THE UNDERREPRESENTATION OF FEMALES IN THE UNITED STATES CYBERSECURITY WORKFORCE: A MULTIPLE-CASE STUDY

by

Sturhonda L. James

HUNG KIEU, PhD, Faculty Mentor and Chair

JOHN MACHNIC, PhD, Committee Member

LINDA DELLOSO, PhD, Committee Member

Todd C. Wilson, PhD, Dean, School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

September 2019
Abstract

The demand for cybersecurity jobs in the United States is growing at a rapid rate, but despite the high demand for cybersecurity professionals to fill these positions, females remain significantly underrepresented in the cybersecurity profession. The purpose of this qualitative multiple-case study was to explore the underrepresentation of females in the cybersecurity profession by examining the factors that contribute to the interest, hiring, development, advancement, and sustainability of females in this profession within the United States. The overarching research question asked, “why is there a disproportionately low representation of female workers in the U.S. cybersecurity industry?” This research question was answered by employing a multiple-case study approach that surveyed three distinct groups of individuals. Semistructured interviews were conducted with participants representing each of the three cases, and then within-case and cross-case analyses were utilized to generate themes from the data. The study’s target population consisted of individuals that are affected by the gender disparity in the cybersecurity profession. The sample included individuals that accurately represented the three cases chosen to explore the phenomenon: (a) female cybersecurity professionals working in the field, (b) female cybersecurity students intending to pursue a career in cybersecurity, and (c) male and female hiring managers responsible for filling cybersecurity positions. Thematic analysis of the interview data was conducted both within the individual cases and across the cases to achieve an overall impression of the phenomenon. Five themes emerged from the data analysis, and these five themes demonstrated that (a) cybersecurity professionals’ confidence levels vary based on gender, (b) stereotypes and biases negatively impact females working in the cybersecurity profession, (c) marketing images and terminology associated with the cybersecurity profession are not gender inclusive, (d) early exposure to cybersecurity is key to increasing female interest
in the profession, and (e) males hold the majority of gateway positions that influence entry into the cybersecurity profession. These findings can be used by scholars and practitioners to improve the recruitment, hiring, development, advancement, and retention of females in the cybersecurity profession in the United States.
Dedication

I would like to thank God for his unwavering favor and love. Without his strength and guidance, I would not be where I am today. I would not have completed this dissertation without him. I would like to dedicate my dissertation to my grandmothers, mother, Uncle Michael, and other family members and friends. You all are the reason I have become the woman I am today.

Grandma Mary, I love and miss you immensely, but thank you for every college book and meal that you paid for or ensured that I had through some means. Without you, I am not sure I would be completing this third degree. Grandma Linda, thank you for being a hard-working, ever-forgiving, and constantly loving woman. You always told me I could be and do anything I wish, and for that, I love you. Sleep in peace. Mommy, thank you for always giving me what you could even when it was not easy and telling me to never worry about how I would finish college. As you would say, “Do you know who your Father is?” It took me a while to figure out you meant my heavenly Father, but you were very right. Uncle Michael, thank you for always being a positive male role model in my life and always supporting me whether it was teaching me how to read, buying my first electronic doll, supporting my choir competitions, or attending all my major accomplishments. I appreciate you more than you will ever know, and I dedicate this to you.

To my partner in life, Shakima, thank you for enduring several years of mood swings, stress levels, and uninviting attitudes throughout my doctoral journey. You have been consistently supportive of the countless hours of my studies, which often deprived us of time for fun activities, yet you nevertheless managed to always inspire me to persevere.
Acknowledgments

I have been enrolled in my doctoral program for the maximum time permitted due to life events and changes. During this time, no one has been more supportive and flexible than my mentor Dr. Hung Kieu, also known as Dr. Q. Thank you for your support throughout my doctoral journey and for engaging in challenging conversations with me. Without your support and guidance, I am not sure whether my research and degree would be complete. God places the right people in a person’s life at the right time for a reason.

I would also like to thank my committee members, Dr. John Machnic and Dr. Linda Dellosso, and my doctoral advisor, Ms. Katie Marshall, for assisting me throughout the process and ensuring that I thoroughly understood how each step in the process would impact my doctoral journey. Everyone was consistently very timely and responsive when necessary. I would also like to thank my employer for offering a program that I could leverage during the past few years for partial financial support in my quest to obtain this degree.

Last, but not least, I would like to thank all of those who participated in this study, whether you only completed a survey or also fulfilled the sample criteria and completed an interview. I would not have been able to complete this study without you dedicating your time despite your busy schedules. I wish you all the best in your future endeavors and nothing but success in your cybersecurity academic and professional careers.
# Table of Contents

Acknowledgments....................................................................................................v

List of Tables ...........................................................................................................x

List of Figures ........................................................................................................ xi

CHAPTER 1. INTRODUCTION ........................................................................................1

Background of the Study .........................................................................................1

Need for the Study .................................................................................................4

Purpose of the Study ...............................................................................................5

Significance of the Study .......................................................................................6

Research Question .................................................................................................8

Definition of Terms...............................................................................................9

Research Design....................................................................................................10

Assumptions and Limitations ..............................................................................11

Assumptions .........................................................................................................11

Limitations ...........................................................................................................13

Organization of the Remainder of the Study .........................................................15

CHAPTER 2. LITERATURE REVIEW ...........................................................................16

Methods of Searching ............................................................................................16

Theoretical Orientation for the Study ....................................................................19

Review of the Literature .......................................................................................23

Cybersecurity .......................................................................................................24

Cybersecurity Workforce Demand .......................................................................27

Cybersecurity Skill Set .......................................................................................33
| Gender Disparity in the Cybersecurity Profession | 36 |
| Gender Barriers and Biases in the Workplace    | 44 |
| Diversity and Inclusion in the Workplace       | 48 |
| Diversity and Performance                      | 50 |
| Synthesis of the Research Findings             | 53 |
| Critique of Previous Research Methods          | 57 |
| Summary                                        | 59 |

CHAPTER 3. METHODOLOGY .................................................................60

| Purpose of the Study                             | 60 |
| Research Question                                | 61 |
| Research Design                                  | 61 |
| Target Population and Sample                     | 64 |
| Population                                       | 64 |
| Sample                                          | 66 |
| Procedures                                       | 68 |
| Participant Selection                            | 68 |
| Protection of Participants                      | 69 |
| Expert Review                                    | 71 |
| Data Collection                                  | 71 |
| Data Analysis                                    | 73 |
| Instruments                                      | 74 |
| The Role of the Researcher                       | 75 |
| Guiding Interview Questions                      | 76 |
Ethical Considerations ................................................................. 78
Summary ................................................................................................. 80

CHAPTER 4. PRESENTATION OF THE DATA .................................................. 81

Introduction: The Study and the Researcher ......................................... 81
The Study ............................................................................................... 81
The Researcher ...................................................................................... 82

Description of the Sample .................................................................. 84

Research Methodology Applied to the Data Analysis ............................... 86
Within-Case Analysis .......................................................................... 89
Cross-Case Analysis ............................................................................. 91

Presentation of Data and Results of the Analysis .................................... 91
Within-Case Findings .......................................................................... 91
Cross-Case Findings .......................................................................... 110

Summary ................................................................................................. 129

CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS ............ 130

Summary of the Results ........................................................................ 130
Discussion of the Results ...................................................................... 133
Subquestion 1 ....................................................................................... 134
Subquestion 2 ....................................................................................... 136
Subquestion 3 ....................................................................................... 139

Conclusions Based on the Results ....................................................... 140

Comparison of Findings with Theoretical Framework and Previous
Literature ............................................................................................... 140

Interpretation of the Findings .............................................................. 143
List of Tables

Table 1. Search Methods for Locating Literature ................................................................. 18
Table 2. National Cybersecurity Workforce Categories and Specialty Areas ...................... 35
Table 3. Case 1: Females Currently Working in the U.S. Cybersecurity Workforce ............... 85
Table 4. Case 2: Females Seeking Entry Into the U.S. Cybersecurity Workforce ................. 85
Table 5. Case 3: Hiring Managers for the U.S. Cybersecurity Workforce .......................... 86
Table 6. Cross-Case Analysis Themes ............................................................................... 111
List of Figures

Figure 1. Literature search method .................................................................19
Figure 2. Conceptual framework explaining female participation in cybersecurity ..........22
Figure 3. Interview data word frequency ..........................................................88
Figure 4. Method applied to multiple-case study ..............................................90
Figure 5. Implications of the study’s findings ..................................................148
CHAPTER 1. INTRODUCTION

The demand for cybersecurity jobs in the United States is growing at a more rapid rate than the demand for any other information technology (IT) job (Bureau of Labor Statistics, 2018a). With a 28% growth rate, the demand for cybersecurity professionals is growing at a rate that is considered much faster than average (Bureau of Labor Statistics, 2018b). Despite the rapid rate of growth in cybersecurity positions, females remain severely underrepresented in these positions and the IT workforce in general (LeClair, Shih, & Abraham, 2014; Rowland, Podhradsky, & Plucker, 2018). The complex challenges currently facing the cybersecurity workforce require a cadre of diverse professionals to increase overall effectiveness in this field (Dodge, Toregas, & Hoffman, 2012). Diversity is vital as it contributes to the creation of a culture in which differing opinions can be shared and synthesized to develop innovative solutions to problems (Suby & Dickson, 2015). The present study addresses the underrepresentation of females in the cybersecurity field by using a qualitative multiple-case study approach to identify why females choose to work in the field of cybersecurity, what criteria apply when hiring female cybersecurity professionals, and how increased representation of females in cybersecurity roles can benefit organizations. Chapter 1 serves as an introduction to the study by providing background information on the topic, a summary of the need for the study, a description of the study’s purpose and significance. Additionally, the chapter identifies the research questions, term definitions, elements of the research design, and the study’s assumptions and limitations.

Background of the Study

The general issue of interest was the underrepresentation of females in the cybersecurity profession. Research indicates that this phenomenon is global but particularly acute in the United
States (Kaspersky, 2017). The underrepresentation of females in the cybersecurity profession is a consequence of the lack of females in general science, technology, engineering, and mathematics (STEM) fields (Gonzalez, 2015; Peacock & Irons, 2017). Researchers have observed the lack of women in STEM-related professions over time and argued that this persistent issue must be addressed (Agosto, 2001; Kaspersky, 2017). As early as 2001, Agosto performed a literature review of research examining females’ lack of interest, underrepresentation, and low levels of participation in computer and technology studies and careers. Landivar (2013) noted that the problem of females’ underrepresentation has continued to worsen with ongoing declines in female participation in IT-related fields since 1990. The problem is particularly acute in cybersecurity where females occupy only 15% of all cybersecurity-related jobs (Rowland et al., 2018).

While there are different causes for the lack of females in the cybersecurity profession, Kaspersky (2017) argued that a fundamental cause is the meager representation of females in IT-related courses at institutions of higher education. Scholars have consistently noted females’ low levels of participation in STEM courses and related occupations (Fouad & Santana, 2017; Weisgram & Diekman, 2015). Gonzalez (2015) argued that STEM education must be supported and encouraged among females to achieve greater representation of females in cybersecurity positions. In the workplace, female underrepresentation in these types of positions is persistent across all types of organizations (Agosto, 2001; Beede et al., 2011; Mangalindan, 2014; Richter, 2018).

The underrepresentation of females in cybersecurity positions has adverse effects on the economy in multiple dimensions (Gonzalez, 2015; Landivar, 2013; LeClair et al., 2014; Woolley & Malone, 2011). First, the lack of females willing to become cybersecurity professionals
exacerbates an already critical shortage of such professionals in the U.S. economy (Gonzalez, 2015). Second, cybersecurity positions are well compensated, and the paucity of women in such positions implies that fewer women are earning high incomes, exacerbating income inequality between the genders (LeClair et al., 2014). Third, a lack of females in cybersecurity positions means there is less diversity on cybersecurity teams. Research has highlighted the importance of diversity as diverse perspectives improve team problem-solving and productivity (McLauren, 2012; Woolley & Malone, 2011). Fourth and finally, the female participation rate in IT positions, including cybersecurity positions, has remained stagnant since 1990, and more extensive efforts must be made to recruit women and meet businesses cybersecurity needs (Chabrow, 2011; Gonzalez, 2015; Landivar, 2013; Rowland et al., 2018).

The literature enumerates many causes of the underrepresentation of females in STEM fields and the cybersecurity profession (Amo, 2016; Gonzalez, 2015; Rowland & Noteboom, 2018). These causes include limited participation of female in STEM courses, perceptions that the field of cybersecurity is male-dominated and unfriendly to females, and higher rates of females choosing to leave the cybersecurity profession (Gonzalez, 2015; Rowland & Noteboom, 2018). The literature includes many quantitative studies that provide numeric values for the identified causes of female under-participation in cybersecurity (Giboney, Hansen, Brigham, & Brigham, 2019; Namin, Aguirre-Muñoz, & Jones, 2016; Peacock & Irons, 2017). However, literature specifically addressing females’ experiences in and perceptions of the cybersecurity profession is limited, with many studies focusing on cybersecurity or STEM students (Amo, 2016; Sarathchandra, Haltinner, & Lichtenberg, 2016). Thus, factors that influence females’ decisions to enter and remain in the cybersecurity profession remain unclear.
The present research was motivated by a need to understand the root causes of females’ relationships with cybersecurity as perceived by females who are professionally involved in cybersecurity, females who are intending to pursue a cybersecurity career following the completion of a degree, and the hiring managers responsible for filling cybersecurity positions. A qualitative multiple-case study research design was selected to address the needs of a wide range of stakeholder groups and explore the perspectives of individuals in the three distinct cases described previously. The present acute shortage of cybersecurity professionals and the attendant suboptimal consequences for the U.S. economy make the present study particularly timely (Kaspersky, 2017; Rowland et al., 2018).

Social identity theory was applied as a theoretical framework in the present study. Social identity theory allows researchers to take an interactionist view “of the role of self-conception and associated cognitive processes and social beliefs in group processes and intergroup relations” (Hogg, 2016, p. 3). The theoretical perspective of interactionism identifies key social processes based on how individuals interact with one another and how society, based on those interactions, shapes individuals (Hogg, 2016). In the present study, this meant that the factors that influence females’ decisions to pursue and stay in cybersecurity positions were viewed through a lens of interaction and social identity. This theoretical framework was well suited to the examination of the roles of females in cybersecurity as it allowed a focus on the interactions of such females with their peers and the broader social environment they experience.

Need for the Study

There is a scholarly need to examine the underrepresentation of females in the U.S. cybersecurity workforce. In 2014, females represented fewer than 15% of cybersecurity professionals in the United States (Setalvad, 2015). That gender distribution has remained
consistent despite high demand and significant numbers of unfilled cybersecurity positions (Rowland et al., 2018). Kaspersky (2017) found that a causative factor of females’ limited representation in cybersecurity positions was their relative absence from STEM programs. Dallaway (2016) noted that one of the drivers of the shortage in cybersecurity professionals was insufficient female interested in the field. Several other researchers have also cited the importance of fostering cybersecurity interests among female college students (Amo, 2016; Gonzalez, 2015; Namin et al., 2016; Rowland & Noteboom, 2018).

Despite the acknowledgment that outreach to younger females is important, few studies have examined the experiences of females actively working as cybersecurity professionals (Hunt, Layton, & Prince, 2015). Further, no studies viewed the phenomenon of the underrepresentation of females in cybersecurity from the perspective of three distinct populations. The present study addressed this gap in the scholarly literature by analyzing participant data from female cybersecurity professionals, prospective cybersecurity professionals, and hiring managers responsible for filling cybersecurity positions. Examining these three groups provided a holistic approach to understanding females’ perspectives on the root causes that either militate toward or against entering and remaining in the cybersecurity profession.

**Purpose of the Study**

The purpose of this qualitative multiple-case study was to explore the underrepresentation of females in the cybersecurity profession by examining the factors that contribute to the interest, hiring, development, advancement, and sustainability of females in this profession within the United States (Scriven, 2013). Scholars have demonstrated that there is a major shortage of female cybersecurity professionals, and this shortage poses serious challenges to the security of private and public data, systems, and infrastructure (Rowland et al., 2018; Stytz
Few empirical studies have addressed the underrepresentation of females in the specific context of cybersecurity, even though gender diversity has been proven beneficial to organizations (Hunt et al., 2015). As a result, an examination of why females are underrepresented in the cybersecurity profession not only addresses a gap in the literature but may assist in explaining why so few females enter the profession.

Challenges associated with cybersecurity are complex and unique, and new challenges related to systems vulnerabilities are continuously arising due to rapid ongoing changes in technology (Caven & Nachmias, 2017). Researchers have demonstrated that diverse teams perform better than more homogeneous teams (Rock & Grant, 2016). Thus, cybersecurity teams would be more diverse, and potentially more effective, if females were better represented on such teams. Rock and Grant (2016) found that team diversity contributes to team effectiveness due to two critical factors. First, diverse teams are less likely to become complacent with their work roles; second, diverse teams include a wider range of perspectives (Rock & Grant, 2016). Based on these two factors, closing the gender gap in cybersecurity could increase organizations’ capabilities to resolve difficult problems while increasing productivity.

**Significance of the Study**

This study was significant to the cybersecurity profession and the field of IT because it added to the larger body of knowledge on factors contributing to the low number of females in this field. Studying the reasons for female underrepresentation was important because increasing the number of females working in the profession helps to address the shortage of cybersecurity professionals and close the gender gap (Burrell, 2018). Furthermore, without intervention, the shortage of females in the field of cybersecurity is expected to continue for several years (Culbertson, Humphries, Ivy, Kolko, & Rodden, 2017). The target audience for this study
included business professionals, academia, and cybersecurity professionals interested in identifying initiatives to fill the knowledge gaps and address problems identified with this study. Increasing awareness of the findings from this study to the groups identified better equips stakeholders to develop new processes and initiatives to attract and retain female cybersecurity professionals. Improving recruitment and retention raises the likelihood of filling both a talent deficit and a larger number of job vacancies in the U.S. cybersecurity profession (Morgan, 2016).

In addition to the wider community, the findings in this study were also significant specifically to cybersecurity practitioners and organizations that employ cybersecurity practitioners and scholars. Cybersecurity practitioners and the organizations that employ these professionals will find this study significant to day-to-day interactions among male and female peers, future employees, and the current workforce. These individuals are positioned to change the hiring, recruitment, and work environment of females in the cybersecurity profession (Burrell, 2018). The findings in this study provided various perspectives on the issues females face when pursuing a career in the cybersecurity field. By providing an unfiltered view of the participants’ experiences, organizations that employ cybersecurity practitioners and cybersecurity practitioners themselves can identify gender-specific barriers and develop processes and policies that support a more inclusive workplace. Efforts can also be made to increase opportunities for females to enter the cybersecurity profession.

Additionally, this study informed future and current female cybersecurity professionals on the experiences females face in the profession. This information allows prospective female cybersecurity professionals to develop a more holistic view of the skills needed to gain entry to the cybersecurity field (Dawson & Thomson, 2018). Female cybersecurity professionals can use the present study’s findings as confirmation of their own experiences, and the experiences shared
by the participants may help some female cybersecurity professionals overcome challenging situations without leaving the field. The findings in this study can also spur conversations on gender disparity issues that may exist within cybersecurity organizations, and these conversations may help generate solutions that address the barriers faced by females interested in cybersecurity as a career.

Lastly, this study was significant to current and future scholars as it supported future research on the underrepresentation of females in the cybersecurity profession. The present study also contributed to the scholarly understanding of the role the social identity theory plays in gender inequality in male-dominated career fields like cybersecurity (Tellhed & Jansson, 2018). Several researchers have acknowledged the need to develop a solution to the gender gap in the cybersecurity profession (Bagchi-Sen, Rao, Upadhyaya, & Chai, 2010; Burrell, 2018; Gonzalez, 2015; LeClair et al., 2014; Peacock & Irons, 2017; Shumba et al., 2013). When reviewing existing scholarly literature, there were gaps in the body of knowledge due to the newness of the cybersecurity profession. Most preexisting literature discussed the low number of women in STEM fields in general and information security or information assurance. Using the sample defined for this study provided the academic community with additionally scholarly material on the gender-disparity observed within the cybersecurity profession. The findings from the present study support the generation of an understanding of the reasons for the gender gap in the U.S. cybersecurity workforce.

**Research Question**

This multiple-case study explored a single overarching research question. The overarching research question asked, “why is there a disproportionately low representation of
female workers in the U.S. cybersecurity industry?” Three subquestions were developed to address relevant aspects of the overarching research question. The subquestions were as follows:

**Subquestion 1.** What factors contribute to the interest, development, and sustainability of female employees in the U.S. cybersecurity career field?

**Subquestion 2.** What criteria are currently applied by hiring managers for recruiting, hiring, and retaining female cybersecurity professionals in the United States?

**Subquestion 3.** How might the increased representation of female cybersecurity professionals contribute to an organization?

**Definition of Terms**

The following terms have been defined to provide clarity.

**Cybersecurity.** Cybersecurity refers to the “organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from attack” (Craigen, Diakun-Thibault, & Purse, 2014, p. 17). Craigen et al. (2014) noted that scholars and practitioners define cybersecurity in many different ways. Thus, in the present study, cybersecurity referred to activities that support Craigen et al.’s multidisciplinary definition.

**Cybersecurity professional.** Cybersecurity professionals are individuals that work in jobs that require expertise defending networks and information systems from cyberattacks (Lingelbach, 2018).

**Cyberspace.** Cyberspace refers to “a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (NIST, 2013, p. 58).
Gender. Gender “refers to the attitudes, feelings, and behaviors that a given culture associates with a person’s biological sex” (American Psychological Association, n.d., p. 1). In the present study, a participant’s gender was characterized as either male or female.

Organization. The term organization “applies correctly to stable associations of persons engaged in concerted activities directed to the attainment of specific objectives” (Bittner, 1965, p. 239).

Social identity theory. “Social identity theory is a social psychological theory of intergroup relations, group processes, and the social self” (Hogg, Terry, & White, 1995, p. 259).

Research Design

The present study utilized a qualitative, multiple-case study research design. A case study is a versatile qualitative research design used to study a central phenomenon through “persons, events, decisions, periods, projects, policies, institutions, or other systems that are studied holistically by one or more methods” (Astalin, 2013, p. 5). Two types of case studies include single case and multiple case. Multiple-case studies are not envisioned to be used to compare multiple cases but rather to use each case individually to gain a more holistic understanding of the phenomenon that bounds the cases together (Stake, 2013).

The case study research design uses multiple data sources to conduct an in-depth exploration of the case rather than a single data source; researchers who adopt this method generally seek to identify interrelated conditions that relate to the central phenomenon of the study (Yin, 2014). The present study explored the underrepresentation of females in the U.S. cybersecurity profession by investigating three distinct cases. Case 1 consisted of female cybersecurity professionals currently working in the profession; Case 2 consisted of prospective female cybersecurity professionals currently working in the profession; Case 3 consisted
of hiring managers responsible for filling cybersecurity positions. The use of a multiple-case study approach enabled an in-depth exploration of the central phenomenon through the direct experiences of the participants.

The qualitative multiple-case study approach was appropriate because it allows researchers to identify factors contributing to a phenomenon based on the experiences of participants in each case study (Yin, 2015). Additionally, a multiple-case research design helps elucidate the phenomenon by focusing on the subjects’ personal experiences (Finlay, 2012). Data were collected using semistructured interviews, and the data analysis process included both a within-case analysis and a cross-case analysis following guidelines set forth by Stake (2013). Chapter 3 contains a more detailed description of the research design.

Assumptions and Limitations

Assumptions

This study had several applicable assumptions surrounding the associated methodology, theory, and topic selected. The first methodological assumption was that a qualitative multiple-case study would be the best research design to answer the research questions in this study. It was also assumed that duplication across cases would strengthen the study’s findings (Scott, Morgan, Plotnikoff, & Lubans, 2015). Based on the research method selected, semistructured interviews allowed the most in-depth understanding of the participants’ lived experiences. During these interviews, it was assumed that all participants were truthful about fulfilling the requirements to participate in the study and that each participant would provide unbiased and honest data during the interviews.

An additional methodological assumption was that exploring the topic from multiple perspectives would yield more holistic insights on the phenomena being studied. As noted
previously, three distinct cases were examined: (a) female cybersecurity professionals working in the field, (b) female cybersecurity students intending to pursue a career in cybersecurity, and (c) male and female hiring managers responsible for filling cybersecurity positions. There was no way to test the assumption that examining these three groups would lead to a more holistic view of the phenomenon, but it was assumed that the nature of reality is subjective, and the best way to form an understanding of a phenomenon is through the analysis of multiple realities (Rahi, 2017). Based on this approach, it was assumed that a multiple-case study was the best approach to answer the research questions defined for this study.

Theoretical assumptions also informed choices related to the research design and implementation. It was assumed that the social identity theory, first introduced by Tajfel and Turner (1979), was the best lens through which to understand the underlying factors contributing to the low number of females in the U.S. cybersecurity profession. Commonalities in the literature on social identity theory indicated that it was an applicable theory in the context of female underrepresentation in the cybersecurity profession (Tajfel & Turner, 1979; Taylor, Thackray, Hodge, & McAlaney, 2018; Wood & Eagly, 2015). Researchers have linked gender to both stereotypical personality traits and in-group and out-group interactions (Tajfel & Turner, 1979; Wood & Eagly, 2015). Thus, it was assumed that exploring the underrepresentation of females in the cybersecurity profession through the lens of social identity theory would provide important insights.

Finally, the study also included topic-specific assumptions. It was assumed that exploring the cause of female underrepresentation in the U.S. cybersecurity workforce was a critical scholarly topic and that the study’s results would contribute to the larger body of academic knowledge. This assumption was based on the significant gender gap in the cybersecurity
industry, a large number of unfilled cybersecurity positions, and the importance of cybersecurity to national defense (Gonzalez, 2015; Kaspersky, 2017; LeClair et al., 2014; Rowland et al., 2018). It was also assumed that increasing the number of females in the cybersecurity profession will create a larger job applicant pool and minimize the number of cybersecurity job vacancies in organizations in the United States (Amo, 2016; Rowland & Noteboom, 2018).

**Limitations**

One limitation of this study was related to the criteria used to recruit research participants for this qualitative study. The inclusion and exclusion criteria limited the size of the sample and restricted the perspectives presented in the findings of the study. Patton (2015) shared that several factors can define the criteria of a sample for a qualitative study, including judgment, peer review, and consensual validation. The criteria for this study were originally defined by the researcher’s judgment and the desire to collect multiple perspectives of the phenomenon. The criteria were reviewed by the dissertation committee and reworked based on feedback provided by the committee. Based on these steps, the small sample size was not expected to affect the study’s findings adversely (Patton, 2015).

The next limitation of this study was related to the study’s focus on female representation in the cybersecurity profession and not in other IT disciplines. Defining a focus for a qualitative study is necessary to allow for an in-depth understanding of the identified problem (Yin, 2014). Narrowly defining the study’s focus does not allow the findings to be generalized across the IT profession. “Qualitative research has, thus, been directed toward providing in-depth explanations and meanings rather than generalizing findings” (Carminati, 2018, p. 1). The decision to focus on cybersecurity was intentional based on the lack of scholarly literature examining the cause of female underrepresentation in the cybersecurity profession, the consistent pattern of low
representation, and the increasing demand for cybersecurity professionals in the United States (Reed, Zhong, Terwoerds, & Brocaglia, 2017).

Another limitation was related to the geographic location of the research participants. It was assumed that the participants sufficiently represented the population of interest. This study focused on the low representation of females in the U.S. workforce. However, no attempt was made to sample the participants from specific areas within the United States. This limitation meant that no conclusions could be drawn about geographic areas within the United States. The decision to only sample participants from the United States meant that the data was not generalizable to the experiences of foreign cybersecurity professionals or foreign organizations that employ cybersecurity professionals.

The last limitation was related to the qualitative nature of the study. The study was limited as it was not possible to use the data to identify correlations about relationships between any of the factors identified by the participants (Patton, 2015; Yin, 2014). Qualitative research does not define variables to allow researchers to quantify factors or the relationships between factors (Yin, 2014). This limitation was accepted based on the desire to descriptively understand the factors contributing to the low number of females in the U.S. cybersecurity workforce. Such a perspective was not possible using quantitative means (Patton, 2015).

One final design flaw limitation was the inability to link the present study to past research on the topic. The cybersecurity profession is still a rather new profession, and there has not been as much research specifically conducted on cybersecurity (Hunt et al., 2015). This limitation was unavoidable, but the lack of previous studies highlighted the need for additional scholarly literature to be generated on the topic (Hunt et al., 2015). It was anticipated that this research
would add to the larger body of knowledge, and future researchers will be able to build upon this study’s findings.

In addition to limitations, the present study also included delimitations. Delimitations are factors that are intentionally not explored (Simon & Goes, 2013). This study was intentionally scoped to provide an in-depth understanding of the phenomena of the underrepresentation of females in the cybersecurity profession without being too broad in scope. The study did not compare the experiences of male cybersecurity professionals to the experiences of female cybersecurity professionals. By excluding male cybersecurity professionals, the study remained focused on the experiences of females. Additionally, by excluding participants from other countries, the study remained focused on the phenomenon of female underrepresentation in the United States. These delimitations helped ensure the study remained focused on the phenomenon of interest.

**Organization of the Remainder of the Study**

The remainder of this study is presented in four additional chapters. Chapter 2 contains a review of the scholarly literature associated with the underrepresentation of women in the field of cybersecurity. Chapter 3 details the methodology used to conduct the study. Chapter 4 presents the findings from the thematic analysis supported by quotes from participant interviews. Chapter 5 concludes the study with a discussion of the meaning of the findings and recommendations based on those findings.
CHAPTER 2. LITERATURE REVIEW

Chapter 2 presents a review of the scholarly literature exploring the underrepresentation of females within the U.S. cybersecurity workforce. Additionally, the literature explores salient theories and assumptions concerning the cause of this phenomenon and contributing factors. As the cybersecurity discipline is relatively new, the literature on this specific topic is limited. Literature reviews synthesize current knowledge concerning a topic, and exploring the additional components that relate to this phenomenon provides enhanced insights into the problem (Machi & McEvoy, 2016). The literature synthesized in this chapter was collected, organized, and analyzed methodically to support the design of the study and the analysis of the data. The literature review delineates the problem, gaps in the relevant knowledge, and the methodology which has been adopted. The chapter includes (a) a description of the methods used for searching, (b) information on the study’s theoretical orientation, (c) the main literature review, (d) a synthesis of the findings identified in the literature, (e) a critique of previous research methods, and (f) a summary.

Methods of Searching

The researcher adopted several search methods to locate, identify, refine, and scope the literature available on the underrepresentation of females in the U.S. cybersecurity profession. Data gathered for this literature review was discovered through several means. First, the researcher used the research problem and questions to identify key terms. The key terms were then used to conduct searches in several search engines and online journal and dissertation databases. File extension types and operations were combined to filter the results returned by the search engines. The use of file extensions and keyword combinations helped refine the overall
literature search. Some key terms used in the search included females, cyber, cybersecurity, diversity, inclusion, gender gap, diversity reports, and workforce.

Once data gathering had been initiated, theories relevant to the problem and new keywords were identified. The new keywords were then used to create new combinations for additional queries across various databases to determine additional relevant literature. Key terms were searched in several online databases and digital media platforms to locate scholarly literature. Table 1 provides a detailed list of the databases searched, individual keywords, and the combinations of keywords and Boolean operators used to refine the search. The list presented in Table 1 is not exhaustive, but it provides insight into how the researcher refined the search engine input to optimize results.

A structured review process guided the literature review for the present study. Figure 1 presents a graphic representation of the steps taken to develop the literature review for this study. The key terms, databases, and search combinations displayed in Table 1 were used when executing the review process illustrated in Figure 1. This process enabled the researcher to implement a replicable method to scrutinize a plethora of journal articles, news articles, books, reports, working papers, dissertations, and industry white papers. Additionally, the process ensured that the data was scholarly, relevant, and appropriately cataloged. If the literature identified was not pertinent to the topic or nonacademic, it was not used.
<table>
<thead>
<tr>
<th>Databases</th>
<th>Search Terms</th>
<th>Search Term Combinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Scholar</td>
<td>Women</td>
<td>women + cyber + security</td>
</tr>
<tr>
<td>Capella Dissertations and Thesis</td>
<td>Girls</td>
<td>women or girls + cybersecurity</td>
</tr>
<tr>
<td></td>
<td>Females</td>
<td>cybersecurity + demand .pdf</td>
</tr>
<tr>
<td>ProQuest</td>
<td>Cyber</td>
<td>cyber + diversity</td>
</tr>
<tr>
<td>IEEE Digital Library</td>
<td>Cybersecurity</td>
<td>cyber + diversity or inclusion</td>
</tr>
<tr>
<td>Safari Tech Books Online</td>
<td>Cyber Security</td>
<td>women + “cyber security”</td>
</tr>
<tr>
<td>Harvard Business Review</td>
<td>Bias</td>
<td>“gender gap” + women + cyber</td>
</tr>
<tr>
<td>Sage Journals</td>
<td>Theory</td>
<td>“gender gap” + cyber</td>
</tr>
<tr>
<td>EBSCO</td>
<td>Hacker</td>
<td>workforce + diversity</td>
</tr>
<tr>
<td>CQ Researcher</td>
<td>Information Security</td>
<td>diversity + performance</td>
</tr>
<tr>
<td>JSTOR</td>
<td>Gender</td>
<td>stereotypes + cyber</td>
</tr>
<tr>
<td>Oxford</td>
<td>Gender Gaps</td>
<td>stereotypes + gender</td>
</tr>
<tr>
<td>World Telecommunication</td>
<td>Disparity</td>
<td>females or girls + stem</td>
</tr>
<tr>
<td>ACM Digital Library</td>
<td>Diversity</td>
<td>stem + gap</td>
</tr>
<tr>
<td></td>
<td>Social</td>
<td>stem + cyber</td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td>women + impact + performance</td>
</tr>
<tr>
<td></td>
<td>Performance</td>
<td>social + theory .pdf or *.doc</td>
</tr>
<tr>
<td></td>
<td>Workforce</td>
<td>social + theory + gender</td>
</tr>
<tr>
<td></td>
<td>Demand</td>
<td>hacker + stereotype</td>
</tr>
<tr>
<td></td>
<td>Stereotypes</td>
<td>bias + cyber .pdf</td>
</tr>
</tbody>
</table>
Theoretical Orientation for the Study

The theoretical orientation of a qualitative study provides clarity concerning the study’s topic and provides a basis for a scientific study (Tavallaei & Talib, 2010). By identifying theories from previous literature, researchers can derive research assumptions. A theoretical framework is defined as “empirical or quasi-empirical theories of social or psychological
processes which exist at a variety of different levels and applies to the understanding of phenomena” (Anfara & Mertz, 2006, p. 27). The present study utilized social identity theory as a theoretical framework. Studying the personal experiences of the sample and their interactions among their intergroup and outgroup align with social identity theory (Peacock & Irons, 2017; Tajfel & Turner, 1979).

In 1979, Tajfel and Turner, two social psychologists, established social identity theory. This theory was initially designed to encompass “three cognitive processes relevant to a person’s being part of an in-group, or of an out-group. Such group membership being, depending upon circumstances, possibly associable with the appearance of prejudice and discrimination related to such perceived group membership” (Tajfel & Turner, 1979, p. 1). Originally, social identity theory exclusively encompassed behaviors and interactions within a group (i.e., intergroup; Tajfel & Turner, 1979). However, researchers have expanded social identity theory to account for a broad array both internal and external subcategories to examine groups and how society impacts the development of a group based on interaction within a specified in-group or with an out-group (Hogg, 2016).

The expansion the social identity theory created “an interactionist social psychological theory of the role of self-conception and associated cognitive processes and social beliefs in group processes and intergroup relations” (Hogg, 2016, p. 3). The theoretical perspective of interactionism identifies key social processes based on how individuals interact with one another and how society, based on interactions, shapes individuals. Interactionism is a foundational concept upon which most sociologists conduct their research (Rubington & Weinberg, 2015). In some cases, stereotypes are established based on how outsiders (i.e., out-group) perceive a group or how members of a group (i.e., in-group) may have behaved previously. Stereotypes about
group behavior heavily rely on both warmth (female) and competence (male), and these two key characteristics are also relevant to how females and males are evaluated in society (Cuddy, Fiske, & Glick, 2008; Haines, Deaux, & Lofaro, 2016).

Theories associated with social roles describe the disparities in how males and females are perceived and treated within society in various settings based on the cultural traits they have (Wulf et al., 2018). Mayo (2016) discovered that females are more likely to demonstrate warmth, but warmth alone does not equate to competence. Men commonly exhibit high confidence with just enough warmth to be perceived as competent. Cuddy et al. (2008) noted that individuals that exhibited low warmth but high competence were more likely to be hired and promoted than those that demonstrated high warmth. Discrepancies in treatment among genders have historically been an accepted norm within society (Tajfel & Turner, 1979; Wulf et al., 2018).

The scholarly literature describes the cybersecurity profession as a male-dominated career field (Bagchi-Sen et al., 2010; Beall, 2018; Gonzalez, 2015; Williamson & Tranter, 2017). Social identity theory posits that cultural transformation requires individuals within the underrepresented group and individuals beyond the underrepresented group to address the issue collectively (Tajfel & Turner, 1979). The literature review for the present study examined previous studies concerning the cybersecurity gender gap, the personal experiences of those involved in the profession, and the potential effects of closing the gender gap for organizations. Creating a framework based on social identity theory helped contextualize the underrepresentation of females in the cybersecurity profession and the impact gender disparity has on the profession and society. This study applies the theories associated with the underrepresentation of females in the U.S. cybersecurity profession to develop research assumptions that support the scholarly literature and the present study’s conceptual framework.
Figure 2 presents the present study’s conceptual framework. A conceptual framework is a tool that identifies concepts, assumptions, and theories that inform the research and expectations (Miles & Huberman, 1994). The conceptual framework for the present study was predicated upon the research problem and key factors associated with relevant assumptions and theories.

![Diagram](image)

*Figure 2. Conceptual framework explaining female participation in cybersecurity.*

The conceptual framework presented in Figure 2 incorporates social identity theory and interactionism. “The roots of gender inequality are found within social constructions of gender, within wider society, within families, within education, and within the cybersecurity profession” (Peacock & Irons, 2017, p. 40). Interaction between groups, both internally and externally, is central to understanding how to create more inclusive environments. Organizational processes
and societal norms shape each gender and drive the continual standardization of gender inequality (Williamson & Tranter, 2017). Interactionism, societal norms, and organizational processes impact females who enter and remain in the cybersecurity profession.

Several studies address the gender gap in the cybersecurity profession and its impact on the cybersecurity profession and the nation. Some pivotal assumptions were incorporated into the present study’s conceptual framework as a result of the previous literature. For example, it was assumed that male managers are more likely to hire male employees for tasks that appear to be male-centric (Coffman, Exley, & Niederle, 2018). It was assumed that managers hire new employees based on similarity to themselves (Johnson, 2017; Rivera, 2012). It was assumed that the gender gap in the cybersecurity profession affects the stability of national security in the United States. (Weingarten & Garcia, 2016; Vogel, 2016). It was assumed that females who enter the cybersecurity profession are less likely to be retained (Reed et al., 2017; Setalvad, 2015). Finally, it was assumed that females are drawn to careers and workplace tactics that directly impact human behavior and environments (Raytheon, 2015). The studies that provided a basis for these assumptions are discussed in greater detail in the next section of the chapter.

**Review of the Literature**

The literature review contains several sections that help to focus the content of the chapter. The first section contains a review of the literature on the cybersecurity profession. The next section contains a review of the literature on demand in the cybersecurity workforce. This section is followed by literature highlighting the gender disparity in the cybersecurity profession. Gender barriers and biases in the workplace are also discussed in detail. Information on the benefits of diversity and inclusion in the workplace follows. A final subheading within the literature reviews studies on diversity and performance.
Cybersecurity

Cybersecurity is a subcategory of information technology that focuses on how to secure data-at-rest and data-in-transit (Singer & Friedman, 2014). Cyberspace constitutes a notional environment defined by the communications that occur over the computer networks that constitute the foundation of modern society. The critical importance of these networks highlights the importance of cybersecurity activities in securing such infrastructure (Singer & Friedman, 2014). By 2012, over 80% of adults in the United States used the Internet daily and were thereby directly connected to the cyber domain (Kay, Pudas, & Young, 2012). Since 2012, dependency on the internet for both professional and personal use has continued to increase along with the need to secure both data and devices connected to the Internet (Ponemon, 2015).

A significant gender gap in the cybersecurity profession has, in the past, jeopardized America’s ability to produce enough cybersecurity professionals to address the country’s growing information security issues (Bagchi-Sen et al., 2010). As recently as 2015, females represented fewer than 15% of cybersecurity professionals in a field that had over 200,000 job vacancies at the time (Setalvad, 2015). The “demand for cybersecurity professionals over the past five years grew 3.5 times faster than demand for other IT jobs and about 12 times faster than all other jobs” (Setalvad, 2015, p. 1). Two factors directly contribute to this ongoing shortfall: (a) the overall supply of qualified candidates does not meet the demand, and (b) the overall supply is constrained by an insufficient number of females interested in working within the field (Dallaway, 2016). Increasing the number of females who are interested in working within the cybersecurity profession is critical and would mitigate both the cybersecurity gender gap and labor supply issues (Suby & Dickson, 2015). The demand for cyber professionals is such that
projections suggest that there will be a shortage of roughly 1.5 million cyber professionals in the United States by 2020 (Suby & Dickson, 2015).

Cybersecurity continues as a critical concern for both American business and government; cybersecurity also embodies serious ongoing national security dimensions in both domains (Cavelty, 2007). Expanding the diversity of the cybersecurity workforce by increasing female participation may help resolve the nation’s most challenging problems involving securing and protecting critical infrastructure. McLauren (2012) noted that “the success of a diverse workforce leads to an innovative culture where ideas flourish, and creativity has no boundaries” (p. 1). In a survey conducted by PricewaterhouseCoopers (PwC) in 2015, 76% of U.S. business executives expressed higher concern for cybersecurity threats in 2015 relative to 2014.

Cyberattacks continue to proliferate even as they increase in both sophistication and prominence (Beard, Mickelberg, Stapf, & Ulsch, 2015). During the past several years, the United States has suffered substantial data breaches as a result of cyberattacks. One of these cyberattacks targeted the Office of Personnel Management, a federal government organization that houses sensitive personally identifiable information used to conduct background investigations for millions of employees (Hussain et al., 2015). As a result of this attack, hackers stole over 20 million records (Hussain et al., 2015). The proliferation of cyberattacks and their associated risks are drivers of the continually rising demand for cybersecurity professionals (Raytheon, 2015).

Cybersecurity is currently one of the most sought-after IT skill sets and specializations in the United States (Wilshusen, 2015). Despite the rapidly increasing demand for cybersecurity professionals, interest from females remains low, and a significant gender gap continues to exist
in the profession (Dallaway, 2016). This literature review explores this gender gap and the factors that contribute to its persistence.

In 2015, the Ponemon Institute conducted a study to examine significant cybersecurity trends in the United States, the United Kingdom and Europe, and the Middle East. The study explored both present trends and projected trends for three years after the study to understand the impact on both private and public-sector organizations. The Ponemon Institute (2015) identified seven significant trends. The first trend was that cybersecurity is becoming a senior executive-level priority and a viable advantage. The second trend was that insider threats are increasing, and cybersecurity professionals need to address employee risk as well as external risk as a result. The third trend was that cybercrime will continue to cause anxiety to organizations and cybersecurity professionals. The fourth trend was the increasing growth of the Internet of Things (IoT) and inadequate preparation for that growth on the part of organizations.

The fifth trend identified by the Ponemon Institute (2015) was that the gap in cyber talent would persist in the face of growing cybercrime. The sixth trend was that there would be a significant change in technologies focused on big data analytics, forensics, and intelligence-driven resolutions. The seventh trend was that cybersecurity postures are improving and will continue to improve.

Ponemon (2015) invited 11,550 senior IT personnel and IT security experts in the United States to participate. A total of 421 completed surveys were analyzed. Cybersecurity professionals concurred that organizations must be more technically astute to handle cyberthreats, but respondents noted that organizations are not currently prepared to confront malicious cyberattacks. The survey respondents also indicated that many organizations have not implemented the proper measures to encrypt data-at-rest. Sixty percent of the participants
expected that the security posture of their organizations would improve, 31% believed their organization’s security posture would remain the same, and 9% expected security readiness to decline. Conclusions of the Ponemon report were that the “inability to hire and retain expert staff” (Ponemon, 2015, p. 1) within the cybersecurity workforce both contributes to a decline in security and reinforces the demand for qualified cybersecurity professionals.

**Cybersecurity Workforce Demand**

Cybersecurity impacts both the dimensions of economic and national security in U.S. government agencies as well as major organizations across the country (Caldwell, 2013). Kay et al. (2012) conducted a study which addressed current and future demand for cybersecurity professionals and the extant capabilities and capacities of the U.S. cybersecurity workforce. When conducting the study, it was difficult for Kay et al. to define what constituted workforce demand as the work roles and skill sets associated with cybersecurity as a profession had not been previously defined. Kay et al.’s findings highlighted the challenge facing both public and private sector organizations when defining what capabilities a future cybersecurity workforce should possess (Kay et al., 2012). Cybersecurity professionals need to be able to ensure that data security can be maintained. In order to do so, these professionals need to ensure that data remains confidential while maintaining the integrity of the data and also ensuring that the data is always available for the appropriate parties when necessary. The preceding reflects the confidentiality, integrity, and availability (CIA) triad, foundational to security professionals’ daily work (Ning, Liu, & Yang, 2013).

In 2013, Suby assessed the state of the information security workforce across various organizations. Suby collected data by surveying over 10,000 qualified candidates to explore information security preparedness. Over 55% of the respondents stated that they did not have the
necessary cybersecurity professionals within their organization. In 2015, Suby and Dickson replicated Suby’s (2013) initial study to determine whether the need for security experts persisted and to identify new trends in the field of cybersecurity. The results of the second study indicated that the need for information security professionals within organizations did not dissipate. Suby and Dickson (2015) noted that the number of organizations without adequate cybersecurity personnel had increased to 62.2%.

In 2016, the unemployment rate among cybersecurity professionals was 0% (Cotenescu, 2017). Cotenescu (2017) noted that this rate is expected to remain 0% for the next five years. As of October 2017, there were 285,681 cybersecurity job openings in the U.S (Cyberseek, 2017). These statistics are based upon the number of online job postings relating to the cybersecurity profession (Cyberseek, 2017). While a 0% unemployment rate appears ideal for those who need employment, this situation is alarming for companies who seek to fill positions associated with the profession (Kullman, 2017). Specifically, it impacts the organizations’ “retention issues, salary inflation, and sub-par candidates getting jobs they’re not qualified to have. Companies are going to have to invest heavily in training young cybersecurity professionals who have a combination of technical, business, and soft skills” (Kullman, 2017, para. 7).

Developing a robust cybersecurity workforce is critical to ensure national and economic security in the United States (Raytheon, 2015). In 2015, Raytheon, a technology company that addresses cyber solutions for both private and public-sector organizations, partnered with the National Cyber Security Alliance (NCSA) to administer a global survey to Millennials between the ages of 18 to 26 across 12 countries. One significant finding was the difference between male and female interest in cybersecurity (Raytheon, 2015). This gender gap is global, but it was largest in the United States. Only 23% of females surveyed indicated that they were likely to
select cybersecurity as a career, relative to 43% of the males surveyed. The survey also found that 21% of Millennials surveyed believed the cybersecurity profession is stressful, 18% believed the job is boring, 15% believed the salaries are inadequate, 21% believed combatting inevitable cyberattacks is a futile effort.

Science, technology, engineering, and math (STEM). Cybersecurity is a top priority for the United States, with researchers noting that cybersecurity poses “serious economic and national security challenges” (Perez, Cromley, & Kaplan, 2015, p. 17). Perez et al. (2015) argued that the number of females receiving undergraduate STEM degrees has declined due to the lack of exposure to these topics among females at a young age and the lack of female role models in these fields. The gender gap in STEM-driven career fields is not new. Computer Science (CS) and information technology are pivotal STEM degrees that provide foundational knowledge for cybersecurity professionals, but these fields have traditionally lacked adequate numbers of females (Dutta & Mathur, 2012).

In 2011, Beede et al. reported that females accounted for roughly 25% of STEM professionals. Of these women, only 60% were expected to remain in STEM fields, relative to the 80% of males who typically remain in their respective STEM fields (Beede et al., 2011). The number of females employed in computer-related occupations has continuously declined since 1990 (Landivar, 2013). In 1990, females represented 41% of computing occupations, as opposed to 25% in 2013; in engineering occupations, females represented 12% in 1990 and had only grown to 14% as of 2013 (Landivar, 2013).

The lack of female representation in these two occupations is critical, considering that computing and engineering occupations represent 80% of STEM careers (Landivar, 2013). Kaspersky (2017) collected survey data from participants between the ages of 16 and 21 from
around the globe, including the United States. Kaspersky also collected data from industry experts to gain insights into technical reasons for the gender disparity in STEM careers. The article indicates that males (49%) are more likely than females (36%) to select mathematics, and males (21%) are more likely than females (7%) to select IT as their preferred subject in school. Females have reported many reasons for not remaining in STEM career fields. These include not receiving equal pay, family pressures, not being supported concerning career advancement opportunities, gender discrimination, and the overall job climate (LeClair et al., 2014).

Historically, the association of females with computing-related studies and careers has been described as a “leaky pipeline” (Dee, Petrie, Boyle, & Pau, 2009, p. 233). Landivar (2013) reported that while females make up 48% of the total workforce, they only represent 25% of STEM jobs. Additionally, females hold a minimal number of STEM undergraduate degrees, and most females who hold a STEM degree are less likely to pursue a STEM-related career (Landivar, 2013). For every 100 female undergraduate students, 12 individuals graduate with a STEM degree, and only 3% continue working in a STEM career field for 10 years after graduation (Carnevale, Smith, & Melton, 2011).

Carnevale et al. (2011) identified key reasons for the gender gap in STEM careers as the lack of female mentors, gender stereotyping, and inflexible work environments. Across all STEM-related fields, females were found to be the least represented in engineering. While STEM courses are foundational to IT and cybersecurity-related qualifications, other factors beyond the relative absence of females in STEM course contribute to the leaky pipeline delivering females to the profession. Kay et al. (2012) noted that in order to maintain a robust cybersecurity stance on an ongoing basis, the United States. also needed professionals in cyberpolicy, law, and other disciplines where females are underrepresented.
Females’ lack of interest in computing-related subjects and work roles is not new; the problem was already prevalent in the 1990s (Craig, 1998). In a 1994 study conducted over the preceding three-year period, the retention rates of females in computing courses who received peer mentoring was compared to the retention rates of to those who did not (Craig, 1998). The study concluded that females appreciated working in teams, receiving emotional support, and not being judged or belittled by other females for gaps in their knowledge. Females in the study expressed that they felt inspired when they were not experiencing the journey alone, but some study participants expressed the desire to quit computing classes even before receiving peer mentoring during the study.

Craig’s (1998) study highlighted that computing classes were male-dominated and unwelcoming to females at the time that the study took place. Craig also identified a higher retention rate in females who participated in the mentoring program because it built self-esteem and confidence and provided a platform to learn how to overcome change, data resources relating to technical concepts and computer-based careers, and a robust support system for female computing students. Twenty years later, Guillen (2018) found that women had equal self-confidence to men in high-technology workplaces, but such self-confidence was perceived differently.

Guillen (2018) noted that organizational influence was tied to perceptions of warmth in the case of female employees but not male employees. Guillen also reported that female employees with high self-confidence did not always appear confident to male colleagues. Guillen concluded that what was at issue was not females’ self-confidence in the workplace but that workplace practices needed to change to reward females equally with males. Guillen made three recommendations to address the issue. First, job requirements needed to be made more explicit
and be disseminated among all employees. Guillen noted that such requirements should acknowledge the specific qualities for which female employees were valued. Second, career promotion and advancement standards need to be made more gender neutral. Third, more diverse role models need to be disseminated in high-technology organizations to make them more friendly to diversity.

Professional certification. There must be a robust pipeline of well-educated candidates who continuously enter the field and then advance within the profession to meet the demand for cybersecurity professionals (Caldwell, 2013). While such a robust pipeline would go far in addressing the cybersecurity workforce shortage, it would also imply significantly increasing the supply of female candidates. This pipeline would supply candidates who may be STEM degree holders, professional certification holders, or both. There are a substantial number of professional certifications that satisfy the professional skills criteria for acquiring cybersecurity jobs.

The International Information System Security Certification Consortium (ISC²) is one of the leading organizations that create courses to train, examine, and certify cybersecurity professionals. One of the most sought after and highly compensated cybersecurity certifications ISC² offers is the Certified Information Systems Security Professional (CISSP). Worldwide, in 2017, only 112,412 people held a CISSP certification, of which, 73,552 resided in the United States (ISC², 2017). Less than 10% of CISSP certification-holders are female (LeClair et al., 2014). The CISSP certification is a highly respected certification that is not easily obtained and requires a candidate to have a certain level of work experience and demonstrate core competencies in eight categories which relate to information security. The fact that less than 10%
of CISSP holders are female demonstrates the ineffectiveness of the pipeline delivering females to both the IT and cybersecurity-related fields.

A consensus exists among leaders in government, academia, and industry that U.S. organizations must take steps to address the present and deepening deficit in highly qualified cybersecurity human resources in the United States (Assante & Tobey, 2011; Vogel, 2016). The Sans Institute noted in 2015 that previously, “women have been a largely untapped resource” (Sans Institute, 2015, p. 1). If females were hired at rates proportionate to their male counterparts, the deficit of cybersecurity professionals would be addressed.

One way that organizations seek to promote the development of human capital is by recognizing certification programs to supplement classroom training (van Zadelhoff, 2017). Examples of certifications other than the CISSP that are both recognized and sought out by organizations employing cybersecurity professionals include the Certified Ethical Hacker (CEH), Network Plus (Net+), and Security Plus (Sec+). Promoting these certification programs to females would also improve gender diversity in the cybersecurity profession.

**Cybersecurity Skill Set**

Cobb (2016) explored how critical the skills deficiency was in the profession of cybersecurity by examining efforts to assess the aptitude and ability of cybersecurity professionals participating in accelerated cybersecurity training programs. These areas were explored to address whether the United States can “produce enough appropriately skilled human defenders of digital systems to defeat the humans who seek to compromise such systems for nefarious purposes” (Cobb, 2016, p. 1). Cobb (2016) noted that the cybersecurity skills gap started within the military.
The U.S. National Institutes of Standards and Technology (NIST) created the National Initiative Cybersecurity Education (NICE) in 2010 (Newhouse, Keith, Scribner, & Witte, 2017). NICE was tasked with establishing national standards defining cybersecurity demand. NICE was also tasked with the creation and promotion of a robust network in support of cybersecurity education, training, and workforce development (Newhouse et al., 2017). The first NIST initiative to create a framework for the cybersecurity workforce commenced in 2008 before the creation of NICE (Newhouse et al., 2017). That framework was launched in 2012, with the first official NICE workforce framework following in 2013 (Newhouse et al., 2017).

The NIST coordinated and led the collaboration with both academia and private industry when developing the NICE Workforce Framework. The NICE Workforce Framework categorizes the various roles in the cybersecurity profession and the relevant education, training, and hands-on experience required to complete specified categories of tasks. The NICE framework defines the cybersecurity profession in terms of seven categories. These categories consist of analytic skills, data collection skills, investigative abilities, the ability to operate and maintain cybersecurity systems, oversight and development skills, skills related to protecting and defending data and systems, and the secure provisioning of services (Newhouse et al., 2017). Each of the seven categories contains specialty areas, and in total, the categories contain 32 specialty areas and 55 work roles. Table 2 presents the National Cybersecurity Workforce Framework work categories and specialty areas.

The “security workforce is one of the fastest-growing subgroups in IT, a unique professional niche with distinctive task responsibilities, job market conditions, and training needs” (Lee, Bagchi-Sen, Rao, & Upadhyaya, 2010, p. 1). In addition to the overall skills categories identified in Table 2, interpersonal skills are also sought for cybersecurity
professionals. Cybersecurity professionals are expected to be able to work in teams, influence decision-makers, and articulate the return on investments to decision-makers within organizations at the highest levels (Suby & Dickson, 2015). Teamwork is essential to organizational success, and the ability to incorporate diverse perspectives within a team is critical in cybersecurity due to the vast range of problems encountered in the field (Ashare, 2017; Reynolds & Lewis, 2017; Rock & Grant, 2016).

Table 2. National Cybersecurity Workforce Categories and Specialty Areas

<table>
<thead>
<tr>
<th>Category</th>
<th>Specialty Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analyze</td>
<td>All source intelligence, exploitation analysis, targets, threat analysis</td>
</tr>
<tr>
<td>Collect and Operate</td>
<td>Collection operations, cyber operations, cyber operations planning</td>
</tr>
<tr>
<td>Investigate</td>
<td>Digital forensics, investigation</td>
</tr>
<tr>
<td>Operate and Maintain</td>
<td>Customer service and technical support, data administration, knowledge management, network services, system administration, systems security analysis</td>
</tr>
<tr>
<td>Oversight and Development</td>
<td>Education and training, information systems security operations, legal advice and advocacy, security program management, strategic planning, and policy development</td>
</tr>
<tr>
<td>Protect and Defend</td>
<td>Computer network defense analysis, computer network defense, infrastructure support, incident response, vulnerability assessment and management</td>
</tr>
<tr>
<td>Securely Provision</td>
<td>Information assurance compliance, software assurance, security engineering, systems development, systems requirements planning, system security architecture, technology research and development, test and evaluation</td>
</tr>
</tbody>
</table>

Furnell, Fischer, and Finch (2017) suggested that the distinction between information security and the broader term cybersecurity is still a new trend. Furnell et al. identified various factors as contributing to the shortage of cybersecurity professionals. These factors included the minimal interest of Millennials in cybersecurity, the scarcity of qualified educators, the absence of clear career paths that relate to cybersecurity, and the lack of coverage of cybersecurity in computer courses. Furnell et al. also asserted that the relative newness of the cybersecurity profession impacts organizations’ abilities to identify appropriate professionals with the proper skills.

Furnell et al. (2017) examined the shortfall in candidates with qualifying cybersecurity skill sets and experience and recommended that organizations with chronic recurring vacancies follow a strategy of investing in upgrading the skills of current employees to produce well-rounded cybersecurity professionals suitable to the organizations’ needs. Furnell et al. also noted that varied skill sets are necessary for cybersecurity professionals, and currency and proficiency need to be maintained across these skill sets. As a result, it is essential for cybersecurity professionals to continue to invest in their educational growth to remain efficient and competitive (Suby & Dickson, 2015).

**Gender Disparity in the Cybersecurity Profession**

Cybersecurity is a complex field that requires innovation and creativity regardless of its source. In a 2014 journal article, Spafford (2014) explored the lack of females in computing, information security, and cybersecurity, identifying the continuous decline in the numbers of females in IT-related professions in the period since 1990. Specifically, Spafford (2014) examined the treatment, while working, of female cybersecurity professionals. This decline in
the number of females working in both IT and specifically the cybersecurity profession is rooted in cultural behaviors and social perceptions (Spafford, 2014).

While Spafford (2014) focused on females in the United States, the problem of a gender gap in the profession also existed in other countries, such as the United Kingdom, Canada, and Australia. Spafford noted that over time, various programs had been created to close the gap; however, these programs had not been sufficiently successful in effecting long-lasting, quantifiable change. Spafford concluded by providing recommendations for both males and females concerning how to resolve the problem. The critical advice for females was to refrain from believing that the problem was specific to them individually. Spafford noted that several professional working groups, platforms, and activities were available to support females’ development and growth in the cybersecurity field. Spafford’s advice to males was to encourage them to be cognizant of how they treated females in the classroom and at work. Spafford stressed that males should be advocates for greater female participation in cybersecurity.

In 2010, Lee et al. explored the attributes that should characterize a cybersecurity professional and how such attributes would differentiate the new career path from other IT work roles. Lee et al. identified the skills necessary for the cybersecurity profession and discussed why professionals enter the cybersecurity profession and why they may leave that profession. Lee et al. were not able to draw significant conclusions about female cybersecurity professionals as distinct from male professionals due to the paucity of female respondents in their study.

To ensure that the U.S. government and major companies are positioned to defend against cybersecurity attacks, the significant shortage of females contributing to the overall shortage of cybersecurity professionals must be addressed (McBrearty & Wainwright, 2013; Gonzalez, 2015). In 2013, the Women’s Security Society held a roundtable discussion to explore
why many females were not being drawn to the cybersecurity profession and why their retention rate was so low (McBrearty & Wainwright, 2013). Several stereotypes were identified as associated with the cybersecurity work role, and the roundtable discussion highlighted that most cybersecurity professionals were perceived as nerds and that entry-level positions required a sophisticated skill set (McBrearty & Wainwright, 2013). These stereotypes led to a lack of interest in the cybersecurity profession on the part of some females.

Mohr (2014) surveyed females and males to identify why females apply for jobs at a lower rate than males and to examine the reduced probability that females will apply for jobs for which they are not qualified as opposed to their male counterparts. Mohr found that young girls are socialized to abide by rules in school and are rewarded for this. Mohr also found that adult females are held to a higher standard than males and must exceed qualifications. Finally, Mohr noted that females overcompensate for formal training and education but undercompensate when building strong professional networks and leveraging advocates (Mohr, 2014). In similar research, Dallaway (2016) found that young females are not attracted to marketing materials associated with the cybersecurity profession and the various work roles associated with it. In another recent study, one in every six females was found to believe that cybersecurity as a professional activity is monotonous (Kaspersky, 2017).

Pittman (2015) suggested the use of alternative education methods to develop female cybersecurity professionals due to the absence of gender diversity in STEM courses in higher education. Pittman recommended leveraging cyber competitions as an alternative education method, and to explore the viability of this option, Pittman examined the theory that cyber competitions are not gender-inclusive. Pittman also examined whether the lack of inclusivity
among cyber competitions applied only to collegiate-level students or to younger students as well.

Pittman (2015) compared competition formats and found that current competition formats are designed to attract males. Pittman noted that culturally males seek to outperform others, whereas females tend to prefer to participate in teams allowing a group to win jointly. Pittman (2015) concluded that current cybersecurity competitions are designed and executed in a manner that does not appeal to the typical psychological and cognitive makeup of females. Pittman also concluded that the lack of inclusiveness in cyber competitions was consistent across all age ranges up to and through the collegiate level. Pittman was not able to address whether differently designed cyber competitions might be more attractive to females.

Another issue that may repel women from the profession of cybersecurity is the terminology employed when discussing cybersecurity. Raytheon (2015) referred to the term cybersecurity and its related terminology as military-centric and not gender-neutral. For example, rather than the term cybersecurity, the term information security may be more appealing as a career discipline to females (Raytheon, 2015). Regardless of the terminology, it is critical that females are taught about opportunities within the cybersecurity profession and that they understand the knowledge and skills required to obtain a job in this career field (Dallaway, 2016).

Williamson and Tranter (2017) conducted a literature review specifically focused on scholarly work related to females in cybersecurity in conjunction with publicly available statistics in an attempt to create a holistic narrative of the phenomenon of the gender gap in cybersecurity. Williamson and Tranter examined the phenomenon from a global perspective and highlighted its impact on Australia’s current posture regarding cultivating and retaining
cybersecurity talent. Williamson and Tranter identified various barriers to women working in cybersecurity, and these included marketing of the cybersecurity profession that was not gender-inclusive, non-gender-neutral hiring practices used to hire cybersecurity professionals, and the absences of reflective role-models.

Williamson and Tranter (2017) noted that there were knowledge gaps that persisted in the cybersecurity profession in regard to issues surrounding the retention of females in the cybersecurity profession. The ongoing existence of such knowledge gaps was supported by Peacock and Irons (2017) who noted that issues associated with the gender gap in cybersecurity involved the attraction, hiring, and retention of females (Peacock & Irons, 2017). Dallaway (2016) also conducted a study to determine why females are not attracted to cybersecurity jobs. Data was collected through interviews and specifically focused on questions regarding increasing diversity in cybersecurity and how an organization should implement diversity. Dallaway’s findings suggested that more females should be used in television advertisements related to the job role and that advocates for the cause should be vocal and adequately portray the cybersecurity profession so that female candidates understand the profession is gender-inclusive.

While gender diversity produces more effective business results, most high-technology-oriented organizations struggle to achieve gender balance within their workforces (Devillard, Sancier-Sultan, de Zelicourt, & Kossoff, 2016). The fact that gender diversity can be challenging to achieve has not stopped organizations from strategizing to increase gender diversity at higher levels within organizations (Barsh & Yee, 2011). Barsh and Yee (2011) gathered data concerning the development, retention, and advancement of females within Fortune 500 organizations.
After surveying over 4,000 employees across multiple countries, Barsh and Yee identified key themes in the data. One finding was that while the organizations surveyed in the study attracted many females for entry-level positions, a significant number of these females did not advance beyond middle-level management (Barsh & Yee, 2011). Barsh and Yee (2011) found that in most cases, females stagnated at the middle management level and less than 5% of the females who started with organizations advanced to the highest levels of leadership. Barsh and Yee also noted that a significant number of females never advanced to middle-level management. These females either left the organization altogether or transferred to staff positions due to a real or perceived lack of opportunities.

Barsh and Yee (2011) also highlighted the relationship between the level of diversity in an organization and the likelihood of females being promoted to senior positions. Barsh and Yee identified companies with staff rosters that were 50% or more female. In these companies, greater than 22% of leadership positions were held by females, and there were more favorable promotion odds for females than for males. Among female middle managers in these companies, at least 55% were in positions that prepared them for senior management positions such as vice president and senior vice president. The companies that fulfilled these criteria approached gender diversity either through fat funnels or steady pipes (Barsh & Yee, 2011).

The fat funnel approach focuses on encouraging a significant number of females to enter the organization with the understanding and expectation that a large number will then leave, but enough females will stay to build gender diversity and acceptable rates of gender balance in the organization (Barsh & Yee, 2011). The steady pipe approach places a greater focus on supporting females. In this approach, there are fewer females hired for entry-level positions, but substantial efforts are made to foster a work environment that is gender-balanced and supports
the retention of females (Barsh & Yee, 2011). Steady pipe organizations not only retain females, but they also allow females to rise to the highest levels of leadership (Barsh & Yee, 2011).

Weingarten and Garcia (2016) examined leaks in the pipeline by researching the factors that caused females to exit the pipeline. Three key areas were identified where the pipeline leaked particularly severely. The first was the period in females’ educations from the 6th through 12th grade. The second was the hiring process, and the third was events that took place in the workplace. Weingarten and Garcia recommended providing additional training to K-12 teachers to address the need for more females to enter the pipeline. This training would address teachers’ conscious and unconscious biases and aid in the removal of societal and cognitive barriers that are ingrained in young females by the time they arrived in school. The removal of these barriers, in turn, would encourage female students to consider STEM courses and to see themselves as potential leaders of organizations.

Kaspersky (2017) reported that females might be interested in cybersecurity, but they are not consistently aware of career opportunities. Females also feel that they do not possess the necessary skills to be cybersecurity professionals (Kaspersky, 2017). Despite females’ perceived lack of understanding or preparedness, females who were interested in cybersecurity were interested in making a difference to society. The purpose of the study was to uncover the interest, influences, characteristics, awareness, and perceptions of cybersecurity as a profession among females (Kaspersky, 2017). Kaspersky noted that between the ages of 15 and 21, most young females have already determined which career path they will pursue. Kaspersky noted that if the gender gap is to be addressed, it is critical for young girls to be introduced to STEM courses and IT-related courses and activities at an early age.
Kaspersky (2017) identified the primary reason for the gender gap in cybersecurity as the lack of female role models. Minimal numbers of females work within the cybersecurity profession, and even fewer females occupy positions of power and influence to act as role models for younger females. Less than 11% of young females have met a female cybersecurity professional and 65% have never met any cybersecurity professional (Kaspersky, 2017). Data gathered by Kaspersky (2017) indicated that over 60% of females have an improved perception of cybersecurity after meeting with a cybersecurity professional.

Peacock and Irons (2017) conducted a quantitative study and collected data through an online survey of both genders. The data was analyzed in its original state and then cross-referenced to determine how perceptions of males and females differed. Results demonstrated that males believed females possessed equal recruitment opportunities and were equally valued at work in the cybersecurity profession. There were notable instances in which females did not agree. Males also believed that both genders were likely to be promoted to senior positions within the cybersecurity profession, while females disagreed.

In 2013, the Association of Computer Machinery (ACM) Innovation and Technology in Computer Science Education (ITiCSE) conference hosted a working group that focused on identifying the reasons for the deficiency of females and minorities in the cybersecurity arena (McBrearty & Wainwright, 2013). The overall purpose was to explore a wide range of factors that influence females’ and minorities’ decisions not to enter the cybersecurity profession. Identified factors included issues surrounding recruitment, hiring, retention, and advancement of females in the cybersecurity profession.

Females continue to be underrepresented within the pipeline filling the cybersecurity profession (Reed et al., 2017). The issue of female underrepresentation is not merely an issue of
academic interest but also a vital U.S. economic and security interest as ensuring that more females advance to careers in cybersecurity will assist in ameliorating the nation’s workforce shortages in the field of cybersecurity. Populating the cybersecurity pipeline must begin with attracting students to the relevant fields before college (Nakama & Paullet, 2018). Kaspersky (2017) list several findings identifying the underlining factors that impact the pipeline.

Among the reasons for not selecting a career in cybersecurity, is a lack of experience in computer coding (57%), not having any interest in computing as a career (52%) and not being aware of or knowing enough about cybersecurity careers (45%) were the most prevalent among females (57%). (Kaspersky, 2017, p. 5)

Stereotypes of who is a cybersecurity professional also create problems in recruiting females to the profession. Cybersecurity professionals have long been stereotyped as young white males who code. This misconception has not provided prospective female candidates with an accurate depiction of who cybersecurity professionals are or what their varied professional roles may include (Weingarten & Garcia, 2016). This stereotyping is especially problematic as Kaspersky (2017) suggested that females are more likely to seek same-gender role models and also work environments where the gender division is not too disproportionate.

Gender Barriers and Biases in the Workplace

Grade school-aged students of either gender share the same level of interest in computer-related subjects such as cybersecurity, but as students grow older, this interest on the part of the female students dissipates (Setalvad, 2015). Setalvad (2015) attributed the decline in female interest in cybersecurity to stereotypes which are not welcoming to females. For example, Setalvad noted that females are deterred by the stereotype that cybersecurity professionals all resemble white male nerds. Females encounter a male-dominated environment as cybersecurity
professionals, and Kaspersky’s (2017) findings suggest that this is problematic as females prefer work environments with less disproportionate gender imbalances.

While throughout the past 100 years, females have continued to surmount social barriers and have both entered and achieved in all the professions, they are seldom represented at the highest levels of leadership (Chandler, 2011). As a result, Chandler (2011) conducted a study exploring three critical aspects of females’ lack of representation in senior leadership roles. First, Chandler examined females’ rise to leadership in organizations where they lead. Second, Chandler examined how females lead, and third, Chandler studied the benefits to organizations of female leaders.

Chandler (2011) observed that females and males lead differently. “Women’s leadership styles have been shown to be more transformational, participative, and inclusive than the leadership styles of their male counterparts” (Chandler, 2011, p. 1). Females are more often transformational leaders, which affords them the ability to lead people more adeptly; males are more often transactional leaders, which jeopardizes the connection and passion among the workforce they lead. A females’ ability to lead interactively empowers those they lead to participate more, form stronger teams, and build greater in-group rapport. However, some perceive females’ abilities to understand and connect as a leader as weak, soft, or emotional (Chandler, 2011).

Females with positions in organizations or careers that are male-dominated find that they often face difficulties when negotiating opportunities to advance their careers (Born, Ranehill, & Sandberg, 2018; Martin & Barnard, 2013). McGinn and Oh (2017) noted that after a female obtains a position, and particularly as she advances in an organization, she must continually prove herself because male colleagues will perpetually underestimate her based on their
valuations of her past accomplishments. Krivkovich, Robinson, Starikova, Valentino, and Yee (2017) noted that these valuations are particularly problematic as men hold most senior positions, and thus, their valuations have disproportionate weight in the network that can be built in the cybersecurity career field.

The right network can accelerate a career. Women are more than five times more likely to rely on a network that is mostly female. Because males typically hold more senior-level positions, this means females are less likely to get access to people who can open doors for them. (Krivkovich et al., 2017, p. 7)

Prime and Moss-Racusin (2009) argued that creating gender balance in the workplace fosters a more accomplished and driven workforce. Prime and Moss-Racusin’s research demonstrated the impact of mentoring on the career advancement of females. Their results indicated that it is vital that employees receive mentorship and sponsorship to support their career progress. The recruitment and retention of females within the cybersecurity profession must begin by informing females of the opportunities within the profession. Once hired, it is important for organizations that females are retained. In order to ensure that this occurs, females should have mentors who resemble them and who thrive in an inclusive work environment. Prime and Moss-Racusin (2009) also found that males are unaware of the challenges their female counterparts encounter as a result of their inability to participate in the good-old-boys network and the weakness of counterpart female professional networks.

Females are penalized for self-glorification and are socialized to be modest and nurturing to others (Williams & Dempsey, 2014). Williams and Dempsey (2014) interviewed 127 females and revealed that females are indeed perceived significantly differently than their male counterparts. Williams and Dempsey reported that females were held to different standards in the workplace while exhibiting the same behaviors. Approximately 67% of females received
negative feedback concerning workplace performance, while less than 2% of males received negative feedback (Williams & Dempsey, 2014).

Alev, Gonca, Ece, and Yasemin (2010) described biases that relate to specific occupational types and the categorization of occupations as male or female solely based on stereotypes. Particular traits were associated with females, such as the natural ability to be caring and nurturing. Males were perceived as dominant and self-sufficient, and as mature leaders (Alev et al., 2010). Throughout the past three decades, females have continued to advance professionally in areas that were not traditionally perceived as female, but by the early 2000s, the acceptance of females in these areas was still being delayed due to the continued prevalence of pre-existing societal norms (Haines et al., 2016).

Haines et al. (2016) replicated a study conducted in 1983 concerning gender stereotypes and compared data collected in 1983 to data collected in 2014 to analyze changes in gender-related stereotypes over the years. The study considered gender traits, roles, occupations, and physical characteristics. By comparing data collected in the early 80s to data collected in the early 2000s, the researchers identified a significant increase in how females are stereotyped based on gender. “These results attest to the durability of basic stereotypes about how men and women are perceived to differ, despite changes in the participation and acceptance of women and men in non-traditional domains” (Haines et al., 2016, p. 1).

Females are less likely to take credit for their accomplishments relative to their male counterparts (Haynes & Heilman, 2013). Haynes and Heilman (2013) conducted a study to test this concept. Multiple-case studies were performed to cross-reference data. In the first set of cases, females and males were placed on the same team and assigned a task to complete. After completing their work successfully, females did not take credit for the work in the same manner
as their male counterparts. Women praised their male teammates more than themselves, and their male teammates praised themselves. Haynes and Heilman noted that when females were paired with other female teammates and were assigned the task, the females took credit for their contributions to the group. Haynes and Heilman posited that gender stereotypes caused females to underestimate their contributions to effective results. These results aligned with the fact that some occupations are still perceived to be more appropriate for males, creating a barrier for females entering or working in these professions. Changes in societal norms lag behind changes in gender roles, and traditional societal norms continue to influence what humans perceive as acceptable (Haynes & Heilman, 2013).

**Diversity and Inclusion in the Workplace**

The cybersecurity workforce must be diverse, robust, and sustainable to be effective in the fast-paced, ever-changing arena of cybersecurity. The workforce and workplace should be both diverse and inclusive with inclusion representing “an active process of change or integration, as well an outcome, such as a feeling of belonging” (Bourke & Dillion, 2013, p. 12). Research has demonstrated that inclusion is perceptible to those whom it impacts; individuals appreciate when organizations include them and respond with feelings of being valued and included (Bourke & Dillion, 2013). Bourke and Dillion’s (2013) findings were supported by research by Hunt et al. (2015) who found that gender-diverse businesses in the top quartile of gender diversity in their study were 15% more likely to have financial returns above their industry medians.

Hunt et al.’s (2015) findings were based on proprietary datasets from 366 companies worldwide, which included metrics of each organization’s financial state as well as the demographic composition of both the organization’s top-tier management and its executive
board. Data collection occurred over three years. Hunt et al. (2015) found that companies that were in the top quartile on racial and ethnic diversity were 35% more likely to have financial returns above industry norms.

Hunt et al. (2015) suggested that due to the globally high (16%) representation of women in senior management in the United States, some of the benefits organizations could garner from gender diversity had already been gained in the United States versus organizations in other global economies. The relationship between the number of women in senior management in the United States with gendered diversity gains was supported by the much more significant gains that Hunt et al. found related to levels of gender diversity in U.K. companies that had the next highest percentage of women in senior management. Organizations with high degrees of either racial or gender diversity tended to produce higher financial returns than organizations with low scores for both racial and gender diversity. Additionally, Hunt et al. (2015) found that organizations that focused on creating greater diversity across racial, ethnic, and gender lines tended to have the best financial returns.

Bias is an issue in workplaces, and the two most common types of bias are conscious and unconscious bias (Peacock & Irons, 2017). Unconscious bias is often detrimental to organizations when such organizations are not aware that this type of bias exists amongst employees (McCormick, 2015; Peacock & Irons, 2017). Over 150 types of unconscious biases have been previously identified related to gender, race, age, name, attire, and many other real or perceived characteristics of individuals (McCormick, 2015). McCormick (2015) noted that it is challenging to be aware of all possible biases but that such biases can be combated when identified. Identified biases can be highlighted and addressed through training of employees to
ensure that organizational employees become aware of these biases and can thus ensure that all organizational employees are treated fairly (McCormick, 2015).

In 2017, McKinsey & Company partnered with LeanIn to conduct a study on the role of females in the workplace (Krivkovich et al., 2017). This study consisted of quantitative data collected from 70,000 employees at 222 companies in addition to 29 qualitative interviews of females from eight organizations at various points during their careers. The study’s conclusions included recommendations that organizations make explicit efforts to understand their previous progress towards closing the gender gap at every level within their organizations. The study recommended this based on the fact that it found that such efforts are necessary in order for organizations to explicitly address previously identified obstacles hindering the organization’s processes for combatting gender bias.

Krivkovich et al. (2017) found that while 99% of organizations agree that supporting diversity is a high priority, less than 40% of employees agree that their organizations genuinely demonstrate that diversity is indeed a high priority. Krivkovich et al.’s study also highlighted that male and female employees perceived gender disparity in organizations differently. Finally, Krivkovich et al. noted that females continue to advance in their careers at slower rates than their male counterparts. Krivkovich et al. (2017) found that the crucial contributor to this slower career progress continued to be lack of mentoring, as only a minimal number of females in the study were mentored by more senior managers and leaders on their ongoing career paths.

**Diversity and Performance**

Peacock and Irons (2017) contended that a more diverse workforce was more likely to foster increases in productivity and creativity than a less diverse workforce. The field of cybersecurity continues to be male-dominated and tends to reflect male in-group dynamics,
values, and methods of problem-solving (Macdonald, 2014; LeClair et al., 2014). The result of these in-group dynamics is to foster a work environment that is unfriendly to females. Such a work environment, in turn, causes “a lack of women interested in the sector reduces the pool of talented individuals that organisations can recruit from” (Caldwell, 2013, p. 8).

Barker, Mancha, and Ashcraft (2014) found that females exhibit higher levels of collective intelligence compared to men. Collective intelligence was defined as “the inference one draws when the ability of a group to perform one task is correlated with that group’s ability to perform a wide range of other tasks” (Woolley, Chabris, Pentland, Hashmi, & Malone, 2010, p. 687). Barker et al. (2014) studied a total of 669 individuals working in small teams (i.e., two to five team members). Barker et al. found that the collective intelligence rose of a team increased in relation to “the number of females in the group” (p. 4). Barker et al. suggested that this correlation was due to females’ higher levels of social sensitivity. Regardless of the reason for the increased performance, Barker et al. noted that organizations “perform better financially, particularly when females occupy a significant proportion of top management positions” (p. 2).

The past scholarly literature has provided findings that suggest that groups who are more diverse tend to outperform groups that only consist of subject matter experts or a single cultural, ethnic, or gender group. These past findings were supported by the results of a study conducted by Hunt et al. (2015). Hunt et al. found that organizations with a high degree of diversity tended to outperform organizations with low levels of diversity. Hunt et al. noted that “Diversity fosters innovation and creativity through a greater variety of problem-solving approaches, perspectives, and ideas. Academic research has shown that diverse groups often outperform experts” (p. 9).

To explore gender diversity in the workplace, Ellemers, Rink, Derks, and Ryan (2012) investigated the impact of gendered leadership beliefs on females within organizations. Ellemers
et al. (2012) reviewed the extant scholarly literature and found that it provided significant support for their findings. Ellemers et al. focused on two convictions. The first was that female employees, as a group, face expectations that they will utilize different leadership styles than male employees. The second conviction was that females who ascend to senior leadership will demonstrate competitiveness and toughness. Ellemers et al. stated that both of these perceptions of female employees are forms of gendered leadership beliefs and constitute bias against females. Ellemers et al. also noted that female employees that internalize these perceptions may have their future career opportunities harmed. Ellemers et al. stated that their model allowed them “to connect ‘glass cliff’ effects to ‘queen bee’ effects showing that both relate to the perceived salience of gender in the organization, as well as individual gender identities” (Ellemers et al., 2012, p. 1). Ellemers et al. concluded that gender stereotypes establish how male and female leaders are expected to behave and that such gender stereotypes are linked to suboptimal outcomes for female leaders in organizations.

Organizations that outperformed peers tended to have smaller gender disparities in the number of promotions to management positions that went to each gender (Krivkovich et al., 2017). In organizations with wider gender gaps, females were 18% less likely to be promoted to manager, but conversely, females were only 4% less likely to be promoted to manager in higher-performing organizations (Krivkovich et al., 2017). Barker et al. (2014) found that gender-diverse organizations achieved higher financial returns compared to organizations with less gender diversity. Barker et al. also found that such organizations possessed better team dynamics and efficiency and produced teams who were disciplined, remained under budget, and demonstrated better employee performance. Thus, the narrowing of gender gaps is correlated
with better organizational and team performance, which suggests that having more women participate in the field of cybersecurity could potentially benefit a wide range of organizations.

Inclusion drives retention in the workforce, and such organizational efforts at inclusion can be active, passive, or both. It is essential that organizations define and focus on inclusion as much as diversity to advance business performance by increasing the retention of talented employees (Bourke & Dillion, 2013). Organizations have focused heavily on diversity, but by refocusing attention on both diversity and inclusion, employers can provide their workforces with confidence that will enable increased innovation and more effective work teams, resulting in higher customer satisfaction and improved organizational performance (Bourke & Dillion, 2013).

Bourke and Dillion (2013) collected data from 1,557 study participants to evaluate how diversity and inclusion were implemented across three organizations. The data suggested that organizations with a better balance of diversity and inclusion had happier employees who thought more highly of their organizations and had higher levels of perceived inclusion. The study also assessed senior-level leadership’s ability to foster an inclusive environment in their organization as well as front-line managers’ abilities to enable such inclusive policies at the operational level. Bourke and Dillion’s study provided insights into some potential solutions for organizations seeking to build and maintain diversity. The identified solutions for supporting diversity rested on three basic concepts: consistency, transparency, and accountability.

**Synthesis of the Research Findings**

The review of the literature demonstrated that the cybersecurity profession has a significant shortage of qualified candidates for critical positions for both private and public-sector organizations (Vogel, 2016). This shortage is a challenge that is projected to continue
unless circumstances change (Vogel, 2016; van Zadelhoff, 2017). Some scholars believe that the gap can be closed by developing and implementing robust programs and initiatives to encourage the interest, recruitment, advancement, and retention of millennials and females (Raytheon, 2015). Cummings (2015) offered the following recommendation for closing the gender gap in cybersecurity.

Commitment to promote organizational change has been identified worldwide as a key element in bridging the gender gap. Institutions, i.e., government, academia and private sector, need to take full responsibility for developing strategies to attract, hire, promote and advance women to leadership. (p. 22)

The scholarly literature on the shortage of cybersecurity professionals and particularly female cybersecurity professionals exhibits a high degree of consensus on the causes of the issue. The extant literature also acknowledges that the problem is not new and is expected to continue for years. Issues identified in the extant literature include the leaky cybersecurity pipeline delivering female professionals to the cybersecurity profession, cybersecurity skill sets, lack of diversity, lack of inclusion, and gender-based stereotypes. These issues are factors in organizations’ abilities to attract, develop, and retain female cybersecurity professionals. The significant gender gap identified by the previous literature has provided evidence of an untapped pool of potential cybersecurity professionals. The following themes related to the underrepresentation of females in the cybersecurity profession were present in the review of the literature.

**Same-gender role models.** Lack of same-gender role models working in the cybersecurity industry at all levels and particularly at executive levels was apparent in the literature. The lack of female role models tended to preclude young females from envisioning themselves in cybersecurity-related work roles. The lack of such role models also increased the
difficulty for new female cybersecurity professionals to envision themselves with long term career progression to future leadership roles in cybersecurity.

**Gender-neutral terminology and marketing.** The images, descriptions, and terminology used to conduct marketing for cybersecurity-related classes, degrees, and events were not gender-neutral and did not appeal to females of any age (Dallaway, 2016).

**Early introduction and encouragement.** Females should be introduced and encouraged to pursue STEM and cybersecurity-related activities as early as grade school (Perez et al., 2015). Additionally, young females should be encouraged to be confident and competitive early. These characteristics are normally inculcated in young males, but the encouragement of such characteristics in young females would benefit females by enabling balance throughout their lives (Kaspersky, 2017).

**Inclusive work environment.** Organizations must create an inclusive work environment (Peacock & Irons, 2017). An inclusive work environment will minimize discrimination regarding ideas, hold all personnel to the same standards, ensure that personal desires to have a family will not limit career potential, and guarantee that everyone will be granted equal opportunities to develop and advance (Barker et al., 2014; Bourke & Dillion, 2013; Krivkovich et al., 2017).

**Gender-diverse workforce.** Organizations that have gender-diverse teams tend to perform better and produce more innovative ideas (Hunt et al., 2015). Cybersecurity is continuously changing and presents some of the most challenging problems the United States faces (Vogel, 2016). Having the best and brightest talent will allow organizations to better and more proactively prepare for cyber threats (Vogel, 2016).

**Training.** Members of academia and professional organizations (e.g., teachers, employers, students, hiring managers, recruiters, executives, professors, and academic advisors)
should mandate training and workshops on conscious and unconscious gender bias and inclusion (McCormick, 2015; Peacock & Irons, 2017). Females are discouraged early in life from pursuing traditionally male careers such as cybersecurity by being taught specific behaviors driven by outdated societal expectations of gendered behavior (Williamson & Tranter, 2017). This theme is supported by past studies that confirm the lack of encouragement and support from peers, teachers, and professors for females pursuing cybersecurity as a career (Williamson & Tranter, 2017).

**Awareness.** The majority of male cybersecurity professionals are unaware of the systemic issues that their female counterparts must cope with Krivkovich et al. (2017).

The extant literature supports the application of social identity theory to developing the conceptual framework that underpins the foundation of the present study and its research design (Hogg, 2016; Rubington & Weinberg, 2015). Social identity theory provides an introductory understanding of how different groups interact internally and externally (Hogg, 2016). Social identity theory also offers theoretical explanations of how external interactions and behaviors can impact a group’s development or lack thereof (Hogg, 2016). In the case of the present study, the two groups are males and females.

The present study’s multiple-case study format allowed the exploration of issues raised in scholarly literature individually before the performance of a cross-case analysis to determine whether further insight could be gained to create a more holistic interpretation of the problem. It must be noted that barriers to career advancement for females who study in STEM fields or work in the cybersecurity profession begin during childhood and persist throughout their careers (Williamson & Tranter, 2017). Exploration of the individual, systemic, and organizational barriers that have suffused STEM and IT fields is necessary to identify solutions specific to the
cybersecurity industry (Williamson & Tranter, 2017). “Research is now needed to determine whether these strategies would apply to the cyber industry, within a framework of examining individual-level barriers, as well as systemic barriers existing in the structure, processes, and cultures of organizations” (Williamson & Tranter, 2017, p. 21).

While cybersecurity is a subfield within IT, it is becoming increasingly specialized in terms of both the subject matter and skill sets required. Williamson and Tranter (2017) conducted a literature review concerning females in cybersecurity and the domains of STEM-based courses and accreditations as well as information technology because of the relationships between these domains and cybersecurity. The findings concluded that barriers for females in STEM and IT begin as early as primary school and persist throughout their academic and professional careers. Williamson and Tranter (2017) also highlighted the ongoing barriers to females in the employment cycle, which affect recruitment and attrition.

The present study attempted to fill the gaps in current knowledge identified in the literature review while contributing to advancing the current state of knowledge related to the causes of female underrepresentation in the cybersecurity profession. The participants’ accounts of their personal experiences assisted in addressing these gaps in existing scholarly knowledge. The findings of the present study may facilitate a better understanding of how to attract, hire, develop, advance, and sustain the female population in the cybersecurity profession in U.S. private and public organizations.

**Critique of Previous Research Methods**

Numerous scholarly and practitioner resources have been examined for the present study’s review of the literature. The present study provided a thorough analysis of the data and findings embodied in each scholarly study as well as the validity of the methods applied to
collect and assess the data supporting each study’s conclusions. Data reviewed from practitioner sources allowed examination of the most current and accurate statistical information concerning the cybersecurity workforce in the United States at the time of the study.

Cybersecurity is a component of IT, but it does not reflect the entire IT discipline. Additionally, distinct literature addresses both cybersecurity and information security, but these terms are not interchangeable (Syed, Padia, Finin, Mathews, & Joshi, 2016). The term cybersecurity has been defined in recent years, but researchers sometimes conflate cybersecurity with previous technical terms. Confusion of terminology can potentially affect data gathering. Despite the use of key terms and an in-depth review of the documents, the possibility existed that pertinent literature was missed due to the use of unique or nonstandard terminology on the part of other researchers.

Another limitation was the lack of statistics available concerning cybersecurity degree-holders. To assess the cybersecurity pipeline or cybersecurity qualifications, investigators across various studies utilized statistical data concerning STEM degrees. While STEM degrees serve as the primary educational foundation for cybersecurity professionals, cybersecurity degrees are now offered at both undergraduate and graduate levels. Future studies should account for statistical data concerning cybersecurity degrees and compare this with the retention rate of female cybersecurity professionals.

Kaspersky (2017) did not agree with the proposition that the gender gap is causing the cybersecurity workforce deficit and skills gap. Kaspersky attributed the deficit to the lack of female role models who work in the cybersecurity profession and to lack of adequate educational guidance. While Kaspersky (2017) is correct in noting that the cybersecurity profession lacks
female professionals, Kaspersky did not address the question of who could act as role models for females who might be interested or qualified to enter the profession.

Past literature has examined the underrepresentation of females in the cybersecurity profession and its significant impact on the nation’s urgency to fill the vacancies in this field. Despite the results of such studies, the number of females in the field of cybersecurity has remained stagnant. Most extant studies have conducted in-depth interviews with females who had been in the cybersecurity field for a significant amount of time and excluded those seeking to enter the profession or who had recently entered the profession. The present study’s multiple-case study approach provided an in-depth understanding of the phenomenon from multiple perspectives and addressed important knowledge gaps.

Summary

Chapter 2 presented a review of the scholarly literature related to the underrepresentation of females in the cybersecurity profession. All literature reviewed was selected based upon its association with the gender gap in the cybersecurity profession. This literature review defined cybersecurity and described the skills required for cybersecurity professionals. The findings reported in the literature justify the necessity of this qualitative multiple-case study.

The next chapter describes the methodology and research design selected for this study and details the execution of the methodology. Selecting the appropriate method is crucial to ensure that scientific research is performed appropriately. Chapter 3 encompasses the following key areas: (a) purpose of the study, (b) research question, (c) research design, (d) target population and participant selection, (e) study procedure, (f) data collection instruments, (g) ethical considerations, and (h) summary.
CHAPTER 3. METHODOLOGY

Chapter 3 details the present study’s methodology. The following step-by-step description enables the replication of this study in future research related to this topic. This chapter encompasses the following sections: (a) purpose of the study, (b) research question, (c) research design, (d) target population and sample, (e) procedures, (f) instruments, (g) ethical considerations, and (h) summary.

Purpose of the Study

The purpose of this qualitative study was to explore the underrepresentation of females in the U.S. cybersecurity profession and answer the research questions. Cybersecurity is a national security concern, and females are significantly underrepresented in the profession, holding less than 15% of cybersecurity-related jobs in the United States (Rowland et al., 2018). Setalvad (2015) estimated that the cybersecurity industry will face a shortage of 1.5 million professionals by the year 2020 if the gender gap in the cybersecurity profession is not addressed. This shortage poses serious challenges to the security of private and public data, systems, and infrastructure (Rowland et al., 2018; Stytz & Banks, 2014). To date, the researcher has identified few empirical studies that address the underrepresentation of females in the specific context of cybersecurity, even though gender diversity has been proven beneficial to organizations (Hunt et al., 2015).

It is critical to understand factors that contribute to the interest, hiring, development, advancement, and sustainability of females in this profession within the United States by exploring the perceptions and experiences of females currently occupying these positions (Setalvad, 2015). The inability to fill cybersecurity vacancies has become an economic and national security concern, and the exploration of why females are underrepresented in the cybersecurity profession not only addresses a gap in the literature but also assists in explaining
why so few females enter the profession (Burrell & Nobles, 2018). The purpose of this study was not to directly resolve the gender imbalance within the cybersecurity profession but to develop a scholarly understanding of the issue and identify factors that might contribute to a solution.

**Research Question**

The central research question guiding this multiple-case study asked, “why is there a disproportionately low representation of female workers in the U.S. cybersecurity industry?” Three subquestions were developed to answer the central question.

**Subquestion 1.** What factors contribute to the interest, development, and sustainability of female employees in the U.S. cybersecurity profession?

**Subquestion 2.** What criteria are currently applied by hiring managers for recruiting, hiring, and retaining female cybersecurity professionals in the United States?

**Subquestion 3.** How might the increased representation of female cybersecurity professionals contribute to an organization?

**Research Design**

The research problem and question determined the selection of the research design (Stake, 2013). A multiple-case study was most appropriate for exploring the specific research questions as it allows researchers to explore multiple bounded systems (Harrison, Birks, Franklin, & Mills, 2017). The case study adopts an investigative approach to examine specific variables in their natural context, and a multiple-case study research design was best suited for the present study based on the nature of the research problem (Creswell & Creswell, 2017). The collection of qualitative data documenting the experiences of the participants facilitated the exploration of why so few females pursue careers in the U.S. cybersecurity profession. The study’s research questions explored the experiences of female cybersecurity professionals and
prospective female cybersecurity professionals to identify factors that contribute to the underrepresentation of females in the cybersecurity profession.

A multiple-case study explores independent cases that are representative of a singular phenomenon (Stake, 2013). The strategy for a multiple-case study investigation aims to focus on a single case at a time and then explore commonalities and variations among the cases (Baxter & Jack, 2008). Identifying duplicated findings across cases strengthens the validity of the data (Scott et al., 2015). “The qualitative case study was developed to study the experience of real cases operating in real situations” (Stake, 2013, p. 7). Investigating a phenomenon across multiple cases strengthens the findings, and multiple-case studies are more valid and reliable than single-case studies (Chmiliar, 2010).

There are several approaches to conducting qualitative research (Ritchie, Lewis, Nicholls, & Ormston, 2013). The cases studied in this multiple-case study were performed in sequential order over a period of one year (Chmiliar, 2010). Data were not collected or analyzed in a specific order within each case, as this is not required in qualitative approaches (Ehrich, 2005). When conducting a case study, the researcher ensures that data collection is focused and provides rich and detailed information on a phenomenon. “Phenomena include anything that appears or presents itself such as feelings, thoughts, and objects” (Ehrich, 2005, p. 2).

The minimal amount of qualitative data available concerning the underrepresentation of females in the cybersecurity profession provided additional rationale for selecting a multiple-case study design (Kruth, 2015). The underrepresentation of females in cybersecurity has persisted for some time, but the demand for cybersecurity professionals is at an all-time high (Glass, 2014). One of the first qualitative studies on females in the cybersecurity profession was executed in 2009 (Bagchi-Sen et al., 2010). Despite growing interest, research on females in the
cybersecurity profession remain limited (Reed et al., 2017). The need to explore why so few females pursue the cybersecurity profession has intensified. The personal experiences of individuals who are part of the cybersecurity pipeline, work in the cybersecurity profession, and hire cybersecurity professionals may enable scholars and practitioners to understand the problem better. Further exploration of this topic also increases awareness of female underrepresentation in the cybersecurity profession and helps to identify common gaps in previous research on the gender disparity in the field of cybersecurity.

Data were collected from participants who share personal experiences of the phenomenon. Semistructured, research-authored, open-ended interview questions served as the means of data collection. Interviews are the most common instrument used to collect data in qualitative studies (Gill, Stewart, Treasure, & Chadwick, 2008; Peters & Halcomb, 2015). “Open-ended questions can evoke responses that are: meaningful; unanticipated by the researcher; and explanatory in nature” (Mack, Woodsong, MacQueen, Guest, & Namey, 2005, p. 4). Interviews for this study provided a unique perspective of the phenomenon from those with personal experience of the research problem.

The interviews were administered through the Internet in real-time using the Web-based computer application Skype. Skype is a free downloadable Web-based application that is accessible on any Internet-capable device for the convenience of the user (Skype, 2016). Use of computer-based applications such as Skype enables the participation of individuals regardless of whether they are in the United States (Symonds, Symonds, & Brown, 2016). In the modern technological era, it is common for researchers to utilize the Internet to gather data for scholarly research (Denissen, Neumann, & van Zalk, 2010).
Exploring the central phenomenon from the perspectives of female participants who (a) currently work in the cybersecurity profession, (b) are currently pursuing entry into the cybersecurity profession, and (c) hiring managers for the cybersecurity profession ensured that the research aligned with the scientific perspectives of Yin (2014), Merriam (1998), and Stake (2013). While each perspective has unique advantages, the overall benefits of qualitative case-study research were well suited to use in the present study based on the study’s focus (Yazan, 2015). The following section explains how the target population and sample were identified for each case in this multiple-case study.

**Target Population and Sample**

This section identifies the population and sample for the present study. The first subsection identifies the population and its characteristics, and the second section provides information on the sample. When addressing the specifics of the population and sample, the subsections provide information on the identities and characteristics of the population and sample for each case.

**Population**

A population denotes a larger, all-inclusive collection of units bounded by mutual characteristics, and in the present study, three distinct populations of interest were identified (Surbhi, 2016). The population of interest for Case 1 consisted of females currently working in the cybersecurity profession. The population of interest for Case 2 consisted of females seeking to enter the cybersecurity profession. The population of interest for Case 3 consisted of hiring managers responsible for filling cybersecurity positions in U.S. organizations. The researcher uses cybersecurity as the bounded characteristic for each population.
As previously noted, Case 1 focused on a general population of females working in the U.S. as cybersecurity professionals. Cybersecurity professionals are in high demand within the U.S. job market (Bureau of Labor Statistics, 2018a; Bureau of Labor Statistics, 2018b). Females constitute only a small minority (15%) of cybersecurity professionals (Rowland et al., 2018). Little research has been conducted on female cybersecurity professionals, but research indicates that females working in cybersecurity roles face discrimination, sexism, and tokenism, and an unfriendly work environment may be the case of the low numbers of females pursuing cybersecurity as a career (Reed et al., 2017). The specific criteria used to draw the sample from the population for Case 1 is described in the sample subsection.

Case 2 included females in the United States currently pursuing entry into the cybersecurity profession. This population was very similar to the population for Case 1, with the exception that most these individuals are either in university completing undergraduate and graduate degrees in cybersecurity or currently seeking a position after having recently graduated. This population did not include individuals that had worked previously as cybersecurity professionals but were temporarily out of the workforce. The purpose of choosing a population with no substantive work experience as a cybersecurity professional was to determine what factors support an interest in the career track before the prospective cybersecurity professionals’ perspectives are altered by actual work experience.

The population of interest for Case 3 included hiring managers responsible for filling cybersecurity positions in U.S. organizations. Unlike the target populations for Case 1 and Case 2, the population for Case 3 was not gender-exclusive, and males were also included. The purpose of utilizing a gender-inclusive target population in Case 3 was to examine the
perspectives of both male and female hiring managers to obtain a more comprehensive perspective on what organizations seek when hiring female cybersecurity professionals.

**Sample**

Inclusion and exclusion criteria defined each of the cases in the present study. The population for Case 1 consisted of females currently working in the cybersecurity profession, and the inclusion criteria required participants to be employed full time in a cybersecurity-related job. A participant was required to be female and between the ages of 21 and 40 to be included in Case 1. Additionally, participants in this group had to have a minimum of three years of work experience in a cybersecurity position. Exclusion criteria eliminated females under the age of 21 to ensure that participants met the requirement for work experience. Females over the age of 40 were also excluded from the study due to the recent development of the field of cybersecurity. By excluding females over the age of 40, there was less chance that a prior career specialty would strongly influence participants’ responses.

In Case 2, the inclusion and exclusion criteria differed slightly from the criteria in Case 1. The Case 2 inclusion criteria still required participants to be female, but the age and experience requirements differed. The inclusion criteria for Case 2 required participants to be between the ages of 18 and 30. The minimum age was selected to ensure the participants were all above the age of majority. The maximum age prevented the sample from being skewed by individuals pursuing a second career. The inclusion requirement related to experience mandated that participants in Case 2 be currently enrolled in a STEM degree program. Participants were also required to have the intention of seeking employment in the cybersecurity profession following graduation. As with Case 1, individuals that did not meet the inclusion criteria were purposely excluded from the sample.
In Case 3, the goal was to sample individuals responsible for hiring cybersecurity professionals. An eligible participant for Case 3 was required to be a hiring manager for cybersecurity professionals in the United States or to have held such a position within the past 10 years. Participants in Case 3 were required to have a minimum of two years of experience as a hiring manager. No age or gender requirements were placed on the participants in Case 3.

The sampling method used in this study was purposeful, not random. Purposeful sampling is common in qualitative studies as it allows researchers to group participants based on predefined criteria (Mack et al., 2005). The present study required the selection of participants with specific experiences directly related to the phenomenon of interest (Englander, 2012). Gathering data from three unique sources strengthened the validity of the study’s findings. The use of three cases supported data triangulation during the data analysis phase by collecting data from three independent sources (Groenewald, 2004). “Triangulation is typically a strategy (test) for improving the validity and reliability of research” (Golafshani, 2003, p. 603). Triangulation is achieved as each group provides a distinct perspective concerning the explored phenomenon.

Creswell and Creswell (2017) suggested that an appropriate sample for a multiple-case study should consist of five to 25 participants. The sample size for this study consisted of 31 participants. This number included 11 females in the working in the United States as cybersecurity professionals, 10 females in the United States currently pursuing entry into the cybersecurity profession, and 10 hiring managers responsible for filling cybersecurity positions in U.S. organizations. The intended sample size in qualitative research is recommended to be an estimate based on various factors, including the ability to conclude valid outcomes, data saturation, and the lack of value in studying larger sample sizes (Marshall, 1996). “Some issues
can affect sample size in qualitative research, but, the guiding principle should be the concept of saturation” (Mason, 2010, p. 1).

**Procedures**

This section of Chapter 3 describes the different procedures used to conduct the present study. The section contains five subsections. The first subsection outlines the procedures used to select participants. The second subsection identifies the procedures used to protect participants. The third subsection describes the expert review process used to pilot test the interview guide. The fourth and fifth subsections provide information on the procedures used to collect and analyze the data.

**Participant Selection**

Initial recruitment of participants was performed through Facebook, LinkedIn, and email, methods that are in alignment with similar research (see McRobert, Hill, Smale, Hay, & van der Windt, 2018). Institutional Review Board (IRB) standards were followed, and public social media pages were used to recruit participants. The use of social media websites did not require administrator permission to post recruitment calls. A data call was created to contact interested participants by posting the link on social media web pages. The data collection calls were posted on social media and professional pages frequented by aspiring and current cybersecurity professionals. All data calls seeking participants included a brief description of the participant sample criteria and a study overview. After participants clicked on the link, participants were redirected to the data collection survey tool, SurveyMonkey.

On the SurveyMonkey site, participants completed a consent form before proceeding to the demographic closed-ended questionnaire. After acknowledging the consent form, the participant proceeded to the demographic questionnaire. The researcher reviewed all submissions
and responded to selected participants using the contact information they provided in the questionnaire. Emails were sent to participants who were not selected to notify them of their status and thank them for their interest. Only participants who did not satisfy the criteria of the study were de-selected. Each participant was contacted via email and asked to indicate a minimum of two potential interview dates and times. The copy of the demographic questionnaire is presented in Appendix A. Once the participants had provided their availability, a follow-up confirmation email was sent to confirm the date and time of the interview.

**Protection of Participants**

In every study, it is important to protect participants (U.S. Department of Health & Human Services, 1979). The protection of participants entails protecting their identity, affiliations, associated risk, and digital information (i.e., IP address, emails, phone numbers). The SurveyMonkey data collection tool was the initial instrument used to receive consent and demographic data directly from potential participants. All questions in the SurveyMonkey data collection tool were multiple choice as opposed to open-ended. At the end of the survey, potential participants could enter their contact information. SurveyMonkey was used to collect data before conducting one-on-one Skype-based interviews. The SurveyMonkey platform provided an automated and controlled environment to distribute and record consent forms, collect demographic data, and gather contact information. Collection of the demographic data allowed the researcher to identify participants who satisfied the sample criteria before beginning the Skype interviews.

On the SurveyMonkey site, participants received additional information about the study and were required to provide consent before proceeding. The consent form applied built-in decision logic. If a participant agreed to the terms, they could proceed, and if they disagreed, the
process was terminated. The consent form included the acknowledgment that the participant was sufficiently comfortable with the terms and conditions of the study to indicate their willingness to participate in an interview via Skype. All participants were permitted to terminate participation in the study during any phase of the study, including both before or during the data collection phase.

Participants were not required to provide personal information to participate with the exception of contact information to schedule one-on-one interviews. The contact information consisted of a name, email address, and phone number. Participants were informed that their contact information would only be used to conduct interviews and would not be shared with anyone. Using SurveyMonkey entailed minimal risk. To certify that IRB standards were fulfilled, the researcher obtained written permission to conduct research using the demographic instrument. A consent form was included on the first page of the survey, and all participants were required to complete an informed consent form before completing the closed-ended demographic survey questions. To ensure the participants’ rights were not violated, a “prefer not to respond” or “no response” option was included for each question.

IP address-tracking was disabled to ensure participants’ anonymity, and no data gathered from the participants was attributed to the participants or any institution or agency they were connected to (Ritchie et al., 2013). Secure Socket Layer (SSL) encryption was enabled to protect sensitive data as it was transmitted over the network. Additionally, as Skype was used to conduct one-on-one interviews, additional Internet security was considered when selecting a tool to administer interviews to support the protection of the participants’ data. Minimal risk was associated with the use of Skype. All Skype voice, video, file transfers, and instant messages are encrypted using the advanced encryption standard algorithm. Encrypted communications protect
Skype users from potential eavesdropping by malicious users (Skype, 2016). Skype has been used as a data collection instrument to conduct interviews using video calls and instant messenger for research in the past (Symonds et al., 2016).

**Expert Review**

An expert review is a process that researchers use to assess the usability and feasibility of an instrument or other processes associated with executing a research study (Given, 2008). Expert review is sometimes used to improve the study’s validity (Given, 2008). The interview questions and procedures used in this study were reviewed and approved by the dissertation mentor, Capella University’s scientific merit review board, and members of the dissertation committee. Capella University did not require an additional expert review as part of the IRB approval process. As a result, no additional expert review was conducted independently of the dissertation approval process.

**Data Collection**

The data collection process followed Stake’s (2013) guidance concerning how to conduct a multiple-case study. Before collecting the data, all participants received consent forms and demonstrated that they understood the entire scope of the study. As previously noted, an initial demographic survey was used to collect information on the participants’ age, gender, educational background, and work experience.

Following the completion of the demographic survey, semistructured one-on-one interviews were used to collect data from the participants concerning their experiences working in the cybersecurity profession, pursuing a career in cybersecurity, or hiring cybersecurity professionals for U.S. organizations. Interviews enabled the researcher to gain an in-depth understanding of the situation (Blumberg, Cooper, & Schindler, 2014). Englander (2012) stated
that “collecting descriptions from others is also an attempt at discovery of the human scientific meaning of a particular phenomenon” (p. 15).

The following steps were executed to collect data through the use of semistructured interviews.

1. An email reminder was sent to participants 48 hours before the agreed interview date and time.

2. Participants were afforded the option to either perform the interview via Skype video call or Skype instant messenger.

3. On the date of the interview, the researcher initiated the Skype call or instant messenger chat two minutes before the scheduled start time.

4. The researcher initiated each conversation with an icebreaker to establish a sense of warmth and rapport with the participants.

5. Predefined, open-ended questions were used to guide the interview. The researcher asked follow-up questions or probing questions to redirect the interview when participants did not clearly answer a question (Turner, 2010).

6. During the interviews, the researcher transcribed notes to describe significant observations, such as the atmosphere or dynamic of the interview setting.

7. If a participant selected a video call, the call was recorded via Skype and transcribed within 48 to 72 hours of the interview. Only one participant selected a video call which later led to instant messenger due to technical difficulties. This information was disclosed to participants in the consent forms. If the participant selected instant messenger, the chat conversation was recorded and was not required to be
transcribed. All transcribed data was saved on the researcher’s computer with a password to protect the file.

8. All participants were provided with a label to connect responses to the participant without revealing the identity of the participant.

By gathering data through general conversation (through the open-ended questions), the researcher created a comfortable environment for the interviewee (England, 2012). Additionally, the researcher recorded additional notes immediately following every interview to ensure the accuracy of data collected, recorded, and observed. Following the completion of the interviews, the data analysis process began.

Data Analysis

Data analysis is one of the most critical steps when conducting qualitative research (Leech & Onwuegbuzie, 2007). Data was analyzed as it was collected and until the researcher had reached a data saturation point. By conducting an ongoing analysis of the data collected, the researcher reduced the likelihood of redundancy (Nowell, Norris, White, & Moules, 2017). This also allowed the researcher to accurately identify a data saturation point earlier in the research process. The researcher transcribed notes to record data and thereby captured data when it was fresh. Miles and Huberman (1994) recommend simultaneously analyzing and collecting data throughout the entire process.

All realms of data were compared to identify relevant themes. After conducting all interviews, the data for each case was analyzed for commonalities using a within-case analysis to identify new results. Data from the individual cases were categorized based on common themes to prepare for the cross-case analysis (Stake, 2013). After conducting all interviews and separate
analysis of each case, additional cross-case analysis was performed to identify themes across cases (Nowell et al., 2017).

In both the within-case analysis and the cross-case analysis, all data collected were categorized, linked to relevant concepts, and synthesized (Miles & Huberman, 1994). Data were summarized rather than redacted, thereby reducing the risk of compromising the integrity of the data initially provided by the participant. Data analysis ceased once a saturation point was reached. In qualitative research, the saturation point is when additional value no longer emerges from the data (Ritchie et al., 2013). Once all the data was collected and transcribed, it was sent to participants to ensure its accuracy. Creswell (2007) emphasized the need to verify the accuracy of data to strengthen validity.

Stake (1995) recommended the following process to conceptualize findings: “gather additional data, replicating or triangulating, to validate key observations” and “review data, gather new data, deliberately seek disconfirmation of findings” (p. 53). Data triangulation was implemented during the data analysis phase to “strengthen the rigor and trustworthiness of the findings” (Leech & Onwuegbuzie, 2007, p. 575). Data triangulation was used “to contrast the data and validate the data if it yields similar findings” (Groenewald, 2004, p. 46). Triangulation applies various methods and sources to deepen the understanding of the study while fortifying integrity (Ritchie et al., 2013). Overall, the information collected and analyzed was intended to add to the larger body of knowledge on the underrepresentation of females in the U.S. cybersecurity profession.

**Instruments**

The instruments used for this qualitative, multiple-case study included Skype, social media applications and platforms, SurveyMonkey, a closed-ended demographic questionnaire
survey, open-ended interview guides, secondary data, and the researcher. The analysis of secondary data, in the form of the literature review, provided additional support for the methodology selection, research design, data collection methods, and the results. Skype was used to conduct the one-on-one semistructured interviews, and interview guides were used to ensure the interviews were consistent for each participant within a case. Using open-ended questions, it was possible to gather data reflective of the participants’ personal experiences (Wiggs, 2011). Open-ended questions provide context and allow reflection on the experiences of the sample. The open-ended questions are among the most common types of interview questions as they encourage interviewees to provide substantial amounts of information (Turner, 2010).

The Role of the Researcher

The researcher’s role involved thematizing, designing, interviewing, transcribing, analyzing, and reporting (Fink, 2000). The researcher was the primary collector and analyzer of the data (Hoflund, 2013). Data collection occurred in an ethical manner and adhered to the approved research plan. Use of data collected for any negative intent was not permitted. The researcher’s analysis of the data was objective because it adhered to approved methods and precluded bias or unfounded assumptions (Creswell & Creswell, 2017).

The researcher fully adopted all responsibilities associated with collecting, analyzing, and utilizing the data. These responsibilities included, but were not limited to, maintaining rapport; listening; and fostering a conversational flow while collecting, transcribing, and analyzing the data. The researcher was also responsible for ensuring no harm came to participants and guaranteeing that the research was conducted in an ethical manner (Mack et al., 2005).

Using a process called bracketing, the researcher disregarded preconceptions and knowledge concerning the phenomenon to limit potential bias (LeVasseur, 2003). The researcher
has served as a female cybersecurity professional for nine years. As a result, it was necessary as part of ethical research, to be proactive when implementing steps to eliminate potential bias. Following advice from Creswell (2007), the researcher described her academic and professional background to participants before receiving consent for their participation. The connections between the researcher and the phenomenon were also stated clearly and concisely to minimize bias (Flick, 2009).

**Guiding Interview Questions**

Interviews for qualitative research focus on exploring participants’ attitudes, beliefs, and experiences (Valenzuela & Shrivastava, 2002). The interview questions were designed by the researcher. Unlike surveys, interviews enable the interviewer to ask follow-up questions based on the interviewee’s responses. Using surveys to collect qualitative data presents disadvantages (Mack et al., 2005). A demographic questionnaire was used to gather demographic and background information about the interviewees, but the remainder of the data were collected during semistructured interviews.

The scope of the questions encompassed the experiences of three groups of individuals: (a) female cybersecurity professionals, (b) females who are pursuing the profession, and (c) male and female hiring managers responsible for hiring cybersecurity professionals. The researcher applied a process of bracketing during the interviews to manage the flow of information while investigating the nature of the participants’ experiences (Rolls & Relf, 2006). A three-stage interview process was implemented to decrease the probability of contaminated data. This three-stage process involved the contextualization of the participants’ life experiences during the interview, the reconstruction of the details of the experience through the recorded data that was
provided to the participants after interviews were completed, and reflection on the meaning of the experience through analysis (Seidman, 2006).

To ensure all items used during the interview were appropriate, the researcher tested all equipment prior to the interview. The researcher also followed the steps for each interview; these steps are listed in Appendix C. These interview methods were adopted to enable consistency across the interviews and to allow for replication. Semistructured interview questions were used to guide the interview and to foster an environment that encouraged a brief conversation (Yin, 2014). The semistructured interview questions for each case are listed below.

**Case 1: Current female cybersecurity profession.** The following questions were asked of all participants in the Case 1 sample.

1. How did you end up in the cybersecurity profession?
2. What are your goals in your current profession?
3. Have you faced any obstacles in your career? If so, what were they?
4. Can you describe your recruitment and hiring experience into the cybersecurity profession?
5. What is the work environment and morale like in your office?
6. What types of opportunities are available for advancement in your company within your profession?
7. What does diversity mean to you?

**Case 2: Females currently pursuing a cybersecurity profession.** The following questions were asked of all participants in the Case 2 sample.

1. Why does the cybersecurity profession interest you?
2. What preparation have you done to gain employment in the cybersecurity profession?
3. Have you faced any obstacles in completing your education or professional certifications required to enter into this profession?

4. What is your current view on cybersecurity professionals?

5. What do you expect in the work environment and morale in your future office?

6. Have you experienced any hiring or recruitment process yet?

7. What does diversity mean to you?

**Case 3: Hiring managers for the cybersecurity profession.** The following questions were asked of all the participants in the Case 3 sample.

1. What is your current recruitment and hiring process for the cybersecurity profession?

2. What skills are you seeking to fulfill vacant cybersecurity professional jobs?

3. What is the current number of cybersecurity professionals that your company employs? How many of them are females?

4. Describe challenges you as a hiring manager have experienced trying to recruit talent.

5. What does diversity mean to you?

**Ethical Considerations**

The proposed population and research topic imposed minimal risk on participants. The researcher adhered to the ethical principles and guidelines outlined in *The Belmont Report* (U.S. Department of Health and Human Services, 1979). *The Belmont Report* provides a framework for researchers who conduct studies that impact human participants based on fundamental principles that ensure respect for human participants, including justice and beneficence (Beauchamp, 2008). The morals delineated in *The Belmont Report* align with the detailed requirements enforced by Capella University’s IRB. Capella University’s IRB approves all
research plans prior to data collection. Universities provide IRB reviews to ensure that research plans contain necessary measures to ensure research is conducted ethically (Yin, 2015).

Informed consent was obtained from each participant before beginning the interview process. Obtaining informed consent confirms respect for the human participant (Yin, 2015). The participants’ rights were safeguarded during all phases of the study. All participants received foundational knowledge about the purpose of the study, details about the researcher, funding, anonymity concerns, participant requirements, and step-by-step guidance regarding how the data would be collected and utilized (Ritchie et al., 2013). Only essential data were collected from the participants to ensure the integrity of the study and decrease the chance of discouraging participation.

Historically, qualitative research has been interpreted as biased because it is subjective (Cope, 2014). This study focuses on the lived experiences of the participants by analyzing the data to discuss findings and develop theories. All procedures involved in this study were clearly outlined to ensure that the study can be replicated. A robust list of scholarly research associated with the phenomenon was also documented to establish the validity of this multiple-case study so that it can be used by other researchers (Yin, 2014). Finally, transferability was fostered through the general selection of participants that were representative of the broader phenomenon. The sample was not limited to participants from one organization or one specific geographical location. Instead, the individual cases were designed to contribute to a broader body of knowledge about the phenomenon and to encourage future research and solutions by those impacted by the phenomenon. Applying the methods of this study to a narrower sample may yield more specific results relevant to a particular organization or geographical area.
Summary

The increasing demand for cybersecurity professionals necessitates a deeper understanding of the key factors that affect female interest, hiring, development, and retention to enable organizations to achieve a gender balance within the U.S. cybersecurity workforce. This chapter provided detailed information about the research method and design of this study as well as the procedures implemented when conducting the research. The research questions informed the selected research design and methods. Additionally, this chapter explained how the research process remained ethical by protecting the participants and respecting their human rights. The next chapter presents the actual data that was analyzed and detailed information concerning how the research method was applied during the data analysis phase. Additionally, Chapter 4 presents the results of the data analysis in the form of themes that answer the study’s research questions.
CHAPTER 4. PRESENTATION OF THE DATA

Introduction: The Study and the Researcher

The Study

The purpose of this qualitative study was to address and explore the problem of the underrepresentation of females in the U.S. cybersecurity profession. Females currently comprise less than 15% of the U.S. cybersecurity workforce and constitute a critically underused resource (Raytheon, 2015). Chapter 4 focuses explicitly on presenting the data, the application of the selected research method, and the results of the analysis. Data were gathered from participants who could provide insights based on their experiences to explore the phenomenon of interest.

A total of 31 semistructured interviews were conducted, 11 participant interviews in Case 1 and 10 participant interviews in both Case 2 and Case 3. The initial objective was to conduct 10 interviews per case, but Case 1 included 11 interviews as the interview had been scheduled and data saturation was not evident before that interview. The other two cases reached saturation by interview 10. Investigating three separate cases yielded insights into the research problem from multiple perspectives. The findings in Chapter 4 are the result of the methods outlined in Chapter 3. As previously noted, data collection and analysis methods described by Yin (2014) and Stake (2013) guided the study.

Chapter 4 presents the data logically. First, the sample is described in detail. Then, the chapter contains a description of how the research methodology was applied to the data analysis. The details of the interview data are presented next, along with the results of the analysis in the form of identified themes and summarized the findings.
The Researcher

In qualitative studies, the role of the researcher is critical to the validity and reliability of a study as well as the data collection and analysis phase. Yin (2014) asserted that reliability is crucial to prevent potential mistakes and prejudice in research. In qualitative research, the researcher performs data collection and analysis. For this reason, it was necessary to adhere to the data collection and analysis procedures approved by the IRB and dissertation committee (Creswell & Creswell, 2017). To ensure the completeness and accuracy of the data and field notes, all study participants received and reviewed transcripts to detect unconsciously inserted biases. The participants also had opportunities to correct any inaccuracies in the data (Stake, 2013; Yin, 2014).

The researcher is a female who currently works in the cybersecurity profession and has nine years of experience at a public-sector organization. After obtaining an undergraduate and graduate degree in computer science, the researcher began her professional career as a cybersecurity professional with the U.S. government. The researcher has held several technical work roles and accumulated experience as a cybersecurity practitioner, technical recruiter, and a manager of a highly technical cybersecurity workforce. Postgraduation, the researcher attended and completed 800+ hours of technical training through various private and public-sector vendors on a variety of cybersecurity topics.

For the past five years, the researcher has worked to encourage young females in grades K-12 to develop an interest in the skills relevant to the cybersecurity profession. The researcher visits local collegiate institutions to conduct resume reviews and offer advice concerning how to pursue a career in cybersecurity. The researcher also volunteers as a technical mentor for national cyber competitions and supports female-focused science, technology, engineering, and
mathematics (STEM) events to encourage young girls to pursue their interests in these study areas. These experiences provided the researcher with both a personal and external perspective of the current climate with the cybersecurity profession. The current environment, from the researcher’s perspective, is predominantly male, and the number of females in the cybersecurity pipeline is significantly lower than the number of males. Based on the researcher’s exposure to the topic and previously existing research, the researcher identified a need for scholarly research on this topic to explore why the phenomenon exists and to uncover any trends that may disprove the relevant theories.

The researcher also sought to contribute to the existing body of knowledge by providing future female cybersecurity professionals and organizations who are responsible for the recruitment and retention of cybersecurity professionals with in-depth insights into the experiences of women working in or seeking a career in the cybersecurity industry. The decision to use data from three different perspectives provided additional insights into the themes and causes of the low number of females in the U.S. cybersecurity profession. Due to the researcher’s direct relationship with the topic, the researcher meticulously adhered to data collection and analysis methods to reduce bias during the data collection and analysis phases.

In preparation for conducting this qualitative study, the researcher enrolled in university research methodology courses to learn how to correctly apply both qualitative and quantitative methods to a research problem. Additionally, the researcher conducted extensive research on general qualitative case studies and multiple-case studies previously conducted by scholars. By being exposed to literature written by academic experts, the researcher developed a better understanding of how to conduct this qualitative multiple-case study thoroughly.
Description of the Sample

The researcher spent approximately one year, May of 2017 to May of 2018, recruiting participants, conducting interviews, and analyzing the data collected. Participants ranged between the ages of 18 and 47, and a total of 42 submissions were received through the SurveyMonkey tool. Only 31 of the 42 submissions were used based on participant qualifications and data saturation. Initially, 10 participants were assigned to each case. However, the researcher had already accepted and scheduled the 11th interview for Case 1. Due to this, the researcher proceeded with the scheduled interview. As the data provided during that interview added value, the participant’s responses were included in the data analysis.

Participants represented a variety of job roles, geographic locations, and work experiences within the federal government, military, and private sector organizations. Each case focused on a different group of participants. Case 1 included females working in cybersecurity positions. Case 2 included females pursuing cybersecurity jobs. Case 3 included hiring managers responsible for recruitment and selection of cybersecurity professionals. The first case consisted of 11 participants, and the last two cases consisted of 10 participants each. In total, the thematic analysis included data from 31 interviews. Table 3 presents specific demographic descriptions of the participants in Case 1.

Case 1 contained a total of 11 participants. Case 1 included females currently working as cybersecurity professionals. These participants lived throughout the United States, predominantly in the Eastern and Western coastal regions of the country. Work experience in the field of IT ranged from six to 18 years, and the most common work role was that of a cyber analyst. Table 3 presents participant descriptions of the individuals included in Case 1.
Case 2 contained a total of 10 participants. Case 2 included females seeking entry into the U.S. cybersecurity workforce. These participants were located throughout the United States, predominantly in the Eastern and Western coastal regions of the country. Some of the participants were actively pursuing an undergraduate degree in a STEM-related field, while the remaining participants were pursuing a graduate degree in a STEM field. Table 4 presents participant descriptions of the individuals included in Case 2.

Table 3. Case 1: Females Currently Working in the U.S. Cybersecurity Workforce

<table>
<thead>
<tr>
<th>Participant Code</th>
<th>Gender</th>
<th>Work Role</th>
<th>Years of Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1P1</td>
<td>F</td>
<td>Organization Leader</td>
<td>11</td>
</tr>
<tr>
<td>C1P2</td>
<td>F</td>
<td>Cyber Threat Analyst</td>
<td>12</td>
</tr>
<tr>
<td>C1P3</td>
<td>F</td>
<td>Cyber Operations</td>
<td>17</td>
</tr>
<tr>
<td>C1P4</td>
<td>F</td>
<td>Cyber Intelligence Analyst</td>
<td>7</td>
</tr>
<tr>
<td>C1P5</td>
<td>F</td>
<td>Cybersecurity Engineer</td>
<td>6</td>
</tr>
<tr>
<td>C1P6</td>
<td>F</td>
<td>Senior Security Analyst</td>
<td>16</td>
</tr>
<tr>
<td>C1P7</td>
<td>F</td>
<td>Cybersecurity Analyst</td>
<td>12</td>
</tr>
<tr>
<td>C1P8</td>
<td>F</td>
<td>Cybersecurity Engineer</td>
<td>16</td>
</tr>
<tr>
<td>C1P9</td>
<td>F</td>
<td>Threat Intelligence Researcher</td>
<td>7</td>
</tr>
<tr>
<td>C1P10</td>
<td>F</td>
<td>Cyber Threat Analyst</td>
<td>8</td>
</tr>
<tr>
<td>C1P11</td>
<td>F</td>
<td>Cybersecurity Analyst</td>
<td>18</td>
</tr>
</tbody>
</table>

Table 4. Case 2: Females Seeking Entry Into the U.S. Cybersecurity Workforce

<table>
<thead>
<tr>
<th>Participant Code</th>
<th>Gender</th>
<th>Degree Earned/Pursuing</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2P1</td>
<td>F</td>
<td>MS Information Technology</td>
</tr>
<tr>
<td>C2P2</td>
<td>F</td>
<td>BS Information and Computer Science</td>
</tr>
<tr>
<td>C2P3</td>
<td>F</td>
<td>MS Information Technology</td>
</tr>
<tr>
<td>C2P4</td>
<td>F</td>
<td>MS Computer Engineering</td>
</tr>
<tr>
<td>C2P5</td>
<td>F</td>
<td>BS Technology Management</td>
</tr>
<tr>
<td>C2P6</td>
<td>F</td>
<td>BS Information Technology</td>
</tr>
<tr>
<td>C2P7</td>
<td>F</td>
<td>BS Computer Science</td>
</tr>
<tr>
<td>C2P8</td>
<td>F</td>
<td>BS Computer Science</td>
</tr>
<tr>
<td>C2P9</td>
<td>F</td>
<td>MS Information Assurance</td>
</tr>
<tr>
<td>C2P10</td>
<td>F</td>
<td>BA Cybersecurity</td>
</tr>
</tbody>
</table>
Case 3 contained a total of 10 participants. Case 3 included males and females that have been a hiring manager in the U.S cybersecurity profession. Each participant was required to have at least two years of experience. Collectively the participants had 106 years of experience in the hiring process, but the majority of the participants had 10 years or less experience. These participants were located throughout the United States, predominantly in the Eastern and Western coastal regions of the country. Table 5 presents participant descriptions of the individuals included in Case 2.

Table 5. Case 3: Hiring Managers for the U.S. Cybersecurity Workforce

<table>
<thead>
<tr>
<th>Participant Code</th>
<th>Gender</th>
<th>Years of Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3P1</td>
<td>M</td>
<td>5</td>
</tr>
<tr>
<td>C3P2</td>
<td>M</td>
<td>8</td>
</tr>
<tr>
<td>C3P3</td>
<td>M</td>
<td>15</td>
</tr>
<tr>
<td>C3P4</td>
<td>F</td>
<td>2</td>
</tr>
<tr>
<td>C3P5</td>
<td>F</td>
<td>7</td>
</tr>
<tr>
<td>C3P6</td>
<td>M</td>
<td>20</td>
</tr>
<tr>
<td>C3P7</td>
<td>M</td>
<td>12</td>
</tr>
<tr>
<td>C3P8</td>
<td>M</td>
<td>6</td>
</tr>
<tr>
<td>C3P9</td>
<td>F</td>
<td>10</td>
</tr>
<tr>
<td>C3P10</td>
<td>F</td>
<td>21</td>
</tr>
</tbody>
</table>

Research Methodology Applied to the Data Analysis

The multiple-case study research design was selected based on the research problem and questions and applied based on the approaches defined by Stake (2013) for executing a multiple-case study. The selection of multiple cases enabled the exploration of a large bounded system comprised of subsystems. The large bounded system consisted of the U.S. cybersecurity industry, and the first bounded subsystem included females seeking entry into the U.S. cybersecurity profession. The seconded bounded subsystem encompassed females currently
working in the U.S. cybersecurity industry. The last bounded subsystem consisted of hiring managers working in the U.S. cybersecurity industry.

The researcher approached the study holistically by gathering and presenting multiple perspectives and recognizing various factors related to the phenomenon (Creswell & Creswell, 2017). Additionally, the researcher documented occurrences that did not directly apply to the research questions but had potential importance. The high number of middle-aged females transitioning to the cybersecurity profession from other career fields that were interested in the study was one such observation. Due to the study’s inclusion and exclusion criteria, these females were unable to participate in this study as the focus was not on the experiences of women making midlife career changes to enter the U.S. cybersecurity industry. However, this observation was documented separately as it constituted a recurring theme beyond the scope of the study. Chapter 5 contains a discussion of this discovery and its implications.

Yin (2014) discussed the challenges of conducting a multiple-case study because it is informal. Yin recommended the use of categorically defined themes and data frequencies. As a result, data inputs for each case were logged in a Microsoft Word document using the participants’ unique identifier codes. The researcher used traditional highlighting and grouping methods to identify themes and frequencies in the data.

When analyzing the data, the researcher identified themes and grouped similar themes (Yin, 2014). Following Bernard and Ryan (2009), the researcher read each participant’s transcript multiple times and highlighted prominent themes first. The researcher then allowed three to five days to pass and reviewed the transcript again to highlight less salient themes. All themes were recorded in a Microsoft Word document and highlighted using specific colors to assist with the organization of the data. Additionally, the researcher used traditional written notes.
on the transcripts and sticky notes to analyze content collected from each participant in each case. While identifying themes, the researcher coded findings by identifying categories and labeling each (Fink, 2000). The researcher used Microsoft Word’s word count feature to conduct a frequency analysis of the words used by participants. These words were identified during the highlighting and grouping phase. Figure 3 presents an illustration of the interview data word frequency.

![Figure 3. Interview data word frequency.](image)

In addition to the general techniques used to identify and highlight themes, the analysis was divided based on the bounded subsystems. Each case was evaluated individually during a within-case analysis. Following the within-case analysis, a cross-case analysis was conducted to contextualize the findings within the larger bounded system. The following sections present brief
descriptions of the processes used to conduct the within-case analysis and the cross-case analysis.

**Within-Case Analysis**

Stake (2013) stated that in a multiple-case study, it is crucial to review and focus on one case at a time to preclude bias. The researcher conducted each case individually. Before transitioning to another case, the researcher solely focused on the data collection and analysis of the present case. A combination of recorded data and observations guided each interview. Data analysis began during the initial data collection phase, which is common in qualitative studies (Creswell, 2007). Following the conclusion of each interview, the researcher reviewed the data collected, transcribed the data, and summarized each interview. All transcript notes and handwritten notes from the interviews were saved in distinct password-protected case files. During the collection phase of each case, the researcher analyzed data as it was collected to remain aware of possible new identifiers for the following collection phase and to be aware when data saturation occurred (Patton, 2015). Once data was completed for each case, the researcher reviewed each transcript and notes to identify themes. These steps were repeated for each case.

To document the data collection and contributions corresponding with participants, the researcher used a coding method to remove the participant names. Tables 3-5 illustrate the coding scheme. The researcher did not use electronic tools to analyze the data as manual coding and analysis ensured self-immersion in the data and full comprehension of the findings (Stake, 1995; Yin, 2014). Figure 4 depicts the application of the selected method of data analysis.
Figure 4. Method applied to multiple-case study.
Cross-Case Analysis

After completing each independent case study, the researcher conducted a cross-case analysis (see Figure 4). Analyzing data across similar cases can demonstrate replication and confirm findings (Yin, 2014). The cross-case analysis compared the individual cases to help form an understanding of the larger bounded system and the experiences of females working in the U.S. cybersecurity industry.

Yin (2014) provided guidance concerning how to ensure the credibility and dependability of the findings by cross-checking the results against the research questions and focusing on significant aspects and opposing perspectives (Yin, 2014). Stake (2013) explained that the researcher is obligated to provide understanding across all cases concerning the factors that bind the cases together, but it is not necessary to include individual case summaries when presenting data in a multiple-case study. The data results presented in this chapter are the aggregated results from the cross-case analysis. The cross-case analysis enables a researcher to examine multiple cases within a larger case, and the findings represent aggregated results representative of all the participants’ experiences (Yin, 2014).

Presentation of Data and Results of the Analysis

The data analysis process involved constructing both case descriptions and also compiling a cross-case analysis. The presentation of the data begins with brief descriptions of the individual cases. The presentation of the cross-case analysis follows the individual case summaries.

Within-Case Findings

Case 1 summary. Case 1 explored the lived experiences of 11 females who currently work in the U.S. cybersecurity profession. The questions designed for Case 1 were scoped to
gain insight from each participant on how their interest in the cybersecurity profession developed; what events occurred during their time working in the profession; and what advice they believe will help attract, retain, and increase female interest in the cybersecurity profession. All the participants in Case 1 studied a computer-related subject in school and or obtained additional technical certifications. Despite studying in computer-based fields, most of the participants shared the desire to enter the field was due to self-interest.

All the participants indicated that their interest in cybersecurity started in high school. C1P2 shared that she always knew she wanted to do something related to computers, so she majored in computer science when pursuing her undergraduate degree. Similarly, C1P3 stated that she was curious about computers in high school. Two participants, C1P10 and C1P2, indicated that a male friend or mentor encouraged them to enter the cybersecurity field. C1P2 stated, “For me, it all started with my major in undergrad, computer science. I knew in high school I was interested in something...anything that had something to do with computers.” C1P1 offered the following response during her interview.

I studied computer science in undergraduate school, and then I had a friend who told me about the program at a different university. It was a university that was a center of academic excellence in information assurance. The information my friend shared with me about this program piqued my interest. (C1P1)

For C1P3, the main driver was curiosity. C1P3 shared, “I started out because I was curious about computers in high school, so I started computer engineering and applied for a public-sector job.” C1P10 also became interested in information technology in high school, but her interest in information security expanded during her time at university.

I was in a Cisco academy vocational program my senior year in high school, and my Dad was an IT Director at his agency. So, I had some exposure, but not too much through my dad. Later in undergrad, I had a mentor during an internship that introduced me to the information security world. (C1P10)
Half of the participants in Case 1 were in government academic programs or the military, which prepared them for entering the cybersecurity career field. Several participants were either a member of the military or received a government funded grant. C1P4 observed, “becoming a government employee, I unknowingly signed up for the cyber intelligence career field, and though the training was challenging, I absolutely enjoy the career path.”

I took all the computer science courses, and I was in a program called Scholarship for Service (SFS). This is a program that supported your education, but you owe time back after you graduate to the organization that provided you the scholarship. (C1P9)

C1P1 pursued her degree with funding from the National Science Foundation. She shared the following statement.

I then went the NSF route to get my master’s degree and received a stipend. As a result, I work for the government for two years after graduation. Both of my degrees were in computer science. Because I was part of the NSF, I received scholarships for service. This made it easier to get a job. I pretty much had my agency of choice. (C1P1)

Other participants found that it was harder to transition into the cybersecurity profession after studying in computer-based degree programs.

My transition started back in 2011, which was four years after I graduated from college. During those four years, it was challenging for me to seek entry-level positions in my career field due highly to what I believe was a lack of networking opportunities. (C1P5)

C1P7 also noted that her first job following the transition was not ideal.

I knew I didn’t want to grab cables forever as a system administrator, so I started doing research and looking into the next big thing. There were a lot of government professors in my college at the time. I didn’t know that, but they encouraged me to so Information System Management. I knew cybersecurity was the next big thing. (C1P7)

Most of the participants experienced challenges early in their academic careers. C1P2, C1P10, and C1P11 shared similar experiences of being one of the few females in their academic
classes that were mostly taught by male professors. C1P4 and C1P9 offered the following statements.

The most challenging part of the training was the terminology. It was a very pace training plan, and I spent most of my downtime trying to learn the jargon. I learned it, but at a far slower pace than my male counterparts. (C1P4)

I went into a rigorous training program. I was the only female. The rest of the class was all white male. It was hard for me to relate. I would be conducting my technical role, and people would assume when I came around, I was not the go-to technical person, and I was there to do administrative functions. They looked at me like what are you doing here, and I had to prove myself. (C1P9)

C1P1 observed, “Most of my professors were male, and they had no expectation for me to stay in or not stay in the field. In my continual learning for these advance technical jobs, none of the instructors were females.” C1P8 shared similar feedback: “I can’t think of any professors in the computer-related classes being female in undergrad or graduate.” C1P2 described the consequences having limited numbers of females her undergraduate technical track classes.

There were very few females in pretty much all of my technical track classes in undergrad. It was maybe a handful of females in each class. So, it felt like we had to go above and beyond to be respected in class with our male peers. I can recall in some of my classes sometimes I felt like my professors valued what the male students were saying in class discussions over what a female student may have to contribute. (C1P2)

When C1P11 changed her major from biology to computer science, her department chair told her she should “consider computer information systems instead because it wasn’t as hard.”

The professor said that I probably wouldn’t be able to keep up with the advanced mathematics, but the professor didn’t even know what my skills and abilities were and didn’t bother to check my history, specifically about math, or they would have seen I was a straight-A student. (C1P11)

Once looking to enter their professional careers, Case 1 participants again faced gender-based obstacles. These challenges included being interviewed predominantly by men. Only two participants recalled having a female interviewer. Despite noting an inherent gender bias in the
hiring process, in most instances, the participants felt they were treated fairly during the interview process. Many of the participants in Case 1 were hired to fill the position for which they had interviewed. However, a few participants felt they were challenged during interviews because they were females, and their male interviewers wanted to test their knowledge. C1P8 stated, “They grilled me for one and half hours, and even my coworker was like ‘that was hard.’” C1P8 was promoted to the new position but felt that her evaluation differed from the experiences of her male coworkers. “I passed, but I do think some of it had to do with being a girl because there weren’t many girl cyber analysts at the time.” C1P8’s experience illustrates that the gender-based challenges shared by the participants did not stop once a female entered the cybersecurity workforce.

Most of the participants in Case 1 experienced uncomfortable work environments as a result of their gender. The participants indicated that they did not always feel comfortable speaking up, and when the participants did provide input, it was not always well-received. The obstacles experienced by the female participants were very similar, and most of the individuals in Case 1 attributed the cause of some of their obstacles to female stereotypes. C1P1 noted that even as a business owner, she was subject to stereotyping.

Now that I own my own company, interacting with clients can be difficult. It is a startup company, so when clients request the services that I provide, they naturally assume that I am going to be a man. One day, I was conducting a vulnerability assessment result at the organization I was servicing and was asked, “How did you get here?” (C1P1)

C1P1 noted that the stereotypical expectation that she had less knowledge compared to a male cybersecurity professional also manifested itself in an educational setting.

I also have been a technical instructor for a while, and I got questioned all the time like people needed to be sure I knew what I was doing. That is why I worked hard and always avoided making mistakes. As a technical woman, you always have to prove who you are and what you know. The career barriers haven’t gotten much better. (C1P1)
C1P8 also shared her experiences with gender stereotyping and low expectations based on gender.

I was a network consultant and would drive to client sites. I’d walk in, and you could tell some of the men got an attitude because they sent a woman. They’d hover or ask questions about if I really knew what I was doing. They’d quiz me, etc. I felt like I had to go above and beyond to prove that I was just as good or better than my male counterpart. (C1P8)

Two challenges participants experienced during their education and training included terminology that was difficult to grasp, and a work environment was unwelcoming to females. The participants shared common experiences of being taught by and working in predominantly male offices that were not very welcoming, and when they did encounter other females in the office, those other women typically performed administrative jobs. Besides having to constantly prove they should be in the career they choose, all the participants in Case 1 shared a desire to be respected as an equal.

C1P5 described having to prove herself in her male dominate classes while pursuing her undergraduate degree.

I do believe that progress has been made but don’t believe we are afforded the same opportunities and respect as our male counterparts. I don’t expect anything to be handed to me, but what I do expect is the same respect and integrity that I give to my counterparts beyond gender and race. (C1P5)

Sharing a similar experience, C1P1 noted that while she did not feel her male peers initially respected her, she eventually earned it. “I was able to earn the respect of peers because of how I scored and ranked in that highly technical training” (C1P1).

While each participant’s experience varied, they all agreed that the cybersecurity profession remains a male-dominated career field, and some participants asserted that improved marketing of the profession could attract more females to work in the cybersecurity field. C1P7
stated, “I would also suggest organizations market the other types of jobs that are in cybersecurity. There are so many, not just one.” C1P9 suggested that organizations should ensure they are properly presenting opportunities available in the cybersecurity profession.

   Everything is not young white guys at a black and green screen. There are other parts that can be highlighted, such as geopolitical, social, investigative, and the human element. Find the relatability piece, cybersecurity loses that in how it is currently marketed. (C1P9)

The participants in Case 1 provided advice for organizations and females seeking to improve the current representation of females in the cybersecurity professions. The participants’ advice included providing female mentors, creating more welcoming and inclusive work environments, and inspiring young females to enter the field early. C1P4 stated, “I’m already in a male-dominated career field.” C1P8 shared a similar experience with the following statement.

   When I first started in the IT world, I was usually the only woman. If there were any other women, it was very few. As the years went by and as I obtained my master’s degree, there were definitely more females, but still not a lot. Some classes still only had one or two females. Same with conferences. It has gotten better with the number of women, but males still dominate. (C1P8)

   C1P9 has experienced being a cyber professional in both the private and public sector. C1P9 described most of her offices as “predominantly male” and noting that “every once in a while, you saw a woman.” C1P9 observed that later in her career when she worked at a larger technology company, the workplace gender dynamic had changed somewhat: “I then went to another organization, well known technical company, where I didn’t have to prove myself. The workforce was very diverse, and the women that were there already had proven themselves and paved the way for other women.”

   C1P2 advised organizations to “be open to change and diversity. Develop mentorship groups for women to help with hiring and retaining women.” Beyond organizational flexibility,
C1P3 felt that mentorship was an important avenue of opportunity for females in the cybersecurity industry. C1P3 explained that she had advocates and mentors who assisted her in exploring career opportunities. C1P3 noted that a majority of her mentors were males as she found that most females saw her as competition.

Since I have been in the field, I have also had the opportunity to be in a position of mentorship. There are opportunities but women are not as vocal, and sometimes they don’t feel like they can. The technical women were more competitive as though we were competing against each other. I think it is important for women to have technical mentors that are women as well. In my case, as I mentioned earlier, mine were predominately male. (C1P3)

C1P5 believed that mentorship was essential to increasing the number of women in STEM fields like cybersecurity. C1P5’s recommendation was to start the mentoring process early, during girls’ formative years.

Like any other career field, it’s very important for leaders and mentors to pay it forward, and what I mean by that is if you notice that there is a need for women in STEM, focus on mentoring and/or recruiting young motivated girls at the elementary, middle, and high school level. (C1P5)

C1P9 echoed the views of some of the other participants on the importance of mentorship, and she suggested that organizations take an active role in fostering female interest in cybersecurity.

I suggest organizations get a campaign going because women are not attracted to the field like they could be. I am not even attracted to the field, but it is what I do. The campaign should focus on how cybersecurity engages with other parts of the mind. Show it in a different light. (C1P9)

C1P6 recommended that organizations adopt “more cultural diversity” as that “practice may attract more women.” C1P6 continued, “It’s important to have a mixed group of people on a team when trying to get solutions and solve problems. I would suggest organizations champion more programs that focus on women in cyber and be visible to potential candidates.”
C1P2 also advised, “Be open to change and diversity. Develop mentorship groups for women to help with hiring and retaining women.” C1P5 noted that gender was not always the sole consideration or barrier to entry.

That I am the only black female among eight white males on my immediate team and have questioned whether I have been discriminated against due to my gender and race when it comes to assignment of task or credibility of knowledge. (C1P5)

Overall, the participants in Case 1 indicated that they experienced a very male-dominated industry. Many participants felt a need to prove themselves or justify their knowledge and expertise in settings where most of the individuals were males. C1P7 offered an example of this dynamic.

On nontechnical teams, there were more males than females but still a lot of females. In technical offices, there were always way more males. I would say something in a team setting or meeting and they are dismissive. A man would say the same thing and it’s a great idea. (C1P7)

The participants in Case 1 described the phenomenon under study from the perspective of females working in cybersecurity. Case 2 encompassed the experiences of females seeking entry into the cybersecurity workforce. The next section contains the findings from the participants’ interviews for Case 2.

**Case 2 summary.** The second case included the experiences of females seeking entry into the cybersecurity profession by interviewing 10 females who fit the criteria established for this study. These females were all students or recent graduates who shared collegiate experience in technical classes, internships, camps, conferences, and, in some cases, interviews for cybersecurity positions. All participants attended male-dominated technical classes taught primarily by male instructors. Some participants reported that their male classmates were
supportive, but other participants reported feeling that they did not belong in technical classes that were part of their preparation for a cybersecurity career.

C2P1 indicated that some of her instructors told her that because of the low numbers of women in the cybersecurity profession, the field offered unlimited potential if she chose to pursue it. Despite this encouragement, C2P1 noted that she often received discouraging responses as well. C2P1 stated, “I find that men question my motives. I get asked all the time, ‘Why would you do that? It’s too hard to continue. Don’t you want a family? Isn’t your master’s good enough?’” C2P3 had a different experience. While C2P3’s foundational technical courses were predominantly male, when she switched to her core cybersecurity courses, her experience changed.

Typically, when I was in technical courses, it was just me, I would turnaround, and they were all male. As I started switching into cybersecurity specifically, I am now around a team that is more diverse, and there are women too. (C2P3)

Participants in Case 2 were asked what caused them to pursue technical academic credentials that put them on the path to enter the cybersecurity profession. Almost half of the participants (40%) indicated they were transitioning into cybersecurity from other IT-related studies or basic computer science tracks. The other 60% of the participants in Case 2 explained they developed their interest in cybersecurity while in high school. Most of the participants in Case 2 expressed the need to pursue a career that would allow them to safeguard information. Additionally, some participants noted the inherent job security in the cybersecurity field.

C2P5 first encountered cybersecurity during her senior year in high school. She shared, “I participated in national CyberPatriot competitions. As my team and I protected systems, investigated the answers to forensic questions, and hardened vulnerable systems, I began to realize that cybersecurity is what I wanted to do as a profession.” C2P10 first learned about
cybersecurity while at a summer camp called GenCyber. C2P10 also joined a cyber club at her school. “I find cybersecurity interesting because I am able to protect my personal information and others’ personal information. Cybersecurity is just an interesting concept to me and a very relevant topic in today’s society” (C2P10). C2P8 highlighted the excitement she felt pursuing cybersecurity.

I think that cybersecurity is something new and exciting to learn about, as well as something that is going to be relevant for a long time. It was a combination of what I'm interested in and what I think would be a good practical career decision. (C2P8)

C2P1 also indicated she was first exposed to cybersecurity when she got to college.

As a student in college, it was presented to me that this field didn’t have a lot of women that looked like me working in it. That this field would never get saturated with people and that my career could grow unlimited bounds. (C2P1)

Several of the participants in Case 2 suggested that organizations and academia could do a better job of educating females about actual opportunities in cybersecurity. Despite this perspective, the participants all noted recent strides that academia and professional organizations had made to increase cybersecurity’s appeal to females. Primarily, participants cited an increase in female-focused technical events. Several participants reported competing in cybersecurity events and competitions, but they noted they were usually the only female on the team.

Advertising how amazing and fun cybersecurity it is. I think, especially in today’s society, that women, or anyone in general, think they can’t do it when they can. Show how beneficial it is towards society and themselves all while being exciting about it. (C2P7)

C2P4 stated, “I love the Women in STEM events. We need more of that, so we can lift each other up and share our frustrations, so we can continue to come up with real solutions, together.”

C2P5 also recommended more female-only events but expressed concern that doing so may appear to create bias in itself.
Females in this group also shared a common experience of feeling pressured to prove themselves or to make a concerted effort to demonstrate that they belonged in the courses and activities that were required for them to enter the cybersecurity profession. C2P10 shared, “I feel that I have to prove myself but in terms of others pressuring me to prove myself.” C2P9 stated, 

When I first started my college degree, a gentleman told me that I would quit because all the girls quit computer science and don’t make it out. From that day, I was determined to prove him wrong. I didn’t really know what I was doing, but I figured I wouldn’t prove that guy right.

These future cybersecurity professionals shared what they desire their future office environment to be like. The majority of the participants desired a challenging workplace with opportunity for growth, continual learning, and the ability to work in a team. C2P1 stated, “I expect to be respected for my skills and knowledge. I would like the morale in my future office to foster continued learning. A place that I can be mentored and also be a mentor.” C2P2 offered a similar response. 

I would like an environment where everyone works as a team. A team that helps each other out; this is super critical. It should also be positive, supportive, and empowering. I would like to want to show up to work. (C2P2)

C2P5 stated, “I would like it to be a serious but fun environment where everyone enjoys each other’s company during lunch, outside of work, etc. But be serious when it comes to work-related projects.” C2P7’s response focused on teamwork.

In my future office, I hope I get to work with a team, so we can all help each other if something were to go wrong. I want to be able to have a confident and stable ground, so I’m able to take whatever challenge that is given to me. (C2P7)

C2P8 noted, “I hope that it will a comfortable place to work and learn. I would want a boss that is fair, doesn’t show favoritism, that encourages teamwork.”
Another commonality among participants was the desire to have a supervisor that does not assume they are incapable of doing something before they have a chance to demonstrate their abilities. C2P1 shared, “I would like my future supervisor to be knowledgeable about cyber and to encourage continual learning in the field, also to foster an environment that yields promotions.” C2P2 offered a slightly different response.

I want a supervisor that is not critical and supportive of my growth. Also, no backstabbing, lies, or drama. I would like a boss that has integrity. I had a supervisor that was super critical of me but was not trained to do the job that I was doing. I feel the supervisor should set the standard and be knowledgeable. (C2P2)

C2P7 stated that she wanted a supervisor who is “strong and confident.” C2P7 elaborated,

Someone who knows what they are doing and is able to guide me when I lost track. I want to be able to look up at them and see how compassionate and understanding they are all while giving me constructive criticism when I need it.

C2P9 looked for very similar characteristics in a future supervisor. “Someone who is confident and strong and knowledgeable. I also need someone that can support and challenge me at the same time. I guess most of all I don’t want an unfair person to be my boss.”

**Case 3 summary.** The third and final case examined by the researcher explored the U.S. cybersecurity profession through the lens of 10 participants who recruit and hire technical talent within the cybersecurity profession. These interviews provided insights into what qualifications organizations seek when cybersecurity professionals. Case 3 also provided insights into the demographic distribution of the hiring pipeline. The hiring managers in Case 3 described their experiences of seeking and interviewing male and female candidates for cybersecurity positions and how candidates’ gender affected the recruitment and hiring process.

The participants in Case 3 first shared what they are looking for in cybersecurity professionals. Most of the participants were open to both entry-level and seasoned applicants.
The participants’ main consideration was that applications possess a background in STEM-focused coursework, the motivation to learn, effective communication skills, and previous exposure to computer network defense skills.

C3P2 expressed that both technical and interpersonal skills were highly desirable. “Good knowledge of programming languages, networking. Some experience in network programming is a plus as well. Certifications are good to have but not required depending on experience” (C3P2).

C3P3 shared a similar sentiment.

Deep technical knowledge, the ability to collaborate, and a person that is articulate, someone that can articulate a message to multiple layers of leadership. They should be able to do this through both verbal and written communication. They need to be able to handle complex ideas and scenarios for leaders or the audience so that the delivery is tangible and useable. I think our organization is struggling to break out of the rut of the typical white male syndrome. We have to break out of that. (C3P3)

C3P5 offered the following response when asked what she looked for in cybersecurity professionals.

They need to be technically sound in the core computer science principles, also in software engineering and architecture. It is also important for them to be able to communicate; it is extremely important to be able to communicate extremely technical content to no technical peers and leadership. (C3P5)

While other participants discussed technical skills, C3P7 and C3P1 shared their perspectives on degree holders. C3P7 offered the following explanation.

I am looking for computer science, math, engineering, cybersecurity, and software design majors/studies. The degree matters to a certain extent, but more so I am looking at the applicant’s ability to work in a team and how they tackle complex tasks. Soft skills are important too, they are a self-motivator and knowledge retention are ideal for a good candidate. (C3P7)

C3P1 shared a similar response. “I look for people who have STEM degrees such as computer science, computer engineering, electrical engineering, and mathematics. Also, I look for anyone who has experience in those areas or within Computer Network Defense.”
Participants noted that cybersecurity professionals did not have to obtain technical skills through academic institutions; they could also obtain skills by acquiring hands-on experience in computer-based competitions and challenges. Most participants in this group shared that such experiences provide future cybersecurity professionals with a more realistic understanding of how networks really work and the best way to secure them. Practical experience gained through competitions also allows cybersecurity professionals to learn how to work in teams. While participants acknowledged that working in a team is not a requirement, they noted that the ability to working in a group is key to solving complex problems.

Every participant in this group shared that companies have not historically required soft skills in the field of IT; these skills are highly sought after in cybersecurity professionals. Some participants in Case 3 commented directly on the importance of soft skills. C3P2 stated,

Soft skills are very important to our company. Being a company that works with various other companies, we need employees that can relay messages to these companies. Technical people do have a tendency to introverts and sometimes have problems using spoken and paper written skills to relay information in a positive way.

C3P3 explained the need for the candidates to possess deep technical knowledge but put a strong emphasis on a candidate’s ability to communicate information effectively at various levels. C3P3 specifically referred to the later as “intangible traits.”

I do care about their technical ability, but I care more about their technical intangible traits. I am looking for an array of skills in the candidates I select to ensure they are suited to do the job I am selecting them for. (C3P3)

When hiring cybersecurity professionals, the participants in Case 3 noted that they encounter challenges. Participants noted that most applicants are men, and when there are fewer female applicants, it becomes more difficult to hire equal numbers of males and females. C3P3 stated, “I would say the applicants are mostly male, 70% [male] to 30% women.” C3P4
estimated that “90% of the applicants are male.” C3P6 also saw predominantly male job
applicants. “I would say that the applicant pool was 80 to 90% males. In some cases, I could be
responsible for reviewing 200 resumes at a time, and they were 80% male” (C3P6).

C3P7 provided a unique insight. C3P7 conducts recruitment efforts to hire cybersecurity
professionals from both the East and West Coast. C3P7 shared that the ratio of male to female
applicants differs based on geographic location. “In both regions, men are the bulk of applicants.
On the West Coast, the split is about 60% men and 40% women. On the East Coast, it is about
80% men and 20% women” (C3P7).

The participants in Case 3 stated that they could not bring more females into the
profession if there are not adequate numbers of female job applicants. Some participants
observed that they have to be creative at times when seeking to achieve a certain level of gender
diversity in the workplace. C3P10 leverages professional events hosted by key technology
organizations as a platform to recruit and hire new candidates. In C3P10’s experience, “only
about 3% of the attendees as the events are women. Of those women, they are typically there as a
marketer or something business related. Very seldom are they technical professionals.”

Several of the participants interviewed shared challenges they face when filling
cybersecurity positions. Examples included geographical challenges, processing issues, and
difficulty finding diverse talent. Most of the participants explained that their hiring processes
consisted of several stages, and sometimes applicants to lose interest due to the length of time
these stages take to complete. C3P3 and C3P7 offered the following statements.

Our main issue is the many layers of our hiring program and just getting out there to
reach out to the candidates more and getting them interested in the field. I think there is
still so much work to do to expose potential candidates to what we can do and how
fruitful the cybersecurity career can be. (C3P3)
As a public-sector organization, we are not as fiscally competitive with the private sector, so that sometimes makes it a challenge, but we have a more rewarding mission. Location is also an issue in some cases because we are not located in some of the more popular places people want to live. (C3P7)

C3P8 hires cybersecurity professionals for employment on the West Coast and shared the challenges he has encountered when seeking new hires. “The women are a bit more hesitant to move to the West Coast for work, maybe because it is further from home, maybe because of comfort” (C3P8). C3P9 described a different hiring process where initial screenings occur before hiring managers even enter the process. In this system, hiring managers receive a pool of prefILTERED candidates to review. This method excludes the hiring managers from participating in the selection process from start to finish.

A lot of the recruiting efforts are done for us, so by the time we see the candidates for interviews, they have already been through a selective process based on information on their resumes, and by that time, we normally see only candidates that may be a potential fit (C3P9).

The majority of the hiring managers indicated that diversity should be at the forefront of an organization’s focus to build a workforce. The participants’ definition of diversity included the diversity of backgrounds, gender diversity, and, most importantly, diversity of thought. C3P2 shared how a lack of diversity impacts a team and its ability to perform. “A lack of diversity hurts any company a lot. Not having enough diversity in one group causes you to lose touch with customers that are part of that group, which in terms hurts a company’s bottom line.”

C3P2 observed that the current cybersecurity workforce predominantly consisted of white males, and organizations need to change. C3P3 shared similar thoughts on the lack of diversity in the cybersecurity workforce.

I would just say our thought process has to mature in cyber. Cyber needs and must have diversity of thought. Diversity in thought links groupthink. I really think groupthink is holding us back from reaching our full potential in cyber. (C3P3)
Other participants shared that diversity should start at an organization’s recruiting booths.

A more immediate approach would be to have more diversity at recruitment booths and among cyber-related events. Get applicants ready and tell them what to expect. I think employers have to be more active and go out to more colleges and make time to talk to the shy young lady that may not rush you like all the guys. (C3P3)

While some organizations, such as the one C3P8 represented, are striving to improve diversity in the cybersecurity profession, there is still work to do. C3P8 observed, “I think the organization that I work for is doing a good job to try and steer in that direction of diversity and hiring more women, but they are not there yet.”

Participants in Case 3 also noted the female applicants they do interview often lack confidence relative to their male counterparts. Despite this difference, participants acknowledged that female candidates were well prepared. When discussing gender diversity, half of the participants in Case 3 shared that over 75% of the applicants they interview are overconfident but poorly prepared males. C3P1, C3P3, C1P4, C1P5, and C3P10 shared a different experience and felt that both male and female applicants were equally unprepared and lacked confidence.

In the interviews, some females come across confident and some do not. There are some that try a little harder to demonstrate confidence, but there are some that are not as confident. The males that I have interviewed definitely are more confident and are comfortable during their interviews. (C3P2)

C3P2 shared that the lack of confidence that females have may also contribute to why more females choose not to remain in the cybersecurity profession. When conducting interviews, C3P4 was disappointed in how some of the interviews would go.

I was a little disappointed in some of the interviews. The males were more prepared, and females generally did not project confidence. Even for a question such as “Tell me about yourself,” the females were more hesitant. The males were overconfident, even on the ones they got wrong. (C3P4)

C3P7 also expressed an opinion on female confidence.
Females are more prepared for interviews 50% of the time and are most amenable to change. However, females appear to be more apprehensive and shyer in the beginning of an interview. They are not instantly confident. I try to create an environment during the interview where they feel they can talk and be comfortable, and eventually, they get there, but in most cases, they are not there at the start of the interview. Males, on the other hand, are confident, so confident that it comes off as cockiness. (C3P7)

Lastly, Case 3 participants provided advice for future female cybersecurity professional and organizations that are seeking to increase their female cybersecurity applicants and hires. The first piece of advice participants provided employers who are seeking to increase their number of female cybersecurity professionals was for employers to be more forward-leaning and more active in the cyber community and on college campuses. Case 3 participants recommended that organizations engage female candidates at an early age to encourage the development of interest in fields that lead to cybersecurity.

C3P3 noted, “When it comes to hiring, diversity has to be something that is at the forefront of your mind. If not, things will not change, and you will not get the change you are looking for.” C3P4, C3P6, and C3P10 offered similar responses.

I think they should increase female representation at events. Include information from other resources and ensure that word of mouth is good. It is important that there is a good atmosphere set if people want other people to advocate for them. (C3P4)

You also have to start early. During national competitions like cyber patriots, high school teams have been all boys, but I am seeing a mix on the middle school teams. I am not saying there are not females, but not on most teams. (C3P6)

I love hack-a-thons. I really do and support them. But they should not focus on only that to get women interested. There is a lot of proving and competition that goes on there. I don’t think that is the time to teach the ladies and try to get them interested. This approach is out of order. Employers should first get the ladies interested or at least teach them how to do it. Let them live it and then see that they can actually do it. Then let them complete. (C3P10)

Next, participants warned that employers must realize when some candidates may need a bit more attention and patience to develop their confidence and potential. Participants also
acknowledged that while employers encounter candidates that are not confident, they should remember that confidence can develop. Increasing female representation at recruitment and networking events would allow females who work in the profession to share their experiences. Lastly, participants explained that employers need to create healthy work environments that allow for both career growth and flexibility.

All participants in Case 3 expressed that increasing the number of females from various backgrounds will contribute to the future success of the cybersecurity profession. Participants shared the perspective that it was important that organizations be intentionally inclusive in recruitment efforts. While all three cases varied in experiences and views, there were commonalities among the three groups explored. These commonalities were explored in-depth by conducting a cross-case analysis.

**Cross-Case Findings**

After analyzing the results of each case, the cross-case analysis was completed. Table 6 delineates the themes identified in during the cross-case analysis. A total of five relevant themes emerged from the data. These themes were related to confidence, gender stereotypes and biases, marketing images and terminology, early exposure, and male dominance. The cross-case findings present in-depth perspectives that prompted the identification of each theme.

**Theme 1.** The first theme identified during the cross-case analysis was that confidence is unequally exhibited, projected, and perceived among females and males. Several participants observed that female interviewees lack confidence. The topic of confidence frequently emerged within and across every case. Participants characterized confidence as equally important as technical knowledge and capability. Hiring managers highlighted the lack of confidence displayed by female applicants during technical interviews.
Table 6. *Cross-Case Analysis Themes*

<table>
<thead>
<tr>
<th>Themes</th>
<th>Supporting Patterns Within Themes</th>
</tr>
</thead>
</table>
| **Theme 1: Confidence is unequally exhibited, projected, and perceived among females and males.** | Female interviewees lack confidence.  
Male interviewees are overly confident.  
Females must continually prove themselves.                                                                                                                                                                             |
| **Theme 2: Gender stereotypes and biases impact the cybersecurity profession.** | Females are stereotyped as excelling at soft skills.  
Males are stereotyped as being more adept at technical skills than female counterparts.  
Cybersecurity is stigmatized as a militaristic career field.  
There is a bias that exists that males perform better in certain jobs than women.  
Technical professionals are stereotyped as white males.  
Societal norms among gender may play a role in what is deemed an acceptable work role for a female or male.                                                                 |
| **Theme 3: Marketing images and terminology used for the cybersecurity profession are not gender inclusive.** | The terminology used in the cybersecurity profession is not gender-inclusive or welcoming to females.  
The image of what a cybersecurity professional looks like is a white male.  
Marketing and branding for cybersecurity are not designed to attract females.                                                                                                                                   |
| **Theme 4: Early exposure to cybersecurity skills and professionals that females can identify with may increase female interest in the field.** | Exposure to technical mentors is important to foster interest and support the sustainability of females in cybersecurity.  
Early exposure to the field of cybersecurity or a related discipline encourages females to enter the cybersecurity profession.  
Females who participate in programs related to the cybersecurity pipeline had a smoother transition into the profession.  
Exposure to mentors and female cybersecurity professionals as role models encouraged females to pursue the profession.                                                                 |
| **Theme 5: Males hold most manager positions, academic professor roles, and mentor roles in the cybersecurity field.** | The cybersecurity profession is male-dominated.  
Cybersecurity courses and computer-based courses are predominantly occupied by white males  
Academic instructors who teach technical coursework are predominantly male.  
Hiring managers for the cybersecurity profession are predominantly male.                                                                                                                                  |
When commenting on the element of confidence during interviews, C3P3 offered the following assessment.

Some females come across as confident, and some do not. There are some that try a little harder to demonstrate confidence, but there are some that are not as confident. The males that I have interviewed are more confident and are comfortable during their interviews. (C3P3)

C3P3 noted that when this happens, he adjusts his interview style to try to ensure that female interviewees are comfortable. C3P3’s goal is to help the female applicant perform better in the interview. Ultimately, C3P3 stated he does not care about the gender of the candidate. What is important as a hiring manager is to confirm the applicant’s technical ability and their intangible technical traits. C3P3 offered the following example of how he handles situations where the females in the interviews are nervous or uncomfortable.

I try to redirect the interview to give them a chance to calm their nerves so that they can perform well in the interview. The men, on the other hand, are overly confident. I am not sure why men are more confident in the interviews, but it does appear to be that way. I am also looking for how confident a candidate is in speaking. (C3P3)

In C3P5’s experience, female interviewees are well prepared and very calculated in their approach during an interview. This rigid preparation made it appear that the female interviewees were not being themselves and were not confident while their male competitors appeared more comfortable during interviewees even when they did not know the information. C3P5 attributed this behavior to the female candidates’ need to be humble and honest. C3P5 stated,

I recommend that females be more confident. Men seem to be more confident than females. It appears that females focus on being humble. I think it’s because females are raised not to speak out. You know, they are taught to be quieter.

C3P4 shared a similar observation that during interviews, males were more prepared, and females generally did not project confidence. C3P4 felt that female applicants even struggled when asked a question such as “tell me about yourself.” C3P4 noted that while the females were
more hesitant, the males were overconfident, even when they sometimes provided the wrong answer.

Although most of the managers interviewed for Case 3 agreed that female applicants demonstrated less confidence during interviews, C3P6’s experience was different from others. C3P6 shared that male and females were equally unprepared for the level of technical questions he asked during interviews. The lack of confidence described by C3P6 appeared to be equal across both genders.

I would, for example, say, “Name me five Linux commands and tell me what they do.” Or, I would want them to tell me about the TCP/IP model or the OSI model and what happens at the various layers. Sometimes I would ask applicants, “What happens when you type a URL in your browser? What happens next?” In most cases, they are unable to tell me the answer to this question. I don’t expect them to know everything, but if they can even come close to the answer, that shows me they are aware and are trying to answer the question. (C3P6)

The lack of confidence was a pattern also observed while interviewing females working in the cybersecurity profession. C1P3 shared that she felt she had to build more confidence to be successful. This was a challenge considering the work role she was in consisted of a very rigorous training program where there were only one or two females at a time in the class, and the failure rate was high. C1P3 stated,

To push through this program successfully, I had to build even more confidence and study on my own and practice. I was approached by the program manager and asked if I knew how to attract more females like myself. I think it is very important that leaders make an extra effort to encourage more females in this career path and create an environment that is safe for them. I had to work very hard and prove myself.

C1P5 discussed her level of confidence and observed that confidence was linked to both personal achievement and the perceptions of peers and supervisors.

Every single day, I feel like I have to prove my work ethic and experience. I don't expect anything to be handed to me, but what I do expect is the same respect and integrity that I give to my counterparts beyond gender and race. (C1P5)
C1P8 shared her experience and confidence as an underestimated female cybersecurity professional.

I noticed it mostly when I was a network consultant and would drive to client sites. I'd walk in, and you could tell some of the men got an attitude because they sent a woman. They’d hover or ask questions about if I really knew what I was doing. They’d quiz me, etc. I felt like I had to go above and beyond to prove that I was just as good as or better than my male counterpart. (C1P8)

The same need to develop and remain confident or prove oneself was also common among young females studying to enter the profession. C2P6 noted, “I had to gain confidence by myself, and with some of the teacher’s help, I did what I could to pass. In calculus, guys would group up with guys, and girls would go with girls.” Additionally, C2P3 stated,

Females interested in the cybersecurity profession should be prepared to come into a man interviewing you or a man in your space. A lot of females show a weakness; they are not confident; they must build trust and confidence in themselves. You have to persevere and truly figure out how much work you are willing to put into work. Keep being willing to learn; I am not smart, I just work hard, and I am not willing to stop learning.

Despite the apparent theme of confidence, one participant expressed an alternative perspective. C3P3 believed that initial confidence was not necessary as it could be developed. C3P3 also suggested that hiring someone who is overly confident could entail negative consequences.

Confidence is good, as I mentioned earlier, but that is not all that is required. You can work and build confidence, so I am going to always select someone that has less confidence than someone that has too much confidence because it is hard to change an overly confident person. So, when you are then trying to assimilate that person into a culture of an organization, it may be harder. Also, people grow when they are not comfortable. What makes you uncomfortable, makes you grow. (C3P3)

C3P6 shared a similar perspective. “I am interested in people who have some self-confidence; you can build self-confidence, but that can sometimes be a problem because people
who lack self-confidence tend to overthink logical reasoning questions” (C3P6). C3P7 offered the following observation.

Females are more prepared for interviews 50% of the time and are most amenable to change. However, females appear to be more apprehensive and shy in the beginning. They are not instantly confident. I try to create an environment during the interview where they feel they can talk and be comfortable, and eventually, they get there; but in most cases, they are not there at the start of the interview. Males, on the other hand, are confident, so confident that it comes off as cockiness. (C3P7)

When asked what advice they would give females who aspire to work in the cybersecurity profession or how they overcame challenges in the workplace, one of the most consistent answers among participants from Case 1 and Case 2 was confidence. Participants shared that confidence helps women push through barriers and biases they face when seeking entry into the field. Participants noted that confidence was also beneficial once they entered the field of cybersecurity.

**Theme 2.** The second theme that emerged was that gender stereotypes and biases impact the cybersecurity profession. Within the cybersecurity profession, organizations and individuals continually strive to appeal to female professionals and ameliorate negative perceptions of females. The cybersecurity workforce remains associated with a technical workforce that is stereotyped as predominantly white and male-dominated. The participants concurred that females do not represent the general image of cybersecurity professionals, and this is demonstrated internally and externally in the workplace.

Most participants across all three cases agreed that a stigma permeates the cybersecurity field. Cybersecurity professionals are primarily male. Participants also shared that stereotypes and biases exist as a result of the lack of gender diversity within the profession. The stereotype
associated with this perspective is that females are not as knowledgeable on cybersecurity subject matter as their male counterparts. C1P2 stated,

Long gone are the years and mindset of females only doing certain jobs like teachers, nurses, secretary, etc. Nothing against these career fields though, just for getting the point across. Now there are more younger females and girls interested in being engineers, IT professionals, cybersecurity, etc.

C2P9 suggested that higher numbers of males working in the cybersecurity profession because of the images that are portrayed on TV. “Because of the representatives that come out to my school and what I have always seen on TV, and now they have more women on TV, but it seems scripted.” C2P8 is currently studying to be a cybersecurity professional, and she admitted that her perception is that mostly, males work in the profession. “I think I assume that a lot of people who work in cybersecurity are male. All of the people I accidentally meet who work in something cybersecurity is usually male” (C2P8).

C2P3 noted that females are sometimes perceived as being less capable than their male counterparts. “When you bring females on board, do not assume that they can’t do certain things or as well as male counterparts” (C2P3). C3P10 shared her perspective stating, “There is a huge challenge to give females an understanding of what the field is. A bunch of geeky guys is how it is depicted and what people think.” C2P9 offered the following response.

While out of town working on a paper one weekend at a hotel, a woman asked me what I was working on, and I shared it was a paper for school. She proceeded to ask what I was getting my degree in. I shared with her I was getting a master’s in computer science. She looked shocked and then she said to me “Oh, you don’t look like you do that. Usually, it’s like young white guys that live in their mom’s basement. You know, like geeky white guys.” I looked at her and just shook my head. This was not the first time, but it was definitely obvious that it didn’t look like I should be there, and that people didn’t expect me to be there. (C2P9)

C2P1 shared a similar experience.
I find that men question my motivations... I would get asked all the time... “Why would you do that?” Meaning pursue high-level technical degrees. They would say “It’s too hard to continue. Don’t you want a family? Isn’t your masters good enough?” (C2P1)

C2P10 is a student who is studying to enter the cybersecurity profession, and she has already observed the stereotype that men are superior candidates for technical jobs. She shared the following explanation.

Seriously, consider hiring females, because in my experience, I know females that have had a lot more experience and knowledge than the men that were being considered before the woman. But not to say to only hire females because everyone has the potential to add to the organization. Females have just as much potential to add to the organization as men, and in some cases, females are more prepared and knowledgeable to add instead of some men who may not be as knowledgeable or prepared. (C2P10)

In some cases, participants were frequently questioned about their intent or presence in the cybersecurity profession. Participants asserted that this behavior surfaced due to the stereotypes and stigmas associated with academic fields that relate to this profession and the typical appearance of these professionals, which related to observations by Williamson and Tranter (2017). C1P3 recalled, “There are a lot of my peers that would say ‘Why computers? Why are you here?’ Or, they would say ‘Are you sure this is what you want to do?’” C1P9 and C3P7 recalled similar interactions.

I would be conducting my technical role, and people would assume when I came around that I was not the go-to technical person, and I was there to do administrative functions. They looked at me like “what are you doing here,” and I had to prove myself. (C1P9)

Always talk and encourage the STEM workforce, no matter what they look like. I can’t say definitively that diversity affects how an employer selects a candidate, but I suggest people do not require applicants to attach photos to resumes. This creates an instant bias sometimes, probably unconscious, but still a bias. The photo isn’t actually needed, so employers should remove it and not accept them with resumes. (C3P7)

C2P3 believed that women often exceed expectations. C2P3 stated, “When women do things, women are dedicated. This is why I think cyber is better for women. Cybersecurity needs
extra care and patients, that is what women can give it, men don’t have a lot of these qualities.”
C1P4 encouraged future female cybersecurity professionals to stay in the profession no matter how males treat them in the workplace. “I would say in cyber, remain who you are regardless of how you’re treated. Unfortunately, we still have hurdles, and there’s still a lot of males who won’t take you seriously.” C1P4 shared that this occurs because women are the minority in the workplace and appear out of place to their male counterparts. C3P6 pointed out the need to stop treating females studying or working in the field of cybersecurity as though they are rare.

I think it is very important that we stop making women feel like unicorns, as women are getting into the roles. People say we can’t find women that can do this job, but we can. It may be harder, but we can. (C1P4)

**Theme 3.** The third theme that emerged from the cross-case analysis was that marketing images and terminology used for the cybersecurity profession are not gender inclusive. Many participants in this study expressed concerns about the modern depiction of the cybersecurity profession. Participants shared the consensus that the profession remains insufficiently inclusive and fails to attract females at a rate that will increase female representation in the profession. The participants attributed some of the lack of inclusiveness to the images used to attract future cybersecurity candidates and the terminology used to teach the fundamental concepts of the technical skills needed to be a cybersecurity professional.

C3P10 shared that an organization’s ability to properly market internal cybersecurity opportunities and jobs is an early barrier to entry.

Over the years, I have realized that there is no elegant way to present cybersecurity. Organizations have not and do not represent cyber well. It is not well organized, and then there is no framework within organizations, and it extends to organizations seeking cybersecurity professionals not marketing themselves good as an industry. (C3P10)
C2P9 shared that her image of a cybersecurity professional is male because of the content marketed on television shows. C2P9 also noted that television shows have begun to include more females on TV in cyber-related roles but that these characters seem unnatural, and the interactions seem scripted. At one of the last technical conferences C2P4 attended, she noticed a pattern that older companies had mostly white males at their information booths, while newer companies had more gender and ethnically diverse individuals representing their organizations. C2P4 described the latter as refreshing to see.

The terminology used in the cybersecurity profession is also not gender inclusive or welcoming to females. C1P4 and C3P10 shared that the terminology used within the cybersecurity profession and in classes that support the cybersecurity profession also constitutes a barrier for some individuals. C3P10 works with elementary age girls, and she noted that the technical terms can be intimidating and make young girls feel that the field is more welcoming to young males. C1P4 echoed this statement when she explained that understanding the terminology and feeling comfortable with it was her hardest challenge when becoming a cybersecurity professional.

C3P5 observed, “The recruitment process is not necessarily designed to be intentionally inclusive. The language and the terminology that is used does not necessarily attract females to the job or make them comfortable about talking.” C2P8 also expressed her feelings on this topic.

I think cybersecurity terminology is off-putting regarding marketing to people. I guess if technical terms are unfamiliar, it can be kind of frightening. The usage of really technical terms can seem impersonal or robotic. I guess most people speak casually, so it’s more relatable if you speak more casually. (C2P8)

C1P4 stated, “The most challenging part of the training was the terminology. It was a fast-paced training plan, and I spent most of my downtime trying to learn the technical jargon.” C1P7
suggested organizations should focus more on marketing the wide array of jobs available in the
cybersecurity profession so young females can see that it is not just about coding. C1P7
suggested that this approach might ensure that females find jobs in cybersecurity more relatable.
C2P7 shared similar sentiments on how organizations and academia can attract females to
cybersecurity by reshaping the markets of the profession. C2P7 recommended “advertising how
amazing and fun cybersecurity is.”

I think, especially in today’s society, that females, or anyone in general, think they can’t
do it when they can. Show how beneficial it is towards society and themselves all while
being exciting about it. People are very influential, and if you could show how passionate
people are, how fun it can be, and what jobs out there are to offer. Females can finally see
how important it is. Just because it’s a male-dominant field, doesn’t mean females can’t
do it. (C2P7)

Theme 4. The fourth theme identified during the data analysis was that early exposure to
cybersecurity skills, mentors, and professionals whom young females can relate to is key to
increasing female interest in the field. Participants shared the belief that it is essential that young
females are exposed to the cybersecurity profession early to ensure females are aware of existing
career opportunities in that field. Participants also strongly encouraged the mentorship of more
young females to foster interest in the field and help these females study for the profession,
obtain a job in cybersecurity, and remain in the profession.

Most female participants currently working in the cybersecurity profession (i.e., Case 1
participants) indicated that they gained awareness of technology or cybersecurity by their
teenage years. Participants in Case 2 described similar experiences but also clarified that they
gained interest through exposure to technical courses and competitions while in high school.
Additionally, most participants in both Case 1 and Case 2 had had a mentor, been a mentor, or
sought work in an environment that promoted mentorship.
Participants’ responses indicated that females who were part of programs related to the cybersecurity pipeline had a smooth transition into the profession. In some instances, these same women had both peer or professional mentors that inspired or encouraged them to pursue the cybersecurity profession. C1P1 shared her experience of receiving peer mentoring and encouragement to enter the field.

I studied computer science in undergraduate school, and then I had a friend who told me about a program at a different university. It was a university that was a Center of Academic Excellence in Information Assurance. The information my friend shared with me about this program piqued my interest. I then went on to do an internship with a tech company. I then went the NSF route to get my master’s degree and received a stipend. As a result, I worked for the government for two years after graduation in the cybersecurity profession. My recruit process was easy because of the degree I had and the program I was part of. I went on to conduct vulnerability research and learn malware engineering and offensive security. (C1P1)

C1P9 entered the profession through the following means.

I was in school for IT, and I overheard a guy talking about computer security, and he was willing to share information about it. So, I decided to get my master’s in information technology with a specialization in security. I took all the computer science courses, and I was in a program called Scholarship for Service (SFS). This is a program that supported your education, but you owe time back after you graduate to the organization that provided you the scholarship. I was lucky I had the right people to take care of me at the right times to guide me, and I was in the right programs that got me exposure to the profession. (C1P9)

C2P5 expressed a desire to be exposed to the field earlier stating, “I do wish I had more exposure, such as capture the flag events, GenCyber Camps, and more, but I do not think they were being run three years ago. I may be wrong.” C3P6 explained, “We are also missing career and technical mentorship. There should be mentorship at all levels for both career and technical growth. When we look at mentorship, it is more career field focus.”

The findings indicated that exposure to technical mentors is highly important to foster interest and ensure the sustainability of females in cybersecurity. Mentorship is a significant tool
that participants believed would ameliorate the gender gap in cybersecurity. C1P10 noted that she became interested in the field through mentorship.

So, I went to undergrad, and I started by pursuing a computer science degree with programming, but I decided that was not for me. I had a mentor during an internship that introduced me to the information security world, who, by the way, was actually a woman. (C1P10)

C3P9 also shared her perspective on mentoring.

I think that we have to reach them [young females] well before they become adult females, such as in elementary and middle schools, so they have a desire to join the technical cyber workforce. I participate in volunteer organizations to get girls exposure to this career field early so that we can change the gender demographics in the future. (C3P9)

C1P2 suggested that developing more mentorship groups for women would help with hiring and retaining women. C1P5 is currently working within the profession but emphasized the importance of creating programs that provide mentorship to young females.

Develop more STEM-specific mentor programs at the grade school level and beyond. Bridge the gap between the STEM mentor programs and the government and private sector organizations that offer STEM employment opportunities. This could be done via internship or fellowship opportunities. As a leader in a cybersecurity organization, it is essential to reciprocate and mentor others. [Name redacted] fervently believes this and therefore mentors future cybersecurity professionals. In order to find good candidates, she mentors and tries to inspire and inform them about how exciting the cybersecurity profession is. She noticed at one of the earlier conferences I attended, DefCon, a major computer security conference, the presence of females was shockingly low. (C1P5)

C3P2 shared the following in support of mentorship.

My suggestion for keeping females in a field is two parts. They need to see other females leading and advancing in that field. We need to provide support for helping them in this field via mentoring and allowing them to grow in this field. (C3P2)

As part of the discussion of mentorship, C3P9 stated, “developing relationships with other females in senior leadership that can develop into a mentorship to help cultivate the next group of emerging leaders is important.” C1P11 also offered a suggestion.
I would encourage them to join a women’s technical professional society and offer to pay the dues. I would also set up mentors that are other females within the company to help them grow and address issues that senior experts might have good advice about how to handle difficulties in a professional manner to create change. (C1P11)

At least one participant expressed that most of the mentors in her career were men and that females in her profession perceive her as competition. C1P3 shared her perspective.

Females should support females. Don’t compete. I think it is important for females to have technical mentors that are females as well. In my case, as I mentioned earlier, mine were predominately male. There are programs such as Cyber Patriots and Girls Who Code who I have made time in the past to support. This allows young ladies to see people that look like them doing these things. These things create a supportive community. I also encourage other females to seek out opportunities and stay plugged into mentor groups. (C1P3)

C1P7 offered feedback on mentorship as a way to retain women in cybersecurity.

For organizations looking to retain more women, I suggest having one-on-one sessions. Have people feel comfortable. Take care of the little problems early so they don’t turn into big problems later. Always talk and encourage the STEM workforce no matter what they look like. Seek out people to mentor. I always make time to mentor other people. For the women working in the field, don’t be afraid to ask for help. Asking for help doesn’t make you look weak. (C1P7)

C3P8 provided an overall assessment of his organization’s efforts to support mentorship and a positive environment for females working in cybersecurity.

I think the organization that I work for is doing a good job to try and steer in that direction of diversity and hiring more women, but they are not there yet. I think they should get a cybersecurity professor in the community and have women working in cyber go back out and mentor other young women. Then you got the young women interested, so what’s next? There needs to be another program or equivalent to support women while they are getting their education and studying this profession. I think this would help produce a more positive workforce. (C3P8)

**Theme 5.** The fifth and final theme was that most cybersecurity hiring managers, academic professors, and professional peers are male. The majority of participants shared experiences of being taught and interviewed by male colleagues within a predominantly male community. Several assumptions tentatively explain the minimal number of females in the U.S.
cybersecurity workforce. One assumption is that the high number of males in the field discourage females from entering the field. While gathering data across all three cases, it was apparent that a significant number of hiring managers, work peers, job candidates, academic classmates, and academic professors in the cybersecurity field were male.

All 10 of the hiring managers interviewed indicated that most of their applicants and interviewees have been male. C3P6 shared the following response.

I would say that the applicant pool was 80 to 90% males. In some cases, I could be responsible for reviewing 200 resumes at a time, and they were 80% male. I am usually looking for both computer scientists and personnel for cybersecurity. When I was a recruiter for one organization, preference went to veterans, and most female applicants were not veterans. But because I don’t see resumes from female applicants very often, I try to look closer at the female applicants. The lack of female applicants is also reflective of the actual workforce among those that work in the cybersecurity profession. Not only is it obvious that the number of females in these offices is low, but in some cases, the morale is also bad. (C3P6)

C1P4 noted the following.

Given the ratio of men to females within the career field, I believe there is either an unconscious or conscious bias. I can’t speak to one’s intent. Or, there is a higher standard placed on females. The technical career field is a “man’s” domain. (C1P4)

Females working in the profession described a gender imbalance in their offices and cybersecurity classes. When describing the gender distribution among applicants and the current workforce, C3P3 stated,

I would say the applicants are mostly male 70%, to 30% females. For those that currently work for me, I would say for every five males, there are two females. I am not sure of the overall number of our organization.

C3P4 estimated that about 95% of the applicants received are male.

I would say for every 20 men there is one woman. I think this could have been due to the location on the West Coast. On the East Coast, there are more programs that encourage entry into the cybersecurity profession. Also, these applicants are all current college students. I am not sure if that matters, but just so you know. (C3P4)
When asked to describe the cybersecurity applicant pool, C3P7 stated,

The applicants that make it past the initial phase are more STEM-focused. I have recruited on both the East and the West Coast. In both regions, men are the bulk of applicants; on the West Coast, the split is about 60% men and 40% females. On the east coast, it is about 80% men and 20% females.

C3P8 shared a similar experience of gender imbalance in the applicant pool of cybersecurity professionals.

For the past six years, my applicant pool is predominantly males; I would say 80% male and 20% females. I don’t have the exact numbers, but the majority are definitely males. When I do see a female applicant, they have been very technical and very qualified. They come well-prepared. (C3P8)

Male dominance does not only exist in the application pool but also in the workplace.

The female cybersecurity professionals described their workplaces as noninclusive, dismissive, unfair, and uncomfortable.

Currently, I am on a team of 19, and two are females, myself and another lady. I would say morale is pretty bad in general. I am new to the shop and have ideas to fix on-going and reoccurring issues, but every time I make a suggestion, it is shot down immediately. We had another female on the team, and she was treated very unprofessionally. She was harassed daily, and one of the men on our team would move things on her desk and power down her workstation. She was singled out, and the behavior of the male colleague was excused, and eventually, when she had enough and retaliated, she was fired on the spot. The females are expected to be treated in a disrespectful way, and if you complain, then you are labeled as a troublemaker. It isn’t right, and I don’t even think it is legal, yet I have seen it many times over the 18 years with my employer at the same location. (C1P11)

Another participant shared her experience of working with peers that would try to make female counterparts feel comfortable.

The culture in every office was a “good old boys” network. It was when I did research and was a malware analyst. I also worked in offensive security and was the only woman at that time. People tried to do things to make you feel comfortable. But they should not have had to. I am not sure of the exact numbers, but there were very few females in my other technical offices. In one work role, in particular, it was very intense and stressful for all that went through it for both men and females. In my continual learning for these advanced technical jobs, none of the instructors were females. I later moved offices, and
the morale of this office was different. I was able to earn the respect of peers because of how I scored and ranked in that highly technical training. Once I went back to the office, again there was no expectation in the office from females. (C1P1)

C1P2 shared that she felt female leaders were not included at the forefront of the leadership planning and organization of task assignment.

I had a situation where one time in creating teams for a team project...no females were selected to be the team leader for the project. I found that odd...the professor set the teams, things like that. Every single day, I feel like I have to prove my work ethic and experience in my current role. I don’t expect anything to be handed to me, but what I do expect is the same respect and integrity that I give to my counterparts beyond gender and race. (C1P2)

C1P3 stated,

My organization provided a good platform of equality in this field itself but not in the actual role I was doing, which was very hands-on technical. I was the only woman or person around me in my unit doing it. It was different when I got to one of my offices, I was the only woman, and the team was given pep talks on how they would have to do things differently because there would now be a woman on the team. I would say it was about one woman for every 30 men. As a cyber operator, there were not many females across different teams as well. A lot of females shy away from these jobs because of parent and family duties. I have, in many cases, been the only woman in classes, training, and on a day-to-day basis. This environment has been most males, white males.

C1P5 also described her experience.

I can say that I am the only black female among eight white males on my immediate team, and I have questioned whether I have been discriminated against due to my gender and race when it comes to the assignment or task or credibility of knowledge. (C1P5)

While all female participants working in the cybersecurity profession agreed that they work in a predominantly male career field and were typically one of several females on the team, several experienced more diverse teams when changing organizations or work roles. C1P9 expressed two different experiences based on whom she was associated with.

In the public sector, there was not a good gender balance on technical teams, but when I switched to the private sector, there were more diverse teams. In most of my private sector organizations, the morale was good. The public sector was stressful for me. I think
it was because of what was at stake and the mission that was being worked. The males were very opinionated and arrogant, typically technical white males. When you speak up, you are complaining, and then that’s when they say females are putting their emotion into it. I was emotionally stressed in one of my private sector jobs. (C1P9)

C1P9 left the government and went to work in private industry where the atmosphere was much better, and the culture was very different from her experiences in the public sector. While she still had to prove herself in the private organization and there was definitely a “good old boys” network, C1P9 noted that there were more females in the private sector office. C1P9 described these individuals as “females that were actually technical.” In CIP9’s experience, while most males in the private sector were humble, most males in the public sector remained arrogant.

Male dominance in the cybersecurity profession does not merely emerge in the workplace or the hiring process. Male dominance is also highly prevalent in technology classrooms, and this presents a challenge to females’ ability to obtain cybersecurity degrees and associated STEM degrees. C2P7 shared her experiences in male-dominated classrooms.

In class, it’s kind of a do-it-yourself. Asking help around my peers was a bit difficult. Sometimes I wouldn’t even get help, and I would have to ask the TA or make time out of my busy schedule to go to office hours. Being a woman in this profession is kind of hard, especially when the class is mostly male dominant. For certain, I could feel the tension in the air and sometimes would even get surprised faces when I enter the room. Despite that, it’s just going forward with my degree. The general education classes are challenging, but overall, it helps improve my skill in programming and eventually getting myself into security electives. (C2P7)

C2P1 shared that while she pursued her degree, there did not appear to be significant gender diversity among faculty or students.

I hadn’t/haven’t found a gender balance. I always have (and continue) to find myself either the other female in the room. Even with my professors, the computer science department is male-dominated. There were many times I wanted to change my major and pursue a different career because I felt overwhelmed. But I had a female professor that told me that quitting or changing was not an option. (C2P1)
C2P3 shared a similar experience.

Typically, when I was in IT classes, it was just me. I would turn around, and they were all male. As I started switching to cybersecurity classes specifically, I am on a team that is more diverse, and there are more females too. (C2P3)

C2P5 also recounted a similar experience at the university she attends.

My major, the competitions, etc., are dominantly male. In RC3, there were at most five girls that actively participated within the club. For the red vs. blue competitions and the CTFs [capture the flags], I was frequently the only girl on the team. The instructors at my school are also dominantly male. I know that we have three female instructors. I was also the only girl on the CCDC [Collegiate Cyber Defense Competition] team, and that has been the “tradition” or “norm” for every CCDC team. (C2P5)

C2P10 provided a different view than the other participants, she shared a mixed experience regarding the gender divide.

My professors for these classes have all been male, but I have had female instructors and teaching assistants. Most students in my classes are male, but there are quite a few female students also in my classes. I would say it may be more around 60/40, where the majority more male. (C2P10)

C2P9 stated that out of a class size of 30 to 40 people, there are usually two females in her cybersecurity class. This was only in her cybersecurity courses. In those courses, all but one of her professors were male. C1P8 was unable to identify a female professor in undergraduate or graduate school where she studied computer science. During her time in the field she has seen growth in the career field and the course room, but she still considered it to be a male-dominated field.

When I first started in the IT world, I was usually the only female. If there were any other women, it was very few. As the years went by and as I obtained my master’s degree, there were definitely more females, but still not a lot. Some classes still only had one or two females. Same with conferences. It has gotten better with the number of females, but males still dominate. (C1P8)
C1P8 described her challenges due to her work environment being male dominant. She noted that at her workplace she felt constantly challenged and as though she had to prove herself.

Most people I won over by fixing their issues efficiently and with a nice, pleasant attitude unlike some of the cocky males I worked with. I could tell when people thought because I was a woman, that I wouldn’t be as knowledgeable as a male in my field, so I would have to show them or prove them wrong. (C1P8)

Summary

Chapter 4 provided detailed information about how the research method was applied to the data analysis portion of this study. Chapter 4 also identified and described themes within the data. A multiple-case study approach was applied to seek in-depth insights from participants who have been directly impacted by the problem and to gather data from 31 participants. The findings for each case were individually analyzed to identify themes within each of the three cases. A cross-case analysis helped to develop a holistic perspective of the problem based on multiple case sources (Baxter & Jack, 2008). Data triangulation through the cross-case analysis provided a robust perspective of the phenomenon. The results of this analysis included five emergent themes. The next chapter assesses those themes in relation to the research questions, and it presents recommendations for future studies.
CHAPTER 5. DISCUSSION, IMPLICATIONS, RECOMMENDATIONS

Females are significantly underrepresented in the field of cybersecurity, holding less than 15% of cybersecurity-related jobs in the United States (Rowland et al., 2018). This study was conducted to answer the overarching question, which asked, “why is there a disproportionately low representation of female workers in the U.S. cybersecurity industry?” A multiple-case study approach allowed for an examination of the phenomenon through three lenses: (a) females seeking entry into the profession, (b) females working within the profession, and (c) hiring managers within the profession. The distinct cases provided various perspectives to identify (a) the factors that contribute to interest, development, and sustainability of females in the cybersecurity workforce; (b) the criteria applied when recruiting, hiring, and retaining female cybersecurity professionals; and (c) how increased representation of females contributes to an organization.

Chapter 1 of this study introduced the problem and research questions to the reader. Chapter 2 provided a robust review of the literature concerning the phenomenon. Chapter 3 offered a detailed description of the methodology, and Chapter 4 presented the data analysis and findings. Chapter 5 presents a summary of the study, discusses the results of the data presented in Chapter 4, and provides recommendations for future research that may supplement these results. Chapter 5 addresses the following elements: (a) summary of the results (b) discussion of results, (c) conclusions based on the results, (d) study limitations and implications, and (e) recommendations for future research.

Summary of the Results

The purpose of this qualitative multiple-case study was to explore the underrepresentation of females in the U.S cybersecurity workforce. This multiple-case study
explored a single overarching research question, which asked, “Why is there a disproportionately low representation of female workers in the U.S. cybersecurity industry?” Three subquestions addressed relevant aspects of the overarching research question.

**Subquestion 1.** What factors contribute to the interest, development, and sustainability of female employees in the U.S. cybersecurity career field?

**Subquestion 2.** What criteria are currently applied by hiring managers for recruiting, hiring, and retaining female cybersecurity professionals in the United States?

**Subquestion 3.** How might the increased representation of female cybersecurity professionals contribute to an organization?

The overarching research question and subquestions were answered by analyzing data collected from participants of this study. A review of scholarly literature aided in the data analysis process by identifying the factors that contribute to the low number of females in the cybersecurity profession, the factors that contribute to female interest in the cybersecurity profession as a career choice, and how to increase the number of females in the profession may impact it (Caldwell, 2013; Cobb, 2018; Raytheon, 2015; Reed et al., 2017; Williamson & Tranter, 2017). The researcher then explored these same aspects through the lived experiences of 31 participants connected to the cybersecurity career field through their academic studies or professional employment. The data collected through the semistructured, in-depth interviews with the 31 participants were examined through the lens of social identity theory to develop additional theoretical insights. The use of a multiple-case study and multiple data sources enriched the understanding of the results from the data collected (Patton, 2015).

The within-case analyses reinforced the necessity of developing a diverse cybersecurity workforce, recruiting more females into cybersecurity, and exposing females to the cybersecurity
profession early. Each participant concurred that the cybersecurity profession has not been successful in promoting gender equity and inaccurate portrayals of the profession continue to influence females seeking entry into the profession. Research indicates that after entering the profession, females face several obstacles that impact their desire to remain in the profession (Reed et al., 2017). Participants from Case 1 noted that they sometimes questioned their decision to continue to work as cybersecurity professionals. Additionally, participants from all three cases agreed that to increase female interest in the profession, exposure to cybersecurity education and involvement must start before a female is in college.

The overall results of this study demonstrated that females are significantly underrepresented in the cybersecurity profession, and several changes must be implemented to close the gender gap in this profession. Five themes emerged from the results of this study. The first theme indicated that confidence is unequally exhibited, projected, and perceived among females and males in the cybersecurity profession. The second theme uncovered stereotypes and biases tied to gender and clarified that these negative perceptions directly impacted the cybersecurity profession. The third theme demonstrated the marketing images and terminology used to attracted cybersecurity professional into the career field are not designed to be gender inclusive. The fourth theme illustrated that early exposure to cybersecurity skills and professionals that young females can relate to is key to increasing female interest in the field. The fifth and final theme indicated that males are the primary holders of various gateway positions that lead into the cybersecurity profession (e.g., hiring managers, academic professors, and peers in both academia and the workplace). The next section presents a discussion of these five themes.
After uncovering the present study’s five themes and analyzing previous literature, the insights gained into the phenomenon were used to assess how the social identity theory aligned with the study’s findings. The application of social identity theory aided in uncovering possible reasons for the lack of females in the cybersecurity profession. The research found that several similarities indicate that females are not part of the intergroup. Instead, females represent an outgroup as it relates to normalized gender representation and attributes in the cybersecurity profession (Tellhed & Jansson, 2018). The conclusion section of this chapter elaborates on these insights.

**Discussion of the Results**

Across all three cases, participants recognized cybersecurity as a complex career field where diversity improves professionals’ abilities to solve difficult problems. This finding supported existing literature. Furnell et al. (2017) noted that many diverse backgrounds are necessary for both nontechnical and technical cybersecurity roles. Unfortunately, Beninger (2014) noted that gender diversity within the cybersecurity profession remains stagnant despite new females entering the field every year. One explanation of the failure to increase female representation in cybersecurity positions is that females exit the field at the same rate at which they enter the field, and the two numbers to offset one another (Williamson & Tranter, 2017). Many of the participants noted they felt as though they were entering a field that was presently suboptimal in terms of its appeal to women, but the participants expressed a desire that cybersecurity would become a field where females could thrive. The cross-case analysis revealed five themes that provided insight into the problem identified. Those five themes answered the research questions. The following subsections discuss the application of those themes in the context of the subquestions.
Subquestion 1

The first subquestion asked, “what factors contribute to the interest, development, and sustainability of female employees in the U.S. cybersecurity career field?” The results of this study indicated that all five themes applied to Subquestion 1. These themes were related to the importance of confidence, gender stereotypes and biases, the absence of gender-inclusive marketing images, early exposure to cybersecurity skills, and the overrepresentation of males in positions of authority within the profession. The first theme that applied was Theme 1, that confidence is unequally exhibited, projected, and perceived among females and males. Some participants inadvertently entered the cybersecurity profession, but most female participants indicated that a sense of self-confidence and intentionality was a factor in the decision to pursue cybersecurity careers. Participants also indicated that the rewarding nature of challenging careers, day-to-day changes in job activities, innovation and interest, enjoyment of problem-solving, and self-identification as a lifetime learner constituted factors that drew them to cybersecurity. In the context of confidence, several participants currently seeking entry into the profession shared their preference for working under confident and knowledgeable supervisors.

Theme 2 also addressed Subquestion 1. Theme 2 highlighted the effects of gender stereotypes and biases. Several female participants expressed that they did not have comfortable and welcoming work experiences. This finding aligned with the standard experiences of females working in cybersecurity, as cited in the literature (Beninger, 2014; Ashare, 2017). In one study, over 50% of females described their experiences working in the cybersecurity profession included discrimination, sexism, and tokenism (Reed et al., 2017). Thus, stereotyping and gender bias was a negative factor affecting females’ interest, development, and sustainability within the industry.
The third theme involved the lack of gender inclusivity within marketing images and terminology used in the cybersecurity profession. The participants noted that the lack of advertising featuring women in cybersecurity roles was disappointing and highlighted the gender disparity. Many participants indicated that if the cybersecurity profession was marketed more strongly toward females that it would likely increase the numbers of women entering the field. Additionally, participants noted that when marketing materials failed to include a mix of males and females, it reinforced the stereotype that cybersecurity is a field for males only.

Theme 4 highlighted the need for early exposure for young females to cybersecurity skills, mentors, and experiences and directly related to Subquestion 1. Many participants indicated that exposure to cybersecurity events and activities at the elementary school level made a significant difference in perceptions about the attractiveness of the profession. Participants cited positive experiences at cyber camps and capture the flag events. Participants also noted the impact mentors could have on young females exploring their interest in STEM and cybersecurity. As a result, it was clear that early exposure to the field was a critical factor in females’ interest, development, and sustainability in the field of cybersecurity.

The fifth and final theme addressed the overrepresentation of males in positions of authority (e.g., hiring managers, academic professors, and senior professionals). Surprise among males in these positions when females show interest in cybersecurity can cause an uncomfortable learning or working environment. This sense of alienation or isolation can, in some cases, discourage females from pursuing a degree or work within the cybersecurity profession. Several the female participants across the 21 female participants shared that they believe increased gender balance in the cybersecurity profession would foster better morale in the workplace and allow females to see a future for themselves in the organizations where they work.
Subquestion 2

The second subquestion asked, “what criteria are currently applied by hiring managers for recruiting, hiring, and retaining female cybersecurity professionals in the United States?” Ten hiring managers that hire cybersecurity professionals were interviewed to gain insight on what criteria are used to recruit, hire, and retain female cybersecurity professionals in their respective organizations. Data were gathered on participants’ recruitment processes, applicant pools, hiring challenges, and the skills required for cybersecurity professionals to address Subquestion 2. Female participants currently working in the profession and those seeking entry into the profession were also asked to provide additional context by sharing how they felt hiring managers and organizations could best approach improving the recruitment and retention processes. Again, all five themes related to Subquestion 2 to some extent.

A variety of skills are necessary for the cybersecurity profession, and these skills vary based on the specific work role and the organization (Dawson & Thomson, 2018; Vogel, 2016). Several hiring managers wanted candidates that were confident and motivated to learn. This observation linked directly to Theme 1 that male and female cybersecurity professionals exhibit confidence differently. Participants in Case 3 required male and female cybersecurity professionals to exhibit the same general qualifications and skillsets. Participants in Case 3 also shared a variety of unique skills ranging from strong soft skills to specific technical skills that they desire in a participant.

Participants in Case 3 indicated that hiring managers seek candidates that possess specific technical skills including an adequate understanding of programming languages, networking, operating systems, core computer science principles, network architecture, and network traffic analysis. Participants in Case 3 also listed effective oral and written communication, self-
confidence, the ability to think critically and handle complex ideas, intrinsic motivation, and the ability to retain knowledge as vital soft skills. Case 3 participants noted that while employers did not require certifications and degree specification, technical certifications and STEM-related degrees are excellent credentials for a candidate to have.

In the required skill and qualification categories, Case 3 participants referred to male and female cybersecurity candidates equally, but when discussing confidence, these participants noted that differences existed between males and females. The participants that worked as hiring managers observed that during the hiring process, female candidates often displayed less confidence compared to male candidates. Participants in Case 3 noted that the lack of confidence was not necessarily an insurmountable barrier as confidence could be learned. Participants in Case 3 noted that because of their preparation before job interviews, female candidates were generally attractive hiring prospects.

The four remaining themes also related to Subquestion 2 to a lesser extent. In the context of Theme 2 participants from Case 1 indicated that they often felt that, as females, they were required to overcome gender stereotypes and biases during the hiring process. Participants in Cases 1 and 2 felt that they were required to prove their skills and knowledge to a greater extent than male candidates for cybersecurity positions. This finding aligned with the observation from Kay et al. (2012) that organizations to adjust how they search for cybersecurity professionals to fill positions to ensure that it is fair to both male and female candidates.

The relationship between Theme 3 and the second subquestion was less direct but still worth noting. Theme 3 addressed the fact that marketing images and terminology are not gender-inclusive. Feedback from participants in Case 2 who were seeking entry into the cybersecurity profession indicated that the existing gender bias did impact the hiring process. Participants in
Cases 1 and 2 did not indicate that the hiring criteria used by organizations were discriminatory, but they did observe that aspects of the hiring process could be perceived differently by males and females, and these differences in perceptions contribute to the gender gap. This finding supported research findings by Weber (2011), Mohr (2014), and Peacock and Irons (2017).

The fifth theme offered similar insights when evaluating the hiring process. Participants in Cases 1 and 2 noted that most hiring managers, academic professors, and professional peers are male. When applied to the hiring process, Theme 5 meant that females have fewer opportunities to engage in gender-based networking, and several candidates used the phrase *good old boys’ network.* As with the gender bias inherent in the marketing materials, the disproportionate number of males in decision-making positions meant that female cybersecurity candidates did not see representative role models and at times had to overcome stereotypes and bias when applying for cybersecurity positions. Hiring managers, like many people, unconsciously gravitate toward groups with which they identify, and research indicates that females hire females 50% of the time, whereas males hire females less than 40% of the time (Coffman et al., 2018).

Finally, Theme 4 represented participants’ hope for the future when applied in the context of Subquestion 2. Theme 4 centered on the participants’ belief that early exposure to cybersecurity skills was key to increasing female interest and representation in the field of cybersecurity. Participants indicated that reaching females at an early age through school-related activities was key to improving the numbers of females applying for cybersecurity jobs. This observation aligned with previous work by Barsh and Yee (2011) and Weingarten and Garcia (2016) that addressed the need for more female representation in the candidate pipeline. The present study’s participants believed that fostering an interest in cybersecurity among girls at an
early age would positively impact the number of females hired and retained in the cybersecurity profession.

**Subquestion 3**

The third subquestion asked, “how might the increased representation of female cybersecurity professionals contribute to an organization?” Two themes directly addressed this subquestion, Theme 2 and Theme 5. Theme 2 centered on the participants’ belief that gender stereotypes and biases contribute to the gender gap in the cybersecurity profession, and Theme 5 indicated that the majority of hiring managers, academic professors, and cybersecurity professionals are male. Both of these themes address the issue of diversity. An increase in females in the cybersecurity profession will increase gender diversity in the field, as less than 15% of cybersecurity professionals in the U.S. workforce are females, even though there are more than 200,000 available job openings in the cybersecurity profession (Rowland et al., 2018).

Participants indicated that the lack of female hiring managers, academic professors, and cybersecurity professionals was detrimental to both the cybersecurity field and to organizations relying on cybersecurity professionals. The lack of females in these senior positions meant that females could sometimes be discouraged from perceiving cybersecurity as a potential career path. Thus, the lack of diversity within the field of cybersecurity constituted a self-perpetuating cycle, and the participants focused on the importance of diversity in these senior positions.

Diversity was discussed with all 31 participants to gain insights into the role of diversity in the cybersecurity profession. All 31 participants acknowledged that diversity was important to any workplace, not just to the field of cybersecurity. The participants explained that diversity impacts decision-making and problem-solving based on the composition of work teams and organizational leadership. Participants shared some specific examples where diversity had
improved outcomes, including the ability to develop new technical concepts and being mindful of the fact that individuals of all races, genders, and ages may need to use a newly developed piece of technology. As one participant stated, a lack of diversity may cause an organization to lose market share by excluding groups who could be a major consumer of their product.

Diversity impacts an organization in a major way. It impacts how decisions are made and how things are created. Take artificial intelligence for instance. In the past 10 years automatic sinks. The sinks did not recognize people of color, it wasn’t designed to recognize the pigmentation of dark skin to cut on, so they kept having issues. Not having diverse teams can cause you to lose market share value. (C1P1)

Previous literature shows that gender diversity boosts the productivity of teams and increases an organization’s ability to solve hard problems within a short time frame (Hunt, Price, Dixon-Fyle, & Yee, 2018). Gender diversity is not the only strategy to diversify a team, but it is among the core beliefs that the cybersecurity profession lacks. Increasing the number of female cybersecurity professionals will improve gender diversity. Diversity in the cybersecurity workforce is an important consideration as diverse teams are more efficient when solving problems (Reynolds & Lewis, 2017).

**Conclusions Based on the Results**

**Comparison of Findings with Theoretical Framework and Previous Literature**

The conclusions from this study align with previous literature concerning the underrepresentation of females in the cybersecurity profession. The conceptual framework in Chapter 2 utilized social identity theory to explain why so few females pursue cybersecurity and STEM degrees. Additionally, previous literature highlighted that addressing the gender gap in the U.S. cybersecurity profession would significantly alleviate job demand (Caldwell, 2013). Based on the participants’ experiences, females are indeed underrepresented in the U.S. cybersecurity workforce. Females also encounter specific challenges within the profession and
When seeking to enter the profession. Hiring managers face challenges in recruiting diverse talent to fill existing positions. These observations all support the need for intervention to address the lingering gender gap in the U.S. cybersecurity workforce. This section contains a comparison of the five themes that emerged from the data analysis with previous literature and the study’s theoretical framework.

When comparing the present study’s findings to the theoretical framework and previous literature, it is necessary to examine the themes that emerged from the cross-case analysis. Theme 1 indicated that confidence is unequally exhibited, projected, and perceived among females and males in the cybersecurity profession. This finding was in alignment with previous research by Mayo (2016), Cuddy et al. (2008), Guillen (2018), and Mohr (2014). Mohr (2014) noted that females are much less likely to apply for positions where they may not be completely qualified, whereas males are much more likely to apply for positions for which they are only partially qualified. Mohr’s finding, combined with the results of the present study, partially explain why there are significantly fewer females in the cybersecurity profession compared to males.

Theme 2 indicated that gender stereotypes and biases impact the cybersecurity profession. Many scholars have noted the presence of stereotypes in the field of cybersecurity. McBrearty and Wainwright (2013) cited stereotypes about nerdiness and the need for advanced skill sets even in entry-level positions. Cuddy et al. (2008) and Haines et al. (2016) both addressed the stereotype that females exhibit more warmth than males. Weingarten and Garcia (2016) even noted that there is a stereotype that cybersecurity is a profession that is exclusive to young, white males that code. Corbett and Hill (2015) also noted that stereotypes and biases cause hiring managers to hire male candidates over female candidates regardless of whether the
female holds superior qualifications. These stereotypes serve as barriers to entry for females, and the participants in the present study indicated that these stereotypes must be overcome to be successful as a female in the cybersecurity profession.

Theme 3 was that marketing images and terminology used for the cybersecurity profession are not gender-inclusive. Theme 3 was in alignment with research by Dallaway (2016), Kaspersky (2017), and Williamson and Tranter (2017). The participants in the present study noted that the lack of representation in marketing materials related to cybersecurity negative impacted young females as they could not see themselves in those positions based on the way cybersecurity was portrayed in the media. Other scholars have not extensively studied the level of gender bias in cybersecurity marketing materials, but based on the present participants’ feedback, this is an issue that should receive further attention.

Theme 4 indicated that early exposure to cybersecurity skills and professionals that females can identify with might increase female interest in the field. Kaspersky (2017) asserted that the lack of female role models was the primary reason for the gender gap in cybersecurity. Many participants recounted their early exposure to cybersecurity as an important element in the formation of their career goals. An added benefit of early mentorship programs is that it provides young females with early opportunities to network. Krivkovich et al. (2017) noted the importance of early mentorship and networking opportunities, a point which was also supported strongly in the present participants’ interview responses.

Finally, Theme 5 was that males hold most manager positions, academic professor roles, and mentor roles in the cybersecurity field. Several participants indicated that the male-dominated nature of the cybersecurity industry presented a barrier to entry into the field, and this observation was supported by previous literature. Born et al. (2018) and Martin and Barnard
(2013) both asserted that it can be very difficult for females to navigate advancement opportunities in male-dominated occupations. The overrepresentation of males in positions of authority can also reinforce preexisting biases and stereotypes (Dallaway, 2016; Peacock & Irons, 2017). For these reasons, many participants felt it was necessary to provide mentoring opportunities to younger females and promote networking activities that help females advance in the field of cybersecurity.

The findings from this study suggest that all stakeholders must actively work together to close the gender gap in cybersecurity. An increased presence of females in the cybersecurity profession would provide a more robust pipeline of candidates for hiring managers and better opportunities for females to enter executive leadership levels in organizations. The lack of female presence in these roles may also contribute to the lack of females in the profession. Most of the participants indicated that their interviewers or supervisors were male. While this section compared the present study’s findings to the theoretical framework of social identity theory, the following section examines alternative explanations for the study’s findings.

**Interpretation of the Findings**

When examining Theme 1, the data from this study highlights females’ lack of confidence during the interview processes and in their ability to perform in the cybersecurity profession. Participants’ responses indicated that confidence is highly necessary both for females seeking to enter the cybersecurity profession and for supervisors within the cybersecurity profession. Female cybersecurity professionals in this study encouraged their peers and future female cybersecurity professionals to be confident and prepared to work harder than their male peers. Females’ lack of confidence has been attributed to the limited success females have

The impostor syndrome was first introduced in the 1970s by Clance and Imes (1978). Clance and Imes (1978) explained the impostor syndrome as a female’s inability to feel comfortable with her success and the fear that she could be revealed as incompetent at any moment. The participants who had worked as female cybersecurity professionals indicated they felt a need to prove themselves. These participants also highlighted low self-esteem and a desire to be validated by external entities as factors affecting their persistence in the cybersecurity profession. The feedback provided by participants echoed findings related to impostor syndrome noted by Sanford, Ross, Blake, and Cambiano (2015).

Theme 2 raised the issue of gender stereotypes and biases and how they impact the cybersecurity profession. Scholars have acknowledged that there is more to cybersecurity than hacking or technical skills (Von Solms & Van Niekerk, 2013). Participants in all three cases cited the importance of soft skills. Several participants noted a stereotype within the field of cybersecurity that females excel at soft skill jobs and the academic fields associated with soft skills, but males are better suited to technical cybersecurity roles. When females work in jobs that defy social norms, they experience discrimination and are made to feel that they do not belong (Agénor, 2018). Participants asserted that the issue of gender stereotyping must be rectified to ensure that females feel welcomed into the cybersecurity profession and sufficiently comfortable to remain in the profession.

One way in which gender stereotypes were perpetuated was through noninclusive marketing images and cybersecurity terminology. Theme 3 addressed the belief among most participants that the cybersecurity profession is not inclusive toward females. Participants noted
that many individuals subscribe to the stereotype that cybersecurity professionals are young, white, *geeky* males who play games incessantly. Participants highlighted the fact that females are rarely depicted on television and in job advertisements as cybersecurity professionals. Additionally, some participants asserted that the terminology used to describe cybersecurity does not thoroughly encapsulate the profession in a manner that attracts females.

The last two themes addressed early exposure to mentorship and balanced gender representation in roles of authority. Participants asserted that it was important for young females to have the ability to interact with female cyber professionals. Participants believed that increasing the number of female mentors, professors, and cybersecurity professionals would lead to better female representation in the profession. Limbago (2018) suggested that organizations seeking to increase the number of females in cybersecurity should provide appropriate role models. Limbago noted, “If they don’t see it, they won’t be it. Women must be visible and seen as experts” (para. 5).

Participants believed that the exposure of young females to mentoring opportunities within the profession could help foster female interest. This research demonstrated that females are attracted to roles in which they can see themselves. This specific finding aligned with existing literature. Veihmeyer, Doughtie, and Dayoan (2015) noted that “eight in 10 women (84%) reported that having positive leadership role models helped them feel confident about what they could accomplish in life” (p. 10). Based on the literature and the present study’s findings, female cybersecurity professionals should be provided with equal opportunities relative to their male counterparts.
Limitations

Several limitations must be acknowledged when examining the present study. One important limitation was associated with the inclusion and exclusion criteria of the sample. The age range for participants in Case 1 was limited to individuals between the ages of 21 and 40 years of age. When recruiting participants, the researcher identified many females who were interested in participating, but they were excluded because the individuals were over the age of 40. Most of these females indicated that they had changed their career paths or become interested in the cybersecurity profession late in life due to other life choices. This group could have potentially provided additional insights and offered a holistic perspective of the lack of females in this profession, but they were excluded to avoid injecting bias into the findings resulting from the participants’ previous work-related experiences.

This study was also limited based on the sample size. Interview data were gathered from 31 participants to explore the underrepresentation of females in the U.S. cybersecurity workforce. Thirty-one participants is a small sample relative to the number of people who work in the cybersecurity profession. While the participants hailed from various geographical regions in the United States, there was not sufficient data from any single region to categorize the experiences of participants based on geographical location. In qualitative research, a smaller sample set is used, increasing the depth of the analysis, but the use of a smaller sample size does diminish the breadth of the research (Trotter, 2012). An understanding of the phenomenon on a larger scale is critical so that the findings are not dismissed as merely the opinions of a few. Thus, the present study can be further validated by a larger quantitative study that is representative of the entire United States.
Another consideration that requires acknowledgment was the researcher’s direct relationship with the underrepresentation of females in the cybersecurity profession. The researcher is a female who currently works within the field of cybersecurity. Several precautionary measures were implemented to limit the potential for bias. These measures entailed using literature to confirm the problem and ensuring that the researcher’s personal experiences and biases did not influence the development of the conceptual framework or the data analysis process. Through bracketing and allowing participants to validate the data, the researcher ensured that the data was reliable.

Lastly, the use of in-depth interviews to understand the phenomenon constituted a weakness based on the participants’ lack of objectivity. One alternative to studying gender diversity within the field of cybersecurity would involve observing participants in the field. Witnessing participants in their natural element could provide another dimension to the factors that impact the underrepresentation on females in the U.S. cybersecurity workforce.

**Implications for Practice**

Valuable insights emerged based on the lived experiences of the participants in the three key cases. These insights directly related to the experiences of females in the U.S. cybersecurity profession and have practical implications for organizations seeking to improve gender diversity within cybersecurity teams. Figure 5 illustrates an overview of the themes identified in the study, and this section addresses the practical implications of those themes concerning recruitment, hiring, and retention of females in the cybersecurity profession.
Figure 5. Implications of the study’s findings.

Theme 1 indicated that males and females exhibited confidence differently in the context of cybersecurity. Organizations should view this difference not as a failure on the part of female candidates or cybersecurity professionals but as a strength. Many participants that worked as hiring managers noted that the difference in confidence levels often meant that female candidates spent more time preparing for interviews. Additionally, scholarly research demonstrates that diversity is an advantage within cybersecurity teams (Reynolds & Lewis, 2017; Rock & Grant, 2016). Thus, organizations should not use a single standard when filling cybersecurity positions. Instead, candidates should be evaluated based on their technical skills and knowledge as well as their ability to increase team diversity and contribute to improved team outcomes.
Theme 2 acknowledged the presence of gender-based stereotypes and biases in the field of cybersecurity. The primary implication of this finding is that more effort is needed to repudiate these biases and stereotypes. Dallaway (2016) and Peacock and Irons (2017) noted that the cultivation of stereotypes could be the result of a feedback loop, and to change this pattern, members of both the in-group (males) and the out-group (females) must work together to achieve change. Organizations and hiring managers must look beyond technical skills and consider how team diversity can positively impact an organization. In doing so, female representation on cybersecurity teams will increase, and organizational outcomes will improve.

Theme 3 acknowledged that the marketing images and terminology used in the cybersecurity profession are not gender-inclusive, and male-oriented marketing materials and terminology discourage some females from pursuing careers in cybersecurity. The primary implication for organizations and hiring managers is that marketing materials need to be gender neutral if the gender gap is to improve. Participants indicated that the male-oriented aspects of the cybersecurity profession could be off-putting, and many participants expressed a desire for female-friendly materials, terminology, and outreach programs. To address this theme, organizations should involve more female cybersecurity professionals in the design and development of programs and materials used to recruit new cybersecurity candidates. This implication was supported by previous research by Dallaway (2016) and Kaspersky (2017).

The fourth theme highlighted that early exposure to cybersecurity is key to fostering female interest in the field. Many participants recounted experiences they had as students that positively influenced their perception of the cybersecurity profession. As a result of this feedback, more programs should be developed to encourage young females to explore cybersecurity as a profession. Participants also recommended engaging in mentorship programs,
but it is important to note that if existing female cybersecurity professionals do not engage as mentors and volunteers, the number of available female mentors will remain low, which is a factor that relates to Theme 5 as well.

The fifth and final theme was that hiring managers, academic professors, and professionals within the cybersecurity discipline are predominantly male. This theme was supported extensively in the literature, and the demographic data on the numbers of males and females currently working in cybersecurity indicates a significant gender gap exists (Rowland et al., 2018; Setalvad, 2015). Because of the size of the gender gap, equal representation of males and females within the cybersecurity profession is difficult to achieve in the short term, but there are still measures that can be taken to improve female representation in senior positions or other positions with decision-making authority. Male hiring managers should review their actions for potential gender bias, male professors should review their use of gender-bias language, and male cybersecurity professionals should review their behavior to determine whether they contribute to the development of an inclusive work environment.

Making the cybersecurity industry more attractive to females will improve diversity and outcomes for a wide range of stakeholders. The practical implications and measures that can be undertaken to address the underrepresentation of females in the cybersecurity profession can help foster greater levels of diversity, but to do so, females must be convinced that the field of cybersecurity is welcoming to females and that females will receive the same level of welcome and acceptance as males. In addition to the practical implications, the findings from the study also resulted in recommendations for future research. Those recommendations are presented in the following section.
Recommendations for Further Research

The present study built upon previous research by Bagchi-Sen et al. (2010), Shumba et al. (2013), LeClair et al. (2014), Dodge et al. (2012), Gonzalez (2015), and Peacock and Irons (2017). The study incorporated necessary design limitations related to qualitative research, and recommendations can be made to address those limitations. One recommendation for future research based on the data derived from the study is to conduct a study that focuses on the male perspective of the phenomenon. While this study investigated the underrepresentation of females in cybersecurity through three different lenses, none of those lenses included the perspectives of male cybersecurity professionals. Understanding the male perspective of the gender balance within the cybersecurity profession could provide opportunities to compare and contrast male and female experiences.

A recommendation for future research that is derived from the research design would be to collect observational data instead of or in conjunction with qualitative interviews. The location for observation should be in the participants’ natural element (e.g., the classroom or at work). Directly observing participants in their natural element may assist the researcher in developing an in-depth understanding of the experience and environmental factors that surround females who are working in cybersecurity or pursuing a cybersecurity degree. The data collected in this study represents the subjective experiences of the participants. Through observation, it would be possible to gain a measure of objectivity when analyzing the phenomenon. This alternative lens may also allow researchers to identify additional environmental and social factors that impact the gender balance in the cybersecurity profession.

Another recommendation based on the limitations of the research design and methodology is to conduct a quantitative study to provide numerical evidence of the level of
interest, hiring, and retention of females working in cybersecurity. While qualitative data provides an in-depth understanding of a phenomenon, quantitative studies allow researchers to sample a larger group and measure relationships between variables. Surveying a larger group may identify cause and effect evidence explaining why the gender gap in cybersecurity exists. The development of a broader scale survey addressing gender disparities among cybersecurity professionals may also enable individual organizations to address the problem more effectively.

Lastly, while this study explored the gender deficit in the cybersecurity profession, no effort was made to examine race or age as contributing factors to the underrepresentation of women in cybersecurity positions. Some studies have indicated that minorities and Millennials are also underrepresented in the cybersecurity profession (McBrearty & Wainwright, 2013; Mohr, 2014). Millennials and minorities may be another untapped resource that could satisfy the growing demand for cybersecurity professionals. Future research concerning how to fill the growing demand for cybersecurity professionals should examine outreach to Millennials and minorities as part of the solution.

Conclusion

Cybersecurity is and has been a male-dominated field for the past decade (Dallaway, 2016; Peacock & Irons, 2017). Currently, less than 15% of U.S. cybersecurity professionals are female (Rowland et al., 2018). Furthermore, over 50% of females who work in the cybersecurity profession have experienced various types of discrimination (Reed et al., 2017). This study was conducted to explore the underrepresentation of females in the U.S. cybersecurity profession and identify the factors that contribute to the phenomenon.

Three distinct cases were examined as a part of this multiple-case study. The first case included 11 females currently working in the profession, the second case included 10 women
seeking entry into the profession, and the third case included 10 hiring managers responsible for hiring cybersecurity professionals. The three cases were bonded together by the lack of females in the U.S. cybersecurity profession. The multiple-case study approach yielded insights into the factors that drive females to study and enter the career field. Participants also offered a range of reasons for the underrepresentation of females in the cybersecurity profession, but five themes emerged from the cross-case analysis.

The first theme that emerged from the data was that confidence is unequally exhibited, projected, and perceived among females and males. The second theme that emerged from the data analysis was that gender stereotypes and biases impact the cybersecurity profession. The third theme that emerged from the data analysis was that marketing images and terminology used for the cybersecurity profession are not gender-inclusive. The fourth theme that emerged from the data analysis was that early exposure to cybersecurity skills and professionals that females can identify with may increase female interest in the field. The fifth and final theme that emerged from the data analysis was that males hold most manager positions, academic professor roles, and mentor roles in the cybersecurity field.

The existing literature demonstrates that organizations are unable to keep up with the growth and demands of cybersecurity and that the shortage of females in cybersecurity positions will continue to be a problem for years (Culbertson et al., 2017). The present study offers insights into the reasons for the gender imbalance and identifies potential measures that can be taken by practitioners and organizations seeking to encourage more females to enter the cybersecurity profession. Based on the feedback from the participants in the present study, the divide between the experiences of females and males in the cybersecurity profession begins early and continues throughout their career. Some of these differences are intentional while others are
not, and while diversity can have many benefits, discrimination and barriers to entry should be eliminated wherever possible. It is critical for academia, cybersecurity professionals, and cybersecurity organizations to collaborate to develop a holistic solution to the problem of the underrepresentation of females in the cybersecurity profession.
REFERENCES


Ellemers, N., Rink, F., Derks, B., & Ryan, M. K. (2012). Women in high places: When and why promoting women into top positions can harm them individually or as a group (and how


161


ISC2. (2017, June 01). Member count. Retrieved from https://www.isc2.org/About/Member-Counts


163


APPENDIX A. DEMOGRAPHIC QUESTIONNAIRE

Demographic Survey Questions

Q1. Gender: What is your gender?
   ☐ Males
   ☐ Female

Q2. Age: What is your current age?

   

Q3. Location: What city and state do you currently live or work in?

   

Q4. Which of the following groups do you belong to?
   ☐ Current student pursuing a career in the cybersecurity profession
   ☐ Currently working in the cybersecurity profession
   ☐ Current hiring manager/technical recruiter for the cybersecurity profession

Q5. Education/Discipline: What is the highest level of education you have COMPLETED? If applicable specify degree title? (e.g. Masters, Computer Science or High School)

   

Q6. If you are currently a student, enter degree you are pursuing and classification? (e.g. Information Technology, Sophomore or Cybersecurity, 2nd year graduate student or Information Security, 3rd year post graduate)

   

Q7. Occupation: What is your current job title? How many years of experience do you have in the given career field?

   

171