Engineering,* 6, 144-159. doi:10.1504/IJSSE.2015.068806

Kerner, S. M. (2016). IT security skills shortage means higher salaries, more risks. *Eweek,* 9. Retrieved from https://www.eweek.com/blogs/careers/it-security-skills-shortage-means-higher-salaries-more-risks

Khan, A. (2014). Qualitative research: A case for a multi-angle view to enhance validity. *International Journal of Business and Management,* 9, 29-40. doi:10.5539/ijbm.v9n9p29

Kim, E. (Ed.). (2015). Hofstede cultural dimensions: Comparison of South Korea and the United States. *Proceedings of Cambridge Business & Economic Conference, Murray Edwards College, Cambridge University, 2015.* Retrieved from http://dentisty.org/hofstedes- cultural-dimensions.html

Kirkwood, A., & Price, L. (2013). Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education. *British Journal of Educational Technology,* 44, 536-543. doi:10.1111/bjet.12049

Kokina, I., & Ostrovska, I. (2014). The analysis of organizational culture with the Denison model (The case study of Latvian municipality). *European Scientific Journal, ESJ, 9*(10), 362-368. Retrieved from http://www.eujournal.org/index.php/esj/article/download/2316/2189

Kruth, J. G. (2015). Five qualitative research approaches and their applications in parapsychology. *Journal of Parapsychology, 79,* 219-233. Retrieved from http://www.rhine.org/what-we-do/journal-of-parapsychology.html

Kundu, S. C., & Mor, A. (2017). Workforce diversity and organizational performance: A study of IT industry in India. *Employee Relations, 39*(2), 160-183. doi:10.1108/er-06-2015-0114

Lambert, J. (2016). Cultural diversity as a mechanism for innovation: Workplace diversity and the absorptive capacity framework. *Journal of Organizational Culture, Communications, and Conflict, 20*(1), 68-77.

Lantos, J. D., & Spertus, J. A. (2015). The concept of risk in comparative-effectiveness research. *New England Journal of Medicine,* 372(9), 884-884. doi: 10.1056/NEJMc1415933

Lawson, R., Hatch, T., & Desroches, D. (2013). How corporate culture affects performance management. *Strategic Finance, 95*(7), 42-50. Retrieved from https://www.researchgate.net/publication/304155640_How_Corporate_Culture_Affects_ Performance_Management

Lehman, D. W. (2017). Organizational cultural theory and research administration

knowledge management. *Journal Of Research Administration,* (2), 52. Retrieved from https://eric.ed.gov/?id=EJ1161988

Leithy, W. E. (2017). Organizational culture and organizational performance. *International Journal of Economics & Management Sciences, 6*(4), 2-6. doi:10.4172/2162-6359.1000442

Lemos, R. (2017). Women's progress in cyber-security stalled over past two years: Survey. *Eweek, 9.*Retrieved from https://www.eweek.com/security/women-s-progress-in-cyber-security-stalled-over-past-two-years-survey

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of family medicine and primary care,* 4, 324-327. doi:10.4103/2249-4863.161306

Lewis, S. (2015). Qualitative inquiry and research design: Choosing among five approaches. *Health promotion practice,* 16, 473–475. doi:10.1177/1524839915580941

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry.* Newbury, CA: Sage Publications.

Liu, X., & Murphy, D. (2016). Engaging females in cybersecurity: K through Gray. *In Intelligence and Security Informatics (ISI), 2016 IEEE Conference on (pp. 255–260).* IEEE. doi: 10.1109/ISI.2016.7745485

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

Mansfield-Devine, S. (2017, June 1). Security skills shortage becomes critical as GDPR looms. *Computer Fraud & Security.* p. 1,3. doi:10.1016/S1361-3723(17)30045-3.

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

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

Martini, A., Bosch, J., & Chaudron, M. (2015). Investigating architectural technical debt accumulation and refactoring over time: A multiple-case study. *Information and Software Technology*, 67, 237-253. doi:10.1016/j.infsof.2015.07.005

Master, A., Cheryan, S., & Meltzoff, A. N. (2016). Computing whether she belongs: stereotypes undermine girls' interest and sense of belonging in computer science. *Journal Of Educational Psychology*, (3), 424. doi:10.1037/edu0000061

Mazur, B. (2014). Building diverse and inclusive organizational culture-best practices: A case study of Cisco Co. *Journal of Intercultural Management*, *6*(4-1), 169-179. doi: 10.2478/joim-2014-0043

McCandless, J. (2017). Serving a Purpose: States look to veterans to help fill the cybersecurity staffing gap. *Government Technology*, *30*(7), 42-43. Retrieved from http://www.govtech.com/security/GT-OctoberNovember-2017-Are-Vets-the-Solution-to-the-Cyberstaffing-Gap.html

McCollum, T. (2015). The cybersecurity imperative: to help organizations lock down

security, internal auditors must raise their skills and understand the latest threats. *Internal Auditor,* (4). 26. Retrieved from http://go.galegroup.com.ezp.waldenulibrary.org/ps/anonymous?id=GALE%7CA426148613

McCusker, K., & Gunaydin, S. (2015). Research using qualitative, quantitative or mixed methods and choice based on the research. *Perfusion,* 30, 537-542. doi:10.1177/0267659114559116

McDermott, R., & O'Dell, C. (2001). Overcoming cultural barriers to sharing knowledge. *Journal of Knowledge Management, 5*(1), 76-85. doi:10.1108/13673270110384428

McFadyen, J., & Rankin, J. (2016). The role of gatekeepers in research: Learning from reflexivity and reflection. *GSTF Journal of Nursing and Health Care (JNHC), 4*(1), 82-88. doi:10.5176/2345-718X_4.1.135

McIntosh, M. J., & Morse, J. M. (2015). Situating and constructing diversity in semistructured interviews. *Global Qualitative Nursing Research,* 2, 233339361559767. doi:10.1177/2333393615597674

Mehralian, G., Nazari, J. A., Nonreported, G., & Rasekh, H. R. (2017). TQM and organizational performance using the balanced scorecard approach. *International Journal of Productivity & Performance Management,* 66(1), 111-125. doi: 10.1108/IJPPM-08-2015-0114

Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative research: A guide to design and implementation.* Hoboken, NJ: Wiley.

Montgomery, E. G., & Oladapo, V. (2014). Talent management vulnerability in global healthcare value chains: A general systems theory perspective. *Journal of Business Studies Quarterly, 5*(4), 173. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.652.8943&rep=rep1&type=pdf

Morcos, P. (2018). *Effective organizational culture strategies for a firm operating in foreign countries* (Order No. 10934911). Available from ProQuest Dissertations & Theses Global. (2115510829).

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

Murphy, P. J., Cooke, R. A., & Lopez, Y. (2013). Firm culture and performance: Intensity's effects and limits. *Management Decision, 51*(3), 661-679. doi:10.1108/00251741311309715

Naranjo-Valencia, J. C., Jimenez-Jimenez, D., & Sanz-Valle, R. (2016). Studying the links between organizational culture, innovation, and performance in Spanish companies. *Revista Latinoamericana De Psicologia, 48*(1), 30-41. doi:10.1016/j.rlp.2015.09.009

National Initiative for Cybersecurity Education [NICE]. (2018). *Strategic Plan.* Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

National Initiative for Cybersecurity Education [NICE]. (August 2, 2017). *Workshop on*

cybersecurity workforce development: Notes from Panel Discussions. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/09/28/chicago_workshop_summary_notes.pdf.

National Institute of Standards and Technology [NIST]. (August 1, 2017). Preparing cybersecurity professionals to make an impact today and in the future. Retrieved from https://www.nist.gov/sites/default/files/documents/2017/08/01/nice_rfi_final_isaca.pdf

National Institute of Standards and Technology [NIST]. (2015). *Cybersecurity framework.* Gaithersburg, MD. Retrieved from http://www.nist.gov/cyberframework/index.cfm

Nikpour, A. (2017). The impact of organizational culture on organizational performance: The mediating role of employee's organizational commitment. *International Journal of Organizational Leadership,* 6, 65-72. doi:10.19236/IJOL.2017.01.05

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science, 5*(1), 14-37. https://doi.org/10.1287/orsc.5.1.14

O'Dell, C., & Grayson, C. J. (1998). *If only we knew what we know: The transfer of internal knowledge and best practice.* New York, NY: The Free Press.

O'Malley, A. S., Gourevitch, R., Draper, K., Bond, A., & Tirodkar, M. A. (2015).

Overcoming challenges to teamwork in patient-centered medical homes: A qualitative study. *Journal of General Internal Medicine, 30*(2), 183-192. doi:10.1007/s11606-014-3065-9

Oltsik, J., & Alexander, C. (2016). The cyber profession at risk: Take control of your cybersecurity career life cycle. *ISSA Journal, 14*(10), 14-15.

Onwuegbuzie, A. J., & Byers, V. T. (2014). An exemplar for combining the collection, analysis, and interpretations of verbal and nonverbal data in qualitative research. *International Journal of Education, 6(*1), p183–p246. doi:10.5296/ije.v6i1.4399

O'Reilly, M., & Parker, N. (2013). "Unsatisfactory saturation": A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research,* 13, 190–197. doi:10.1177/1468794112446106

Overcoming Barriers to Advancement - CIA Diversity in Leadership Study. (2015). Retrieved from https://www.cia.gov/library/reports/dls-report.pdf

Ovidiu-Iliuta, D. (2014). The link between organizational culture and performance management practices: A case of IT companies from Romania. *Annals of the University of Oradea, Economic Science Series, 23*(1), 1156–1163. Retrieved from https://doaj.org/article/143472a819064e2abace6080bb97ef9e

Palinkas, L. A. (2014). Qualitative and mixed methods in mental health services and implementation research. *Journal of Clinical Child & Adolescent Psychology, 43*(6), 851-861. doi:10.1080/15374416.2014.910791

Palinkas, L. A., Horwitz, S. M., Green, C. A., Wisdom, J. P., Duan, N., & Hoagwood, K.

(2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544.

Para-González, L., Jiménez-Jiménez, D., & Martínez-Lorente, A. R. (2018). Exploring the mediating effects between transformational leadership and organizational performance. *Employee Relations, 40*(2), 412-432. doi: 10.1108/ER-10-2016-0190

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). Thousand Oaks, CA: Sage.

Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science, and Technology, 9*(1), 25-44. Retrieved from http://genderandset.open.ac.uk/index.php/genderandset/article/viewFile/449/824

Perrotta, C. (2015). Beyond rational choice: How teacher engagement with technology is mediated by culture and emotions. *Education and Information Technologies*, 1-16. doi:10.1007/s10639-015-9457-6

Peticca-Harris, A., DeGama, N., & Elias, S. R. (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

Petty, N. J., Thomson, O. P., & Stew, G. (2012). Ready for a paradigm shift? part 2: Introducing qualitative research methodologies and methods. *Manual Therapy, 17,* 378–384. doi:10.1016/j.math.2012.03.004

Prado-Gascó, V., Pardo, I. Q., & Pérez-Campos, C. (2017). Knowledge management and organizational culture in a software development enterprise. *Journal of Small Business Strategy, 27*(1), 37. Retrieved from https://libjournals.mtsu.edu/index.php/jsbs/article/view/759

Prager, A., & Prager, J. D. (2016). Cybersecurity talent gives locations an edge. *Site Selection, 61*(4), 56-58. Retrieved from https://siteselection.com/issues/2016/jul/cybersecurity-talent-gives-locations-an-edge.cfm

Pretorius, H. W., Mawela, T., Strydom, I., de Villiers, C., & Johnson, R. D. (2015). Continuing the discourse of women in Information Technology. *Gender, Technology & Development, 19*(3), 346. doi:10.1177/0971852415597100

Purohit, B., & Singh, P. P. (2013). Data leakage analysis on cloud security. *International Journal of Engineering Research and Applications, 3*(3), 1311-1316. doi:10.1.1.418.9020&rep=rep1&type=pd

Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and for underrepresented populations. *IEEE Security & Privacy, 14*(6), 90-95. doi: 10.1109/MSP.2016.119

PWC. (2017). *Women in cybersecurity: Underrepresented, untapped potential.* Retrieved from pwc.com: https://www.pwc.com/us/en/cybersecurity/women-in-cybersecurity.html

Rick Van der, K., Geert, K., & Heather, Y. (2017). Computer security incident response

team effectiveness: A needs assessment. *Frontiers In Psychology, 8*(2017). doi:10.3389/fpsyg.2017.02179/full

Ritchey, D. (2016). Breaking the cyber glass ceiling. *Security*, *53*(2), 14-19. Retrieved from https://www.securitymagazine.com/articles/86895-breaking-the-cybersecurity-glass-ceiling

Rivers, 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

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

Ruetzler, T., Taylor, J., Reynolds, D., Baker, W., & Killen, C. (2012). What is professional attire today? A conjoint analysis of personal presentation attributes. *International Journal of Hospitality Management, 31*(3), 937-943. doi:10.1016/j.ijhm.2011.11.001

Ruiz-Palomino, P., & Martínez-Cañas, R. (2014). Ethical culture, ethical intent, and organizational citizenship behavior: The moderating and mediating role of person-organization fit. *Journal of Business Ethics*, 120, 95-108. doi:10.1007/s10551-013-1650-1

Rule, P., & John, V. M. (2015). A necessary dialogue: Theory in case study research.

International Journal of Qualitative Methods, 14(4), 1-11. doi:10.1177/1609406915611575

Ruygrok, C. M. (2016). Building a strong team culture for sustained performance. *AAACN Viewpoint, 38*(1), 14–15. Retrieved from https://www.aaacn.org

Ryan, K. J., Brady, J., Cooke, R. E., Height, D. I., Jonsen, A. R., King, P., … Turtle, R. (2014). The Belmont report: Ethical principles and guidelines for the protection of human subjects of research. *The Journal of the American College of Dentists,* 81(3), 4-13. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/25951677

Saffold III, G. S. (1988). Culture traits, strength, and organizational performance: Moving beyond "strong" culture. *Academy of management review, 13*(4), 546-558. doi:10.5465/amr.1988.4307418

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. Journal of Management Information Systems, 34(4), 1023-1053. doi: 10.1080/07421222.2017.1394049

Saunders, B., Kitzinger, J., & Kitzinger, C. (2015). Participant anonymity in the internet age: From theory to practice. *Qualitative Research in Psychology,* 12, 125-137. doi:10.1080/14780887.2014.948697

Schein, E. (1985). *Organizational culture and leadership: A dynamic view.* San Francisco, CA: Jossey-Bass.

Schein, E. H. (1992). *Organizational culture and leadership* (2nd e.d.). San Francisco, CA: Jossey-Bass.

Schein, E. H. (1996). Culture: The missing concept in organization studies. *Administrative Science Quarterly,* 41, 229-240. doi:10.2307/2393715

Schein, E. H. (1999). *Sense and nonsense about culture and climate.* Sloan School of Management, Massachusetts Institute of Technology.

Schein, E. (2004). *Organizational Culture and Leadership* (3rd ed.). San Franscisco, CA: Jossey-Bass.

Schein, E. H., Costas, J., Kunda, G., Schultz, M., Connolly, T. H., Wright, S., & Wah, D. W. H. (2015). Opinions: All about culture. *Journal of Business Anthropology, 4*(1), 106-150. Retrieved from http://ej.lib.cbs.dk/index.php/jba

Schein, E. (2010). *Organizational culture and leadership*. San Francisco, CA: Jossey-Bass.

Schmidlein, R., Vickers, B., & Chepyator-Thomson, R. (2014). Curricular issues in urban high school physical education. *Physical Educator, 71*(2), 273-302. Retrieved from https://js.sagamorepub.com/pe

Schober, M. M., Gerrish, K., & McDonnell, A. (2016). Development of a conceptual policy framework for advanced practice nursing: An ethnographic study. *Journal of Advanced Nursing, 72*(6), 1313–1324. doi:10.1111/jan.12915

Security skills shortage becomes critical as GDPR looms. (2017, June 1). *Computer Fraud & Security.* p. 1,3. doi:10.1016/S1361-3723(17)30045-3.

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

Serban, A. M., & Luan, J. (2002). Overview of knowledge management. *New Directions for Institutional Research,* 113, 5-16. doi:10.1002/ir.34

Shafritz, J. M., Ott, J. S., & Jang, Y. S. (2015). *Classics of organization theory.* Boston, MA: Cengage Learning.

Shah, H. (2014). An ethnographically-informed analysis of the influence of culture on global software-testing practice (Doctoral dissertation, Georgia Institute of Technology). Retrieved from https://smartech.gatech.edu/handle/1853/53983

Shannon, P., & Hambacher, E. (2014). Authenticity in constructivist inquiry: Assessing an elusive construct. *Qualitative Report, 19*(52), 1-13. Retrieved from http://nsuworks.nova.edu/tqr/vol19/iss52/3

Shehadeh, R. M., Al-Zu'bi, M. F., Abdallah, A. B., & Maqableh, M. (2016). Investigating critical factors affecting the operational excellence of service firms in Jordan. *Journal of Management Research, 8*(1), 157-190. doi:10.5296/jmr.v8i1.8680

Shumba, R., Hall, L., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., … Bace, R. (2013). *Cybersecurity, women, and minorities. Proceedings of the ITiCSE Working Group Reports Conference on Innovation and Technology in Computer Science Education-Working Group Reports - ITiCSE -WGR '13.* doi:10.1145/2543882.2543883

Simou, E., & Koutsogeorgou, E. (2014). Effects of the economic crisis on health and healthcare in Greece in the literature from 2009 to 2013: *A systematic review. Health Policy, 115*(2-3), 111-119. doi:10.1016/j.healthpol.2014.02.002

Šimundić, A. (2013). Bias in research. Biochemia Medica, 23(1), 12-15.

doi:10.11613/BM.2013.003

Sloan, A., & Bowe, B. (2015). Experiences of Computer Science Curriculum Design: A Phenomenological Study. *Interchange, 46,* 121. doi:10.1007/s10780-015-9231-0

South, J. R. (2015). Cybersecurity education: The growing pressure to fill one million jobs. *Security: Solutions For Enterprise Security Leaders, 52*(11), 83-86. Retrieved from http://digital.bnpmedia.com/publication

Spillman, L. (2014). Mixed methods and the logic of qualitative inference. *Qualitative Sociology, 37*(2), 189-205. doi:10.1007/s11133-014-9273-0

Stake, R. E. (1978). *Case studies in science education, volume II: Design, overview and general findings.* Retrieved from http://eric.ed.gov/

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., … Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy, 13*(4), 20–29. doi:10.1109/msp.2015.71

Stern, C., Jordan, Z., & McArthur, A. (2014). Developing the review question and inclusion criteria. *American Journal of Nursing*, *114*(4), 53-56. doi:10.1097/01.NAJ.0000445689.67800.86

Stevens, M. R., Lyles, W., & Berke, P. R. (2014). Measuring and reporting intercoder reliability in plan quality evaluation research. *Journal of Planning Education and Research, 34(*1), 77-93. doi:10.1177/0739456X13513614

Sturmberg, J. P., Martin, C. M., & Katerndahl, D. A. (2014). Systems and complexity

thinking in the general practice literature: An integrative, historical narrative review. *Annals of Family Medicine, 12*(1), 66-74. doi:10.1370/afm.1593

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

Szulanski, G. (2017). Intra-firm transfer of best practice, appropriate capabilities and organizational barriers to appropriations. *Academy of Management Best Papers Proceedings*, 47-51. doi:10.5465/AMBPP.1993.10315237

Taylor, G., McNeill, A., Girling, A., Farley, A., Lindson-Hawley, N., & Aveyard, P. (2014). Change in mental health after smoking cessation: systematic review and meta-analysis. *British Medical Journal, 348*(1151), 1-22. doi:10.1136/bmj.g1151

The 2017 (ISC)2 global information security workforce study. (2017). Retrieved from https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Thien, L. M., Thurasamy, R., & Razak, N. A. (2014). Specifying and assessing a formative measure for Hofstede's cultural values: A Malaysian study. *Quality & Quantity*, 48, 3327-3342. doi:10.1007/s11135-013-9959-5

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

Tong, A., & Dew, M. A. (2016). Qualitative research in transplantation. *Transplantation, 100*(4), 710-712. doi:10.1097/tp.0000000000001117

Tong, C., Tak, W. I. W., & Wong, A. (2015). The Impact of knowledge sharing on the relationship between organizational culture and Job satisfaction: The perception

of information communication and technology (ICT) practitioners in Hong Kong. *International Journal of Human Resource Studies, 5*(1), 19-47. doi:10.5296/ijhrs.v5i1.6895

Tran, V., Porcher, R., Falissard, B., & Ravaud, P. (2016). Point of data saturation was assessed using resampling methods in a survey with open-ended questions. *Journal of Clinical Epidemiology*, 80, 88-96. doi:10.1016/j.jclinepi.2016.07.014

Trompenaars, F. (1994). *Riding the Waves of Culture: Understanding Diversity In Global Business.* London: Economist Books.

Trompenaars, F., & Hampden-Turner, C. (1998). *Riding the waves of culture: Understanding Diversity in global business.* New York: McGraw-Hill.

Tsang, E. W. (2014). Generalizing from research findings: The merits of case studies. *International Journal of Management Reviews*, 16, 369-383. doi:10.1111/ijmr.12024

Uricco, R. (2016). Females could fill gaps in the InfoSec workforce. *Credit Union Times, 27*(35), 8-9. Retrieved from https://www.cutimes.com/2016/10/09/females-could-fill-gaps-in-the-infosec-workforce/?slreturn=20200009125810

U. S. Department of Health & Human Services. (2015). Belmont report 1979. Retrieved from http:// www.hhs.gov

U.S. Department of Labor, Bureau of Labor Statistics. (2018). *Computer and information technology occupations.* Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/home.htm

U.S. House Committee on Homeland Security (September 7, 2017). *Challenges of*

recruiting and retaining a cybersecurity work force: Hearing before the subcommittee on cybersecurity and infra-structure protection, 115th Cong., 1st sess. Retrieved from https://docs.house.gov/meetings/HM/HM08/20170907/106359/HHRG-115-HM08-Transcript-20170907.pdf

U.S. Secretary of Commerce & U.S. Secretary of Homeland Security. (May 2018). *A report to the president on supporting the growth and sustainment of the nation's cybersecurity workforce: Building the foundation for a* more *secure american future.* Retrieved from https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis. *Journal of Nursing Education and Practice, 6*(5), 100-110. doi:10.5430/jnep.v6n5p100

Vaismoradi, M., Turunen, H., & Bondas, T. (2013). Content analysis and thematic analysis: Implications for conducting a qualitative descriptive study. *Nursing & Health Sciences, 15*(3), 398-405. doi:10.1111/nhs.12048

Valmohammadi, C., & Roshanzamir, S. (2015). The guidelines of improvement: Relations among organizational culture, TQM and performance. *International Journal of Production Economics,* 164, 167-178. doi:10.1016/j.ijpe.2014.12.028

Vanclay, F., Baines, J., & Taylor, N. (2013). Principles for ethical research involving

humans: Ethical professional practice in impact assessment Part I. *Impact Assessment and Project Appraisal*, 3, 243-253. doi: 10.1080/14615517.2013.850307

Vasile, A., & Nicolescu, L. (2016) Hofstede's cultural dimensions and management in corporations: Theoretical article case study. *Cross-Cultural Management Journal, XVIII*(18), 35-46. Retrieved from http://cmj.seaopenresearch.eu/

Von Bertalanffy, L. (1968). *General systems theory: Foundations, development, application* (Rev. ed.). New York, NY: George Braziller.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cybersecurity professionals. *Computers & Security*, 3, 97-102. doi:10.1016/j.cose.2013.04.004

Wahyuni, D. (2012). The research design maze: Understanding paradigms, cases, methods, and methodologies. *Journal of Applied Management Accounting Research, 10*(1), 69-80.

Walker, J. L. (2012). The use of saturation in qualitative research. *Canadian Journal of Cardiovascular Nursing, 22*(2), 37-46. Retrieved from www.ncbi.nlm.nih.gov/

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

Wei, Y. S., Samiee, S., & Lee, R. P. (2014). The influence of organic organizational cultures, market responsiveness, and product strategy on firm performance in an emerging market. *Journal of the Academy of Marketing Science*, 42, 49-70. doi:10.1007/s11747-013-0337-6

White, J. (2016). Cyber threats and cyber security: National security issues, policy and strategies. *Global Security Studies*, *7*(4), 23-33. Retrieved from http://www.globalsecuritystudies.com/archives.htm

WhiteHouse.gov (2019). Executive Order on America's Cybersecurity Workforce. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

WhiteHouse.gov (2018). Statement from President Donald J. Trump on H.R. 3210. Retrieved from https://www.whitehouse.gov/briefings-statements/statement-president-donald-j-trump-h-r-3210/

Whitney, K., Bradley, J. M., Baugh, D. E., & Jr, C. W. C. (2015). Systems theory as a foundation for governance of complex systems. *International Journal of System of Systems Engineering*, *6*(1-2), 15-32. doi: 10.1504/IJSSE.2015.068805

Wilshusen, G. (2018). *Cybersecurity: DHS needs to enhance efforts to improve and promote the security of federal and private-sector networks*. Retrieved from https://www.gao.gov/products/GAO-18-520T

Wilson, C., Broughan, C., & Hillier, R. (2017). A new lens on a persistent problem: using emergent theory to investigate the barriers to progression of female STEM academics at a UK university. *International Journal of Gender, Science & Technology, 9(*1), 45. Retrieved from https://pdfs.semanticscholar.org/53c9/1ad46d7e9579861ffc90bea6cb5061bb6ea1.pdf?_ga=2.6530354.1027973444.1578580769-799422799.1548754619

Wohlin, C., & Aurum, A. (2015). Towards a decision-making structure for selecting a

research design in empirical software engineering. *Empirical Software Engineering,* 20(6), 1427-1455 doi:10.1007/s10664-014-9319-7

Wolgemuth, J. R. (2014). Analyzing for critical resistance in narrative research. *Qualitative Research, 14*(5), 586-602. doi:10.1177/1468794113501685

Women, Minorities, and Persons with Disabilities in Science and Engineering. (2013). *PsycEXTRA Dataset.* doi:10.1037/e558442013-001

Wynn, D., & Williams, C. K. (2012). Principles for conducting critical realist case study research in information systems. *MIS Quarterly, 36*(3), 787-810. doi:10.2307/41703481

Xiao, L., & Dasgupta, S. (2005). The impact of organizational culture on information technology practices and performance. *AMCIS 2005 Proceedings,* 466. Retrieved from http://aisel.aisnet.org/amcis2005/466

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

Yilmaz, G. (2014). Let’s peel the onion together: An application of Schein's model of organizational culture. *Communication Teacher, 28*(4), 224. doi:10.1080/17404622.2014.939674

Yin, R. K. (1981). The case study as a serious research strategy. *Science Communication, 3*(1), 97-114. doi:10.1177/107554708100300106

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

Yin, R. K. (2015). *Qualitative research from start to finish.* New York City, NY: Guilford Publications.

Zheng, W., Yang, B., & McLean, G. N. (2010). Linking organizational culture, structure, strategy, and organizational effectiveness: Mediating role of knowledge management. *Journal of Business Research, 63*(7), 763-771. doi:10.1016/j.jbusres.2009.06.005

Zhu, Y-Q., Gardner, D. G., & Chen, H-G. (2018). Relationships between work team climate, individual motivation, and creativity. *Journal of Management*, *44*(5), 2094-2115. doi:10.1177/0149206316638161

Zitomer, M. R., & Goodwin, D. (2014). Gauging the quality of qualitative research in adapted physical activity. *Adapted Physical Activity Quarterly, 31*(3), 193-218. doi:10.1123/apaq.2013-0084

Zohrabi, M. (2013). Mixed method research: Instruments, validity, reliability and reporting findings. *Theory and Practice in Language Studies, 3*(2), 254–262. doi:10.4304/tpls.3.2.254-262

Appendix A: Interview Protocol

Topic**:** Exploring Strategies for Recruiting and Retaining Diverse Cybersecurity Professionals.

Eligibility Criteria

Eligibility criteria are the guidelines for who can and cannot participate in a study. Thus, they will be used to identify potential interview participants. To be selected as a study participant, the candidate must satisfy at three of the five eligibility criteria, which include:

a. Cybersecurity leaders that have the authority to attract, recruit and retain cybersecurity professionals within their organizations or government agency;
b. Cybersecurity leaders that have conducted or been involved in attraction, recruitment, and retention activities and campaigns within the same organization or government agency or at any other organization or government agency for a minimum of five years;
c. Cybersecurity leaders that have prior or current knowledge and extensive experience in cybersecurity strategic planning/implementation, cyber threat mitigation, remediation, training, auditing, compliance, technical and non-technical controls within their organization or government agency;
d. Cybersecurity leaders that work in the metropolitan area of Atlanta, Georgia;
e. Cybersecurity leaders, I have never had a recurring working relationship.

Interview Script

1. Introduce myself, describe my role as a student and researcher, and thank the participant.

   Good morning or evening. Thank you for your time and for participating in this study as an interview participant. My name is Vivian Lyon, and I am a doctor of information technology candidate at Walden University. My doctoral study Chair is Dr. Nicholas Harkiolakis. I have both studied and worked in the Information Technology and Security industry since 1997.

2. Confirm that the participant has signed the informed consent and any address questions and/or concerns.

   I want to discuss the consent form and ask if you would like a signed copy. The signed consent ensures that the participant understands that their participation in this interview is voluntary, the participant has a right to withdraw their informed consent and stop the interview at any time, and the interview will be conducted in a manner that does not harm the participant and the researcher.

3. Remind the participant of the purpose of the study.

   The purpose of this study is to explore strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to protect sensitive information from rising cyber threats.

4. Describe the reason for their participation.

The information you provide today via interview responses, any documentation, or other sources, will support my study in partial fulfillment of the degree of Doctor of Information Technology from Walden University.

5. Describe the benefit of their participation, if any.

   This information could add to academic and professional bodies of knowledge on cybersecurity attraction, recruitment, and retention strategies and is geared towards increasing diversity in the cybersecurity workforce to efficiently and effectively protect sensitive information from rising cyber threats. There is no compensation of any sort associated with your participation in this study.

6. Verify the interview procedure concerning the audio recording and the steps I will take to protect the participant's privacy and the confidentiality of the material. Inform the participant that the interview will be recorded, obtain their permission to record the audio and take notes throughout the session. Discuss ethics and go through the steps to ensure the participant's protection and the confidentiality of the material before beginning to record.

To maintain ethical standards and respect your right to privacy, I am requesting your permission to record the audio of this interview and take written notes throughout this entire session starting now. The interview will be limited to one hour. Once the audio recording begins, I will introduce this session using your participant ID <Participant ID> and ask you to reconfirm your permission to record and take notes on this session. All information you provide will be treated as strictly confidential. I request that you avoid using any identifying information to include name, address, organization

name, and location or any identifying indicators in your responses. However, any identifying information that are mentioned in the interview by accident will be removed from the transcripts and final report. I also request that you do not discuss your participation in this study with anyone until the study concludes. Any information provided in any form in this session will be presented in a composite form as opposed to individual form in a doctoral study that may be published. The research files containing the recorded interview any other materials you provide in the course of this interview (e.g., thumb drive, hard copy) will be in an encrypted and password-protected format in a locked safe with access by the researcher only for five years, after which it will be permanently destroyed.

7. Ask if there are any questions and confirm the participant is ready to proceed with the interview. Or if a break is needed, and if required, allow for a short break, and agree upon a time to return to begin the interview.

    Do you have any questions for me before we start? If no, is it ok to start recording now? Or do you need a break? If so, what time do we convene to begin the interview?

8. When the participant is ready, inform the participant as the audio recording is about to begin and start the audio recording. State the researcher's name, the date and time of the interview, the participant's assigned identification number for the study and whether this is the initial or follow-up interview. Confirm whether the participant received background information about the study and approved of the recording and note-taking.

My name is Vivian Lyon, and I am here with Participant <X>; today's date is <Y>; the time is <Z>, and this is the initial interview. Would you please confirm that I have provided you with background information on this study including the purpose, the reason for your participation, benefits of participation and that you approve of my recording and taking notes during this session?

9. Start the interview beginning with the first question and continuing until the final question while allowing for re-ordering of the questions depending on how the interview progresses. Once the participant has indicated, he/she has answered the question and does not have additional responses, proceed to ask further questions based upon the participant's answer, if applicable. If a clarifying question is not needed, then proceed to the next interview question.

This is a semi-structured interview, and I have a few open-ended questions outlined for which your answers are much appreciated to provide insights about the phenomenon under study.

   A. *Without including your name or your organization's name, what is your current role and how long have you been in similar roles?*
   B. *What is your background in cybersecurity education/training and/or recruiting cybersecurity personnel?*
   C. *What strategies do you have for ensuring the highest possible attraction, recruitment, and retention of diverse cybersecurity professionals to protect sensitive systems?*

Probe: *Do you differentiate between attract, recruit, and retain in your strategy?*

D. *What strategies have you found to be least effective and efficient*

E. *What is your perception of the impact of the culture of your organization on your strategies to attract, recruit, and retain diverse cybersecurity professionals? Please explain.*

F. *What is your perception of consideration of diversity in the work place? Please explain.*

G. *What, if any, challenges do you face regarding the application of attraction, recruitment, and retention best practices for diverse cybersecurity professionals? Please elaborate.*

H. *How would you describe the effects of your strategies to attract, recruit, and retain diverse cybersecurity professionals on the team's performance to protect sensitive systems?*

I. *Is there anything else you would like to add in relation to your cybersecurity attraction, recruitment, and retention strategies that we have not addressed already?*

10. Ask the participant if they are aware of any documentation that might be relevant to the topics discussed.

That concludes the interview portion of the meeting. Do you have any documents or multimedia presentations or other information you would like to provide to me regarding the topics discussed at this time?

11. Explain the concept of member checking and schedule a follow-up interview to review my interpretations with them.

    To ensure that I have interpreted your responses correctly. I would like to schedule a follow-up interview with you in a few days. Will that be acceptable? Is there a preferred method of communication for rescheduling?

12. Stop audio recording.

Thank the participant for partaking in the study. Confirm the participant has my contact information for any follow-up questions and concerns.

Thank you again for partaking in this study. I appreciate your time today. I would like to confirm that you have my contact information for any follow-up questions and concerns.

Appendix B: Invitation to Participate Email Template

Dear <First name>,

My name is Vivian Lyon, and I am a Doctor of Information Technology candidate at Walden University. As part of my doctoral program, I am researching strategies used by cybersecurity leaders to attract, recruit, and retain diverse cybersecurity professionals to effectively and efficiently protect sensitive information from rising cyber threats. I believe that you support the principles I am researching and would like to include you in my research.

I have attached a copy of the Walden University's Institutional Review Board approval to conduct my research and a consent form with details of my study for your consideration. If you read through the consent form and would like to participate, please forward a signed copy of the consent form to me at <email address redacted>. If you do not wish to participate for any reason, no communication is necessary. Participation in this study is entirely voluntary; you can choose to not participate or withdraw from the study with no personal or professional consequences. Interviews and other data collection activities are anticipated to occur in <date to come>, possibly extending into <date to come>. I will work with you to schedule participation times that do not interfere adversely with your work tasks or schedule.

I thank you for your consideration and look forward to working with you.

Vivian Lyon, Doctor of Information Technology Candidate
Walden University
<email address redacted>

Appendix C: Human Subject Research Certificate of Completion

Certificate of Completion

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

Date of completion: 09/08/2017.

Certification Number: 2482568.