NSU Florida
NOVA SOUTHEASTERN UNIVERSITY

Nova Southeastern University
NSUWorks

CEC Theses and Dissertations

College of Engineering and Computing

2018

Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field

Kembley Kay Lingelbach
Nova Southeastern University, lingelbach8@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University College of Engineering and Computing. For more information on research and degree programs at the NSU College of Engineering and Computing, please click here.

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd


Part of the Computer Engineering Commons, and the Databases and Information Systems Commons

Share Feedback About This Item

NSUWorks Citation

Kembley Kay Lingelbach. 2018. *Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field.* Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1056)
https://nsuworks.nova.edu/gscis_etd/1056.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field

by

Kembley K. Lingelbach

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2018

We hereby certify that this dissertation, submitted by Kembley Lingelbach, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

Steven R. Terrell, Ph.D.
Chairperson of Dissertation Committee

11/20/18
Date

Yair Levy, Ph.D.
Dissertation Committee Member

11/20/18
Date

Alex Koohang, Ph.D.
Dissertation Committee Member

12/3/18
Date

Approved:

Meline Kevorkian, Ed.D.
Interim Dean, College of Engineering and Computing

11/20/18
Date

College of Engineering and Computing
Nova Southeastern University

2018

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field

by
Kembley K. Lingelbach
November 2018

Despite multiple national, educational, and industry initiatives, women continue to be underrepresented in the cybersecurity field. Only 11% of cybersecurity professionals, globally, are female. This contributes to the growing overall shortage of workers in the field. This research addressed the significant underrepresentation of females in the cybersecurity workforce. There are many practitioner and industry studies that suggest self-efficacy, discrimination and organizational culture play important roles in the low rate of women in the cybersecurity field. A limited number of scholarly studies identify causal factors; however, there is not a general consensus or framework to explain the problem thoroughly. Moreover, there exists a significant gap in theoretical framework utilizing qualitative methods to demystify the complex factors of engaging females to pursue the cybersecurity field.

This study utilized a grounded theory approach to interview twelve female cybersecurity professionals to discover their perceptions of the cybersecurity field. The participants revealed strategies that could encourage females to pursue the cybersecurity field. Data analysis included a data coding process and a constant comparative method of interview transcripts. This study identified four factors of engagement and one unexpected co-factor that are perceived to have an impact on decisions to pursue the cybersecurity field. The four factors identified were awareness, support, intrinsic and extrinsic values. The interesting find of the cybersecurity mindset profile factor that is perceived to enhance the success of career trajectory warrants additional research to discover the impacts on decision to pursue the cybersecurity field.

This findings of this research gives women a voice in recommending strategies to encourage other females to pursue the cybersecurity field. The findings also aid in demystifying the complexity of the factors by organizing and categorizing them in a logical sense in order to present a theoretical model to encourage females into the field of cybersecurity. Moreover, this study provides holistic insight to academicians and practitioners in developing future cybersecurity professionals. Additionally, it adds to the body of knowledge by answering the call for that additional qualitative approaches in methodology by bringing data richness and to generate new theoretical frameworks in cybersecurity research.

Acknowledgements

First, I would like to thank God for allowing me the opportunity to pursue my passion in academia. I have been granted many opportunities throughout my life and am very grateful for each and every one of them. Secondly, my husband, Scott is to be thanked for his love and support throughout this journey. It takes a special person to support someone pursuing a PhD. He was always the first person to give me encouraging words when I thought I wanted to give up. Especially, when I lost my mother earlier in the year. Thank you for being my best friend and I love you. Next, I want to thank my advisor, Dr. Steven Terrell for his unlimited support and devotion of his time and instrumental advice. He was encouraging and constructive at all times. Without his help and guidance, the completion of this dissertation would not have been possible. Gratitude is also expressed to my two other committee members, Dr. Yair Levy whom I have the utmost respect and who played an important role in giving me valuable advice, even when I did not want to hear it. For my other committee member, Dr. Alex Koohang, who has been extremely supportive and always gave me encouraging words when I was at a roadblock. Dr. Koohang, you are definitely an inspiration to me and I looking forward to working with you in the future. For my children, Ashley, Scotty & Savannah, you have seen your mother attend college courses, probably more than you would like. I have tried to be a good mother, student, cybersecurity professional and now an academic professor. You have always been encouraging and I hope that I did not miss too many things in your lives. There are multiple friends and coworkers too numerous to mention or this acknowledgements page would become an acknowledgements chapter. So, you know who you are, and I thank you from the bottom of my heart for your support and friendship. I would like to thank my Mom and Dad, they have always supported me in anything I wanted to do. They gave me valuable advice when I needed it and when I thought I did not need it. Their encouragement and support made me the person I am today. A special thanks to the 12 wonderful women that participated in this study. Without you, I would not have been able to complete this research. I am very grateful that you agreed to participate and hope the results will give you something of pride or accomplishment in helping all women interested in the cybersecurity field.

Table of Contents

List of Tables

Tables

List of Figures

Figures

Chapter 1

Introduction

Background

Cybersecurity applies to everyone and every organization within a technology dependent and interconnected society. Businesses and other organizations that operate in the cyberspace require a well-trained workforce to adequately defend and protect their critical systems and services. In light of rapidly changing technology, behaviors and sophisticated advanced persistent threats, the consequences of not having a well-trained cybersecurity workforce can be catastrophic on organizations, locally and nationally (Haney & Lutters, 2017).

Cyberattacks are escalating at an exponential rate, complexity, and sophistication, which are endangering sensitive and personal information (Symantec Corporation, 2015; Verizon Enterprise Solutions, 2016). The costs of global cybercrime are averaging $9.5 million annualized cost with the United States experiencing the highest average cost of cybercrime of $17.36 million (Ponemon Institute, 2017). According to the 2017 International Information System Security Certification Consortium (ISC^2) Global Information Security Workforce Study on Women in Cybersecurity, the cybersecurity profession is one where the demand is far outweighing the supply and expected to continue on this trend for years to come as projections indicate there will be a cybersecurity workforce shortage of 1.8 million people by the year 2022 (Frost & Sullivan, 2017).

According to the 2016 United States Bureau of Labor Statistics, the cybersecurity field is experiencing a growing shortage of personnel with over a quarter-million positions remain unfilled in the United States alone and expecting to increase by 18% from 2014 to 2024. The 2015 ISC^2 Global Information security workforce study documented the profession is growing but falling increasingly behind the demand (Suby, 2015a). The current workforce is 90% male, even though women are consistently graduating with the highest concentration of advanced degrees (Suby, 2015a, 2015b).

The relatively low number of females in the field may be problematic (D'Hondt, 2016; PricewaterhouseCoopers (PwC), 2017; Wei, 2017). For example, the 2017 ISC^2 Women in Cybersecurity report suggests the information security workforce remains stagnant at a rate of 11% women, despite the fact women hold 56% of all professional jobs in the United States and have the largest number of advanced degrees (Frost & Sullivan, 2017; Higgins, 2015; National Center for Women & Information Technology, 2015; Suby, 2015b). The cybersecurity workforce shortages can be potentially countered by addressing the gender imbalance. It is imperative to gain a better understanding of why women are not entering the cybersecurity field.

The remainder of this document includes the problem investigated, the purpose of the study and the research questions. This is followed by a discussion of the barriers and issues that may affect the results. Chapter 2 discusses the literature related to these topics. A discussion of the study's methodology, to include the research design, sampling, data collection procedures and specific data analysis used to generate emerging theoretical concepts as well as a definition of terms.

Problem Statement

The problem this research addressed is the significant underrepresentation of females in the cybersecurity workforce. Only 11% of cyber professionals are female and continue to be underrepresented in the cybersecurity field (Bagchi-Sen, Rao, Upadhyaya, & Chi, 2010; LeClair, Shih, & Abraham, 2014; Suby, 2015a, 2015b). This contributes to the growing overall shortage of workers in the field. A report from Harvard Kennedy School of Government attributes the low rate of females in cybersecurity to militaristic culture, cultural biases, and perceptions of work–life balance that inhibit women from pursuing the cybersecurity field (D'Hondt, 2016). Yet, without a plan for recruiting and retaining females in the cybersecurity field, the overall security of the United States may be diminished (D'Hondt, 2016).

There have been strides accomplished in other male dominated fields, such as the medical field toward gender equity where women represent approximately 48% of medical degrees and 34.3% of all physicians and surgeons in the United States (Freedman, 2010; Warner, 2014). However, other medical subfields, such as radiology has not seen the participation of females increase due to lack of exposure, few role models and mentors, hesitance with technology, limited human contact and long training (Kaplan, 2015). Kaplan (2015) also reports that early exposure to technology (radiology) and the impact on the role of radiology to help people may be the disconnect. Warner (2014) details that leadership roles, such as deans of medical schools, the rates are much lower at 15.9%. Similar constructs have been seen across the cybersecurity field as well with respect to female participation rates (D'Hondt, 2015).

Another area where females are achieving parity with men is the legal field, the American Bar Association in 2014 reports 45.4% women in the field even though women

are graduating with law degrees at 47% (Warner, 2014). However, the percentage drops as the more senior positions are evaluated. Warner (2014) reports that 45.4% are associates, but only 25% are non-equity partners and only 15% are equity partners. Smith (2012) suggests that retention in the legal field is the most critical challenge to gender parity where they see females entering law schools at similar rates. Yet, the gender gap in the cybersecurity field remains a critical issue and calls for future research in "lessening the gender gap" in women in STEM and cybersecurity fields (LeClair et al., 2014, p. 4) are still prominent and since there is no overarching universal "magic bullet," more research is needed in this area (Peacock & Irons, 2017). LeClair et al. (2014) also calls on more research to reduce the male/female imbalance in technological fields and suggest that guidance and role models can lead women into technology, but once they are in the field, efforts need to be made to increase the likelihood that they will stay. Trauth and Quesenberry (2007) suggests that the reasons for underrepresentation of females in the information technology field is a complex and challenging area of study because no single factor can be identified as a root cause.

As there have been relatively few scholarly studies on this issue, this research addressed factors and barriers women experience in the cybersecurity field to uncover strategies to increase the cybersecurity participation rate. This research focused on the perceptions of current female cybersecurity professionals to develop a theoretical framework and strategies to attract females to the cybersecurity field.

Dissertation Goal

The main goal of this research study is an investigation of the reasons why few qualified females are not entering the cybersecurity workforce and determine what can be

done to increase their numbers. Based on the development of a grounded theory from interviews with females in the cybersecurity field, the information gained provided the factors that can impact decisions to enter and stay in the cybersecurity field. Another goal as a result of this research is to provide holistic insight to academicians and practitioners to develop programs that will help balance the gender disparity.

Research Questions

Main Research Question

What are the factors that attract females to the cybersecurity field?

Sub or probing interview questions

1. How are females represented in the cybersecurity field?
2. What are the factors that discourage females from entering the cybersecurity field?
3. What strategies can be developed to recruit females into the cybersecurity field?

Relevance and Significance

This study focuses on increasing the number of females in the cybersecurity workforce and developing future cybersecurity professionals. This study is relevant given that the United States is in a dire situation in attracting, retaining and developing the future cybersecurity professionals to protect the nations' critical infrastructure (D'Hondt, 2016). It is hoped that this study uncovered strategies to entice females to enter the cybersecurity field.

Despite multiple federal government, industry, academic and professional organization initiatives, women are still not proportionately represented in cybersecurity

fields (Frost & Sullivan, 2017). The goal of the research is to provide framework for organizations, academia and government to attract, retain and develop female cybersecurity specialists which, in turn, offer diverse and creative solutions from the female perspective (Caldwell, 2013; Ingalhalikar et al., 2014). For any organization with a diversified team or group, performance and solutions are greater, and offer an additional perspective to help advance the strategic and operational goals to protect critical resources (Caldwell, 2013; LeClair et al., 2014). This research aims to add to the academic body of knowledge with a theoretical framework grounded in the data that delineate the multitude of factors presented in prior studies, and create a more meaningful concise framework or theory.

This study focused on current cybersecurity professionals in order to provide interventions or strategies for recruitment and retention of cybersecurity professionals. The resultant framework or theoretical framework can be applied to other similar locations of the same size and characteristics.

Significance

The significance of this research has long term implications in the nations' defense, economy, and security. The Department of Homeland Security identified cybersecurity as one of the critical areas of the national strategy for homeland security. President Obama signed an Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" in 2013 to establish a policy "to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment to encourage efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy and civil liberties" (National Institute of Standards and Technology, 2015). The

cybersecurity workforce is critical in implementation of this policy and "without a robust workforce as well as diversity of perspectives, vulnerabilities will persist" (D'Hondt, 2016, p. 7). The limited number of skilled cybersecurity workforce to meet demands is placing our nation in a dire situation and as the severity and technology of cyber threats increase, the cyber workforce must be prepared and developed from early educational career throughout their cybersecurity career (Newhouse, Keith, Scribner, & Witte, 2017). For example, the U.S. democracy was threatened during the 2016 Presidential elections as nation-state hackers (i.e., foreign government hackers), attempted to influence the election results by hacking into party email servers and releasing them to the public by a third party (Osborne, 2016). However, with a skilled, cybersecurity workforce, threats, such as this, might have been prevented.

Long-term implications are significant for the cybersecurity industry as well; by utilizing females in cybersecurity, it will not only decrease the gender gap, but also increase the pipeline for future cybersecurity professionals and provide more innovative solutions (Frost & Sullivan, 2017). Cybersecurity professionals are critical to solving security problems while implementing new information technologies in organizations (LeClair et al., 2014). Having women in the cybersecurity field can increase future female cybersecurity professionals' implicit identification with science, while decreasing the gendered stereotypes regarding science (LeClair et al., 2014). Recent studies indicate that, cognitively, women investigate problems differently than men and may provide better overall creative solutions (Caldwell, 2013; Ingalhalikar et al., 2014). Caldwell (2013) suggests that diversity and cultures or any group of people with a common purpose, perform better when functioning together, and with a more gender equity, perform 26% better than male-only groups. Ingalhalikar et al. (2014) suggests that men

are “more likely better at learning and performing a single task, whereas women have superior memory and social cognition skills, making them more equipped for multitasking and creating solutions that work for a group”. Still, other studies suggest there’s no difference in gender and creativity, and do not differ in terms of intellectual abilities, but may in cognitive strategies, functional task sets or cognitive styles and suggests further studies on gender differences in creativity (Abraham, 2015).

Olbrich, Trauth, Niederman & Gregory (2015) articulated four arguments for diversity in the IT field, a feeder field for cybersecurity (Olbrich, Trauth, Niedermann & Gregor (2015). The arguments are the innovation argument, the consumer argument, the equity argument and the policy argument (Trauth, 2011; Trauth & Howcroft, 2006; Trauth, Huang, Quesenberry & Morgan, 2007). The innovation argument argues that as economies become knowledge intensive, the highest value is placed on creativity and continuous innovation that places emphasis on talent regardless of individuals’ characteristics. The consumer argument argues that the greater the diversity in design teams lead to products that better respond to a diverse consumer group because the designers’ have a better understanding of diverse customer needs and wants. The equity argument argues that because of the fairness to all in democratic societies that all members of a society should have equal opportunity to share in the economic benefits of working in a high wage field such as in information systems field. Finally, the policy argument argues that as governments become proactive about increasing the participation of underrepresented groups (specifically STEM fields), companies and other organizations are being encouraged to provide evidence of initiatives geared toward diversity (Olbrich et al., 2015). These studies lead us to believe that organizations would

benefit from including female cybersecurity professionals on a diversified cybersecurity team.

Barriers and Issues

One barrier for this study was obtaining permission to interview cybersecurity professionals. Institutional Review Board (IRB) approval was required prior to conduct the study and interview participants. Since this research involves collecting data from people about people, researchers must protect their participants by developing trust, promoting integrity of the research, guarding against any misconduct and any impropriety that may reflect on their organization or institution and cope with challenges that might arise (Creswell, 2009). The researcher has an obligation to respect the rights, needs, values and desires of the participants. The following precautions were used to protect the participants' rights:

1. Participants were advised in writing of the voluntary nature of their participation that they can withdraw from the study at any time. They were advised that at any time during the process, they could decline to answer any question.
2. The research objectives were clearly defined in writing and articulated to the participants prior to the interview phase.
3. A written consent form was obtained from each participant.
4. The participants were informed in writing of all data collection methods and activities.
5. Provisions were made for monitoring the data collected to ensure the security of the participant's information. Anonymity was used to protect the participant's confidentiality by use of pseudonyms or aliases.

6. A transcript of their interview was made available to each participant.
7. The participants rights, interest, and wishes were considered first as choices were made regarding reporting the data and the final decision regarding the participants privacy rest with the participant.
8. The risk to the participants was considered to be minimal.

Assumptions

Assumptions are those issues that are out of the researcher's control and without them, the research study is at risk (Leedy & Ormrod, 2013). It is assumed that the participants were truthful and honest in their responses and the sample was a true representation of the population. To counter these assumptions, anonymity and confidentiality was discussed and how the data and recordings were preserved and destruction disposition after no longer needed. The option to withdraw from the study at any time with no ramifications was also discussed to encourage the truthfulness of the participant's responses. For the sample population, based on the demographics, the participants that did not meet the selection criteria were not asked to participate.

Limitations

Limitations are factors outside the control of the research may that may place restrictions on your methodology and conclusions and potential weaknesses in the research. Limitations for this research included not having a large enough response rate, however, from prior grounded theory studies, it is suggested the number of participants be 15 to 20. The limitations also included the availability of female cybersecurity professional's participants or scheduling conflicts. In order to alleviate some uncertainty

of the availability of the participant, the researcher had some flexibility in scheduling the interviews at the participant's convenience.

When considering the findings, the limitations of purposeful sampling was kept in mind. Generalizability is always a concern when using this type sampling as well as with qualitative studies in general.

Although every effort was made to ensure objectivity, the researcher's own personal bias and experiences may shape the views and understanding and interpretation of the data collected as the researcher belongs to the population sample. The researcher recognized the need to be open to the thoughts and opinions of others and to set aside personal experiences in order to understand those of the participants. The researcher's background includes over 30 years as a Department of Defense (DoD), U.S. Air Force civilian employee in the information technology field, in particular, the cybersecurity career field. The researcher has numerous information security certifications to include CompTIA Security+, ISC^2 Certified Information System Security Professional, Information Assurance Certification Review Board Certified Computer Forensics Examiner, and E-C Council Certified Ethical Hacker certifications. The researcher has teaching and education experience in the U.S. Air Force and in academia as an information technology and cybersecurity faculty member. The researcher believed these experiences enhanced the awareness, knowledge, and sensitivity to the issues addressed in this study and was beneficial to working with the participants.

Delimitations

Delimitations are characteristics that limit the scope and define the boundaries of a research. The first delimitation was the choice of the research issue, participants and the

site of the study. The choice of underrepresented females in cybersecurity as a research problem implied there may not exist enough of a population sample to complete the study, thereby by selecting a grounded theory methodology and the suggested number of participants between 15 and 20, the sample size was attainable. For this study, a sample size of 25 was requested in order to account for attrition. The location and site of the study is a very heavily populated military town and a very lengthy Department of Defense IRB process approval from the Pentagon is required to conduct research within the federal government framework, including the employees as a focus of a study. The researcher instead conducted the study in the local public library and recruited volunteers regardless of industry. The location and the method of recruitment was selected to eliminate any generalizability concerns of focusing on a particular group. However, there still may be some generalizability concerns since this city is a heavily populated military town with a large presence of defense industry contractors, the results may not be applicable to other non-military towns or cities. In general, there exists criticism of grounded theory regarding generalization, however, Yin (1994) defended that "grounded theory specifically attempts to investigate the real world, usually through interview data and discovers concepts to build theory which minimizes the criticisms" (p. 13).

This research was studied through the lens of social constructivism or interpretivist views through a grounded theory approach. "The assumption is that reality is socially, culturally and historically constructed and that individuals develop subjective meanings of their experiences" (Bloomberg & Volpe, 2016, p. 43). The role of the researcher is to understand those multiple meanings from the perspectives of the participants. Grounded theory is used in studies where little is known about a phenomenon and the purpose is to inductively develop a theory that is grounded in or emerges from the data (Bloomberg &

Volpe, 2016). Corbin and Strauss (2008) suggested that the goal is for the researcher to discover a theory grounded in the participants views.

Definitions of Terms

Cultural bias: For the purpose of this study, cultural bias is defined as interpreting and judging phenomena in terms particular to one's own culture. Cultural bias occurs when people of a culture make assumptions about conventions, including conventions of language, notation, proof, and evidence (D'Hondt, 2016).

Cyberattacks: For the purpose of this study, cyberattacks are defined as illegal activities or a crime that takes place on an information system (i.e., theft of software, data, unauthorized access, or modification of information or attempt to gain access to system services, and resources in order to compromise the confidentiality, integrity and availability of the system (Libicki, Senty, & Pollak, 2014; National Institute of Standards and Technology, 2013, p. 1; Ramim & Levy, 2006).

Cybersecurity: For the purpose of this study, cybersecurity is defined as the ability to protect or defend the use of cyberspace from cyber-attacks (Kissel, 2013).

Cybersecurity professionals: For the purpose of this study, cybersecurity professionals are defined as experienced and qualified workforce to protect networks and information systems (NICE Cybersecurity Workforce Framework, 2017, p. 13).

Gender gap: For the purpose of this study, gender gap is defined as the discrepancy in opportunities, status, attitudes, and so on, between men and women.

Militaristic culture: For the purpose of this study, militaristic culture is defined as the related to military conflict and violence. Or ideology that reflects the level the glorification of military and power, and is male-dominated (D'Hondt, 2016, p. 23).

Retention: For the purpose of this study, retention is defined as workforce retention, an effort to maintain a working environment which supports the current staff remaining with the organization or company. According to the Office of Personnel Management, many retention policies are aimed at addressing the needs of the employees to enhance job satisfaction and reduce the substantial costs involved in hiring and training new staff.

List of Acronyms

DoD – Department of Defense

AFCEA – Communications and Electronics Association AFCEA

CAP – Certified Authorization Professional

CISM- Certified Information Security Manager

CISSP – Certified Information System Security Professional

ISC^2 – International Information Systems Security Certification Consortium

NICE– National Initiative for Cybersecurity Education

NIST– National Institute of Standards and Technology

Summary

Chapter 1 presents the background of cybersecurity and its importance to everyone and every organization that operates in the cyberspace and the significance of a well-trained workforce to adequately defend and protect critical systems and services. This chapter also discussed the overall workforce shortages in the cybersecurity field and the importance of developing and increasing the rate of women in the field may alleviate these shortages. This chapter also discussed the underrepresentation of females in the cybersecurity field as the main problem investigated; and the relevance and significance of increasing not only women in the field, but increasing participation in the field

altogether. The research goal is discussed, along with the problem statement, research questions, the relevance and significance of the study, the barriers and issues, along with the assumptions, limitations, delimitation, and definition of terms used in this research.

Chapter 2

Review of Literature

Introduction

In this chapter, a literature review is presented to provide a synthesis of relevant literature concerning the factors of underrepresentation of females in the cybersecurity field. The limited research published in this field primarily focuses on self-efficacy and student motivation (Amo, 2016; Bashir, Wee, Memon, & Guo, 2017; Lishinski, Yadav, Good, & Enbody, 2016; Roach, McGaughey, & Downey, 2011), lack of encouragement from families (Ashcraft, Eger, & Friend, 2012; D'Hondt, 2016, Fisher, Lang, Craig, & Forgasz, 2015; Wang , Hong, Raviz, & Ivory, 2015), organizational culture, knowledge, skills and abilities (KSAs) (Bagchi-Sen et al., 2010; Huang & Bashir, 2015; Levy, 2005; Ramim & Levy, 2015), the education system, and lack of female role models or mentors (Huang & Bashir, 2015; LeClair et al., 2014; Jethwani, Memon, Seo, & Richer, 2017) as well as conscious and unconscious discrimination and retention factors (Frost & Sullivan, 2017) were prominent in the list of factors and barriers limiting women in the cybersecurity field. Trauth & Quesenberry (2007) suggests the reason for the disproportionate representation of women in the field is a complex and challenging area of study because no single factor can be identified as a root cause. They provided an overview of three theoretical perspectives – the essentialist theory, the social construction theory and the individual differences theory of gender and IT to understand the gender gap in IT fields. They make the argument the essentialist and social construction theories

do not provide the analytical robustness required to pay attention to more nuanced managerial recommendations. They also demonstrate how the individual differences theory of gender and IT can significantly contribute to the reconfiguration of analytical knowledge of the IT gender gap and spur innovative management policies (Trauth & Quesenberry, 2007). However, other studies suggest that finding the commonalities and not differences in gender will be more beneficial to advancing female participation in information technology and cybersecurity fields (Frieze & Quesenberry, 2015). Research on gender and IT tends to focus on gender differences primarily positivist studies with regards to technology adoption (Olbrich, et al., 2015). Trauth suggests that earlier gender research and information systems was predominantly quantitative in nature and focused on gender differences, but has shifted over time to focus only on women, and suggests qualitative approaches in methodology "will bring more richness in the data" and "present more nuances than just research in gender and IT use research" (Olbrich et al., 2015, p. 37).

In review of practitioner and academic literature, there are numerous practitioner and industry research reports on STEM disciplines that include engineering and computing fields as a whole rather than on cybersecurity field independently. The gaps in the literature point to the limited awareness of cybersecurity and its intricacies over other STEM domains as well as limited qualitative studies to give depth and dimension to the issues (Trauth & Quesenberry, 2007; Olbrich et al., 2015). Research on gender issues in cybersecurity is underdeveloped on developing the domains' unique framework and theories as well as advancing awareness of this relatively new field could be that female students do not know the career choices awaiting them. The awareness and newness of

the field, itself, could possibly be deterrent affecting the participation of women in cybersecurity. This would suggest there is a need for a specific discipline understanding.

Self-Efficacy and Student Motivation

Self-efficacy refers to "beliefs in one's capabilities to organize and execute the courses of action required to manage prospective situations" (Bandura, 1995, p. 2). Research has demonstrated that self-efficacy and motivational characteristics influence academic success (Alfassi, 2003; Bandura, 1997; Caraway, Tucker, Reinke, & Hall, 2003; Linnenbrink & Pintrich, 2002; Pintrich & Schunk, 2002; Ramdass & Zimmerman, 2008; Schunk, 2003). Researchers have also found that self-efficacy is one of the primary factors in successfully completing computer tasks, suggesting that self-confidence is very important to a cybersecurity professional (Bashir, Lambert, Wee, & Guo, 2015). Yet, another study proposes that mathematics self-efficacy has an impact on students pursuing STEM related careers (Blotnicky, Franz-Odendaal, French & Joy (2018). Computer self-efficacy pertains to the individual's judgment of their capabilities to use computers in various situations and demonstrates a positive contribution to cybersecurity computing skills (Choi, Levy, & Hovav, 2013; Compeau & Higgins, 1995; Marakas, Yi, & Johnson, 1998). Recent work has shown that self-efficacy and engagement with female mentors and teachers contributed to girls increased interest in cybersecurity field in single gender collaborative settings (Jethwani et al., 2017). Whereas, other research states that female students' self-efficacy rates increased at post cyber camp check points (Amo, 2016). Yet, other studies used cybersecurity competitions to profile the type and mindset of participants for recruitment (Wee, Bashir, & Memon, 2016a, 2016b). These studies appear to be more concerned either in the computer science academic programs and cyber camps in hopes of generating an interest in the field. However, according to Bashir

et al. (2017), research on cybersecurity competitions is still in its embryonic state on how effective these completions are in attracting women to the field.

Mentor and Role Models

Prior studies stress the importance of mentorship and suggest mentoring should begin as early as the fifth grade for females to succeed in STEM-related field (Chioma, 2011; Frieze & Quesenberry, 2015; Poor, 2013; Young, Rudman, Buettner, & McLean, 2013). However, recent studies on cybersecurity and female participation suggests there should be mentors and role models at all levels of the pipeline from early education, college and throughout the career in order to keep women on track, generate an interest, and retain them in the field (Jethwani et al., 2017; LeClair et al., 2014). Other studies suggest that as women look for support and social support in the information technology fields, female mentors and role models are also under represented (Ahuja, 2002; Balcita, Carver, & Soffa, 2002). The literature shows strong support of female roles models in the information technology field and has been identified as a contributing factor in gender imbalance (Ahuja, 2002; Ashcraft et al., 2012). Other studies support that providing appropriate role models to girls can have a positive impact on encouraging and supporting women in IT careers (Ahuja, 2002; Ashcraft et al., 2012; Bandias & Wayne, 2009; Klawe, Whitney, & Simard, 2009). Moreover, Klawe et al. (2009) suggests providing role model interventions, such as ‘female role models speaking to girls in schools to encourage them to study in the IT field but calls for more research on the impact of talks from role models over a longer period of time. Huang and Bashir (2015) investigated challenges, barriers, skills and knowledge required and how women in cybersecurity viewed success from early career throughout their careers. The results

showed that personal factors such as skills, cybersecurity knowledge and job experience set cybersecurity apart from other IT professions and there were different challenges according to each phase of their career. For example, early career phase, the barriers were in terms of lack of actual practical experience in that they possess theory out of college, but no real practitioner experience. They also lacked the experience of working in teams or collaborative environments. Other issues found were 'male dominated work environments' and perceived gender bias. The success factors included reputation among peers and customers seeking advice on security protections (Huang & Bashir, 2015). Bacgchi-Sen et al. (2009) also indicates that as female cybersecurity professionals advance in their career, they face different barriers. Early barriers are technical cybersecurity specific skills and being available 24X7. The most critical skill barrier was communication skills. For career advancement, organizational loyalty, and client relationships were also critical skills. One of the influences that has been cited as a contributing factor to the educational gender gap in technology is the lack of female role models (Pearl, Pollack, Riskin, Thomas, Wolf & Wu, 2002). The US Department of Education (2007) supports that exposing girls to female role models who are successful in math and science can counteract the 'stereotype threat' – negative stereotypes that girls may develop about themselves and those in STEM fields (Lyon & Jafri, 2010).

Organizational Culture

Previous research on the underrepresentation of female representation in cybersecurity can be addressed by organizational and cultural changes (Suby, 2015b). D'Hondt (2016) also proposes that cultural biases and gendered culture contributes in the alienation of women entering in the field. Other recent studies support that by acknowledging the

unique experiences and perspectives of each individual, the organizational culture can be seen as inclusive (Frieze & Quesenberry, 2015). A global cybersecurity study suggests that computer security offers exciting and challenging work, but barriers still remain for women even though there is a perception that anyone with the knowledge, skills, and experience can work in cybersecurity (Suby, 2015a, 2015b). These barriers include both male and female participants viewing computer security as a "man's job" or a masculine by society and perceived gender inequality in recruitment, opportunities, and progression (LeClair & Pheils, 2016; Peacock & Irons, 2017). Even so, the Abraham (2016) study posits there is no difference in terms of global or specific intellectual abilities between men and women, but, significant differences exist in cognitive strategies, functional tasks, and cognitive styles. Hussein, Hirst, Saylers, and Osuji (2014) indicates that organizations are "not gender neutral and inscribe gendered practices, social mores and norms on individuals" and posit that to 'address systemic and structural mechanism which entrench gender inequality", there will need to be 'large-scale' workplace interventions (p. 22). This leads to the supposition that changing the culture of cybersecurity to be inclusive of women, by acknowledging their unique experiences and perspectives, can help bring about their potential and innovative solutions to complex problems. However, women, as a group do not have common backgrounds, values, behaviors and mannerisms, but come from a diverse range of backgrounds, i.e., race, socio economic, geographic and generational (Frieze & Quesenberry, 2015; Trauth & Quesenberry, 2007). With this in mind, women as a group have experienced a wide range of challenges in history, needs and aspirations and goals. Therefore, more cross-cultural comparisons are needed to examine a range of diverse factors encouraging women to participate in IT fields and science (Frieze & Quesenberry, 2015; Schiebinger &

Schiebinger, 2001). The individual difference theory accounts for a diverse perspective of people and does not generalize individuals by demographic group (Trauth & Quesenberry, 2007, p. 29). Adam and Richardson (2001) explain that gender research should emphasize the making of knowledge through the lived experiences of women's lives and is important because a more detailed analysis is required in organizational settings versus typical approaches.

Educational System

Studies that suggest the educational system influences skills development and recommend that the learning environment be expanded to be 'inclusive' of female students and so that 'female students' can negotiate the environment (Margolis & Fisher, 2001; Nielsen et al., 2000). However, Frieze & Quesenberry, 2016 suggests that by simply changing the educational system or making 'girl friendly' curriculum may work against the efforts of attracting females to the cybersecurity field. They suggest not focusing on the differences between females and male students, but on the sameness and by looking for the differences may further enhance the gender divide (Frieze & Quesenberry, 2016). A 2014 Google study proposes that the lack of opportunity at an early age to take computer courses before entering college may also be a contributing factor as to why many students, including women not pursuing a technical major (Google, 2014). Adya & Kaiser (2005) indicated that access to computers at home and in school can generate interest among students to pursue computer science, a feeder field for cybersecurity, at the university level. The Google study also indicated that by taking computer courses and early exposure to computer science before college can increase the interest and establish a sense of competency in female students and lead to a decision to purse a technology major (Google, 2014). Another study recommends that college

campuses should continue to emphasize how majoring in technology will create future job opportunities with excellent salary prospect; reimage the technology major to be 'inclusive' instead of having it seen as the 'stereotypical' nerdy or smart students only major (Jung, Clark, Patterson, & Pence, 2016, p. 7.) Jung et al. (2016) also suggests the following in regard to generating female interest in technology majors:

1. Recruitment to technology majors should be implemented in science courses as an alternative because results of the study showed males and females switch majors from a science related course or engineering due to 'difficulty'.
2. Beginner programming courses should be offered to middle school, high school and college students to increase exposure to programming at an earlier age.
3. One on one tutors should be available to help students in the programming courses to increase the student's confidence and understanding before college.
4. AP Computer Science should be made more readily available to students in high school.
5. Female technology role models should be more prominent on television. Incorporate more women in technical roles on television or media. These women can show the benefits of majoring in technology and not always following the 'nerd' stereotype (Jung, 2016, p. 6).

Jung et al. (2016) also suggests that future research should also focus on retention in the major and target women in the field to determine their satisfaction with the courses and the major and what influences are causing women to leave the field (p. 6).

Family Encouragement

The support and encouragement of the family has also been suggested to have an impact on students selecting a technical field or STEM domain and may have the same impact on selecting cybersecurity as a career field as well (Ashcraft et al., 2012; Google, 2014; National Center for Women & Information Technology, 2015, 2012). According to National Center for Women & Information Technology, another influential factor on whether women choose a technology related major or field may reside with parental support. In 2012, pre-college and college majors were asked to participate in a survey to gather data about their selection of majors and asked who was the most influential in their selection. 30% respondents selected 'myself"; 25% selected parents; 19% selected high school teacher and less than 10% selected peers (George-Jackson, 2012). The 2014 Google study observed that women who were computer science graduates were more likely to have their mother or father encourage them to study computer science compared to graduates of other degrees (Google, 2014). Wang et al. (2015) suggests the decision to pursue, computer science, which is also a feeder field for cybersecurity, lies with the family and early exposure to computers and technology.

A 2012 study by the National Center for Women & Technology posits encouragement of parents to go into a field of technology was the most influential factor compared to peers, teachers and counselors (Ashcraft et al., 2012). Whereas, Turner, Brent, and Percora (2002) posits that the occupation of one's parents may also contributed to the reasoning as to whether or not women choose to major in technology. However, Ashcraft et al. (2012) argues that there is no single answer to changing girls interest in the Information Technology fields and suggests large scale social change will take time and will involve many people including teachers, family and role models and requires a

longitudinal and qualitative studies on interventions to determine impacts (Ashcraft et al., 2012; Fisher et al., 2015). It is apparent family encouragement and early exposure to technology is an important factor to bringing females into the cybersecurity field and is "crucial to examine the societal and family factors and what impacts it has on cybersecurity professionals, but also on those who are influential in their encouragement in their lives" (D'Hondt, 2016, p. 11).

Knowledge, Skills, and Abilities

Cybersecurity knowledge, skills, and experience have been found to be barriers that female cybersecurity professionals face in early stages of their cybersecurity profession (Bagchi-Sen et al., 2010; Huang & Bashir, 2015). Levy (2005) defined skill as a combination of knowledge, experience and abilities that enable users to perform well. Cybersecurity computing skill (CCS) is stated as the knowledge, ability and experience of an individual to use protective applications to protect computers, computer networks and IS (Levy, 2005). Ramin and Levy (2006) posits that limited technology knowledge and skill is linked to Information systems failure and increasing CCS will increase the security of the IS. Acquiring skill is a learning process across several stages (Anderson, 1982). These stages begin with an initial declarative stage where instruction and information regarding a particular skill is given to the user (Anderson, 1982; Fitts, 1964). The user establishes the knowledge as a foundation for the next stages in stage 1. The second stage allows the user to practice the knowledge acquired in the first stage and transforms it to procedural knowledge (Fitts; 1964; Neves & Anderson, 1981. Knowledge becomes more organized and users begin to connect the actions required to complete a task. The last stage is called automaticity (Fitz, 1964; Marcolin, Compeau, Munro &

Huff, 2000). This stage is more efficient and autonomous by increasing the experience level (Anderson, 1982). As the experience level increases so does the competency level as the skill is practiced over time (Ramin & Levy, 2015).

The National Institute of Cybersecurity Education (NICE) cybersecurity workforce framework Special Publication (SP) 800-181 establishes the taxonomy and lexicon to describe the cybersecurity workforce that can be used and applied to the public, private and academic sectors. The framework identifies the knowledge, skills and abilities (KSAs) required for a cybersecurity professional based on the following components:

- Seven Categories – overarching grouping of common cybersecurity functions
- 33 Specialty areas – distinct areas of cybersecurity work
- 53 Work roles – detailed groupings of cybersecurity work that include specific knowledge, skills, and abilities (KSAs) required to perform cybersecurity tasks in the work role.

The KSAs as defined by SP 800-181 area 'attributes required to perform tasks, generally demonstrated through relevant experience or performance based on education and training" (NIST SP 800-181).

The NICE framework aids several key stakeholders in the cybersecurity community to include employers, future and current cybersecurity professionals, training and certification providers, education and technology providers. Employers can use the framework to assess their current workforce KSAs and determine the gaps for continuous training and for recruiting and hiring future cybersecurity professionals. Future and current cybersecurity professionals can use the framework to develop their skills and KSAs. Education and academic providers can utilize the framework as a resource when

developing curriculum and research related to the KSAs and technology providers can use the framework to assess their services, hardware and software products they provide.

Cybersecurity knowledge, skills, and abilities have been found to be barriers that female cybersecurity professionals face in their cybersecurity profession in early stages of their careers (Bagchi-Sen et al., 2010; Huang & Bashir, 2015). In latter stages, the barriers include a shortage of communication, teamwork, assertiveness, and experiencing gender bias in male-dominated work environments (Bagchi-Sen et al., 2010; Huang & Bashir, 2015). Still, the most critical skills barrier is the deficiency of effective communication skills (Bagchi-Sen et al., 2010). However, for career advancement, teamwork, and organizational loyalty, client relationships have also been noted as critical skills (Frost & Sullivan, 2017).

Huang and Bashir (2015) investigated the psychological factors of motivational and cognitive processes as it relates to gender differences in the information assurance field. They investigated the challenges, barriers, skills, and knowledge required and how women in cybersecurity view success from early career throughout their careers. The results showed personal factors (i.e., skills, cybersecurity knowledge, and job experience) that set cybersecurity apart from other information technology professions. Early career barriers were in terms of shortage of actual practical experience in that they possessed theory out of college, but a deficiency in practical experience and working in collaborative team environments (Huang & Bashir, 2015).

As the woman cybersecurity professional's career advances, they face different barriers. Early career, the barriers are technical skills and effective communication skills (Bagchi-Sen et al., 2010). For career advancement, teamwork, organizational loyalty, and client relationships were critical skills. Women who have advanced to management roles,

also have a wider range of a variety of undergraduate degrees than men in the cybersecurity field (Frost & Sullivan, 2017). According to the report, this reflects different skillsets, backgrounds that illustrate that females without a STEM education can bring richness to the profession (Frost & Sullivan, 2017).

In addressing the experience barrier, there are multiple academic and organizational initiatives to increase skills and awareness. For example, supporting cybersecurity education in primary schools, offering internships in higher education, pairing new hires with mentors and compensating with not only monetary but also non-monetary incentives (Jethwani et al., 2017; LeClair et al., 2014; Suby, 2015a, 2015b). Other efforts in higher education have been made to align cybersecurity curriculum with the 10 ISC^2 domains to increase the probability of successful cybersecurity certification testing required by most cybersecurity jobs (Ashford, Koohang, & Floyd, 2012; Smith, Koohang, & Behling, 2010). The Ashford et al. (2012) study disclosed that male and female students equally had a positive view toward acquiring the knowledge and skills during their educational career. Technical knowledge, skills, and practical experience play an important role in the cybersecurity field for women as well as men. However, to acquire the right skills at the right time can be a daunting task as technology and complexity of threats are ever changing.

Discrimination

Discrimination is another factor that deters women from the cybersecurity field even though there are laws against it. Discrimination against women in cybersecurity is more prevalent the higher a woman rises in rank (Frost & Sullivan, 2017). Their report suggested that over 51% of women participants experienced some form of discrimination

in their cybersecurity careers. According to the 2017 Global Information Security Workforce Study on women in cybersecurity, unconscious discrimination ranked at 87% with overt discrimination at 19% (Frost & Sullivan, 2017). In terms of career advancement, other studies suggest barriers include females having reservations with being assertive and being in male-dominated work environments where gender bias is prevalent (Huang & Bashir, 2015). A recent gender study on women programmers also suggests gender bias exists in the open source software community as men's contributions were accepted higher rate than women, but only when their profile identifies them as female (Terrell et al., 2016). LeClair and Pheils (2016) discuss key issues preventing women from remaining in STEM fields and found that 63% have experienced some form sexual harassment, and suggest organizations need to reinforce the importance that women can make in the cybersecurity field and implement solutions that cause women to leave the field.

Congress enacted the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002, known as the "No Fear Act," which requires federal agencies to be accountable for violations of antidiscrimination and whistleblower protection laws. The underlying premise is that agencies cannot be run effectively if they practice or tolerate discrimination in the workplace (Office of Inspector General, 2002). This law only applies to federal agencies and it provides provisions for employees or applicants who believe they are a victim of discrimination. However, the law does not assume that discrimination does not exist in federal agencies, but it would be prudent to assume that less discrimination occurs in federal agencies versus private sector corporations.

Retention

Retention is a factor will be defined in this study as cybersecurity workforce retention, an effort to maintain a working environment which supports the current staff remaining with the organization or company. Dropout rates of women in STEM/IT and cybersecurity arenas is a troubling issue since more than half of the women in these fields leave during their 20s to mid 30s (Melymuke, 2008). There are many factors influencing females to leave the STEM field including pay gaps, discrimination and low rates of advancement due to "social institutional and personal challenges" (Bagchi-Sen et al., 2010, p. 47). Other factors include job or climate dissatisfaction, pressure from family issues, lack of social change, and lack of support from employers for advancement (LeClair et al., 2014). LeClair et al. (2014) also calls for more research to reduce the male/female imbalance in technological fields and suggest that guidance and role models can lead women into technology, but once they are in the field, efforts should be made to increase the likelihood that they will stay. Suby (2015a, 2015b) suggests that organizations must take direct action to improve retention. Those suggestions include supporting cybersecurity education in primary schools, offering internships, pairing new hires with mentors, and compensating with not only monetary means, but also non-monetary incentives, i.e., flexible work arrangements and diverse training options. The Office of Personnel Management advocate that many retention strategies are aimed at addressing the needs of the employees to enhance job satisfaction and reduce the substantial costs involved in hiring and training new staff and provides an impact on an employee's decision to stay or leave. According to Frost and Sullivan (2017), organizations should reflect on how different skillsets, backgrounds, and interdisciplinary

skills can be used to recruit women in the cybersecurity workforce. It is clear that retention is difficult for a number of reasons which consists of both internal and external factors. Frieze and Quesenberry (2015) focuses on cultural changes that can affect recruitment, retention and promotion of women in computer science and IT fields. They suggest "that different and/or similar ways in which students relate to computing, are a large part the product of a specific culture and environment and are not produced by any intrinsic distinctions between men and women" (Frieze & Quesenberry, 2015, p. 109). They suggest that using gender alone is not a determining factor as to why women pursue opportunities in computer science, but is a combination of many factors including not only demographic differences, but also socio-cultural factors (Frieze & Quesenberry, 2015; Trauth & Quesenberry 2012;).

Summary

In summary, there are multiple studies on generating interests of girls to pursue cybersecurity for K–12 grades and universities through cyber camps or competitions (Amo, 2016; Bashir et al., 2017; Jethwani et al., 2017; Lishinski et al., 2016). Yet, other studies suggest that female mentors starting in early academic throughout career stages with encouragement from family and teachers will generate participation in the field (Chioma, 2011; Frieze & Queensberry, 2015; LeClair et al., 2014; Poor, 2013; Suby, 2015b; Young et al., 2013). Calls for qualitative research on gender in the information technology fields and generating theory of its own have been noted which can bring out the nuances in the field as well as presenting more richness in the data (Olbrich et al., 2015). However, future research in computing and IT fields should not only examine demographic factors, but also cultural, environment, and organizational factors to

examine recruitment and retention of females (Frieze & Quesenberry, 2015; Trauth & Quesenberry, 2012; Trauth, Quesenberry & Huang, 2009). Very few qualitative studies were found that examined female cybersecurity professionals in the workplace, with the exception of three that investigated barriers women face as they advance through their careers and serves as a guide for this research (Bagchi-Sen et al., 2010; Huang & Bashir, 2015; LeClair et al., 2014). In search of studies on female cybersecurity professionals currently in the field, a small number of studies were found and quite possibly due to so few female cybersecurity professionals exist in the field to be able to have an acceptable sample. Because this topic is currently one of the critical issues in cybersecurity, there is a probability of a plethora of emerging studies in the very near future. Based on the prior literature, it is clear that the barriers and factors preventing females entering into the cybersecurity field is a large and complex issue and as diverse as women themselves. In interpretation of the literature, the major barriers found included self-efficacy, encouragement from families, teachers, early access to computers, mentors, organizational culture change, retention efforts and the knowledge, skills and abilities should provide the stimulus to increase the interests and participation in the cybersecurity fields. However, the calls for qualitative studies of female cybersecurity professionals and generation of cybersecurity theories are guiding this study (Ashcraft et al., 2012; Fisher et al., 2015). Even though the issue is complex, it is clear that there are both internal and external factors that influence females to pursue the cybersecurity field.

Chapter 3

Methodology

Approach

This study utilized a grounded theory approach to identify the structure of experiences as described by the research participants. This approach was selected to understand the perspectives of the participants and explore the meaning they give to observe a process in depth (Creswell, 2009, 2013). It is suggested that when the goal of the research is to develop a conceptual model for building theory around a specified phenomenon or process, an interpretive approach utilizing a qualitative methodology may be appropriate (Levy, 2006). A qualitative approach allowed the elaboration of perceptions and views to emerge into patterns and themes instead of numerical data studies that would limit the study in strict boundaries or parameters. Qualitative research was used to focus on the participants' perspectives, their meanings, and multiple views (Creswell, 2009, 2013). This study employed a grounded theory approach to describe the experiences of females in the cybersecurity field (Charmaz, 2014). The focus was the development of a theory grounded in data from the field and the type of problem best suited for investigating problems based on the views of the participants (Charmaz, 2014; Creswell, 2009, 2013; Glaser & Strauss, 1967; Terrell, 2016).

This research aligned well with qualitative research as opposed to quantitative as it is "suited to promoting a deeper level of understanding of a social setting or activity viewed from the research participant's perspective" (Bloomberg & Volpe, 2016, p. 38). Because

the research purpose was to better understand the reasons for the significant underrepresentation of females in the cybersecurity field, qualitative research was used to delve deeper into the essence of issues and discovered holistically a fuller and richer data than quantitative. However, quantitative research does allow for gathering consensus of the norm, investigating cause-and-effect relationships and quantifying results, but does not seek to provide a range and variation in findings or to discover and understand meaning of an experience (Bloomberg & Volpe, 2016). This research determined the perceptions of the participants' experiences in the cybersecurity field to answer the research question, and provide a theoretical framework to aid organizations and academia in promoting females in the field.

In constructing a grounded theory design, the research question was formed based on the literature review and gaps in the literature, participants were recruited to collect the data and analysis began with coding, categorization with constant comparative methods. After the coding processes, links were formed to construct a theoretical framework to answer the research question. In summary, the research methodology for this study fit well with grounded theory because of how the research participants make sense of their experiences, then the researcher conducted an analytic sense of the meanings and actions through the use of grounded theory.

The design of this research began with the site approval letter (see Appendix A) and an approval from the IRB (see Appendix B). Then followed a development of the participant recruitment email (see Appendix C) and development of a script or guide for the researcher during the interview session to help keep the interview on track (see Appendix D). The script developed by the researcher was submitted to subject matter experts to validate whether the script questions answered the research questions. Next,

the participant recruitment began with a research pamphlet (see Appendix E) via recruitment activity in two professional organizations, ISC^2 and Armed Forces Communications and Electronics Association (AFCEA). ISC^2 is an information systems security organization and AFCEA is computer engineering professional organization. Both have local membership organizations in the location of the research. A request to AFCEA for research volunteers was made prior to granting access to their membership. The president of the local AFCEA chapter invited the researcher to discuss the purpose of the research and recruit volunteers. The ISC^2 local chapter membership conducted monthly meetings in proximity to the site location and allowed the researcher to address the membership for volunteers, as well as in other sponsored cybersecurity forums. No more than 12 participants were interviewed and were held in the local public library meeting rooms. Flyers were distributed during ISC^2, cybersecurity forums, cybersecurity conferences and AFCEA membership meetings to recruit volunteers; each volunteer received information by email regarding the study and a consent form (see Appendix F). Once the consent form was signed and participants agreed to the interview, each interview was scheduled. Data collection was in the form of recorded audio and transcribed, Data analysis began with coding each line of the transcription and then linking codes for themes and development of a theoretical framework, and finally, a dissertation report on the findings are presented.

Sample

The population characteristics in this study were female cybersecurity professionals. In absence of a direct database of the population; a subset of that population was used. The participants were purposefully selected because of their unique expertise and

participation in the cybersecurity field. Purposeful sampling is commonly used in qualitative research and involves selecting research participants according to the needs of the study (Glaser & Strauss, 1992). This type of sampling is used in qualitative studies to purposely select participants that meet certain criteria (Terrell, 2012; Terrell, 2016). The selection criteria for inclusion were female, age 18 and older, and have been in the cybersecurity field for at least one year. The sampling was conducted through volunteer participation from local ISC^2 chapter memberships and from the AFCEA, an international nonprofit professional organization focused on increasing knowledge of issues in information technology, communications and electronics for the defense, homeland security and intelligence communities. Due to the concentration of federal and defense industry workers in this small community, the likelihood of participants connected in some fashion to the federal government was high. According to the ISC^2 Workforce study, the highest percentages per industry of women in cybersecurity are in the federal government in DoD and are required per DoD Directive 8570 to possess an Internet security certification to work in the field. Participants were recruited and interviewed until theoretical saturation of data was achieved. Saturation is the point at which data replicates and no new information emerges from the interviews (Morse, Barrett, Mayan, Olson, & Spiers, 2002). Explicit guidelines regarding the number of participants in a grounded theory study is conflicting and there is not a general consensus on the exact number; however, what is, recommended is the guidance on data saturation. The sample number of participants in a grounded theory study has been generally been determined to be in the range of 15 to 20 participants or until theoretical saturation has been attained. This study anticipated data saturation at 20 participants; however, the researcher recruited

25 participants to allow for attrition. Data saturation was obtained by the 12th participant where further recruitment was terminated.

Instrumentation

The data was collected via interviews focusing on the study's research questions. An interview protocol was developed by the researcher used only as a guide or script. The interview questions reflected the study's research questions (See Appendix D). The interview protocol script with questions were validated by experts in the field and used only as a guide to keep the flow of the interview at a constant pace and on target.

Reliability and Validity

As noted, member-checking was used to determine the accuracy of the findings through taking the final report or specific descriptions or themes back to participants to determine accuracy (Creswell, 2009, 2013). Validity was ensured through trustworthiness, authenticity, and credibility (Creswell & Miller, 2000). Trustworthiness was determined by credibility, transferability, dependability, and confirmability. *Credibility* was accomplished by analyzing the data through the process of reflecting, sifting, exploring, justifying its relevance and meaning, and ultimately developing themes and essences that accurately depict the experience. Credibility was established through member checking by sending participants their transcripts for review and verification. *Transferability* refers to the 'applicability of the findings to another setting. *Transferability* was accomplished with specific descriptions of the research, participants, methodology, interpretation and emerging theory (Sikolia, Biros, Mason, & Weiser, 2013). *Dependability* was established with audit trails to provide the maintenance and

preservation of the transcripts, notes, and audio files. *Authenticity* refers to the reporting of each participant's experiences so that it maintains respect for the context of the data and presents all perspectives equally so that the reader can arrive at an impartial decision. *Confirmability* was determined by linking the data to their sources (Creswell, 2009, 2013; Creswell & Miller, 2000).

Data Collection Procedures

The data collected from interview transcripts were analyzed inductively so that the results can be used to understand a specific scenario or event (Terrell, 2016). A protocol consisting of standard interview questions was developed and used as a guide or script to conduct the interviews and to obtain the data. This research used open-ended questions in the interview protocol which allowed the participants the freedom to express their thoughts and feelings on the subject matter. Follow-up and probing questions were used during the interview in order to get an in depth understanding and clarification of the answer. The participant's information was recorded with the participant's approval and anonymity provisions. Additional sub questions were utilized as needed. The sample questionnaire script was initially field tested with two subject matter experts to assess the type of questions, validity and reliability of the data and revised as needed.

Other data collected during the interview were descriptive statistics on the demographics of the participants, such as age, education, industry, and certifications in the cybersecurity field. Once the interview data was collected on the digital recorder, it was transferred to a computer and encrypted to protect confidentiality. The interview transcripts were professionally transcribed to add to the validity of the process. Significant statements and phrases were extracted from each transcript and organized into

themes; the consolidation of which was consolidated into categories and an overarching theme.

Data Analysis

This study used data from interviews and field notes to identify overarching themes, develop coding schemes and presented a narrative analysis for holistic insights into the phenomenon. Data analysis began with open-coding of the transcripts to discover general ideas and to identify axial codes that relate to overarching themes. Selective coding was then subsequently used to link the axial codes into the overarching theme which is the core of grounded theory (Terrell, Snyder, & Dringus, 2012).

For a grounded theory study, it is suggested to create and organize files for data (interview transcripts); read through the transcript text and make margin notes and form initial codes (Creswell, 2013, p. 190); next describe the open coding categories and select one open coding category for a central phenomenon in process, then engage in axial coding which identifies the causal condition, context, intervening conditions, strategies, or consequence (Creswell, 2013, p. 190). Next, to interpret the data, selective coding was accomplished to make sense of the findings and lastly, representing or visualizing the data to present a model or theory and present any propositions (Creswell, 2013, p. 191). The data is represented in forms of tables, diagrams and narrative forms to aid with understanding of each stage of the process and the resultant framework or model.

Process

The data collection procedures began with recruitment brochures (See Appendix A) dispersed through cyber forums, cybersecurity conferences and cybersecurity

professional membership meetings to recruit volunteers that met the criteria. The criteria were that the participant be a current female cybersecurity professional, over the age of 18 and in the field over one year. The next step was gathering the contact information of those interested in participating in the study and then sent recruitment letters (See Appendix C) explaining the research. A copy of the research study informed consent for (Appendix F) was given to the participants to read and sign. Once the participants agreed to participate, an interview was scheduled at the approved location for approximately 30-45 minutes. The interview consisted of open ended questions (See Appendix D for sample questions). The researcher used a handheld digital recorder to record each interview. The data collected from interviews and transcripts and were analyzed inductively so that the results can be used to understand a specific scenario or event (Terrell, 2016). A protocol consisting of a standard interview questions were used as a guide or script to conduct the interviews and to obtain the data. This researcher used open-ended questions in the interview protocol allowing the participants the freedom of expressing their thoughts and feelings on the subject matter. Follow-up and probing questions were asked during the interview in order to get an in depth understanding of the answer. The participant's information was recorded with the participant's approval and anonymity provisions. Additional sub-questions were utilized when needed. The sample questionnaire script was initially field tested with two subject matter experts to assess the type of questions, validity and reliability of the data.

Other data collected during the interview was descriptive in nature on the demographics of the participants on the demographics of the participants, such as age, education, industry, and certifications in the cybersecurity field. Once the interview data was collected on the digital recorder, it was transferred to a computer and encrypted to

protect confidentiality. The interview transcripts were then professionally transcribed to add to the validity of the process. Significant statements and phrases were extracted from each transcript, coded, and then organized into themes; the consolidation of which was consolidated into categories and an overarching theme.

Validation was ensured by allowing participants to view and comment on the researcher's descriptive results. Triangulation from different data sources was used to build coherent justification for the themes and a summary is presented in the findings section. In addition, grounded theorists recommend researchers begin analytical processes during the interviews and use memoing to record any observations. However, because the interviews were recorded, notetaking or memoing was not required.

Resource Requirements

Participants

- Access to female cybersecurity professionals in the United States: The sample was collected from a sample population through volunteer recruitment from ISC^2 membership and AFCEA membership and cybersecurity forums or conferences. This sample was approved prior to the beginning of the study through the IRB process.

Subject Matter Experts

- Access to cybersecurity subject matter experts from academia, industry, and military were available to review accuracy of results.

Summary

Chapter 3 includes a discussion on the research design and methodology for this research to include the rationale for the particular approach, and how this particular phenomenon aligned well with the proposed methodology. Next, a discussion of the research settings and context were discussed by providing background and issues germane to the problem. Then, a discussion on the research sample and the selection criteria for participants, data collection methods, data analysis methods, issues of trustworthiness, limitations and delimitations, and concludes with the resources utilized to accomplish this research.

The research purpose is to better understand the reasons for the significant underrepresentation of females in the cybersecurity field and develop a theory or framework that will provide holistic insights to academicians and practitioners in developing future cyber professionals.

Chapter 4

Results

Overview

Outlined within this chapter are the results of the data analysis for this research investigation. The results for this study were completed over several steps. Details of

each step are presented in the order conducted. The first step details the data collection from qualitative interviews; the interview recordings were then professionally transcribed verbatim and imported into the qualitative data analysis (QDA) software *Quirkos* to analyze the data line-by-line. In the second step, data analysis was immediately conducted during and after the interviews with notes and after each batch of interviews, transcripts were immediately forwarded to the transcriptionist. This means that steps one and two overlapped as data analysis begins during and after each interview. The researcher forwarded interview recordings to the transcriptionist immediately following each interview. Data analysis began as soon as possible to identify similar themes and determine when data saturation became apparent.

The results of the first and second step address the main research question through qualitative grounded theory coding analysis themes. In the third step, development of a theoretical model is presented that may assist in future research of this type and to aid in future cybersecurity professional development.

The Research Question

This research study using in-depth interviews began with an overarching research question designed to explore factors that would engage females to pursue the cybersecurity and generate a substantive theory to increase the participation rate of females in the field. The main research question was supplemented with additional sub-questions only to clarify how they feel about females in the cybersecurity field and any factors that may have discouraged them along their journey as successful cybersecurity professionals. Initially, the question regarding the factors that discourage females from entering the field became a sub-interview question as the participants focused more on

the strategies to attract females to the field. The question regarding the discouraging factors is still important in this study to understand what issues can be addressed, however, the discouraging factors and the strategies were in direct opposition of each other. Discussion on the factors and barriers are also included in this study to illustrate the polar opposition of the data obtained. The main research question also aligns to perceived strategies that can be implemented to increase the participation rate of females in the cybersecurity field:

Overarching Research Question:

- What are the factors that attract females to the cybersecurity field?

Sub or probing interview questions:

- How are females represented in the cybersecurity field?
- What are the factors that discourage females from entering the cybersecurity field?
- What strategies can be developed to encourage females to the cybersecurity field?

In this study, the participants had strong opinions on how to engage females in the cybersecurity field. They suggested that providing awareness and early exposure of technology and computers would result in increased self-efficacy. In turn, contributing to an interest and passion in computing and security. Initially, some of the participants were reluctant to answer if they experienced any factors or barriers on their journey to the field, yet, as the interview proceeded, they began to offer more details. The overarching theme of factors and barriers were lack of awareness, lack of support and most importantly, the perception that the cybersecurity field is predominantly male-dominated.

This chapter details the data analysis and findings through the process of interviewing, coding, and generating substantive theory and themes.

Researcher Role and Bias

The researchers' bias may stem from professional experience as a cybersecurity professional and as a cybersecurity professor. This researcher possesses over 30 years of experience in the information technology field; primarily in the information and cybersecurity field with the United States Department of the Air Force as a federal employee. The researcher is highly security-minded with a will to protect national security information systems and its users. Security of the information systems and its users are the utmost importance for a Department of the Defense cybersecurity professional. The researcher is also a cybersecurity professor who has taught at a local university for 8 years (7 years as an adjunct and the last year as a full time professor). Bias may be rooted in not only women not engaging the field, but also cybersecurity being a male dominated culture not welcoming or taking the female perspectives and diversity into consideration when developing creative solutions. Therefore, these biases are from two perspectives – the male dominated culture and reasons why women shy away from the field.

The challenge of this researchers' bias requires rigor to avoid imposing personal views upon the data and the ability to block out experiences that occurred in past. The advantage of the use of bias is to increase the sensitivity to hear what the participants are telling the researcher (Corbin & Strauss, 2008). It is also advantageous that the field terminology and the government terminology and background is known to the researcher. Having some interest and knowledge of the field itself will allow the researcher to

understand the perspectives of the participants. This researchers' objective is to hear what is said with sensitivity and to capture the significances with "the creativity and feeling that gives qualitative research its soul" (Corbin & Strauss, 2008, p. 90).

Participants

In order to participate in this study, participants must have been a female over the age of 18 and in a cybersecurity career field for at least one year. A recruitment brochure was distributed in cybersecurity forums and at conferences, with a recruitment letter sent to 25 interested participants randomly selected from the total eligible. Fifteen potential participants contacted the researcher to express an interest in participating in the research. Twelve of those participants were interviewed while three could not participate due to scheduling conflicts. The participants took part in a recorded interview. Demographic information related to education, industry, and cybersecurity certifications were obtained during the interview for each participant. All twelve participants were located in the southeastern United States and interviews were conducted during May and June of 2018.

Data Analysis

Data analysis included the data collection, demographic analysis, and data coding analysis. Through the use of grounded theory coding and constant comparison techniques, themes, and categories emerged from the data. During the data analysis stage, overarching themes and relationships were revealed that led to the proposition of a theoretical framework.

Data Collection

The data collection began with identifying subject-matter experts in cybersecurity for in-depth interviews on their perceptions of females in the field and how to encourage and

attract them to the cybersecurity field. During the two separate cybersecurity forums and conferences, the researcher distributed brochures to interested female cybersecurity specialists, once a list of 25 proposed participants was gathered, the researcher followed up with an emailed letter and telephone calls to each explaining the specifics of the study. Fifteen participants agreed to participate and interviews were scheduled to gather the data. Once they agreed to participate, interviews were scheduled to discuss and gather the data. The projected time for the interviews were 30 to 45 minutes. The actual interviews ranged from seven to 31 minutes. The researcher scheduled the interviews in a library located in southern Georgia. The interviews were conducted over a four-week period in May of 2018. A limited number of participants rescheduled the interview, which increased the interview schedule timeframe. The rescheduling was due to conflicts and work demands. The interview schedules were designed to allow the participants to meet with the researcher at their convenience and the majority of the participants elected to be interviewed after work hours. The library hours were from 10:00 am until 6:00 pm, so the interview schedule had to be scheduled within this time-frame. The research location was remote for the researcher (approximately a 30-minute drive time away from researchers' office), therefore, interviews were scheduled in succession on some days to make better use of time. Interviews ensued following participant agreement to be recorded and signed the informed consent form. Once the interviews were completed, each participant was offered a ten-dollar gift card as gratuity for participation.

The participants ranged from the mid-20s to early 60s in age, were all female and cybersecurity professionals. They all lived within a 20-mile radius of the geographical location and worked either for a government contractor or for the federal government as this location is heavily populated with federal employees and a federal installation. This

federal installation, however, is the largest industrial complex employer in the State of Georgia with 25K-plus employees.

Immediately after recording an interview, each audio file was reviewed to ensure the recording was successful. The audio files were sent to a professional transcriptionist and returned to the researcher within 24 hours. The verbatim transcripts resulted in 112 pages. The transcripts were reviewed for accuracy and imported into a qualitative data analysis software (QDAS) tool*, Quirkos*. This software allowed the researcher to code and understand the data by managing, sorting and exploring the data. *Quirkos* also generated a summary report of 161 pages. The primary function of a QDAS tool is to manage the qualitative data of the project. However, the analysis part is the responsibility of the researcher. Twelve respondents were successfully interviewed. They were assigned aliases in documentation and transcripts to provide anonymity. From the initial interview recording, the researcher noted the concepts and themes of each participant as they occurred. Pilot interviews were conducted with the first two participants to confirm the interview script would satisfy the purpose of the study. The first two transcripts were forwarded to a qualitative subject matter expert to also determine if the research questions were being answered and to gain advice on interview skills for the subsequent interviews. The transcripts represent the raw data.

Demographic Analysis

The demographic data was gathered during each interview, recorded in the transcript and entered into a spreadsheet. Table 1 provides an understanding of the participant data set. The ages of the participants ranged from 26 to 62 and with over 75% over the age of 40. 83% of the participants were federal government cybersecurity professionals and 17% were defense contractors in the cybersecurity field. 75% of the participants possessed

Security+ certifications and all but two had more than one certification; only one participant did not possess a certification and was a mid-level manager of a cybersecurity office.

Table 1

Descriptive Statistics for the Population (N=12)

Characteristic	***N***	**Percentage (%)**
Age		
25-34	2	17%
35-44	3	25%
45-54	3	25%
55-59	2	17%
60-64	2	17%
Academic Level		
College Degree	6	50%
Graduate Degree	6	50%

Table 1 (cont.)

Descriptive Statistics for the Population (N=12)

Characteristic	***N***	**Percentage (%)**
Security Certification		
Security+	8	66%
CISSP	3	25%
CISM	1	8%
CAP	1	8%
Test Out Security Pro Certified Computer User	1	8%
Industry		
Federal Government	10	83%
Defense Industry Contractor	2	17%

Education levels varied from Associates to Master's degree and in varied fields. Fifty percent possessed a Master's degree and ranged from Masters in Information Technology, Information Technology Management, Information Systems and Technology Management, Business Administration, Cybersecurity, and Business. The undergraduate degrees ranged from fields such as Computer Science, Accounting,

Chemical Engineering, Business Administration, Information Technology, Geology, and Pre-Med (Biology).

Data Coding

This research employs the classic grounded theory in which the coding phases are open coding, selective coding, and theoretical coding. Through coding, the researcher defines what is in the data and begins to grapple with what it means (Creswell, 2007). "The coding strategy divided the narrative data into discrete units of analysis (quotes) relative to the themes embedded in the words of the participants" (Jethwani et al., 2017, p. 11). During the initial open coding stage**,** the researcher generated as many ideas as possible inductively from the data called open coding. Selective Coding was conducted in the next stage which is more focused in pursuit of central codes throughout the dataset. This required decisions about which initial codes were more prevalent and contributed to the analysis. In the last stage, theoretical coding occurred in which the researcher refined the final categories and related or linked them to one another. Charmaz emphasizes coding quickly and keeping the codes relatively similar to the data as possible. The transcripts were read and re-read to identify the general concepts and identified them with *Quirkos* using color coding. Initial or open coding stage of analyzing data is where the data are coded for all possibilities (Glaser, 1978). In this phase, the data was analyzed line-by-line. The initial coding procedures generated 33 codes with 758 occurrences. These open codes were then categorized into 14 subgroups and through axial coding further classified the open codes into 8 axial codes. The selective coding phase allows the researcher to code only the data that sufficiently relates to the core category, called inductive methodology. In this phase, the focus is on a core category (Glaser, 1978). The researcher continues to saturate the core category and related categories, delimiting data

collection and analysis to establish the boundaries of an emerging theory. Once theoretical saturation is reached, the researcher begins theoretical coding to outline a theory. Theoretical saturation was achieved by the 12th interview as data was found to be recurring with no new concepts noted.

Theoretical coding is the fundamental step in classic grounded theory. The aim is to explore the relationships between the core category and related categories to develop a set of conceptual linking hypotheses that integrate into a final theoretical framework. Theoretical coding allows for a model for integrating theory by arranging the substantive codes together into an organized structure (Glaser, 1978). The coding system was developed by the researcher, the subject matter experts, and research advisor.

Constant Comparative Method

The constant comparative method and theoretical sampling are the core of qualitative analysis in ground theory research (Boeije, 2002; Glaser, 1992; Glaser & Strauss, 1967; Strauss, 1987). The researcher began the grounded theory analysis constant comparative method by comparing codes and data searching for overarching themes as shown in Figure 1. This method was used to also determine at what point data saturation occurred.

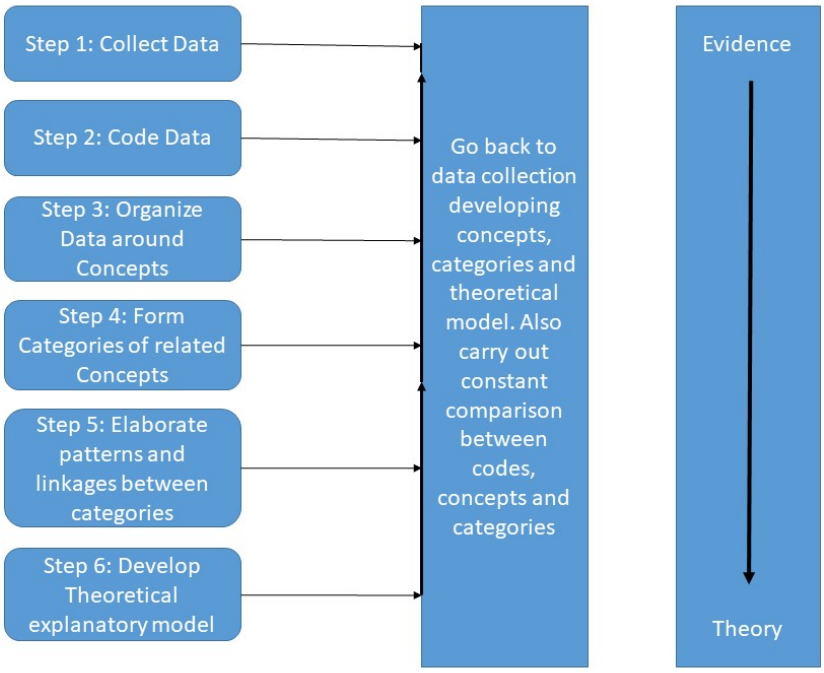

Figure 1. Grounded theory data analysis steps (O'Hagan & O'Connor, 2015, p. 7).

In the grounded theory analysis constant comparative method, the researcher collected the data from the interview transcripts and proceeded to code, organized and categorized the data around core concepts. The researcher arranged the categories in related concepts to discover patterns, linkages or relationships between the categories (Boeije, 2002). Lastly, the researcher developed a theoretical model to help explain the results of the study.

Coding began with verbatim or in vivo codes from the interview transcript or raw data. Then sorted or grouped into categories and subcategories, from the categories, a general overarching theme or concepts emerge. From these themes or concepts, relationships were investigated to propose the theoretical framework. Coding progressed from real data to more abstract as the theory emerged. This process advanced from

particular codes to more generalized categories and themes during the coding process as indicated by Figure 2.

An example of coding in text transcripts may be seen in Figure 3. Each interview transcript was worked line-by-line to discover any codes, categories and overarching themes. The next section will discuss the results of the coding analysis.

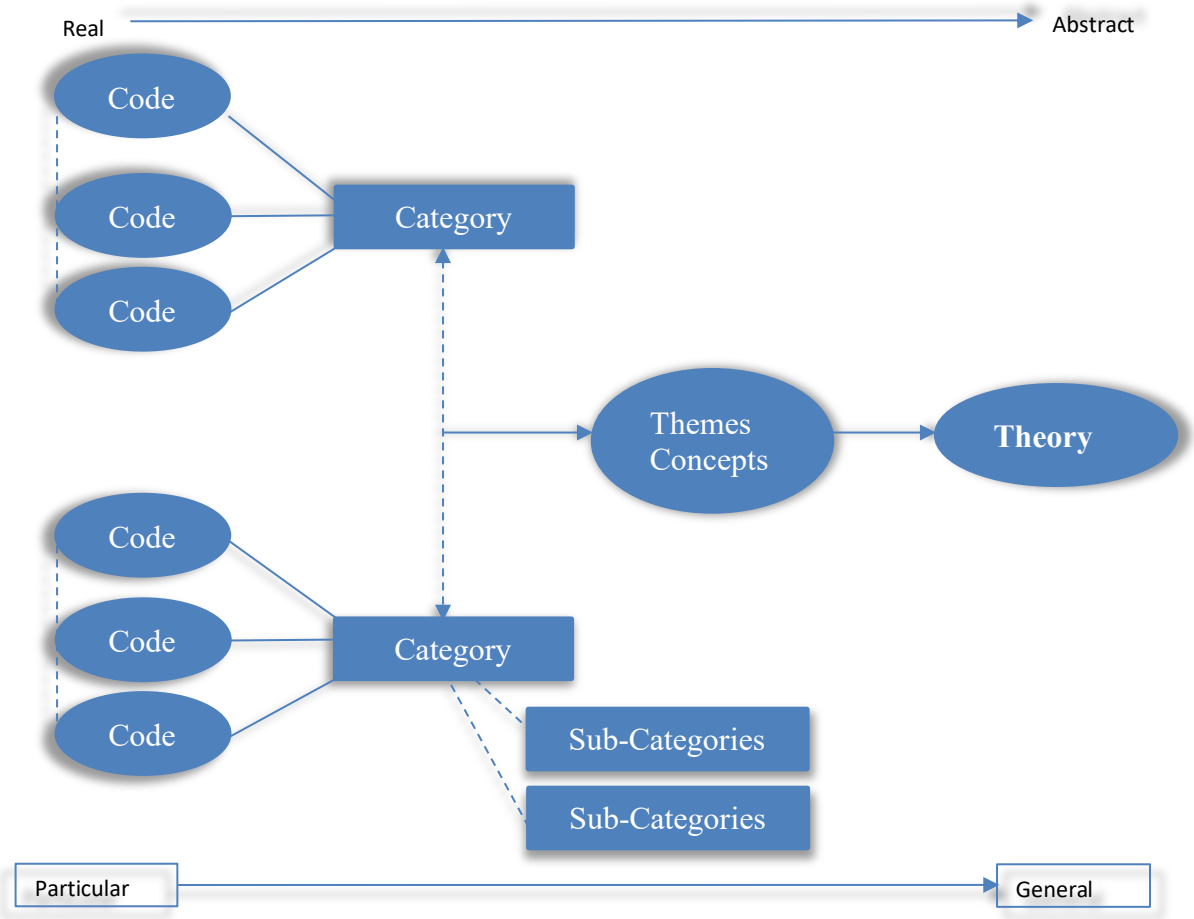

Figure 2. Diagram of a streamlined codes-to-theory model for qualitative inquiry (Saldana, 2016).

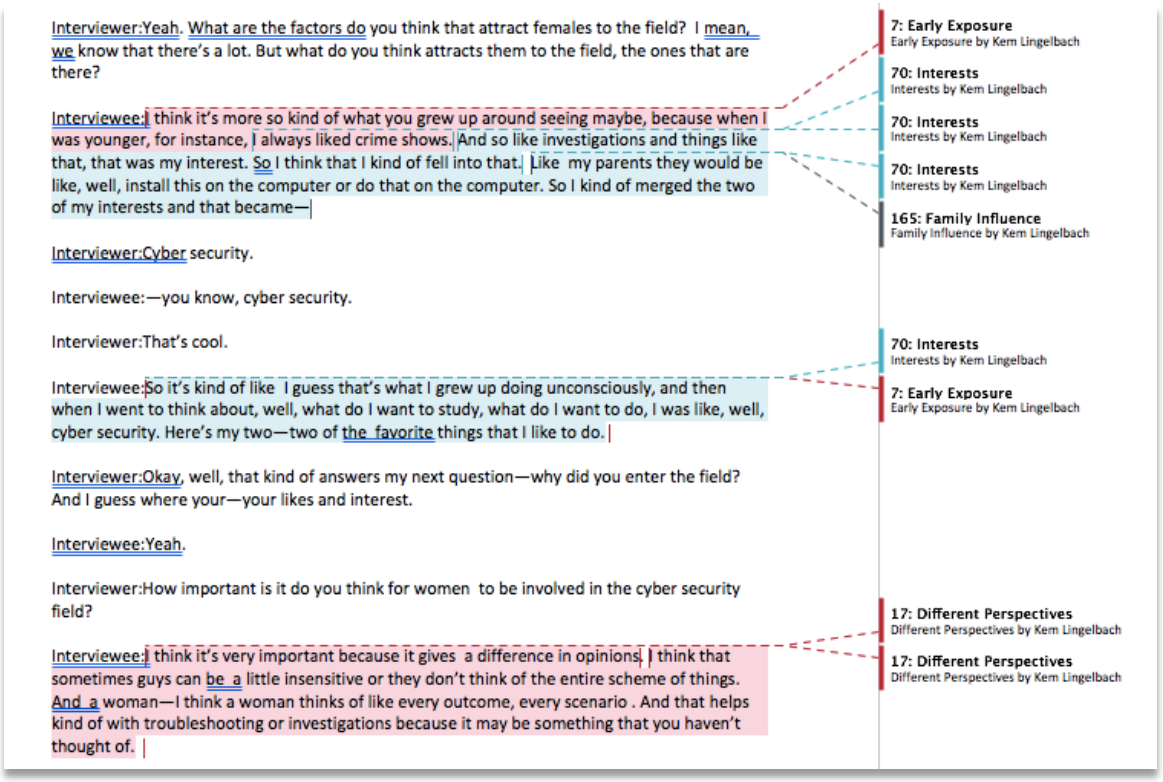

Figure 3. Coding example of an interview transcript.

Coding Analysis

Initial Coding

The initial coding procedures generated 35 codes with 767 occurrences as shown in Table 2. These open codes were then categorized into 14 subgroups and through axial coding further classified the open codes into eight axial codes. During selective coding, the eight axial codes were narrowed down to five codes. Those five overall themes were Awareness, Support, Intrinsic Factors, and Extrinsic Factors. Another theme emerged, that merits attention, was one of the personal characteristics or mindset factors. This unanticipated theme represents a profile that females should possess to increase the potential for successful cybersecurity career path. The sub-questions assisted in developing the factors to attract females to the field. The first sub-question regarding the

factors and barriers experienced by female cybersecurity professionals resulted in factors, such as the cybersecurity field is a male-dominated field and the culture is not accepting of females. Other factors seen in direct opposite of the factors that attract females to the field were a lack of awareness, support, mentors and role models, as well as intrinsic and extrinsic factors. Another sub-question relating to how females feel women are represented in the field generated results such as low representation overall. Only one participant stated the rate of women is equal to that of men in her office.

These factors were perceived by the participants to be contributing factors that can influence a female's career path decision in cybersecurity. The following is examples of the initial and selective coding in *Quirkos*, the codes that have the most occurrences are considered to be significant in the study. The codes that have only one or two occurrences are dropped from the results or removed during the selective coding processes.

Table 2

Summary of Open and Axial Codes

Initial or Open Codes	**No. of Occurrences**	**Axial Codes**
Awareness	66	Awareness
Interest	84	Profile Characteristics
Support Groups	33	Support
Experience	76	KSA
Education	43	Awareness
Culture	38	Culture
Knowledge	28	Profile Characteristics
Early Exposure	48	Awareness
Communication Skills	21	KSA
Confidence	13	Self-efficacy
Stereotyped	11	Discrimination
Pay	14	Extrinsic
STEM Program	46	Awareness
Male Dominated Field	31	Culture
Fun	29	Intrinsic
Mentor	28	Support

Table 2 (cont.)

Summary of Open and Axial Codes

Initial or Open Codes	No. of Occurrences	Axial Codes
Math	28	Education
Family	25	Support
Skills	17	KSA
Technical (minded)	13	Profile Characteristics
Assertiveness	8	Self-efficacy
Discrimination	8	Discrimination
Exciting	8	Intrinsic
Profile (Characteristics)	6	Profile Characteristics
Hands On Skills	6	KSA
Networking (Group Support)	6	Support
Personal Characteristics	5	Profile Characteristics
Challenging	4	Intrinsic
Security Minded	4	Profile Characteristics
Role Models	3	Support
Abilities	3	KSA
Pride	3	Extrinsic
Training	4	KSA
Certifications	5	KSA
Conferences	2	Awareness
35 Codes	**767 Occurrences**	**14 Categories**

Quirkos screenshots are illustrated in Figure 4 of the initial open coding, and selective coding of the awareness factor. For example, the awareness factor includes early exposure and STEM programs as the major themes. The interview transcripts are analyzed line by line, and color coded according to the open codes or quirks, then are more generalized through selective coding. This hierarchical view in Figure 4 illustrates the awareness theme.

Figure 4. Quirkos example of qualitative coding.

Selective Coding

Selective coding was conducted following axial coding to categorize the codes into generalized groups**.** From the axial codes, selective codes were generated which reduced fourteen themes to eight. These selective codes were either attraction factors, discouraging, or both as indicated in Table 3.

Table 2

Summary of Selective Codes – First Iteration of Attraction and Discouraging Factors

Selective Code	No. of Occurrences	Factor
Awareness and Exposure	205	Attraction/Discouraging
Knowledge, Skills, & Abilities (KSAs)	132	Attraction/Discouraging
Intrinsic	125	Attraction
Support	95	Attraction/Discouraging
Culture	69	Discouraging
Personal Characteristics Profile	68	Attraction/Discouraging
Discrimination	19	Discouraging
Extrinsic	17	Attraction

In the next refinement, Knowledge, Skills, and Abilities were aligned under the personal characteristics profile were aligned as indicated in Table 4. Early exposure and education were aligned under the category of awareness. The codes that were only discouraging factors, according to the perceptions of the participants, were removed because they do not answer the main research question. The codes that are both discouraging factors and attraction factors were retained as indicated in Table 4.

Table 4

Summary of Selective Codes – Second Iteration

Selective Code	No. of Occurrences	Factor
Awareness	205	Attraction/Discouraging
Personal Characteristics Profile	132	Attraction/Discouraging
Intrinsic	125	Attraction
Support	95	Attraction/Discouraging
Extrinsic	17	Attraction

Theoretical Coding

Several theoretical codes emerged from the coding process to answer the research question, one code is chosen as the theoretical code for the study. The theoretical theme strategies and engagement factors are comprised of the awareness, support, intrinsic and extrinsic categories. Strategies and engagement factors along with the unexpected

personal profile characteristics factor are proposed to lead to a successful cybersecurity career trajectory. The study's theoretical code is the relational model through which all codes/categories are related to the core category. Theoretical codes conceptualize how the substantive codes may relate to each other. The substantive codes break down or fracture the data while the theoretical codes weave the fractured story back together again (Glaser, 1978, p. 72).

Discouraging Factors Discussion

As stated previously, the discouraging factors did not answer the research question but aided in this research. A sub-question regarding discouraging factors the participants experienced was probed to uncover negative factors that could be addressed in answering the research question. During further category refinement, the factors or barriers that discourage females from entering the cybersecurity field were observed. A short summary on these factors is discussed in this section.

The participants perceived the cybersecurity culture and discrimination factors in a negative sense. That is, the culture is not accepting of women and is primarily male-dominated, which are barriers for women. Table 5 presents the factors that discourage females from entering the field included lack of awareness of the cybersecurity field that included the perception of the field being too complex and too hard to obtain certification, a male-dominated culture, feelings of not feeling valued and lack of support. Some participants indicated they felt they were discriminated against simply for being a woman and were stereotyped. Results from the main research question on factors that attract and the sub-question on discouraging factors were in direct opposition. However,

since the overall goal was to find out how to encourage females to the field, the factors that discourage aided in uncovering the factors that attract.

Table 5

Theoretical Codes – Discouraging Factors

Theoretical Code	No. of Occurrences	Factor
Awareness	114	Attraction/Discouraging
Support	95	Attraction/Discouraging
Experience	76	Discouraging
Culture	69	Discouraging
Discrimination	19	Discouraging

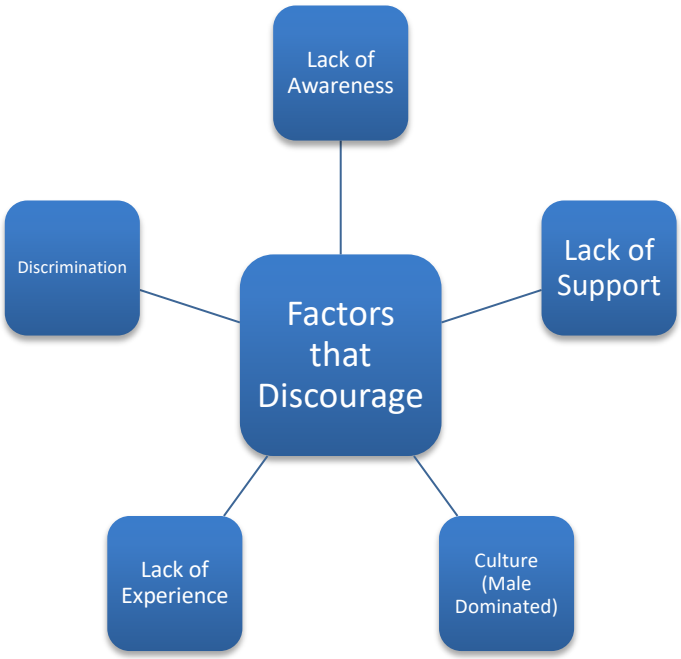

Figure 5. Diagram of factors that discourage females from cybersecurity.

Factors that Attract Females to the Cybersecurity Field

The factors that attract or draw females to the cybersecurity field is the main research issue. The overarching themes across all participant perceptions were awareness, support, intrinsic, and extrinsic factors. The following is an example of each theme and participant's quotes to illustrate the findings are grounded in the data. Table 6 presents

the selective codes, occurrences, and factors for attracting females to the field. This indicates that both awareness, exposure, and support can affect negatively or positively the participation rate.

Table 6

Summary of Theoretical Codes – Attraction Factors

Theoretical Code	No. of Occurrences	Factor
Awareness	114	Attraction/Discouraging
Intrinsic	125	Attraction
Support	95	Attraction/Discouraging
Extrinsic	17	Attraction

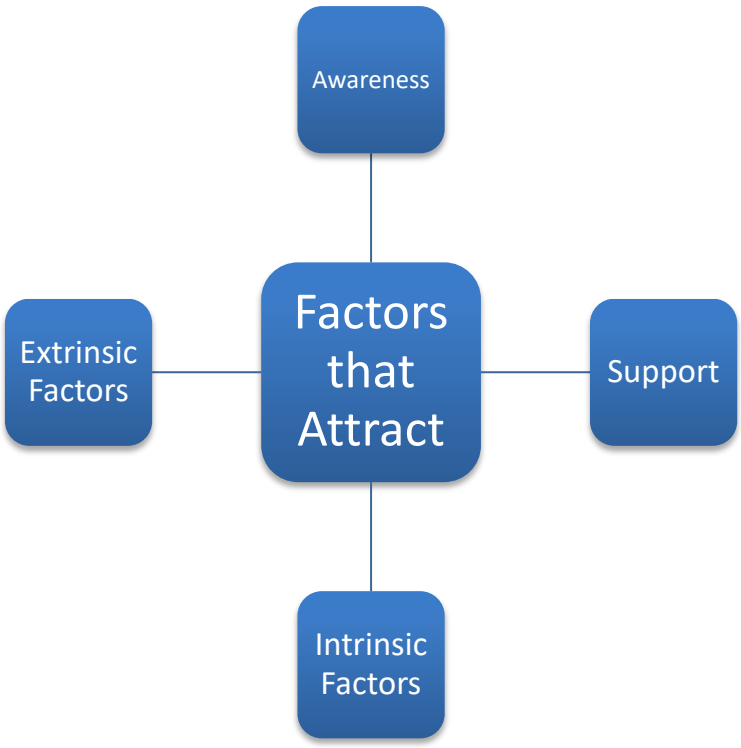

Figure 6. Diagram of factors that attract females to the cybersecurity field.

Personal Characteristics Profile Factor

An unexpected prominent category emerged during data analysis that included personal characteristic factors. The participant's perception is that if the female fits a certain profile then it is more likely that females will be engaged and pursue the

cybersecurity career field. This factor is in line with research that utilized cybersecurity competitions to recruit females based on a profile or mindset (Wee et al., 2016a, 2016b). The top factor in this theme is a natural inherent interest in technology or a natural affinity to computers, among other factors in this theme, included self-efficacy factors, such as assertiveness; KSAs, especially communication skills, as well as analytical mindset and being technically savvy. Other factors were mentioned, but not prevalent in this research.

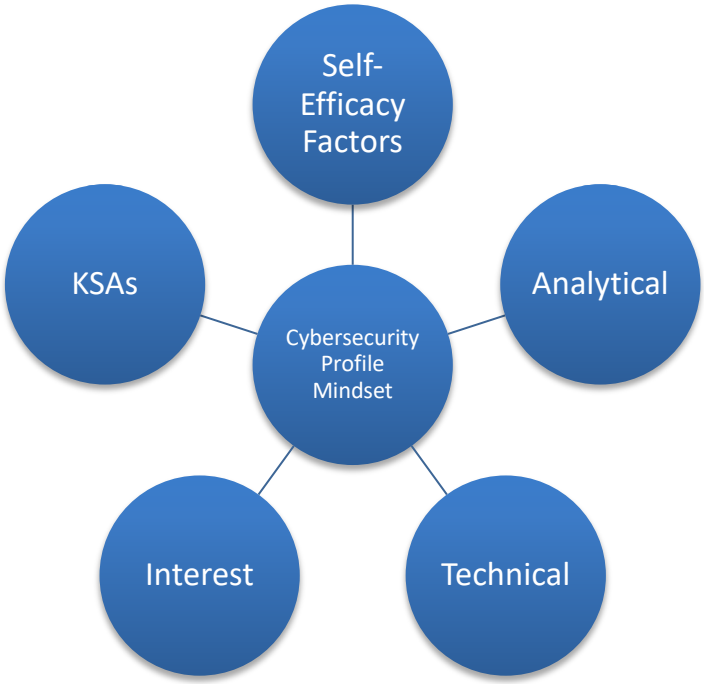

Figure 7. Diagram of cybersecurity profile mindset factors.

Findings

Findings were consistent according to qualitative approaches and include quotes from interviews to support the findings. The approach is a grounded theory study which has the aim of generating theoretical constructs. The overarching main research question is

"What are the factors that attract females to the cybersecurity field?" The overarching themes across all participant perceptions are the factors of awareness and exposure, support, interests and, intrinsic and extrinsic factors and possessing certain personal characteristics answers the main research question. The following is an example of each theme and participant's quotes to illustrate the findings are grounded in the data. Each theme according to the research questions will be discussed in the next section.

Perceptions of Females in the Cybersecurity Field

Participants agree that there is a definite perception of low representation of females across the cybersecurity field. Participant's provided instances or examples from their own workplaces. In several instances, they were the only females in their office. Participant number 4 gave possible reasons for the low participation rates:

> *"I don't think there's[there are] very many women at all. We are very rare. Maybe they don't feel like they are wanted in the industry. You kind of feel like an outsider. You look around in meetings and you are like, I'm like, whoa, I'm like the only girl in here. You know, you have everybody kind of looking at you like that's the only girl in here, you know. It's like an eye-opening experience, but it's almost like a keep going kind of thing. Maybe you're knocking down barriers for someone else, another female to come behind you."*

Participant 11 agreed concerning the low participant rate:

> *"They're seriously underrepresented and part of this is the usual, girls are not encouraged to go into science and technology."*

Participant 9 also agreed in that females are not represented in the cybersecurity field but has hope this will change:

> *"The large majority [in the cybersecurity field] is still male, it is getting, in my opinion, from what I've seen, over the last ten plus years, the pendulum is swinging just a little bit to where it's more diverse….so I feel that it's going to change, but I think it's going to take some time."*

Awareness

The participants suggested an awareness that includes early exposure and education will increase confidence and interest in cybersecurity. In agreement with the literature, there exists limited awareness of cybersecurity and its intricacies over other STEM domains as well as limited qualitative studies to give depth and dimension to the issues (Olbrich et al., 2015; Trauth & Quesenberry, 2007). Engaging with early exposure of technology and cybersecurity awareness as well as knowledge and practice can increase confidence and self-efficacy (Amo, 2016; Anwar et al., 2017; Bagchi-Sen et al., 2010; Konak, 2018; Pelham, 1991; Turner, Deemer, Tims, Corbett, & Mhire, 2014; Zeldin & Pajares, 2000). Figure 8 illustrates the results of the *Awareness* theme. Open coding consists of early exposure from K-12, STEM and Cyber programs, computers in the home, computers and technology courses along with math and science courses. The axial or selective codes exposure and education are groups or more generalized categories that were selected to group the open codes and finally, the *Awareness* theoretical code which is more abstract includes exposure and education.

Participant 1 expressed her idea of educating girls early: “Early education, like elementary age, having girls participate in computer related activities”. Participant 1 also states: I would say, too—like you were saying earlier about the programs and stuff, the STEM programs for girls. They didn’t have that when I was growing up. I think that would help increase females coming into the industry. Nearly all participants agreed that early education and exposure is needed. Participant 2 explained:

> Exposure. Early Exposure, you know, from kindergarten on up, and introducing it more in schools. They do have those girl camps, but they do not have them here locally. I mean, I think they are beginning to get around the world but they haven’t made it yet. Because I’ve looked at them for both my kids.

Participant 8 also agrees early education can increase engagement in the field*:*

> I think if we start educating them [female students] early, getting them engaged, and then they'll [they will] be excited about it [cybersecurity], and become confident in it. And so, as they move on into [higher] grade level, middle school, and then high school, and then college, secondary education, they will be comfortable in the field.

Participant 4 suggests awareness and exposure can benefit girls pursuing cybersecurity though programming programs:

> I like the outreach programs that they have, like Girls Can Code. I love that. So those type of things to start them [female students] when they are younger and develop them to get excited about cybersecurity and the computer industry.

In summary, Figure 8 illustrates the results of the *Awareness* theme. Open coding consists of early exposure from K-12, STEM, and Cyber programs, computers in the home, computers and technology courses along with math and science courses. The axial or selective codes exposure and education are groups or more generalized categories that were selected to group the open codes and finally, the *Awareness* theoretical code which is more abstract includes exposure and education.

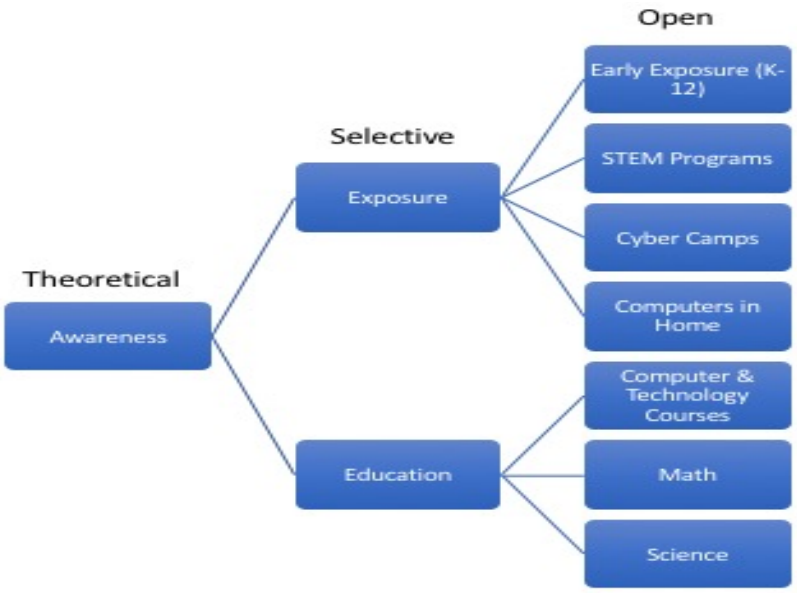

Figure 8. Diagram of open, selective and theoretical codes for awareness.

Support

Support groups such as networking groups, cybersecurity conferences and industry conferences, STEM programs, family influences as well as role models and mentors were suggested to help young girls become aware of cybersecurity.

Mentors and Role Models

Participant 11 believed that opportunities and role models will help girls become engaged**:**

> When I used to fence, my fencing coach said, 'If you want girls to do something, you provide them with a group to do it in, and let them have fun, and they'll do anything.' He was a world-class coach. And I think providing girls with that opportunity, and also providing them with role models, really helps a lot.

Participant 9 suggested solutions for mentors: "We have to try and figure out when we are in the process of mentoring and the communication and awareness is finding people's strengths, realizing what their strengths are and using those things along with tools, to

enhance their abilities that they can provide on the cybersecurity side." Participant 9 also stated: "I've had a lot of great mentors. And just being encouraging, just, you know—and helping". Participant 8 suggested mentors should be females in the field: "We, as professionals, we, as women in the field, have to open up others' eyes and make them aware". Participant 11 believed support groups, mentoring and visiting the schools will help: "Support groups, mentoring, actually going to the schools, engaging early and letting them see a woman in the field". Participant 4 again agreed that women mentors and role models are needed: "And have women mentors and things like that. I think that seeing a woman is encouraging on its own, but to see a woman in the cybersecurity field and they may say, hey, I want to be like her".

Organizational Support

The participants believed that by having organizational support, peer support and opportunities females will be encouraged to pursue the field of cybersecurity. Participant 5 illustrates how her supervisor encouraged her to grow and pursue the cybersecurity field:

> My supervisor at the time said, 'You would be very good at blah, blah, blah, security engineering kind of thing, if we get you spun up. And I was like, 'Whatever.' And that's kind of where I went. Coming into that and being exposed to it and—'Here, try that. See what you can do with that.' You know, getting to know the coworkers and what they were doing. And they would give you a little bit and you would do that and—'Oh, try that.' You know, do a little bit more. 'Oh, try that.' And before I knew it I was one of the team.

Participant 10 has received support from her male peers in the field:

> I've gotten a lot of support from males in this field. By just having that support and definitely letting women know that, you know, this is something you can do and that you are wanted in this field. And I have been seeing a lot of articles about that. I've been seeing a lot of things out there on LinkedIn and the schools. So, yeah, just continue putting it out there that this is something they can do and it is fun, it is interesting. If they like

> puzzles, you know, problem-solving, these brain puzzles which, you know—then it's a good place to be.

Family Influence

The participants agreed that family influence including support and having a computer in the home had an effect on attracting her to the cybersecurity field. Participant 1 states that having a mother that works full time and three brothers had an effect on her attraction to the cybersecurity field. Participant 1 suggested that how you were raised may have had an effect on how she views herself and does not see that she is any different from a man:

> Okay, another thing I would say that it is how you were raised. I was raised by my dad. My mom worked primarily all of the time, so it was my dad and my three brothers. So, I didn't see myself as being any different than them, so if something happened along the way as far as some type of discrimination because I'm a female, I wouldn't even notice it because I was raised that anything a man can do, I can do better.

Participant 4 believes the support she received from her parents and having access to a computer at home during her younger years influenced her interest in computers: "Like my parents, they would be like, well, install this on the computer or do that on the computer. So, I kind of merged the two of my interests…". Participant 5 also had a computer at home: "Our first family computer, I was 15". Participant 10 grew up not doing the traditional 'girl things' and had more male friends than female friends: As a child, I'd get into my grandfather's tool -well, he had a junk drawer that he had his tools and stuff in it, and I'd go around taking things apart. So, they already knew…you know as far as mechanical skills, I had more of that drive. I didn't play with dolls and you know, babies and stuff like that. I was more - all of my friends were males. So, for me it wasn't intimidating because I was always around guys and I had better relationships with guys. So, I had no problem working with a bunch of guys. I was like, ooh, that's going to be fun!

Intrinsic Factors

Several intrinsic factors are seen by the participants as being instrumental in attracting females to the cybersecurity field. Those factors include having a natural interest in the field, seeing cybersecurity as fun, exciting, challenging, and rewarding.

Interest

Almost all participants agreed there must be an interest in technology and computers. Having a natural interest and affinity to computers, networking and cybersecurity is what led some of the participants to the cybersecurity field as stated by participant 4:

> I guess that's what I grew up doing unconsciously, and then when I went to think about, well, what do I want to study, what do I want to do, I was well, cybersecurity. Here's my two of the favorite things that I like to do. Yeah, I think some of the interest will be natural…

Participant 10 also agreed that interest in technology is natural interest: "For me personally, it was just something that came to me naturally. I was always very aware of the things that – what it took to be secure and I have always had a drive towards technology". Participant 11 believed that networking classes led to her interest:

> I ended up taking networking classes and liking them and there have been studies that show that girls in elementary school are just as interested in science as boys and then it drops out in middle school. So, I think programs that would encourage girls to continue through middle school and high school and get them through that period in time—once they're in college then they 've got more of a mindset of yes, this is interesting, I want to do it. I think that that's probably another thing that really needs to be addressed is those middle grades up through high school.

Fun, Exciting, Challenging, and Rewarding

Participant 10 believed that cybersecurity is fun:

> It's not just a matter of numbers and coding and programming and knowing the hardware. It's a higher level of thinking that's, yeah, interesting and fun. So just continue putting it out there that this is something they [girls] can do and it is fun. If they like puzzles, like problem-solving, brain puzzles…then, it's a good place to be.

Participant 12 also agreed*:* "Or learning, learning networking it's kind of—I think it's kind of fun. I'm kind of a nerd, I guess. Because that's all puzzles".

Extrinsic Factors

Extrinsic factors such as salary, opportunities, independence and sense of contribution were discussed as being factors to pursue the cybersecurity field. Participant 6 feels like she is contributing to something worthwhile:

> I feel like I get to really contribute in a way that matters. I mean, you know, I've had some jobs that I felt like, you know, I'm not really doing anything, you know, that's worth anything and I feel like, you know, in this way I feel like I'm really contributing toward something.

Participant 12 thought cybersecurity is the best job and the salary is attractive:

> Pay scales are great, especially in the civilian world, for cyber and I got into IT because I was 28 years old, about to be divorced and I needed a job and a career that would pay well and I flipped through college catalogs and I thought this is what I want to do. And oddly enough, I've enjoyed every minute of it. It's the best job anybody could have.

Participant 5 believed cybersecurity is challenging**:** "It's very challenging and it can be very rewarding, but I can't think of a single thing that would pull me into this if I had not fallen into it and just was good at it". Participant 5 also considers this her way of contributing to her county: "I consider this the way I serve my county. It's the only way I can".

Personal Characteristics Mindset Profile

Perceptions of personal characteristics such as analytical thinkers, and being 'tech-savvy' is also a contributing factor to pursue the cybersecurity field. Other personal characteristics the participants felt that may impact females entrance into the field is a profile fitness for the field. Participants felt that females that 'fit a profile' will provide successful entry and retention in the cybersecurity field. Such profile characteristics

include personal interests, knowledge, skills, & abilities, prior experience, assertiveness, personality, and self-efficacy factors. Prior research indicates that a person may fit a certain profile that will enable successful entry and successful. All participants' perceptions indicate that some level of personal characteristics will contribute to engage females in cybersecurity field.

Participant 4 believed: "If I wasn't personally technically savvy, why would I choose to be in the [cybersecurity] field"? Experience is a major player according to participant 6: "They have critical positions they've got to fill and you can't find anybody that has experience or education or knowledge". Participant 8 agreed that knowledge is important: "And we want to make sure that women stay knowledgeable. That is key. You have to have the certification, stay subscribed in something. Read IT professional. We have to keep them knowledgeable. You need to stay current – technology changes". Participant 8 also perceived that understanding the cybersecurity field is important:

> Understanding your field is number one. Don't get comfortable in just one particular area. Don't concentrate on one area. Become an expert in one area but knowledgeable in several areas. And I think that will be the key to attracting them and how to maintain [retain] them.

Participant 3 believed that self-efficacy factors play a big role:

> If they want to say something they speak their mind. And I think that could be a barrier if a woman is not prepared and equipped to trust in herself and trust and be self-confident and just push forward, you know. But I believe if we start educating our girls early, they get the confidence, self-esteem, knowledge, and then they're unstoppable. I just think they'll be totally unstoppable and they can go any direction they want. get confidence in them

> and tell them they're just more than, you know, just a female, and most of all you're just a female mind—I've heard that one as well! And so, yes, a powerful female mind. And take whatever that negative comment is, make it positive, make it work for you.

Participant 9 explained communication, awareness and understanding the field is important: "I keep mentioning communication, understanding, awareness, training. All those things to me are key". Other participants believed personality and physical appearance could have an effect on pursuing the field.

Participant 9 stated: "I think, you know, sometimes if you have a meek, mild-mannered female, it might not bode well and they may go home crying at night". Participant 9 also stated: "So, if we can, you know, track that somehow to what the KSAs are, what's your person's knowledge, skill, and abilities are, we may be more successful in the field". Participant 6 believes that because of the way a female looks, may have an effect on how people view them: "Well, and it's like sometimes, you know—like I think one time, there was a pretty girl and they're like oh, yeah, she doesn't know anything about IT". Participant 9 also mentioned that she feels she has been taken more seriously because of her physical characteristics: "So sometimes I feel like, you know, sometimes I do get taken advantage of—I mean, not taken advantage of but taken a little bit more seriously because I'm not, you know, super pretty". However, other factors include having experience, participant 12 indicated:

> So, I mean, it [cybersecurity] does require you to have, especially the Government require[s] you to have certifications. And so that's a lot of training, especially if you don't really have any hands-on IT background experience. I found having the hands-on experience to be probably one of my biggest challenges. I mean, I had to learn Linux commands and things that I—that wasn't something I had done before. But everything you look at [job listings] says they want you to have experience first.

Summary of Results

This chapter details the evolution of the research project as it unfolded from data collection that includes interviewing, coding, and generating substantive theory and themes. The overall view from the participant perspective is there exists a definite low participation rate of female's in the cybersecurity workforce, they give their perceptions regarding the factors and barriers they or others have encountered in their careers or in their own lived experiences in pursuit of the field. They give insights that allow the readers to understand the factors that can draw females to the field. Strategies and solutions are presented that include awareness, early exposure to technology and computers, family influence and support, to having female mentors and role models encourage young females.

Theoretical Model

The resulting theoretical model in Figure 9 is presented based on the evidence grounded in the data. The theoretical framework indicates strategies and engagement factors together with a cybersecurity profile mindset will enable successful cybersecurity career trajectory. A discussion of this model is presented in this section.

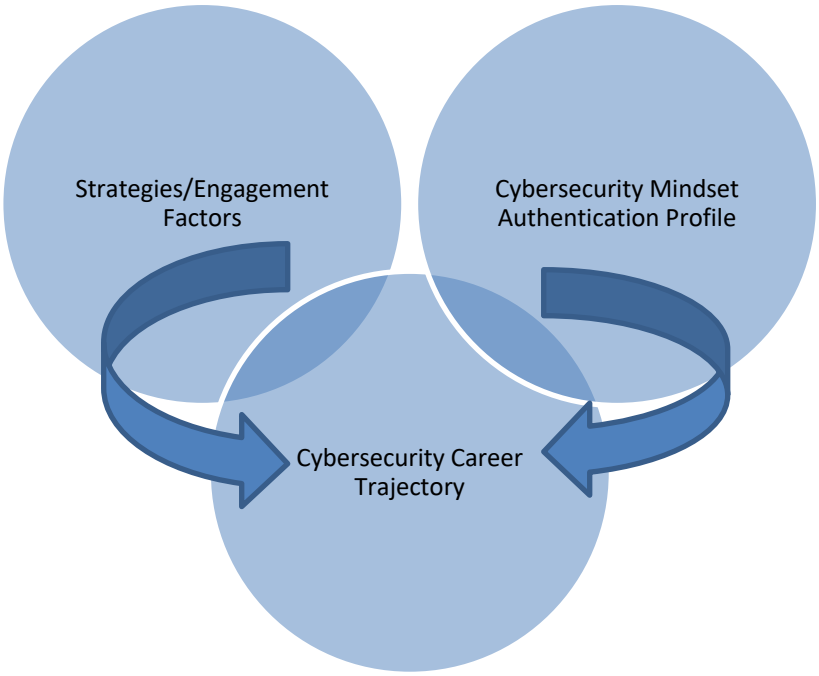

Figure 9. Theoretical model - cybersecurity engagement model.

Strategies and Engagement Factors

The data analysis refines and simplifies the multitude of factors that attract females into the field and included awareness, support, exposure, intrinsic and extrinsic factors. The most important factor, according to the participants is awareness. Awareness includes the sub categories of exposure and education. Exposure includes early exposure from K-12, STEM programs, Cyber camps and having computers in the home. The sub-category of education also include education in K-12 grades with computer and technology courses offered as well as math and science courses. The other themes that were suggested by the participants were support which includes organizational support, family support, support groups, mentors and role models. The last two themes included are intrinsic and extrinsic factors that include possessing a natural interest in cybersecurity, seeing the field as fun, exciting and challenging with a sense of pride and

belonging. The extrinsic factors included opportunities such as internships and high salary, independence and sense of contribution. However, the cybersecurity profile or mindset was also perceived to be a successful cybersecurity professional as discussed by the participants.

Cybersecurity Profile and Mindset

The cybersecurity profile and mindset factors include analytical-minded, technically savvy, possessing experience, knowledge, skills and abilities, self-efficacy factors, and having certain personality factors as assertiveness. Participants believed these factors can contribute to a successful career path and retention in the cybersecurity field. Prior research indicates that if a person fits a certain profile and possesses soft skills, not just technical skills, they may have a successful entry into the cybersecurity field (Merhout, et al., 2009; Wee, et al., 2016a, 2016b). All participants believed that on some level, personal characteristics and mindset will contribute to the engagement of females in cybersecurity field. The cybersecurity mindset factors include personal characteristics and factors that will make it possible to succeed in the cybersecurity field. Other prior research suggests a certain work-role fit will enable successful access to the cybersecurity (Bagchi-Sen et al., 2010; Dawson & Thomson, 2018). Cybersecurity professionals should be similar to the networks they operate; they must be reliable, trustworthy, and resilient (Dawson & Thomson, 2018). Analogous to the to the three factors of authentication: something you have, something you know, and something you are, aligns neatly with the cybersecurity mindset perceived to be factors of a successful cybersecurity career trajectory. Dawson and Thomson (2018) also suggest, “There exists a requirement for systemic thinkers, team players, a love for continued learning, strong communication

skills, a sense of civic duty and a blend of technical skills and social skills" (p. 1). They also suggest that researchers should focus on not only the technical skills for future cybersecurity workforce but also the organizational fit, personality traits, and values Penn and Lent (2018) also agree that self-efficacy and personality has an impact on career decisions.

This cybersecurity mindset construct emerged through the research on engaging females in the field and suggests by the data that fitness of the cybersecurity profile will enable successful a cybersecurity path. Figure 10 illustrates the personal characteristics, cognitive, and social skills as well as experience factors that play an important role in a successful journey to the cybersecurity field. The cybersecurity mindset authentication includes the following factors based on the perceptions of the participants of this research.

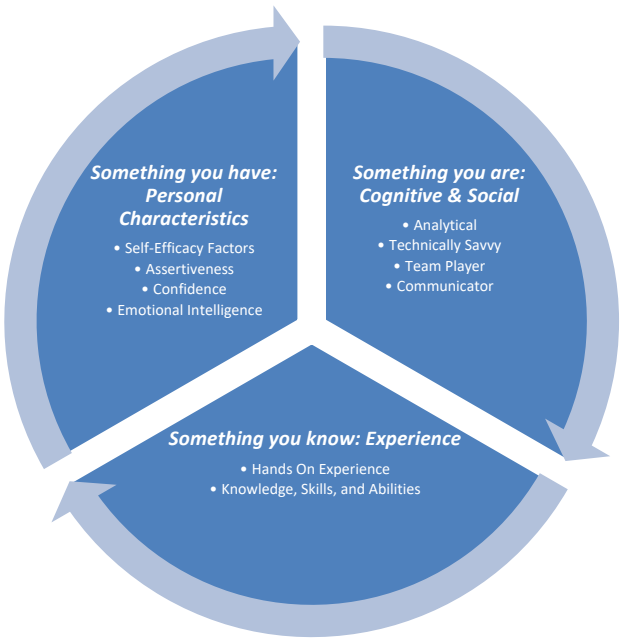

Figure 10. Cybersecurity mindset authentication profile factors.

Cybersecurity Career Trajectory

The cybersecurity career trajectory is the successful path to the cybersecurity field. It is influenced by many factors, however, once in the field, there are other factors that must be maintained. Those factors are to continually educate self in current technologies, maintain security certifications and seek peer and support groups.

The model in Figure 9 indicates if the strategies and engagement factors in place along with the cybersecurity profile or mindset, then a successful cybersecurity career path is possible. Notice all three parts of the model overlap, this means that these three factors are interrelated and should be maintained throughout the career. In a technology career, one must keep abreast of current technology changes continuously or cease to be relevant. This model assumes the cybersecurity professional will be successful by utilizing the factors of the model throughout their career.

Summary

In this chapter, the results of the study were presented. This chapter details the research data analysis and findings through the process of interviewing, coding, and generating substantive theory and themes. First, the chapter began with the introduction of the analysis process which involved qualitative research conducted via the grounded theory approach with interview data of 12 female cybersecurity professionals. The data was then transcribed professionally and the coding analysis began. The coding analysis involves initial coding, selective coding and finally theoretical coding processes. The analysis used a constant comparative process during the coding analysis to discover categories, themes and an overall relationship among them. The chapter concludes with a theoretical model that answers the main research question.

The goals of this study were attained using grounded theory coding analysis to develop the theoretical model. At the end of the data collection and analysis, a proposed model inductively emerged from the focused coding and the relationships among them. The next chapter will detail the conclusions, implications, recommendations, and summary of the research.

Chapter 5

Conclusions, Implications, Recommendations, and Summary

Conclusions

Because there is a significant underrepresentation of females in the cybersecurity workforce as well as a huge cybersecurity skills shortage and expected to worsen by the year 2024, this research addressed actions and strategies to assist in alleviating these issues. This research was driven by the question: What are the factors that attract females to the cybersecurity field?

The gender gap in the cybersecurity field negatively influences the number of cyber professionals in the pipeline. To decrease the overall rate of unfilled cyber positions, the main goal of this research study was to understand the perceptions of female cybersecurity professionals of the field and their experiences to bring forth strategies and solutions to aid future females in their quest for cybersecurity careers. In this study, 12 female cybersecurity professionals were interviewed to uncover their perceptions of the field through their own lived experiences and to provide answers to the research question. This research gave these women a voice in suggesting strategies to encourage other females to pursue the cybersecurity field.

The study built on prior research studies on women in the cybersecurity field with regards to a multitude of factors and barriers (Amo, 2016; Bagchi-Sen et al., 2010; Bashir et al., 2017; Huang & Bashir, 2015; Jethwani et al., 2017; LeClair et al., 2014; Lishinski et al., 2016). The results are in agreement that there is not a single factor or issue that

contributes to the significant underrepresentation and is an amalgamation of numerous factors. This study demystifies the complexity of the factors by organizing and categorizing them in a logical sense in order to present a model to encourage females into the field of cybersecurity. Overall, this study concludes that the factor of awareness is the key to increase the knowledge, education, self- efficacy and encouragement through support groups including role models and mentors. In turn, increasing the participation rates of females in the field. Moreover, this research adds to the body of knowledge by answering the call for that additional qualitative approaches in methodology by bringing data richness and to generate new theoretical frameworks in cybersecurity research (Olbrich et al, 2015; Trauth, 2015).

The study met its overall goal of answering the research question and generating a theoretical framework. This study utilized a grounded theory approach by interviewing 12 female cybersecurity professionals regarding their own personal experiences, beliefs, and perceptions of the cybersecurity field. By researching the factors and barriers of female cybersecurity professional's journey to the cybersecurity profession, this research presents strategies and interventions to engage and attract females to the field. The participants were extremely vocal on how they perceived the cybersecurity field as a whole and how they perceived future female cybersecurity professionals can be encouraged to the field. The overall consensus is that awareness is the major factor with early exposure and support from role models, mentors, family and organizational support with the extrinsic and intrinsic motivations can provide a gateway to the cybersecurity career. An unpredicted factor emerged during data analysis that a female may be more successful in her cybersecurity venture if she meets a certain profile warrants additional research to determine if this is just an extraneous factor or should be employed in

determining success in the path or journey to the field. The strengths of this study is an initial investigation into the perceptions of current female cybersecurity professionals that give women a voice to support other females interested in the field. Not only will this study aid future cybersecurity professionals, it will also inform academicians and cybersecurity managers how to generate strategies and interventions in reaching an underrepresented population. The weakness found in this is that it may not be generalized across other populations of cybersecurity professionals unless they are in the same type of federal military based geographic locations and are closely aligned with the United States military or federal defense industries. Another weakness is not testing the suggested model to ensure its accuracy and benefits. This is out of the scope of a grounded theory study, but will have future research potential. The limitations of this study include the access to the cybersecurity professionals, and interview scheduling. The time it took to do qualitative research is a limitation when the researcher is on a short time limit. The transcription and coding processes conducted involved large amounts of time before the final data analysis could begin. Future qualitative research should include long term studies utilizing focus groups and quantitative methods to test the proposed model.

Implications

These findings contributed notably to the body of knowledge, and have several implications for providing other researchers and practitioner's insight into the perceptions of female cybersecurity professionals and strategies to encourage them to pursue the field. The results make it evident, through the beliefs of 12 women, that women can do cybersecurity and well. Generating an interest early in a girls' life can bring more women to the field, therefore, reducing the overall shortages in the United States and worldwide.

Moreover, the results can be utilized to reduce the gender disparity in the cybersecurity field. This study may also have implications in other male dominated career fields, as well, where the theoretical model can be applied to increase the female participation rates.

Recommendations

This study was a grounded theory research designed to discover insightful information from seasoned female cybersecurity professionals that will enable the advancement of females in the field. Future research is recommended in completing studies of both male and female participants in the field and in broader industries to discover if these results can be generalized. By having only women participants in a localized area and all employed for the defense industry, may not be generalized in other locations or industries. Comparing both men and women perceptions and conducting the research from a focus group perspective, may give further insightful information. Future research to test the theoretical model is also recommended, however, this may require a lengthy timeline to determine the results. Other future recommendations are to utilize another research method. A survey method or a focus group with both male and female cybersecurity professionals at all levels may provide further insight. For example, include early entry level cybersecurity specialists, mid-level cybersecurity specialists and senior cybersecurity management in deep discussion over issues to ensure inclusiveness for women. Grounded theory research is suggested as only the first step and should be followed up by deductive studies to test the generalizability of the proposed theory (Sminia, 2017). Other recommendations are to expand the geographical location across the United States or even to other countries where the underrepresentation rate of females is even less. This study adds to the body of knowledge in qualitative research in IS as

well as presenting a unique theoretical framework in addressing the problem of significant underrepresentation of females in the cybersecurity field.

Other recommendations is to investigate the relationship of the cybersecurity fitness profile to determine if personal characteristics have an impact on successful career trajectory in cybersecurity for females. How to test for the fitness factor and how to utilize it deserves more research. Based on the findings of this study, recommendations are made to encourage families, school and academic institutions and industry to make changes in connecting females with cybersecurity through awareness programs, internships (high school and college), role models and mentors, and overall culture change to be inclusive of women.

Summary

In summary, this research address the significant underrepresentation of females in the cybersecurity field through a grounded research study of twelve female cybersecurity professionals. Despite multiple national, educational, and industry initiatives, women continue to be underrepresented in the cybersecurity field. Only 11% of cybersecurity professionals, globally, are female. There are many practitioner and industry studies that suggest self-efficacy, discrimination and organizational culture play important roles in the low rate of women in the cybersecurity field. A limited number of scholarly studies identify causal factors; however, there is not a general consensus or framework to explain the problem thoroughly. This study is relevant given that the United States in a dire situation in attracting, retaining, and developing the future cybersecurity professionals to protect the nations' critical infrastructure. Attracting and retaining females in the cybersecurity field will not only increase the cybersecurity pipeline, it will also provide different perspectives in solving diverse cybersecurity issues. Knowing the reasons why

females are not entering into the cybersecurity field will aid in development of interventions to increase the number of females in the cybersecurity workforce and develop future cybersecurity professionals.

The literature review reveals a significant gap in theoretical framework utilizing qualitative methods to demystify the complex factors of engaging females to pursue the cybersecurity field. This study identifies four factors of engagement and one unexpected co-factor that are perceived to have an impact on decisions to pursue the cybersecurity field. The four factors this study identified and analyzed were awareness, support, intrinsic and intrinsic values and their impacts on females' decision to pursue the cybersecurity field. The extraneous factor that was unanticipated was a cybersecurity mindset profile that must be present for the other four factors to have the greatest impact on successful career trajectory.

This study utilized a grounded theory research approach to interview twelve female cybersecurity professionals to discover their perceptions of the cybersecurity field. By understanding their experiences and journeys in the field, they revealed strategies that could encourage females to pursue the cybersecurity field. A grounded theory analysis was conducted in this research by which a coding process was employed on the interview data of twelve cybersecurity professionals. The interview transcripts represented the raw data in which each line of the transcript was analyzed and coded through initial, selective and theoretical coding processes.

This findings of this research primarily gives women a voice in suggesting strategies to encourage other females to pursue the cybersecurity field. The study built on prior research studies on women in the cybersecurity field with regards to a multitude of factors and barriers. The results are in agreement with prior research that there is not a

single factor or issue that contributes to the significant underrepresentation and is an amalgamation of numerous factors. The findings demystifies the complexity of the factors by organizing and categorizing them in a logical sense in order to present a model to encourage females into the field of cybersecurity. The interesting find of the cybersecurity mindset profile factor that will enhance the success of career trajectory warrants additional research to discover the impacts on decision to pursue the cybersecurity field. Overall, this study concludes that the factor of awareness is the key to increase the knowledge, education, self- efficacy and encouragement through support groups including role models and mentors. In turn, increasing the participation rates of females in the field. This study provides holistic insight to academicians and practitioners in developing future cybersecurity professionals. Moreover, it adds to the body of knowledge by answering the call for that additional qualitative approaches in methodology by bringing data richness and to generate new theoretical frameworks in cybersecurity research.

In summary, this research addressed the research problem of significant underrepresentation of females in the cybersecurity field. The research study uncovered the factors that attract females to the cybersecurity field by asking in-depth interview questions regarding the factors and barriers to the field. The results uncovered a multitude of interventions and strategies to engage females to the field. This proposed theoretical model includes an element that addresses a profile fitness for the field which may need further investigation. The main goal is to understand the perceptions of 12 female cybersecurity professionals in the quest to determine strategies that will increase the participation rate of females in the cybersecurity field. Another goal is the discovery of an emerging theoretical framework to aid in this mission. Building on prior research,

this study answered the calls to extend gender research with qualitative methods to understand the nuances of the field. This study also answered the call to understand and demystify the complex factors of increasing female participant rates in cybersecurity.

In conclusion, young women must be encouraged to push back against stereotypes from K-12 and beyond. Encourage females to stand up to unconscious bias of others including women and men. They may not know they are actually discouraging knowledgeable, brilliant and beyond capable women to fulfill the unfilled cybersecurity positions. Women role models must be visible to these young women and instill the mantra that they have unlimited potential.

Appendix A

Site Approval Letter

WARNER ROBINS BRANCH
Nola Brantley Memorial Library
721 Watson Boulevard
Warner Robins, Georgia 31093-3413
(478) 923-0128
Fax: (478) 929-8611
wrlibrary@houpl.org

CENTERVILLE BRANCH
206 Gunn Road
Centerville, Georgia 31028-1210
(478) 953-4500
Fax: (478) 953-7850
cvlibrary@houpl.org

Houston County Public Library System
www.houpl.org
PERRY BRANCH
(Administrative Office)
1201 Washington St., Perry, Georgia 31069-2555
(478) 987-3050
Fax: (478) 987-1862
pelibrary@houpl.org

Nova Southeastern University
3301 College Avenue
Fort Lauderdale, FL 33314-7796

Subject: Site Approval Letter

To whom it may concern:

This letter acknowledges that I have received and reviewed a request by Kembley Lingelbach to conduct a research project entitled "Perceptions of Female Cybersecurity Professionals on Barriers and Factors of Low Female Participation Rates" at the Houston County Public Library Nola Brantley Memorial Library Branch in Warner Robins, Georgia and I approve of this research to be conducted at our facility.

When the researcher receives approval for his/her research project from the Nova Southeastern University's Institutional Review Board/NSU IRB, I agree to provide access for the approved research project. If we have any concerns or need additional information, we will contact the Nova Southeastern University's IRB at (954) 262-5369 or irb@nova.edu.

Sincerely,

MAB

Mark Bohnstedt
Branch Manager, Nola Brantley Memorial Library
478-923-0128
mbohnstedt@houpl.org

Appendix B

Institutional Review Board Approval Letter

NOVA SOUTHEASTERN UNIVERSITY
Institutional Review Board

MEMORANDUM

To: **Kembley Lingelbach**

From: **Ling Wang, Ph.D.,**
Center Representative, Institutional Review Board

Date: **April 18, 2018**

Re: **IRB #: 2018-198; Title, "Perceptions of Female Cybersecurity Professionals Toward Barriers and Issues Leading to Gender Disparity in the Field"**

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

1) CONSENT: If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.

2) ADVERSE EVENTS/UNANTICIPATED PROBLEMS: The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.

3) AMENDMENTS: Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Steven R Terrell, Ph.D.
Ling Wang, Ph.D.

3301 College Avenue • Fort Lauderdale, Florida 33314-7796
(954) 262-0000 • 800-672-7223, ext. 5369 • Email: *irb@nova.edu* • Web site: www.nova.edu/irb

Appendix C

Participant Recruitment Email

Dear Fellow Cybersecurity Professionals,

I am a Ph.D. Candidate in Information Systems and Cybersecurity at the College of Engineering and Computing, Nova Southeastern University, working under the supervision of Professor Steven Terrell. My research is seeking to gain a better understanding the reasons for the significant underrepresentation of females in the cybersecurity field.

I am requesting your assistance as a subject matter expert (SME) in the cybersecurity field. You will be asked to participate in an anonymously recorded interview. After transcription, the interview will be returned to you for your verification of its' authenticity.

This study is expected to take no more than 30 to 45 minutes with personal recorded interviews which will be transcribed and analyzed at a later date.
If you are willing to participate, please reply to this email and I will contact you to schedule the interview.

Thank you in advance for your consideration. I appreciate your assistance and contribution to this phase of my research study.

If you wish to receive the results of this study, please notify me by email and I will be gladly provide you the results.

Very Respectfully,

Kembley Lingelbach, PhD Candidate
Email: kl762@mynsu.nova.edu
Information Systems and Cybersecurity

Appendix D

Qualitative Sample Script/Interview Guide

Sample Script/Interview Questions

1. What is your education and experience in the cybersecurity field?
2. Why did you enter the cybersecurity field?
3. How important is it for women to be involved in cybersecurity? Why?
4. What barriers did you overcome to be able to pursue the cybersecurity field?
5. What can help young women in pursuing the cybersecurity field?
6. Do you have anything else to share?

Appendix E

Research Study Recruitment Flyer

Women In Cybersecurity Study

Have your voice heard! Come take part in cybersecurity research!

I am a PhD Candidate in Information Systems with a concentration in Cybersecurity at the College of Engineering and Computing, Nova Southeastern University in Ft. Lauderdale, Fl. I would like to invite you to take part in my research that is seeking to uncover the barriers and factors of female cybersecurity professionals in order to determine why women are underrepresented in the cybersecurity field. This study aims to determine strategies and interventions to increase the participation rates of females in the cybersecurity workforce. ***The criteria for participants are:***

- ***Female***
- ***18 years old or older***
- ***Have been in the cybersecurity field for at least one year***

What: *An interview of female cybersecurity professionals (no more than 30 minutes)*

Who Should Attend: *Women cybersecurity professionals*

When: *TBD*

Where: *Nola Brantley Library, Warner Robins, Ga*

Cost: There's no cost to participate

For more information and to participate on the research study, please contact Kem Lingelbach - kl762@mynsu.nova.edu

Appendix F

Research Study Informed Consent Form

General Informed Consent Form
NSU Consent to be in a Research Study Entitled
Perceptions of Female Cybersecurity Professionals Toward Barriers and Issues Leading to Gender Disparity in the Field

Who is doing this research study?

College: College of Engineering and Computing, Nova Southeastern University

Principal Investigator: Kembley K. Lingelbach, BSLS, MMIS

Faculty Advisor/Dissertation Chair: Steve Terrell, Ph.D.

Site Information: Houston County Public Library, Nola Brantley Branch, Watson Boulevard, Warner Robins, Ga 31093

Funding: Unfunded

What is this study about?

This is a research study designed to investigate the reasons why so few qualified females are not entering the cybersecurity workforce and determine what can be done to increase their numbers. The study will also focus on strategies that can be implemented to attract and retain females in the cybersecurity workforce in developing future cybersecurity professionals.

According to the 2016 United States Bureau of Labor Statistics, the cybersecurity field is experiencing a growing shortage of personnel with over a quarter-million positions remain unfilled in the United States. Only 11% of the cyber professionals are female and continue to be underrepresented in the cybersecurity field. This study will focus on why there exists such a gender imbalance and hope to discover the factors that can help increase the participation rate of women in the field.

Why are you asking me to be in this research study?

You are being asked to be in this research study because you are a part of the sample group possessing the criteria needed to understand the barriers and issues that may be limiting females' participation in the cybersecurity field. The criteria for participation is female, age 18 or over and have been in the cybersecurity field for at least one year.

This study will include about 15 - 20 people.

What will I be doing if I agree to be in this research study?

While you are taking part in this research study, you will be asked to schedule an FT risk of harm than you would have in everyday life. Risks to you ae minimal, meaning they are

not thought to be greater than any other risks your experience every day. Being recorded means that confidentiality cannot be promised. If sharing your opinions make you anxious or stressful, we can refer you to someone who may be able to help you with these feelings.

What happens if I do not want to be in this research study?

You have the right to leave this research study at any time, or not be in it. If you do decide to leave or you decide not to be in the study anymore, you will not get any penalty or lose any services you have a right to get. If you choose to stop being in the study, any information collected about you **before** the date you leave the study will be kept in the research records for 36 months from the conclusion of the study but you may request that it not be used.

What if there is new information learned during the study that may affect my decision to remain in the study?

If significant new information relating to the study becomes available, which may relate to whether you want to remain in this study, this information will be given to you by the investigators. You may be asked to sign a new Informed Consent Form, if the information is given to you after you have joined the study.

Are there any benefits for taking part in this research study?

.
There are no direct benefits from being in this research study. We hope the information learned from this study will help your organization in recruiting and retaining females in the cybersecurity field.

Will I be paid or be given compensation for being in the study?

You will not be given any payments or compensation for being in this research study. However, there is a small incentive for participation. You will be offered a $10 Starbucks gift card to participate in the research.

Will it cost me anything?

There are no costs to you for being in this research study.

How will you keep my information private?

Information we learn about you in this research study will be handled in a confidential manner, within the limits of the law and will be limited to people who have a need to review this information. The interview data will not contain any identifiable information that could like you to the data and will be digitally encrypted to protect privacy. This data will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any regulatory and granting agencies (if applicable). If we publish the results of the study in a scientific journal or book, we will not identify you. All confidential data will be kept securely. The data will be stored and encrypted on the researcher's computer. All data will be kept for 36 months and destroyed after that time by deleting and formatting the disk drive.

Will there be any Audio or Video Recording?

This research study involves audio and/or video recording. This recording will be available to the researcher, the Institutional Review Board and other representatives of this institution, and any of the people who gave the researcher money to do the study (if applicable). The recording will be kept, stored, and destroyed as stated in the section above. Because what is in the recording could be used to find out that it is you, it is not possible to be sure that the recording will always be kept confidential. The researcher will try to keep anyone not working on the research from listening to or viewing the recording.

Whom can I contact if I have questions, concerns, comments, or complaints?

If you have questions now, feel free to ask us. If you have more questions about the research, your research rights, or have a research-related injury, please contact:

Primary contact:
Ms. Kembley K. Lingelbach, BSLS, MMIS can be reached at (478) 951-2906.

If primary is not available, contact:
Steve Terrell, Ph.D. can be reached at (561) 753-3430.

Research Participants Rights
For questions/concerns regarding your research rights, please contact:

Institutional Review Board
Nova Southeastern University
(954) 262-5369 / Toll Free: 1-866-499-0790
IRB@nova.edu

You may also visit the NSU IRB website at www.nova.edu/irb/information-for-research-participants for further information regarding your rights as a research participant.

Research Consent & Authorization Signature Section

Voluntary Participation - You are not required to participate in this study. In the event you do participate, you may leave this research study at any time. If you leave this research study before it is completed, there will be no penalty to you, and you will not lose any benefits to which you are entitled.

If you agree to participate in this research study, sign this section. You will be given a signed copy of this form to keep. You do not waive any of your legal rights by signing this form.

SIGN THIS FORM ONLY IF THE STATEMENTS LISTED BELOW ARE TRUE:

- You have read the above information.
- Your questions have been answered to your satisfaction about the research.

Adult Signature Section

I have voluntarily decided to take part in this research study.

Printed Name of Participant	Signature of Participant	Date
Printed Name of Person Obtaining Consent and Authorization	Signature of Person Obtaining Consent & Authorization	Date

References

Abraham, A. (2016). Gender and creativity: An overview of psychological and neuroscientific literature. *Brain Imaging and Behavior, 10*, 609–618. doi:10.1007/s11682-015-9410-8

Adam, A., & Richardson, H. (2001). Feminist philosophy and information systems. *Information Systems Frontiers*, *3*(2), 143-154.

Adya, M. & Kaiser, K. (2005). Early determinants of women in the IT workforce: a model of girls' career choices. *Information Technology & People*, *18*(3)*,* 230–259. doi:10.1108/09593840510615860

Ahuja, A. (2002). Women in the information technology profession: A literature review, synthesis, and research agenda. *European Journal of Information Systems, 11*(1), 20–34. doi:10.1057/palgrave.ejis.3000417

Alfassi, M. (2003). Promoting the will and skill of students at academic risk: An evaluation of an instructional design geared to foster achievement, self-efficacy and motivation. *Journal of Instructional Psychology*, *30*(1), 28-40.

Amo, L. (2016). Addressing gender gaps in teens' cybersecurity engagement and self-efficacy. *IEEE Security & Privacy, 14*, 72–75. doi:10.1109/MSP.2016.12

Anderson, J. R. (1982). Acquisition of cognitive skill. *Psychological Review, 89*(4), 369-406. doi:10.1037/0033-295x.89.4.369

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

Ashcraft, C., Eger, E., & Friend, M. (2012, November 30). Girls in IT: The facts. *National Center for Women in Information Technology (NCWIT),* Boulder, CO. Retrieved from https://www.ncwit.org/resources/girls-it-facts

Ashford, T., Koohang, A., & Floyd, K. (2012, March). *The importance of acquiring the security domains' knowledge and skills in student's educational experience*. Paper presented at the Southern Association for Information Systems Conference, Atlanta, GA.

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

Balcita, A. M., Carver, D. L., & Soffa, M. L. (2002). Shortchanging the future of information technology. *ACM SIGCSE Bulletin, 34*(2), 32. doi:10.1145/543812.543825

Bandias, S., & Warne, L. (2009, December). Women in ICT – Retain and Sustain: An overview of the ACS-W Survey. *20th Australasian Conference on Information Systems*, (pp. 2-4).

Bandura, A. (1995). *Self-efficacy in changing societies*. New York, NY: Cambridge University Press.

Bandura, A. (1997). *Self-efficacy: The exercise of control*. New York: W.H. Freeman and Company.

Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015, August). An examination of the vocational and psychological characteristics of cybersecurity competition participants. *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE).*

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security, 65*, 153–165. doi:10.1016/j.cose.2016.10.007

Bloomberg, L. D., & Volpe, M. (2016). *Completing your qualitative dissertation: A road map from beginning to end* (3rd ed.). Thousand Oaks, CA: Sage.

Blotnicky, K. A., Franz-Odendaal, T., French, F., & Joy, P. (2018). A study of the correlation between STEM career knowledge, mathematics self-efficacy, career interests, and career activities on the likelihood of pursuing a STEM career among middle school students. *International Journal of STEM Education*, *5*(1), 22. doi: 10.1186/s40594-018-0118-3

Boeije, H. (2002). A purposeful approach to constant comparative method in the analysis of qualitative interviews. *Quality & Quantity*, *36*, 391- 409.

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

Caraway, K., Tucker, C. M., Reinke, W. M., & Hall, C. (2003). Self-efficacy, goal orientation, and fear of failure as predictors of school engagement in high school students. *Psychology in School*, *40*, 417-427. doi:10.1002/pits.10092

Charmaz, K. (2014). *Constructing grounded theory* (2nd ed.). Thousand Oaks, CA: Sage

Chioma, J. (2011). Mentoring women in organizations for change and continuity - a feminist intervention: Chapter 32. *IFE PsychologIA, 2011*(*Special issue 1*), 433–447. Retrieved from http://journals.co.za/content/journal/ifepsyc

Choi, M., Levy, Y., & Hovav, A. (2013, December 14). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. *Workshop on Information Security and Privacy 2012 Proceedings, 29*. Retrieved from http://aisel.aisnet.org/wisp2012/29/

Compeau, D. R., & Higgins, C. A. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*, 189–211. doi:10.2307/249688

Corbin, J. & Strauss, A. (2008). *Basics of Qualitative Research* (Vol 3.). Thousand Oaks, CA: Sage.

Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W. (2013). *Qualitative inquiry & research design: Choosing among five approaches* (3rd ed.). Thousand Oaks, CA: Sage.

Creswell, J. W., & Miller, D. L. (2000). Determining validity in qualitative inquiry. *Theory into Practice, 39*, 124–130. doi:10.1207/s15430421tip3903_2

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

D'Hondt, K. (2016). *Women in cybersecurity* (Master's thesis). Retrieved from https://wappp.hks.harvard.edu/files/wappp/files/dhondt_pae.pdf

Fisher, J., Lang, C., Craig, A., & Forgasz, H. (2015). If girls aren't interested in computers can we change their minds?. *ECIS 2015 Completed Research Papers*, Paper 45.

Fitts, P. M. (1964). Perceptual-motor skill learning. *Categories of Human Learning,* 243-285.

Freedman, J. (2010). Medscape. Women in medicine: Are we "There" yet? Retrieved from http://www.medscape.com/viewarticle/7321997

Frieze, C., & Quesenberry, J. (2015). *Kicking butt in computer science: Women in computing at Carnegie Mellon University*. Indianapolis, IN: Dog Ear.

Frost & Sullivan. (2017). *The 2017 Global Information Security Workforce Study: Women in cybersecurity* [White paper]. Retrieved from https://iamcybersafe.org /wp-content/uploads/2017/03/WomensReport.pdf

George-Jackson, C. E. (2012). Generation ME: Influences of sudents' choice of major. *Project Step-up. University of Illinois at Urbana-Champaign*.

Glaser, B. G. (1978). *Advances in the methodology of grounded theory: Theoretical sensitivity*. Mlll Valley, CA: Sociology Press.

Glaser, B. G. (1992). *Basics of grounded theory analysis: Emergence vs. forcing*. Mill Valley, CA: Sociology Press.

Glaser, B. G., & Strauss, A. L. (1967). *Discovery of grounded theory: Strategies for qualitative research*. Mill Valley, CA: Sociology Press.

Google. (2014, May 26). *Women who choose computer science – What really matters. The critical role of encouragement and exposure*. Retrieved from https://edu.google.com/pdfs/women-who-choose-what-really.pdf

Haney, J. M., & Lutters, W. G. (2017). The work of cybersecurity advocates. In *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (pp. 1663–1670). New York, NY: Association for Computing Machinery. doi:10.1145/3027063.3053134

Higgins, K. J. (2015, September 28). New data finds women still only 10% of security workforce. *Dark Reading*. Retrieved from https://www.darkreading.com/messages.asp?piddl_msgthreadid=25151&piddl_msgid=305764

Huang, H. Y., & Bashir, M. (2015). Examining the gender gap in information assurance: A study of psychological factors. *Communication in Computer and Information Science HCI International 2015 – Posters Extended Abstracts, 117-122. doi:10.1007/978-3-319-21380-4_21*

Hussein, M. E., Hirst, S., Saylers, V., & Osuji, J. (2014). Using grounded theory as a method of inquiry: Advantages and disadvantages, *The Qualitative Report*, *19*(27), 1-15. Retrieved from http://nsuworks.nova.edu/tqr/vol19/iss27/3

Ingalhalikar, M., Smith, A., Parker, D., Satterthwaite, T. D., Elliott, M. A., Ruparel, K., ... & Verma, R. (2014). Sex differences in the structural connectome of the human brain. *Proceedings of the National Academy of Sciences*, *111*(2), 823-828. doi:10.1073/pnas.1316909110

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2017). "I can actually be a super sleuth": Promising practices for engaging adolescent girls in cybersecurity education. *Journal of Educational Computing Research*. Advance online publication. doi:10.1177/0735633116651971

Jung, L., Clark, U., Patterson, L., & Pence, T. (2016). Closing the gender gap in the technology major. *Information Systems Education Journal. 15*(1), 26.

Kaplan, D. A. (2015). Why aren't there more female radiologists? Retrieved from http://www.diagnosticimaging.com/practice-management/why-arent-there-more-female-radiologists#sthash.0Ld6W6vF.dpuf

Kissel, R. (Ed.). (2013). *NIST IR 7298 Glossary of key information security terms.* NIST Interagency/Internal Report (NISTIR) 7298-rev2. Retrieved from https://www.nist.gov/publications/glossary-key-information-security-terms-1

Klawe, M., Whitney, T., & Simard, C. (2009). Women in computing---Take 2. *Communications of the ACM, 52*(2), 68-76. doi:10.1145/1461928.1461947

Konak, A. (2018). Experiential learning builds cybersecurity self-efficacy in K-12 students. *Journal of Cybersecurity Education, Research and Practice*. *1*(6).

LeClair, J. & Pheils, D. (2016). *Women in cybersecurity.* Albany, NY: Excelsior Niche.

LeClair, J., Shih, L., & Abraham, S. (2014, February). Women in STEM and cybersecurity fields. In *Proceedings of the 2014 Conference for Industry and Education Collaboration* (pp. 5–7). Washington, DC: American Society for Engineering Education.

Leedy, P. D. & Ormrod, J. E. (2013). *Practical research: Planning and design* (10th ed.). Upper Saddle River, MJ: Prentice Hall.

Levy, D. (2006). Qualitative methodology and grounded theory in property research. *Pacific Rim Property Research Journal, 12*, 369–388. doi:10.1080/14445921.2006.11104216

Levy, Y. (2005). A Case study of management skills comparison in online and on-campus MBA programs. *International Journal of Information and Communication Technology Education, 1*(3), 1-20. doi:10.4018/jicye.2005070101

Levy, Y., & Ramim, M. M. (2015). An assessment of competency-based simulations on e-learners' management skills enhancements. *Interdisciplinary Journal of e-Skills and Lifelong Learning, 11*, 179-190. doi:10.28945/2309

Libicki, M., Sentry, D., & Pollak, J. (2014, June). *An examination of the cybersecurity labor market*. Rand Research Report, Retrieved from http://www. rand.org/pubs/research_reports/RR430. html

Linnenbrink, E. A., & Pintrich, P. R. (2002). Motivation as an enabler for academic success. *School Psychology Review*. *31(3),* 313-327.

Lishinski, A., Yadav, A., Good, J., & Enbody, R. (2016, August). Learning to program: Gender differences and interactive effects of students' motivation, goals, and self-efficacy on performance. In *Proceedings of the 12th Annual International ACM Conference on International Computing Education Research.* (pp. 211–220). New York, NY: Association for Computing Machinery.

Lyon, G. & Jafri, J. (2010). Project exploration's sisters4science: Involving urban girls of color in science in out of school. *Afterschool Matters, 11,* 15-23.

Marakas, G. M., Yi, M. Y., & Johnson, R. D. (1998). The multilevel and multifaceted character of computer self-efficacy: Toward clarification of the construct and an integrative framework for research. *Information Systems Research, 9*, 126–163. doi:10.1287/isre.9.2.126

Marcolin, B. L., Compeau, D. R., Munro, M. C., & Huff, S. L. (2000). Assessing user competence: Conceptualization and measurement. *Information Systems Research, 11*(1), 37-60. doi:10.1287/isre.11.1.37.11782

Margolis, J., & Fisher, A. (2001). *Unlocking the clubhouse: women in computing*. Cambridge, MA: MIT Press.

Melymuka, K. (2008). Why women quit technology careers. Retrieved from https://www.cio.com/article/2435573/staff-management/why-women-quit-technology-careers.html

Merhout, J. W., Havelka, D., & Hick, S. N. (2009). Soft skills versus technical skills: Finding the right balance for an IS curriculum. *AMCIS 2009 Proceedings, 9*.

Morse, J. M., Barrett, M., Mayan, M., Olson, K., & Spiers, J. (2002). Verification strategies for establishing reliability and validity in qualitative research. *International Journal of Qualitative Methods, 1*(2), 13–22. doi:10.1177/160940690200100202

National Center for Women & Information Technology. (2015). *Recruiting, retaining, and advancing a diverse technical workforce: Data collection and strategic planning guidelines*. Retrieved from https://www.ncwit.org/datacollectionguide

National Institute of Standards and Technology (2015). *Framework for improving critical infrastructure cybersecurity.* Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214

Neves, D. M., & Anderson, J. R. (1981). Knowledge compilation: Mechanisms for the automatization of cognitive skills. *Cognitive skills and their acquisition*, 57-84. doi:10.4324/9780203728178.

Newhouse, B., Keith, S., Scribner, B., & Witte (2017, October 19). *NICE cybersecurity workforce framework* (Publication No. 800-181NCWF). Retrieved from National of Standards and Technology website: https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

O'Hagan, A. O., & O'Connor, R. V. (2015, September). Towards an understanding of game software development processes: a case study. In *European Conference on Software Process Improvement* (pp. 3-16). Springer, Cham.

Office of Inspector General. (2002). *No Fear Act*. Retrieved from https://oig.pbgc.gov/nofear.html

Olbrich, S., Trauth, E. M., Niedermann, F., & Gregor, S. (2015). Inclusive design in IS: Why diversity matters. *Communications of the Association for Information Systems, 37*(37*),* 767-782.

Osborne, S. (2016, November 17). *Nation state made 'conscious effort to influence US election' by leaking Hillary Clinton's emails, NSA director says*. *Independent*. Retrieved from http://www.independent.co.uk/us

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*, 25–44. Retrieved from http://genderandset.open.ac.uk

Pearl, A., Pollack, M. E., Riskin, E., Thomas, B., Wolf, E., & Wu, A. (2002). Becoming a computer scientist. *ACM SIGCSE Bulletin, 34*(2), 135-143.

Pelham, B.W. (1991). On confidence and consequence: the certainty and importance of self-knowledge. *Journal of Personality and Social Psychology*, 60(*4*), 518.

Penn, L. T., & Lent, R. W. (2018). The Joint Roles of Career Decision Self-Efficacy and Personality Traits in the Prediction of Career Decidedness and Decisional Difficulty. *Journal of Career Assessment*. doi:10.1177/1069072718758296.

Pintrich, P. R., & Schunk, D. H. (2002). *Motivation in education: Theory, research and applications* (2nd ed.). Englewood Cliffs, NJ: Merrill/Prentice Hall.

Ponemon Institute. (2017, February 6). *2016 Cost of cybercrime study & the risk of business innovation*. Retrieved from https://www.ponemon.org/library/2016-cost-of-cyber-crime-study-the-risk-of-business-innovation

Poor, C. (2013). Increasing retention of women in engineering at WSU: A model for a women's mentoring program. *College Student Journal, 47*, 421–428. Retrieved from http://www.projectinnovation.biz/college_student_journal

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

Quesenberry, J. & Trauth, E. M. (2012). The (dis)placement of women in the IT workforce: An investigation of individual career values and organizational interventions. *Information Systems Journal, 22*(6), 457-473. doi:10.1111/j.1365-2575.2012.00416.x

Ramdass, D. & Zimmerman, B. J. (2008, Fall). Effects of self-correction strategy training on middle school students' self-efficacy, self-evaluation, and mathematics division learning. *Journal of Advanced Academics*, *20*(1)*,* 18-41. doi:10.4219/jaa-2008-869

Ramim, M. and Levy, Y. (2006). Securing e-learning systems: A case of insider cyber-attacks and novice IT management in a small university. *Journal of Cases on Information Technology (JCIT)*, *8*(4)*,* 24-34.

Roach, D., McGaughey, R. E., & Downey, J. P. (2011). Gender within the IT major – a retrospective study of factors that lead students to select an IT major. *International Journal of Business Information Systems, 7*(2), 149–165. doi:10.1504/IJBIS.2011.038509

Saldana, J. (2016). *The coding manual for qualitative researchers.* Thousand Oaks, CA: Sage.

Schiebinger, L., & Schiebinger, L. L. (2001). *Has feminism changed science?* Cambridge, MA: Harvard University Press.

Schunk, D. H. (2003). Self-efficacy for reading and writing: Influence of modeling, goal setting, and self-evaluation. *Reading and Writing Quarterly, 19*(2)*,* 159-172.

Sikolia, D., Biros, D., Mason, M., & Weiser, M. (2013). Trustworthiness in grounded theory methodology research in information systems. *MWAIS 2013 Proceedings*, *16*. Retrieved from http://aisel.aisnet.org/mwais2013/16

Smith, J. (2012). Women lawyers gaining, but still underrepresented at the top. *The Wall Street Journal*. Retrieved from http://blogs/wsj/com/law/2012/12/05/women-lawyer-gaining-but-still-underrepresented-at-the-top/

Smith, T., Koohang, A., & Behling, R. (2010). Formulating an effective cybersecurity curriculum. *Issues in Information Systems, 11*(1), 410–416. Retrieved from http://www.iacis.org/iis/iis.php

Suby, M. (2015a). *The 2015 (ISC)^2 Global information security workforce study* [White paper]. Retrieved from https://www.boozallen.com/content/dam/boozallen /documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf

Suby, M. (2015b). *Women in security: Wisely positioned for the future of InfoSec study* [White paper]. Retrieved from https://iamcybersafe.org/wp-content/uploads /2017/01/2015-Women-In-Security-Study.pdf

Sminia, H. (2017). Grounded theory building in process research. *Process Research Methods*. Retrieved from http://processresearchmethods.org/prmusings/grounded-theory-building-in-process-research/

Strauss, A. L. (1987). *Qualitative analysis for social scientists.* New York, NY*:* Cambridge University Press.

Symantec Corporation. (2015). *Internet security threat report* (Vol. 2). Retrieved from http://know.symantec.com/LP=1233.

Terrell, J., Kofink, A., Middleton, J., Rainear, C., Murphy-Hill, E., Parnin, C., & Stallings, J. (2017). Gender differences and bias in open source: Pull request acceptance of women versus men. *Peer J Computer Science 3*. Advance online publication. Retrieved from https://peerj.com/computer-science/

Terrell, S. R. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. New York, NY: Guilford Press.

Terrell, S. R. (2016). *Writing a proposal for your dissertation*. New York, NY: Guilford Press.

Terrell, S. R., Snyder, M. M., & Dringus, L. P. (2012). A grounded theory of connectivity and persistence in a limited residency doctoral program. *The Qualitative Report, 17*, 1–14. Retrieved from http://nsuworks.nova.edu/tqr/

Trauth, E. M. (2011). *Rethinking gender and MIS for the twenty-first century*. Oxford, UK: Oxford University Press.

Trauth, E. M. (2013). The role of theory in gender and information systems research. *Information and Organization*, 23(4), 277-293.

Trauth, E. M., & Howcroft, D. (2006). Social inclusion and the information systems field: Why now? In *IFIP International Federation for Information Processing*, 3-12, New York: Springer.

Trauth, E. M., Huang, H., Quesenberry, J., & Morgan, A. (2007). Leveraging diversity in information systems and technology education in the global workplace. *Information Systems and Technology Education: From the University to the Workplace*, Hershey, PA: Idea Group, 27-41.

Trauth, E. M. & Quesenberry, J. L. (2007). Gender and the information technology workforce: Issues of theory. *Managing IT Professionals in the Internet Age*, 18-36.

Trauth, E. M., Quesenberry, J. L., & Huang, H. (2009). Retaining women in the US IT workforce: theorizing the influence of organizational factors. *European Journal of Information Systems, 18*(5), 476-497.

Turner, S. V., Brent, P. W., & Pecora, N. (2002). Why women choose information technology careers: Educational. Social, and Familial Influences, Annual Educational Research Association, New Orleans, LA.

Turner, G., Deemer, E., Tims, H., Corbett, K., & Mhire, J. (2014). Cyber value and interest development: Assessment of a STEM career intervention for high school students. *Electronic Journal of Science Education, 18(*1), 1-15. Retrieved from http://ejse.southwestern.edu/article/view/11946/8546

Verizon Enterprise Solutions. (2016). Verizon 2016 data breach investigations report. Retrieved from http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

Wang, J., Hong, H., Raviz, J., & Ivory, M. (2015, June). Gender differences in factors influencing pursuit of computer science and related fields. *In Proceedings of the 2015 ACM Conference on Innovation and Technology in Computer Science Education ACM*, 117-122.

Warner, J. (2014). The women's leadership gap: Women's leadership by the numbers. *Center for American Progress*, 1-7.

Wee, C., Bashir, M., & Memon, N. (2016a, June). *The cybersecurity competition experience: Perceptions from cybersecurity workers*. Paper presented at Twelfth Symposium on Usable Privacy and Security, Denver, CO.

Wee, J. M. C., Bashir, M., & Memon, N. (2016b, August). *Self-efficacy in cybersecurity tasks and its relationship with cybersecurity competition and work-related outcomes*. Paper presented at 2016 USENIX Workshop on Advances in Security Education, Austin, Texas.

Wei, M. (2017, March 15). *Research shows women in cybersecurity face underrepresentation, discrimination & stagnating careers* [Press release]. Retrieved from http://www.ewf-usa.com/news/335470/Research-Shows-Women-in-Cybersecurity-Face-Under-representation-Discrimination--Stagnating-Careers.htm

Yin, R. (1994). *Case study research: Design and methods* (2nd ed.). Beverly Hills, CA: Sage.

Young, D., Rudman, L., Buettner, H., & McLean, M. (2013). The influence of female role models on women's implicit science cognitions. *Psychology of Women Quarterly, 37*, 283–292. doi:10.1177/0361684313482109

Zeldin, D. L., & Pajares, F. (2000). Against the odds: Self-efficacy beliefs of women in mathematical, scientific, and technological careers. *American Educational Research Journal*, *37*(1), 215-246.