

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/329754528>

THE PERCEIVED IMPACT OF BARRIERS TO RETENTION ON WOMEN IN CYBERSECURITY

Thesis · November 2018

DOI: 10.13140/RG.2.2.13275.62244

CITATION

1

READS

611

1 author:



[Carl Willis-Ford](#)

University of Fairfax

1 PUBLICATION 1 CITATION

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



University of Fairfax DIA, topic area: gender diversity in cybersecurity [View project](#)

THE PERCEIVED IMPACT OF BARRIERS TO RETENTION ON WOMEN IN
CYBERSECURITY

by

Carl D. Willis-Ford

A Dissertation Submitted in Partial Fulfillment of the Requirements for the
Doctor of Information Assurance (DIA) Program

University of Fairfax

2018

COPYRIGHT STATEMENT

Copyright © 2018 Carl D. Willis-Ford

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or media, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the author.

Abstract

The Perceived Impact of Barriers to Retention on Women in Cybersecurity

by

Carl D. Willis-Ford

2018

The cybersecurity industry has a significant employment gap, with over 301,000 open jobs in the United States, up from 285,000 jobs in 2017 (Cybersecurity Supply and Demand Heat Map, n.d.). The unfilled positions span the country and the spectrum of cybersecurity work. At the same time, the cybersecurity industry has a gender gap, with women making up only 10-15% of the United States cybersecurity workforce while making up about 50% of the general workforce (LeClair, Shih, & Abraham, 2014). One of the reasons for the low representation of women in the cybersecurity workforce is that the retention rate of women in these fields is significantly lower than the retention rate of men (LeClair, et al., 2014). This study will be used to investigate factors that may impact a woman's decision to stay in the cybersecurity industry, including lack of mentorship, Impostor Phenomenon, and hostile work environment. Respondents will assess the perceived impact of these retention barriers on the desire to stay in the cybersecurity industry. Results of this study present evidence that the selected barriers to retention are noteworthy and that significant relationships exist between some demographic factors

and the perceived impact Impostor Syndrome on retention of women in the cybersecurity industry. Additionally, a significant relationship was found between the composite perceived impact of the retention barriers and the demographic *time working in the cybersecurity industry*.

Dedication

To my wife and best friend, Brenda, who has always believed and supported me in my decades-long academic journey. From the 18 years it took for my bachelor's degree, through both master's programs, and now the doctorate, she has been unwavering in her 'you can do it' message.

Also, to my sons, Christopher and Geoffrey, who helped me to remember to keep my sense of humor and not take everything so seriously.

Lastly, to my grandkids, Nora and Jack, who illuminate my life with their curiosity and energy.

Acknowledgements

This dissertation would not have been possible without the encouragement and support of a multitude of mentors, faculty, peers, friends, and family. I am very grateful to Dr. Hargiss for her patience and guidance on the path as my academic advisor and committee chair.

To Dr. John Bordeaux, who first told me, 'Sure, you can do it.'

A large thank-you goes out to my colleagues at work, who provided significant support and helped keep things rolling when I had to be focused on school.

To my myriad Facebook friends – thanks for the positive thoughts and supportive posts – they really did help!

Lastly, thanks to my family, and especially my wonderful wife, who had to listen to me as I excitedly explained my research concept over and over and over to pretty much anyone that would listen.

Table of Contents

List of Tables.....	xiii
List of Figures.....	xiv
Chapter 1: Rationale	1
1.1 Introduction.....	1
1.2 Background of the Study	2
1.3 Problem Statement.....	5
1.4 Purpose of the Study.....	6
1.5 Significance of the Study.....	7
1.6 Rationale	8
1.7 Nature of the Study.....	9
1.8 Research Questions.....	10
1.9 Research Hypotheses	12
1.10 Conceptual Framework.....	13
1.11 Assumptions and Limitations.....	16
1.11.1 Assumptions.....	16
1.11.2 Limitations	17
1.11.3 Delimitations.....	18
1.12 Summary.....	18
1.12.1 Organization of the remainder of the study	18

Chapter 2: Research Review and Synthesis.....	21
2.1 Process Overview.....	22
2.2 Historical Context.....	23
2.3 Cybersecurity Industry Employment	26
2.4 Women in Cybersecurity.....	28
2.5 Pipeline	28
2.5.1 Awareness of industry	29
2.5.2 Industry image	30
2.5.3 Cyber competitions	32
2.5.4 Lack of mentors	33
2.6 Retention.....	33
2.7 Independent Variables.....	35
2.7.1 Time working in the cybersecurity industry	35
2.7.2 Current position level.....	37
2.7.3 NICE cybersecurity workforce framework category.....	38
2.8 Dependent Variables	40
2.8.1 Lack of mentorship	40
2.8.2 Impostor Phenomenon	44
2.8.3 Hostile work environment.....	48
2.9 Conclusion	57

2.10 Summary	58
Chapter 3: Methodology	61
3.1 Research Method and Design Appropriateness	61
3.2 Population, Sampling, and Data Collection Procedures and Rationale	62
3.3 Population	62
3.4 Data Collection	64
3.5 Validity – Internal and External	72
3.6 Data Analysis	76
3.7 Chapter Summary	82
Chapter 4: Results and Findings	84
4.1 Population Demographics	84
4.2 Data Collection Procedures	84
4.3 Sample Size	85
4.4 Demographic Data	86
4.4.1 Age (question 2)	86
4.4.2 Highest level of education (question 3)	86
4.4.3 Time working in the cybersecurity industry (question 4)	89
4.4.4 Current working position level (question 5)	89
4.4.5 NICE Cybersecurity Workforce Framework category (question 6)	89
4.5 Dependent Variable Descriptive Information	93

4.5.1 Lack of mentorship (question 7)	93
4.5.2 Impostor phenomenon (question 8)	93
4.5.3 Hostile work environment (question 9)	93
4.5.4 Composite	94
4.6 Stage One of Inferential Analyses.....	96
4.6.1 Research question one.....	97
4.6.2 Research question two	97
4.6.3 Research question three	98
Retention Barrier.....	99
4.6.4 Research question four.....	99
4.6.5 Research question five	99
4.6.6 Research question six.....	100
4.6.7 Research question seven	101
4.6.8 Research question eight	102
4.6.9 Research question nine	103
4.7 Stage Two of Inferential Analyses	105
4.7.1 Time working in the cybersecurity industry	105
4.7.2 Current working position	106
4.7.3 NICE cybersecurity workforce framework category.....	106
4.8 Summary	107

Chapter 5: Implications and Conclusions	108
5.1 Overview of the Research Problem and Questions.....	108
5.1.1 Research questions.....	110
5.1.2 Research hypotheses	111
5.2 Contributions to Knowledge.....	112
5.2.1 Lack of mentorship	113
5.2.2 Impostor Phenomenon	113
5.2.3 Hostile work environment.....	114
5.2.4 Time working in the cybersecurity industry	114
5.2.5 Current position level.....	115
5.2.6 NICE Cybersecurity Workforce Framework category.....	116
5.3 Limitations of the Study.....	119
5.4 Implications for Practitioners.....	119
5.4.1 Barriers to retention	119
5.5 Implications for Policy-Makers	121
5.5.1 Lack of mentorship	121
5.5.2 Impostor Phenomenon	122
5.5.3 Hostile work environment.....	122
5.6 Implications for Future Research.....	124
5.6.1 Lack of mentorship	125

5.6.2 Impostor Phenomenon	125
5.6.3 Hostile work environment.....	126
5.7 Conclusions from the Study Results.....	126
5.8 Assessment of Research Objectives.....	127
5.9 Summary.....	127
Appendices.....	128
Appendix A: Definition of Terms	129
Appendix B: Survey Instrument	130
Appendix C: IRB Certification of Approval.....	132
References.....	133
Biography.....	140

List of Tables

Table 1: Guidance for Questionnaires.....	70
Table 2: Avoiding Risks to Internal Validity.....	74
Table 3: Null Hypotheses.....	80
Table 4: Sample Personal Demographics, n = 141	87
Table 5: Sample Professional Demographics, n = 141	90
Table 6: Dependent Variable Descriptives, n = 141	94
Table 7: Correlations of time working in the cybersecurity industry and Retention Barriers, n = 141	99
Table 8: ANOVA Results for Barriers to Retention by Current Working Position, n = 141	101
Table 9: ANOVA Results for Barriers to Retention by NICE Specialty Areas, n = 141.....	104
Table 10: Descriptives for Impostor Phenomenon by NICE Specialty Area, n = 141.....	104
Table 11: Correlations of Time Working in the Cybersecurity Industry and overall composite of the Retention Barriers, n = 141	105
Table 12: ANOVA Results for the Composite of the Barriers Retention by Current Working Position and NICE Specialty Areas, n = 141	107

List of Figures

Figure 1: The conceptual framework for the study.....	14
Figure 2: Johnson's model for the low numbers of women in STEM senior management (2013, p. 13).	41
Figure 3: Instruction page for the survey instrument.....	66
Figure 4: Verification by respondent of fitness for survey.....	67
Figure 5: Capturing the Time in Industry independent variable.....	67
Figure 6: Capturing the Current Position Level independent variable.	68
Figure 7: Capturing the NICE Cybersecurity Workforce Framework independent variable.....	69
Figure 8: Capturing the dependent variables.	70
Figure 9: Types of relationships (Trochim, Donnelly, and Arora, 2016, p. 16)...	79
Figure 11: Respondent Education Level.	88
Figure 10: Respondent Age Distribution.	88
Figure 12: Time Working in the Cybersecurity Industry.	91
Figure 13: Respondent Current Working Position Level.....	92
Figure 14: Respondent NICE Cybersecurity Workforce Framework Category...	92
Figure 15: Impact of Lack of Mentorship.....	95
Figure 16: Impact of Impostor Phenomenon.	95
Figure 17: Impact of Hostile Work Environment.	96

Chapter 1: Rationale

1.1 Introduction

Information Technology (IT) has grown from a technological curiosity to a powerful and complex set of technologies and capabilities that drives nearly all aspects of business today. The power and complexity have led to opportunistic, malicious attacks from those desiring to disrupt or steal. In 2017, Kaspersky Lab solutions (only one vendor of antimalware) stopped 1,188,728,338 unique attacks launched from around the world, with targets ranging from governments to businesses to individual residential networks (Kaspersky Lab, 2017b). The landscape keeps shifting, as Kaspersky Lab notes that 2017 saw a shift from Internet Explorer and Adobe vulnerabilities to Microsoft Office and a renewed focus on social engineering. The WannaCry and ExPetr ransomware attacks showed how a network attack exploiting an old, well-known vulnerability could still wreak havoc in businesses. Focusing more locally, nearly 20% of U.S. businesses experienced critical systems disruption due to cybercrime in 2017 (Computer Security Online, 2017). Again, per Kaspersky Lab (2017b), the United States was the source of over 33% of the world's web-based attacks. Arrayed in defense against cybercrime are the nation's cybersecurity professionals, working across 33 specialty areas as defined by the National Initiative for Cybersecurity Education (Newhouse, Keith, Scribner, & Witte, 2017). These specialty areas are categorized into seven categories:

- Securely Provision (focused around risk management, software development, and introducing new technology)
- Operate and Maintain (focused around the technical foundation: database, network, customer service, systems administration)

- Oversee and Govern (focused around legal compliance, training, management strategy, leadership)
- Protect and Defend (focused around incident response, vulnerability assessment, cybersecurity defense)
- Analyze (focused on threat analysis, exploitation analysis, language analysis, target analysis)
- Collect and Operate (focused on collecting data, target planning, gathering evidence)
- Investigate (focused on digital forensics, surveillance, interview/interrogation, counter surveillance)

The cybersecurity industry has a significant employment problem in that there are not enough skilled cybersecurity personnel to fill the available positions (Cybersecurity Supply and Demand Heat Map, n.d.). With a cybersecurity workforce of over 768,000 people, there are still over 301,000 job openings left unfilled. In early 2015, there were about 209,000 jobs open in the cybersecurity industry, indicating that the employment trend is not in the right direction (Setalvad, 2015). This research improved the industry's understanding of factors that may assist the industry in closing the cybersecurity employment gap.

1.2 Background of the Study

The cybersecurity industry has far more job openings than skilled workers, with an employment gap of 301,000 job openings (Cybersecurity Supply and Demand Heat Map, n.d.). These unfilled cybersecurity positions are across the spectrum of work, including:

- Cybersecurity Engineer
- Cybersecurity Analyst
- Network Engineer/Architect
- Cybersecurity Manager
- Systems Engineer
- Software Developer/Engineer
- Vulnerability Analyst
- Penetration Tester
- Systems Administrator

- IT Auditor

With this significant number of unfilled positions in the cybersecurity industry, cybersecurity industry research is being performed to explore the causes of the gap and possible approaches to narrowing the gap with skilled workers (Vogel, 2016; Bedding & de Jongh, 2017; Pierce, 2016; Fuller, 2016; Cobb 2016). Efforts to close the employment gap include:

- gaining a better understanding of the type of work being done and the skills needed for that work (Newhouse, Keith, Scribner, & Witte, 2017)
- creating cyber competitions in high schools to increase interest in cybersecurity careers (Pierce, 2016)
- improving the curriculums of post-high school education with schools earning designations from the National Security Agency (NSA) (Vogel, 2016).

There is an aspect of the cybersecurity employment market that is under-researched and significantly contributes to the employment gap – the gender gap in the cybersecurity industry (Peacock & Irons, 2017). In the United States, women make up about 50% of the workforce, but only 10-15% of the cybersecurity workforce (LeClair, Shih, & Abraham, 2014). Globally, women represent 11% of the cybersecurity workforce, and recent efforts to raise that number have made no significant improvement (Reed, Zhong, Terwoerds, & Brocaglia, 2017). Per the same study, in North America men are five times more likely than women to be in C-Level positions, four times more likely to be in executive positions, and nine times more likely to be in managerial positions.

Cybersecurity is part of the so-called STEM (Science, Technology, Engineering, and Math) field. Cybersecurity is considered one of the STEM fields, being part of Technology. There are parallels between STEM and cybersecurity regarding the gender gap in employment – the STEM gender gap is not as severe as that in cybersecurity –

25% of the STEM workforce are women (LeClair, Shih, & Abraham, 2014), but it still does not represent the gender split in the overall workforce.

There are two primary aspects of the gender gap in STEM and cybersecurity: the low number of women entering the industry and the low retention rate of women after joining the ranks of cybersecurity workers. While both aspects are deserving of more study, this research focused on the retention of women in the cybersecurity field.

A longitudinal study by Glass, Sassler, Levitte, and Michelmore (2013) showed a significant difference between retention of women in STEM (50% exit rate) and women in other professional fields (20% exit rate). The authors note that the study does not show this percentage of women leaving the workforce, just leaving the original STEM fields. The women are leaving STEM fields and going to other professional occupations outside STEM. LeClair et al. (2014) note that 80% of men stay in the cybersecurity field, while only 60% of women are retained in cybersecurity over time. Studies (LeClair et al., 2014; Silbey, 2016; Shine, 2016; Glass et al., 2013) suggest multiple retention factors (or barriers to retention) for women in STEM and cybersecurity. There are two primary types of sexual harassment per Kabat-Farr and Cortina (2014): sexual advance and gender. Sexual advance harassment is unwanted sexual overtures, where gender harassment is not sexual in nature but is gender-based and manifests in anger, scorn, or rejection aimed at women in the workplace. Perceived bias in performance evaluation ties to the 'good old boy' network problem, described by LeClair and Pheils (2016) simply as men taking care of each other regarding workplace advancement and promotions. Impostor Phenomenon is also called Impostor Syndrome and is the situation where, although one is qualified for a position, the employee feels inadequate in ability

compared to the requirements of the job. As Neureiter and Traut-Mattausch (2016) describe it, the person feels incapable even with objective indications that demonstrate otherwise. Research (Clance & Imes, 1978) shows that women are more frequently affected by Impostor Phenomenon and the effects are of a higher magnitude. Hacker mentality relates to the image of the cybersecurity industry as full of hackers or outlaws (especially seen at conventions such as DEFCON) (Shumba et al., 2013). Other retention factors include inequal pay, lack of teamwork, relegation to non-technical roles in teams, and limited access to female mentors.

1.3 Problem Statement

There is a critical shortage of skilled cybersecurity workers in the United States (Cybersecurity Supply and Demand Heat Map, n.d.). This labor shortage can negatively impact the ability of government and commercial efforts to protect business and critical infrastructure. One approach to helping reduce the shortage is to encourage more women to enter and stay in the industry since women are significantly underrepresented in the field (LeClair et al., 2014). Work is underway to encourage more women in high school and earlier to consider cybersecurity as a career, and studies are needed to understand better why retention of women is low in the overall STEM field and, more specifically, in cybersecurity. With few studies focusing specifically on how barriers to retention impact women in the cybersecurity industry, this research provides better insight into barriers to retention of women in the cybersecurity industry.

Review of the extant literature shows that, while researchers (LeClair et al., 2014; Peacock & Irons, 2017) lament the lack of research on the overall gender gap in cybersecurity, research focusing on retention of women in cybersecurity is particularly

lacking. The lack of research regarding the retention of women in cybersecurity established the need for this study. With the pipeline of women into cybersecurity low, retention becomes even more important, as a cycle is created, with the lack of women providing evidence to girls that the cybersecurity industry is not female-friendly. This study focused on the perceived impacts of identified barriers to retention as seen by women in the cybersecurity field.

1.4 Purpose of the Study

The purpose of this quantitative correlational study was to aid the cybersecurity industry in understanding why women have a lower retention rate than men in the industry. The study leads to improving the retention rate and thereby reducing the employment gap. The study provides guidance to executives on how changing the corporate culture would help keep female cybersecurity employees from leaving.

The independent variables were demographic data to be collected from the respondent:

- Time working in the cybersecurity industry
- Current position level
 - Executive management
 - Senior management
 - Middle Management
 - Individual contributor
- National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework category
 - Securely Provision
 - Operate and Maintain
 - Oversee and Govern
 - Protect and Defend
 - Analyze
 - Collect and Operate
 - Investigate

These demographics aid in describing categories of respondents to establish relationships between those categories and the dependent variables. The NICE cybersecurity workforce framework category provided insight as to which types of cybersecurity work experience the most significant impacts from retention barriers.

The dependent variables were the perceived impact of selected barriers to retention of women in the cybersecurity industry, as identified in the extant literature and evaluated by the respondent:

- Impact of lack of mentorship
- Impact of Impostor Phenomenon
- Impact of a hostile work environment

The dependent variables reflect aspects of the corporate culture or workplace that have varying levels of impact on retention of women in the cybersecurity industry.

The data collection consisted of an online survey advertised to women in cybersecurity industry organizations. Messaging was sent to members of cybersecurity industry organizations via online groups in LinkedIn, through internal messaging within the organization, and through Twitter. While most respondents were members of one or more of the organizations, word of mouth was encouraged and resulted in some respondents from outside one of the target organizations.

1.5 Significance of the Study

This research examined the relationships between demographic factors and the respondents' perceived impact of barriers to retention. This research shed light on how women in cybersecurity perceive the impact of various potential retention barriers on the desire to maintain a cybersecurity career. Improved understanding of these relationships may help organizations prioritize and focus efforts to modify corporate benefits and

culture to mitigate impacts of barriers to retention for women in cybersecurity. The findings also contribute to the growing body of literature in cybersecurity workforce development. A better understanding of retention barriers may also help organizations recruit more women into the cybersecurity industry. The combination of improving retention rates and increasing the number of women recruited into the industry may help in closing the employment gap in the industry.

1.6 Rationale

Cybersecurity is a human-intensive practice – in specialty fields as wide-ranging as risk management, data administration, training, incident response, and digital forensics (Newhouse, Keith, Scribner, & Witte, 2017). With the identified employment gap of (currently) 301,000 open positions (Cybersecurity Supply and Demand Heat Map, n.d.), government agencies and commercial organizations are scrambling to maintain or improve security postures. The 301,000 open positions occur across all industries, including health, government, finance, transportation, technology, and academia. The open positions also cross the spectrum of work within the cybersecurity industry, including engineering, system administration, vulnerability analysis, penetration testing, architecture, and software development. Delving into cybersecurity employment figures, one sees a significant gender gap – while the general workforce is roughly even between women and men, women make up only 10-15% of the cybersecurity workforce (LeClair, Shih, & Abraham, 2014). It is possible that, in closing the gender gap, the addition of thousands of women into the cybersecurity industry may also close the overall employment gap, reducing the number of open positions in the industry. Again, delving into the gender gap, one sees two primary factors – the number of women joining the

industry and the number of women leaving for a different industry (LeClair et al., 2014). Both factors require more research to gain a better understanding of means/methods to close the gender gap and therefore reduce the overall employment gap. While there are numerous initiatives to encourage women to enter into the study of cybersecurity in college, high school, and even middle school, there is a dearth of information and effort on improving the retention of women in the cybersecurity industry. Women leave the cybersecurity industry at a rate of at least 40%, while men leave at only a 20% rate (LeClair et al., 2014). This study focused on gaining a better understanding of the factors affecting the retention rate of women working in the cybersecurity industry in the United States.

The rationale for studying this relevant topic using a quantitative method design was to investigate the links between demographics, retention barriers, and the intent to stay in the cybersecurity field. This study helps commercial companies and government agencies better understand where to focus resources that will improve the retention rate of women in cybersecurity, resulting in a narrowing of the employment gap in the industry.

1.7 Nature of the Study

This study was a quantitative correlational study to investigate the strength and nature of relationships between the independent variables (time working in the cybersecurity industry, current position level, and type of cybersecurity work (as referenced by the NICE Cybersecurity Workforce Framework)) and the dependent variables (lack of mentorship, Impostor Phenomenon, and hostile work environment). Per Cooper and Schindler (2011), a qualitative study's purpose is to investigate 'how' and

‘why.’ Creswell (2012) states that quantitative methodology is appropriate for studying relationships between variables. The goal of this study was to determine the nature of the relationships between the research variables. Thus, quantitative research was more appropriate.

Quantitative methodology encompasses multiple research designs. Experimental designs require before and after measurements of at least two groups, with one group acting as a control and other groups receiving some type of treatment (e.g., training) (Creswell, 2012). The goal of a quasi-experimental design is to identify causality in a relationship between variables. Correlational research, which is a subset of Descriptive Design (Cooper & Schindler, 2011) has a goal of describing relationships between variables without identifying causality. A correlational design was appropriate for this study.

1.8 Research Questions

The extant literature identified demographics and retention factors for women in cybersecurity and in STEM (Claggett, 2016; Johnson, 2013; LeClair, Shih, & Abraham, 2014; Littlejohn, 2016; Peacock & Irons, 2017). The demographics, which were the independent variables, consist of *time working in the cybersecurity industry*, *current position level*, and *type of cybersecurity work*. For this study, the NICE Cybersecurity Workforce Framework category was used to identify the type of cybersecurity work. Barriers to retention, which were the dependent variables, identified in the literature (Claggett, 2016; Johnson, 2013; LeClair, Shih, & Abraham, 2014; Littlejohn, 2016; Peacock & Irons, 2017; Silbey, 2016) were *lack of mentorship*, *Impostor Phenomenon*, and *hostile work environment*.

The overarching research question for this study was: What is the nature of the relationships between the demographic factors and the respondent's perception of the impact of the retention barriers? Through quantitative methods, the research helped to determine the strength and directness or indirectness of each pair relationship between the demographic factors and the barriers to retention. The research questions that guided this study are:

RQ1: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of lack of mentorship?

RQ2: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of Impostor Phenomenon?

RQ3: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of a hostile work environment?

RQ4: What is the nature of the relationship between *current position level* and the perceived impact of lack of mentorship?

RQ5: What is the nature of the relationship between *current position level* and the perceived impact of Impostor Phenomenon?

RQ6: What is the nature of the relationship between *current position level* and the perceived impact of a hostile work environment?

RQ7: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of lack of mentorship?

RQ8: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon?

RQ9: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of a hostile work environment?

1.9 Research Hypotheses

Based on the research questions presented above, the following hypotheses were tested in this study:

H01: There is no significant relationship between time working in the cybersecurity industry and the perceived impact of lack of mentorship on retention

HA1: There is a significant relationship between time working in the cybersecurity industry and the perceived impact of lack of mentorship on retention

H02: There is no significant relationship between time working in the cybersecurity industry and the perceived impact of Impostor Phenomenon on retention

HA2: There is a significant relationship between time working in the cybersecurity industry and the perceived impact of Impostor Phenomenon on retention

H03: There is no significant relationship between time working in the cybersecurity industry and the perceived impact of a hostile work environment on retention

HA3: There is a significant relationship between time working in the cybersecurity industry and the perceived impact of a hostile work environment on retention

H04: There is no significant relationship between current position level and the perceived impact of lack of mentorship on retention

HA4: There is a significant relationship between current position level and the perceived impact of lack of mentorship on retention

H05: There is no significant relationship between current position level and the perceived impact of Impostor Phenomenon on retention

HA5: There is a significant relationship between current position level and the perceived impact of Impostor Phenomenon on retention

H06: There is no significant relationship between current position level and the perceived impact of a hostile work environment on retention

HA6: There is a significant relationship between current position level and the perceived impact of a hostile work environment on retention

H07: There is no significant relationship between NICE Workforce Framework category and the perceived impact of lack of mentorship on retention

HA7: There is a significant relationship between NICE Workforce Framework category and the perceived impact of lack of mentorship on retention

H08: There is no significant relationship between NICE Workforce Framework category and the perceived impact of Impostor Phenomenon on retention

HA8: There is a significant relationship between NICE Workforce Framework category and the perceived impact of Impostor Phenomenon on retention

H09: There is no significant relationship between NICE Workforce Framework category and the perceived impact of a hostile work environment on retention

HA9: There is a significant relationship between NICE Workforce Framework category and the perceived impact of a hostile work environment on retention

1.10 Conceptual Framework

This research focused on the relationships between a set of demographic factors and the perceived impact of a set of barriers to retention in the cybersecurity industry.

The goal of the study was to determine the strength and direction of the matrix of relationships between the independent and dependent variables. Per Creswell (2012), correlational research designs “...describe and measure the degree of association (or relationship) between two or more variables...” (p. 338). The conceptual framework is illustrated in Figure 1.

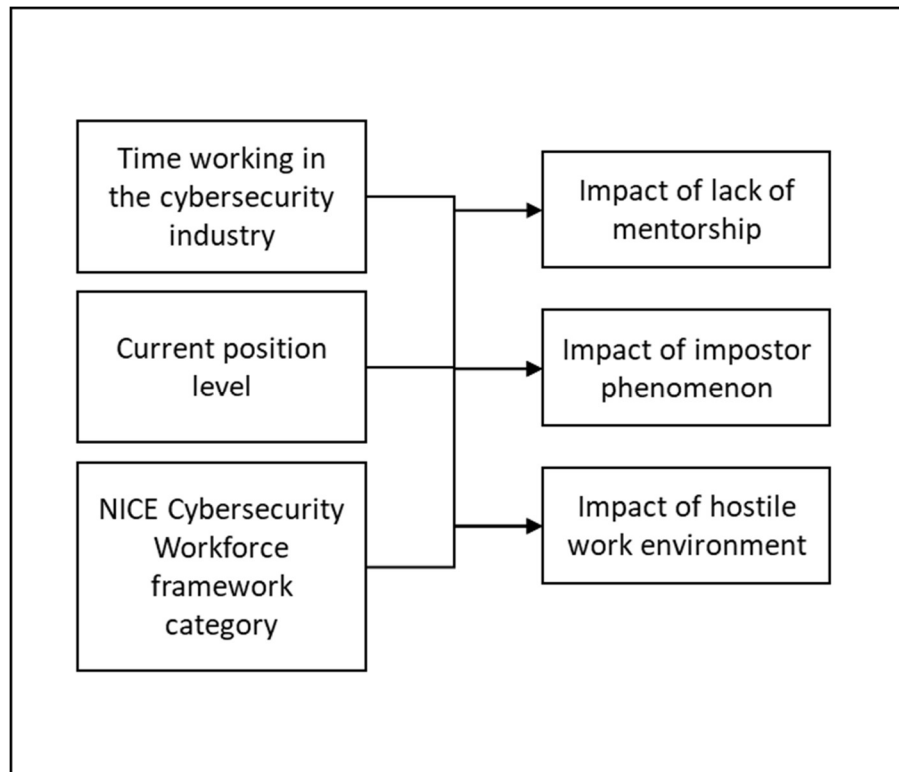


Figure 1: The conceptual framework for the study.

The demographics (independent variables) were chosen based on extant research:

‘*Time working in the cybersecurity industry*’: Chen, Ployhart, Thomas, Anderson, and Bliese (2011) provide a link between organizational tenure and the impact of factors

affecting retention. Per the authors, the longer an employee works in an organization, the less the employee expects working conditions to change.

‘Current position level’: Blau and Kahn (2017) demonstrate that there are differences in pay inequality based upon position level in the organization. This led to the inclusion of this independent variable, to investigate the possible relationships between position level and the impact of other barriers to retention.

‘NICE Cybersecurity Workforce Framework Category’: Kabat-Farr and Cortina (2014) show that gender underrepresentation in a field is directly related to incidence of gender-based harassment. The NICE Framework provides a taxonomy, breaking down the different types of cybersecurity work. The goal of this demographic being included was to investigate if the specific type of cybersecurity work (e.g., risk management, incident response, cyber operations) influences the perceived impact of the retention barriers.

The retention barriers which were the dependent variables were also drawn from extant literature. Leclair et al. (2014) point to lack of mentorship and gender discrimination (hostile work environment). Cech, Rubineau, Silbey, and Seron (2011) show that “...professional role confidence predicts behavioral and intentional persistence, and that women’s relative lack of this confidence contributes to their attrition” (p. 4), which directly relates to Impostor Phenomenon.

1.11 Assumptions and Limitations

1.11.1 Assumptions

Assumptions are conditions that the researcher assumes to be true as part of the research process. This study relied upon the following assumptions about the respondents, the survey instrument, sample, and population:

Assumption One - Since the research data was collected by a self-administered, web-based survey, an assumption was that the respondents would answer accurately and truthfully, and that the respondents were women currently working in the cybersecurity industry in the United States.

Assumption Two - Respondents only responded to the survey once. The researcher offered a gift card drawing for five \$50 Amazon gift cards given to five respondents if the respondent provided an email address. The survey instrument instructions noted that the email address (if provided) would only be used for the gift card drawing. Duplicate email addresses would have been filtered out. There was no incentive for a respondent to take the survey multiple times.

Assumption Three – Survey instruments are used to measure, observe, or document quantitative data (Creswell, 2012). Correlational designs attempt to describe one or more relationships between independent and dependent variables, without attempting to show causality (Cooper & Schindler, 2011). This study assumed that an online, Likert-type survey instrument would be a suitable instrument for collecting needed data within a correlational descriptive research design.

Assumption Four - The study population had access to the internet to complete the survey. Since the respondents were cybersecurity professionals, it is expected that respondents had access to both computers and the internet.

Assumption Five – The sample size was large enough for the results to be relevant to the topic and outcomes. Current estimates show about 768,000 employed cybersecurity professionals in the United States (Cybersecurity Supply and Demand Heat Map, n.d.). Using estimates from literature that women account for 10-15% of the cybersecurity workforce in the United States (LeClair, Shih, & Abraham, 2014) and 11% globally (Reed, Zhong, Terwoerds, & Brocaglia, 2017), this study used 12.5% of 768,000 (96,000) as an estimate of the total number of women working in the United States cybersecurity industry. Selecting a confidence level of 95% and a confidence interval of 5% and using a standard sample size calculator (<https://www.surveysystem.com/sscalc.htm>) the resulting recommended sample size was 383.

1.11.2 Limitations

The survey sample was self-selected by advertising the survey through cybersecurity industry organizations, associated LinkedIn groups, and Twitter. Some of the organizations have a general membership, and some have a specifically female membership. A primary limitation of this study was the willingness of female cybersecurity practitioners to participate in the study, which reduced the sample size. Another limitation is that not all cybersecurity organizations participated in the study. The organizations contacted were selected by the learner through personal connections or availability of contact information.

1.11.3 Delimitations

A delimitation of this study was the selection of the sample frame, which is women in cybersecurity industry organizations. This choice reduced the generalizability of the results to the larger population of all women in cybersecurity. It is possible that whatever qualities cause women to join professional organizations were not shared by the wider population of women in cybersecurity.

1.12 Summary

The purpose of this study was to examine the strength and direction of relationships between the independent variables (time working in the cybersecurity industry, current position level, and type of cybersecurity work) and the dependent variables, or barriers to retention (lack of mentorship, Impostor Phenomenon, and hostile work environment). The cybersecurity industry has a large number of unfilled positions, currently 301,000 (Cybersecurity Supply and Demand Heat Map, n.d.). Contributing to the gap is the low number of women participating in the field. While women make up about 50% of the general workforce, they only make up about 10-15% of the cybersecurity workforce (LeClair et al., 2014). One of the causes of the low participation of women in the cybersecurity industry is that the retention rate of women in the industry is lower than the retention rate of men in the industry. This study improved understanding of the causes of the lower retention rate for women in the cybersecurity industry.

1.12.1 Organization of the remainder of the study

The remainder of this study will be divided into four chapters. Chapter 2 presents a review of the literature, which is organized into five sections. The first section

describes the approach to the literature search, including the search process, sources, and keywords or phrases. This section also describes how literature is evaluated and categorized. The second section provides an overview of the state of cybersecurity industry employment. This section begins with a historical view of cybersecurity workforce development, from the initial attempts to define computer security to the current day. Next, the literature provides an overview of cybersecurity industry employment is reviewed. Lastly, literature will be presented that provides insight into the two-pronged basis of the cybersecurity gender gap, the pipeline of women entering the industry and retention of women working in the industry. The third section focuses on the retention of women in STEM fields, including cybersecurity. The fourth section reviews literature relevant to the independent variables of the study (time in industry, current position level, and NICE cybersecurity workforce framework category). The fifth section reviews literature relevant to the dependent variables of the study (lack of mentorship, Impostor Phenomenon, and hostile work environment).

Chapter 3 discusses the research methodology and design (quantitative correlational) selected for the evaluation of the research questions and testing of the research hypotheses. The chapter also explains why the methodology and design were appropriate for the study. It also discusses the research population, sample frame, and sample. The data collection instrument will be described along with how the instrument will be used. Chapter 3 also presents, explains, and justifies the statistical analyses that will be employed. Lastly, the validity, reliability, and ethical considerations of the study will be presented.

Chapter 4 will provide the results of the statistical analysis of the data collected. These results will be tied to the research questions and hypotheses. Chapter 5 will summarize and discuss the results from Chapter 4 after providing an overview of the entire study. It will also discuss the implications of the study, identified limitations, and recommendations for further research. This chapter will conclude the study and will be followed by references and appendices (including a copy of the survey instrument and definition of terms).

Chapter 2: Research Review and Synthesis

The purpose of this study was to aid in reducing the cybersecurity employment gap by improving our understanding of retention factors for women in the cybersecurity industry. Retention factors are those aspects of cybersecurity employment that may either encourage or discourage women from staying in the cybersecurity industry. This study focused specifically on retention factors that act as barriers to retention of women in the cybersecurity industry, i.e., that discourage women to remain in the cybersecurity industry. The impact of barriers to retention reduces the probability that a person will stay in the cybersecurity industry. The study measured the strength and direction of relationships between a set of demographic factors and a selected set of barriers to retention.

Women are significantly underrepresented in the cybersecurity industry. Women makeup roughly 50% of the general workforce, but only makeup 10-15% of the cybersecurity workforce in the United States (LeClair, Shih, & Abraham, 2014). A better understanding of the impact of barriers to retention provides information to organizations to help improve the retention of women in the cybersecurity industry, thereby reducing the gender gap and the large number of extant open positions in the industry. The results provide organizations information for improving retention and may point to further research into factors causing the low retention rate of women in the industry.

The literature review is organized into six sections. The first section introduces the literature review including information about how the review was conducted, sources of research, and keywords used in the search for extant literature. The second section

provides the historical context for cybersecurity workforce development and initiatives for diversity within the cybersecurity industry. The third section is an overview of cybersecurity employment in general, while the fourth section presents information regarding women in the cybersecurity field. The fifth section discusses the independent variables (demographic factors) used in this research, and the sixth section discusses the dependent variables (barriers to retention). The research studies presented in the literature review represent a comprehensive overview of the current literature regarding women in cybersecurity, specifically focused on topics relevant to the retention of women employed in the cybersecurity industry.

2.1 Process Overview

The literature search started with a general review of topics in non-scholarly sources related to the cybersecurity workforce in the United States and the associated gender gap. This early phase included online articles in publications such as CIO Magazine, Slate, and Information Security Magazine. It also included conversations with attendees at the 2017 National Initiative for Cybersecurity Conference in Dayton, Ohio. This generalized information served as the foundation for a narrower focus on reasons underlying the gender gap and the scholarly literature search. The second phase of the literature search focused on scholarly journal articles published in English between January 2011 and 2018 and included the following sources:

- Google Scholar
- IEEE Xplore Digital Library
- Association of Computing Machinery (ACM) Digital Library
- ProQuest Central
- ProQuest Computer Science Collection
- ProQuest Dissertations & Theses Global
- ResearchGate

The search terms used include the following terms and phrases, and various combinations of each:

- women
- retention
- cybersecurity
- information assurance
- impostor syndrome
- impostor phenomenon
- hostile work environment
- wage inequality
- sexual harassment
- gender harassment
- STEM
- teamwork
- cyber competitions
- hostile work environment
- good old boy network
- girls
- cybersecurity workforce development
- cybersecurity workforce gap
- NICE Framework
- National Bureau of Standards
- National Institute of Standards and Technology

The researcher also found articles by following citations in selected articles. The research articles selected for this study were selected from a total of 112 articles.

2.2 Historical Context

Warner (2015) notes that, while many tend to think of the 1990s as the emerging point of a national focus on cybersecurity, history points to the early 1960s as the beginning of computer security as a recognized need within computer science. The Brooks Act of 1965 was the first federal legislation recognizing the need for "...the security of the information they stored and processed, and the privacy of individuals providing that information" (p. 9). The Brooks Act also standardized purchase of computers through the General Services Administration and authorized the National Bureau of Standards (NBS, now known as the National Institute of Standards and

Technology (NIST)) to set mandatory standards for computer security. A government study by the Senate Committee on Government Operations in 1976 concluded that “Crimes involving computers were proliferating across the public and private sectors, and federal information systems were vulnerable to real and potential threats ranging from sabotage to theft to privacy” (p. 9). At the same time, RAND Corporation’s Spring Joint Computer Conference included papers reporting on federal time-sharing computer systems and the resulting concerns about security (Misa, 2016). Personal computing and security were not on the radar yet. As an example, one of the personal computer security powerhouses of today (Symantec) didn’t enter the computer security business until 1989, with its first antivirus product for the Macintosh (Aspray & Cortada, 2016). In 1984 the Reagan administration was “...the first to conceive of a national security threat of adversaries entering American computer networks and databases surreptitiously” (Warner, 2015, p. 11), issuing a National Security Decision Directive focused on computer security. The Computer Security Act of 1987 modernized the Brooks Act and reinforced NBS’ role in setting standards for computer security, including security awareness training for all federal employees. The Federal Information Security Management Act (FISMA) of 2002 shifted the federal computer security focus over to risk management, with NIST (formerly NBS) as the implementing organization. The initial version of NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, includes security awareness training and role-based training, but does not account for the larger question of workforce development (Ross et al., 2005). President Bush, in 2008, signed the Comprehensive National Cyber Security Initiative, which included a consolidation of cyber education efforts (Aitoro, 2008),

including the National Security Agency's Centers for Academic Excellence program, which was started in 2004 ("National Centers of Academic Excellence in Cyber Defense - NSA.gov," n.d.). It appears to be the first federal-wide initiative concerning cybersecurity workforce development. President Obama, in 2010, signed the Comprehensive National Cybersecurity Initiative, which included as Initiative #8 'Expand Cybersecurity Education.' This action launched the National Initiative for Cybersecurity Education (NICE), which developed the cybersecurity workforce framework used in this study (Petersen, 2015). In 2012, the NICE leadership framed three components of strategic goals: Awareness, Education, and Workforce.

Baker (2016) addresses diversity as a significant factor in the "...drastic shortage of adept cybersecurity professionals..." (p. 6) but does not provide insight into any national initiatives to improve diversity in the cybersecurity industry. Kaspersky (2017a) provides insight into why girls do not choose careers in cybersecurity but does not discuss any national initiatives to get more girls interested in the industry. Pusey, Gondree, and Peterson (2016) suggest that efforts exist to make cyber competitions more diverse and inclusive, but these efforts are on a competition-by-competition basis. Shumba et al. (2013) describe a program from the National Science Foundation (NSF) titled Broadening Participation in Computing that has a goal of increasing the number of underrepresented minority students receiving post-secondary degrees in the computer sciences. The authors point out that "Although much has been reported on broadening participation in CS and IT, little has been reported on the specific field of Cybersecurity" (p. 3).

The idea of computer security has been around since the early 1960s, but a focus on cybersecurity workforce development is relatively new, and a focus on diversity in cybersecurity is even newer. There appears to be a limited national-level focus on gender or minority diversity in the field.

2.3 Cybersecurity Industry Employment

The cybersecurity industry has an employment gap problem. According to Cyber Seek, a project supported by the National Initiative for Cybersecurity Education (NICE), there are about 750,000 cybersecurity professionals currently working in the U.S., with over 301,000 jobs remaining unfilled (Cybersecurity Supply and Demand Heat Map, n.d.). In 2015, there were an estimated 209,000 jobs unfilled in cybersecurity (Setalvad, 2015). The rise in the number of openings between 2015 and the present shows that the employment gap is getting worse. This employment gap is not limited to the U.S., as the expected global shortage in cybersecurity workers is expected to be 1.8 million workers by 2022 (Frost & Sullivan, 2017). Per Frost and Sullivan (2017), the most cited reason for the shortage in North America is “Qualified personnel difficult to find” (p. 3), with the fourth highest reason being low retention of workers (which could be tied to the shortage, with employees job-hopping for better pay, since this retention measure is retention with specific companies, not retention in the industry).

Regarding cybersecurity professionals, Libicki, Senty, and Pollak (2014) point out that “Drastic steps taken today to increase their quantity and quality would not bear fruit for another five to ten years” (p. xv). The researchers go on to express concerns that the dramatic shortage of cybersecurity professionals may be short-term, partially mitigated by advances in technology. The technologies suggested include greater use of thin client

architectures, where the processing is performed centrally (e.g., in the cloud), and greater use of whitelisting rather than blacklisting. The numbers presented by CyberSeek (over 301,000 jobs unfilled and growing) belie the concern of the workforce shortage being short-lived, as any country-wide shift in technology of the sort described by Libicki, Senty, and Pollak (2014) will take considerable time. The addition of new technologies (including the large numbers of newly connected devices referred to as the Internet of Things) also adds to the burden of work in cybersecurity. Per Bedding and de Jongh (2017), the increasing digitization and interconnectedness of the world are increasing the demand for cybersecurity professionals. Additionally, as attacks become more sophisticated (resulting in a global cost of over \$400 billion), cybersecurity professionals must also improve individual skills and abilities. Again, from Bedding and de Jongh (2015, pp. 10-11):

However, cybersecurity is an ever-changing field; tools were only valid for a short amount of time before they were outdated. Threats were constantly evolving and required workers who could learn and develop in order to continually combat a sea of changing threats.

The impact of the cybersecurity workforce shortage is widespread. 68% of U.S. cybersecurity professionals report insufficient staff, while globally 66% of cybersecurity professionals report security staff shortages (Frost & Sullivan, 2017). Per the same study, 32% of hiring managers in the United States want to increase cybersecurity workforce staffing by at least 15% (21% want to increase by more than 20%). The desire to increase the cybersecurity workforce is stymied by the shortage of available cybersecurity professionals to fill the new billets. Because cybersecurity professionals work across all industries, including Healthcare, Manufacturing, Retail, Construction, and Government, all industries are similarly affected by the cybersecurity workforce shortage,

with the two greatest skillset shortages being Operations and Security Management and Incident and Threat Management. Frost and Sullivan point out that in the cybersecurity industry “...historically demand has outpaced supply” (p. 5).

2.4 Women in Cybersecurity

Cybersecurity employment is included in STEM (Science, Technology, Engineering, and Math) employment, as cybersecurity is part of the Technology aspect of STEM. Rogers (2015) shows that women’s participation in Information Technology (part of the Technology component of STEM) has dropped steadily since the 1990’s. In 1996, women made up 41% of IT employees, dropping to 34.9% in 2002 and 26.6% in 2012. Per Rogers, “These statistics are shocking and actually do not require great interpretation. The percentage of women in IT is shrinking” (p. 95).

When looking at the demographics of cybersecurity industry employment, a striking imbalance is noted. Women make up roughly 50% of the general workforce, but only make up 10-15% of the cybersecurity workforce in the United States (LeClair, Shih, & Abraham, 2014). Per Reed, Zhong, Terwoerds, and Brocaglia (2017), the gender gap is similar across all position levels, with men being five times more likely to hold a C-level position or managerial position, and six times more likely to hold a non-managerial staff position.

2.5 Pipeline

One of the reasons for the gender imbalance in the cybersecurity industry is the reduced size of the ‘pipeline’ of women entering the industry from school. Shumba, et al. (2013) report that interest by girls in STEM (Science, Technology, Engineering, and Math) fields drops dramatically between 2nd and 8th grades. Per Pusey, Gondree, and

Peterson (2016), the gender split in middle school technology classes is even, but female participation drops to under 18% in high school. Per the National Center for Education Statistics (U.S. Department of Education, 2016), women earned over 180,000 undergraduate degrees in health-related fields, but just over 30,000 undergraduate degrees in computer science and engineering combined in 2014-2015. In the same period, men earned over 127,000 undergraduate degrees in computer science and engineering, and about 33,000 undergraduate degrees in health-related fields. Women earned more degrees in these two professional industries, yet significantly fewer in STEM-related degree areas.

2.5.1 Awareness of industry

Baker (2016) points out that women are as likely as men to earn a college degree, so the challenge is raising interest in the cybersecurity field among female students. A survey by Raytheon (2016) found that the awareness of cyber-attacks by young adults in the United States rose from 36% to 64% between 2015 and 2016, which is a positive indicator for the workforce. Regarding whether or not respondents understood what cybersecurity professionals do for work, young men's affirmative response grew from 46% to 54% from 2015 to 2016, while young women's affirmative response only grew from 33% to 36%. Kaspersky (2017a) found that 69% of young people have not met anyone employed in the cybersecurity industry, and only 11% have met a woman employed in the cybersecurity industry. Additionally, respondents had decided on career choices before 16th birthdays. After meeting someone (regardless of gender) working in the cybersecurity industry, 63% of women have a positive view of the field. Role models have a powerful impact on views of the industry.

Awareness of the cybersecurity industry in young adults is improving, but data shows that the awareness of young women is lagging that of young men. There are initiatives by cybersecurity organizations such as Women in Security & Privacy and the Women's Society of Cyberjutsu to increase awareness of the industry in younger women.

2.5.2 Industry image

The way that the cybersecurity industry is presented in popular media influences how interested girls might be in pursuing a career in cybersecurity. Pusey et al. (2016) suggest that girls may be put off by the image of cybersecurity being a solitary rather than team-based occupation. Turner et al. (2014) found that the perception of the cybersecurity field has an important impact on early decisions by girls regarding the selection of cybersecurity as a career. Girls tend to look for environments conducive to developing relationships with others. "For girls, then, social situations provide the primary context in which competence perceptions develop, whereas individual achievement situations afford boys more frequent opportunities to infer competence" (p. 3). The presentation of the cybersecurity industry as populated with loners would push girls away.

Setalvad (2015) quotes a middle school teacher at an all-girls school as saying "Popular culture always portrays [cyber-professionals] as nerdy males who live in their mom's basement, drinking Mountain Dew out of the bottle with chips all around them. So girls have already developed this resistance to it." Drew (2015) found that women "...expressed a preference for working in a challenging but also supportive environment that valued team spirit and endeavor but not in a cut-throat manner" (p. 7). Per Kaspersky (2017a),

Among the reasons for not selecting a career in cybersecurity, a lack of experience of 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 women (p. 5)

The continuing perception of cybersecurity as male-dominated and as an individual-oriented career, however true or not, reduces the number of girls interested in the field in middle and high school. Johnson (2013) points out that in pre-college classrooms, there needs to be a higher focus on mentoring girls and encouraging them to participate in STEM and cybersecurity programs in order to disperse the perceptions of cybersecurity as a male domain industry. Johnson also found that respondents felt “...most characteristics of the field were geared toward men...” (p. 56) and that men were seen as more competitive and more drawn toward the concepts of ‘attack’ and ‘defend.’ Kaspersky (2017a) found that young people looking at careers in cybersecurity think of cybersecurity professionals as being “...driven (44%), ambitious (33%) and adventurous (25%)” (p. 9). The researchers point out that stereotypes presented in media do not match the reality and present an image problem for the industry’s ability to recruit interest in school.

The extant literature generally agrees that the image of the cybersecurity industry as presented in popular media (including websites, movies, and books) acts as a deterrent for young women. Young women are not drawn towards the image of the lone, hoodie-wearing male working alone in a darkened room. Even with initiatives to change the image to a more realistic perception, popular television shows such as Mr. Robot perpetuate the image of the lone, hoodie-wearing male.

2.5.3 Cyber competitions

The growing number of both pre-college and college cybersecurity competitions (e.g., National Cyber League, CyberPatriot) focus on increasing the number of students in the cybersecurity workforce pipeline. Per Tobey, Pusey, and Burley (2014), only about 15% of the participants are female, roughly equivalent to the participation in the cybersecurity workforce. Pusey et al. (2016) suggest girls have lower confidence in personal skills, therefore do not want to compete. Wee, Bashir, and Memon (2016) surveyed one of the largest cyber ‘capture the flag’ competitions and found only 5% of the participants were female. 71% of the teams were all male, with 23% having a female minority. Bashir, Lambert, Wee, and Guo (2015) found that over half of all students participating in cyber competitions felt that participation in such competitions led to changes in career plans, moving toward the cybersecurity industry. The researchers found that, of the 492 respondents in the study, only 67 were female. In the study, males in cyber competitions scored higher in efficacy (self-confidence) while females scored higher in all other categories: Intuitive, Conventional, Enterprising, Social, Artist, and Neuroticism (tendency toward negative emotions). The lower scores in efficacy foreshadow the discussion of impostor syndrome later in this chapter. Cybersecurity competitions have grown interest in the field and have provided more experienced students entering college and the workforce, but reductions in the gender disparity in the cybersecurity workforce have not been seen.

While competitions overall are raising awareness and participation in cybersecurity activities, the participation of young women roughly mirrors the participation of women in the cybersecurity industry. Outreach programs by schools,

universities, competition organizers, and other organizations are working to improve the gender imbalance in competitions.

2.5.4 Lack of mentors

Studies (Shumba et al. (2013); Glass et al. (2013)) point to the lack of mentors and role models as a significant factor in fewer girls entering cybersecurity studies in middle school, high school, and college. Younger females, looking at the cybersecurity industry, see men rather than women, which amplifies the perception that it is a male-domain industry. Cheryan, Siy, Vichayapai, Drury, and Kim (2011) found that the gender of the mentor was not as important as the image projected by the mentor in helping women believe in the possibility of success in STEM fields. If the mentor projected a stereotypical ‘solo geek’ image, girls were less likely to believe that success was possible in the field presented by the mentor.

Lack of mentors and role models for young women is a significant problem in getting more young women interested in the cybersecurity industry. While the literature disagrees on the impact of a gender-mismatched mentor, the image presented by the mentor has a significant impact on the interest of the mentee in the cybersecurity industry.

2.6 Retention

The other major factor contributing to the lower participation of women in the cybersecurity industry is the lower retention rate of women in the industry. Per LeClair, Shih, and Abraham (2014), the retention rate of women in Science, Technology, Engineering, and Math (STEM) is about 60%, while the retention rate of men in the field is 80%. The researchers point out numerous possible reasons for the lower retention rate,

including "...job or climate dissatisfaction, pay inequity, pressure from family issues, gender discrimination, lack of social change, or lack of support from employers for advancement" (p. 2). Rogers (2015) points out that women are almost three times as likely to leave the IT industry (which includes cybersecurity) as men.

Cech, Rubineau, Silbey, and Seron (2011) found that nearly as many women leave male-dominated professions (such as the cybersecurity industry) as do enter, which would leave the gender gap essentially stable unless the field was growing, in which case it could cause the gender gap to widen. The cybersecurity industry is growing rapidly. The researchers also found that the decision to leave was voluntary, but strongly influenced by factors that are discussed later in this chapter, such as Impostor Phenomenon.

Singh et al. (2013) note that about 50% of women trained as engineers leave the field compared with only 10% of men leaving the engineering field. The researchers focused on the intent to leave an organization as a signal for leaving the field and note that research is lacking regarding why women choose to leave STEM fields.

Rather than comparing the retention rate of women to that of men, Glass, Sassler, Levitte, and Michelmore (2013) compare the retention rate of women in STEM occupations to the retention rate of women in non-STEM occupations. The authors found a significant difference in the retention rate of women in STEM versus other professional fields. After 12 years, 50% of women in STEM have left the field, versus only 20% of women in non-STEM occupations (50% retention in STEM versus 80% retention in non-STEM). The authors note that "...the disparity in retention between STEM and non-STEM professionals is almost entirely due to STEM women switching out of STEM

fields but not out of the labor force” (p. 11). Women are not leaving the workforce: women are leaving STEM fields.

There is a clear difference in the retention rate of women and men in STEM and the cybersecurity industry. Combined with the smaller pipeline of women than men entering the cybersecurity industry, this leads to the current gender gap in the industry. A better understanding of why women leave the industry may help organizations ameliorate the conditions that are causing the lower retention rate. Higher retention along with initiatives for getting more young men and women interested in the field may help close the current employment gap.

2.7 Independent Variables

The independent variables in this study are comprised of demographic information about the respondent. While many different demographics can be collected, this study reduced the possible independent variables to a set of three, based on the necessity of limiting the scope of the study and on the extant body of research literature.

2.7.1 Time working in the cybersecurity industry

Regarding time working in the cybersecurity industry, the literature is not settled. Glass et al. (2013) found, while tracking job tenure among women in a longitudinal study, that “...many bad job matches end quickly in the first year of employment” (p. 8). The researchers found that most of the moves out of STEM fields happen in the first five years of employment. Additionally, the researchers found that women in STEM fields do not experience the ‘settling’ effect that is observed in other industries. There was little connection between higher age/skill levels and a lower rate of women leaving STEM industries:

However, women in STEM fields do not react as positively to increasing job satisfaction, job tenure, and advancing age, suggesting that climate issues or lack of “fit” between worker and job persist for longer periods of time in STEM careers. (p. 16)

The researchers also found that, with increasing tenure in a job, men are more likely to be promoted into supervisory positions than women. This could tie back to the lack of settling of women in STEM over time. Because women are not being promoted into supervisory positions, women with tenure are not settling into roles in STEM fields.

In contrast, Buse, Bilimoria, and Perelli (2013) studied why women persisted in the engineering fields rather than why women leave engineering fields. The researchers found that women with longer tenure in engineering fields were more adaptable, finding ways to ‘fit in’ with the male-dominated field. The persisting women experienced similar workplace issues as did the women who opted out of engineering but adapted to the environment. The impact of barriers to retention may be reduced over time as women are forced to adapt in order to maintain tenure. This disagrees with the findings of Glass et al. (2013), who found that women did not tend to ‘settle’ in the industry.

The extant literature disagrees on the importance of the length of the career on the retention rate of women in the cybersecurity industry. On the one hand, there was no ‘settling’ effect, where the retention rate of women rose along with tenure in the cybersecurity industry. Alternatively, the women that stay in the industry are seen as more adaptable and likely to persist. Using this demographic as an independent variable in the study may help clarify how time in the cybersecurity industry relates to retention in the industry by measuring the perceived impact of the retention barriers compared to the respondent’s time in the industry.

2.7.2 Current position level

A phenomenological study by Johnson (2013) investigated why there were so few women in executive positions in the cybersecurity industry. The results of the study suggest that issues such as work/life balance and the scarcity of mentors increase in impact as a woman climbs the corporate ladder. Increased duties result in longer hours at the office (and less teleworking), while the lower numbers of women in the upper echelons of the cybersecurity industry reduce the probability of finding a female mentor as a woman is successful and climbs higher on the corporate ladder.

Reed et al. (2017) found significant variance based upon position level in women reporting any form of workplace discrimination based on ethnicity, gender, or cultural group. In what seems to be a counter-intuitive result, women in the upper echelons experienced significantly more workplace discrimination than women in lower-level positions. 67% of female C-level executives reported workplace discrimination, while that number dropped to 51% for female managers and 35% for female entry-level workers. One possible factor for a higher percentage of women in higher level positions experiencing discrimination is that the women have been in the industry longer, resulting in more time to experience discrimination. Another possibility is that, with fewer positions available for any gender at higher levels, the competition results in higher levels of discrimination. In Blau and Kahn's study (2017), the gender wage gap was found to be narrowing more slowly in the upper echelons of wage levels, and the higher skill level positions have larger wage gaps.

The literature appears to show that there is a relationship between position level of women and retention of those women in the cybersecurity industry. Additionally, there

appears to be a relationship between position level and the experience of discrimination or harassment, which makes up one of the barriers to retention in this study. It may be that, because there are so few women in the executive levels of the industry, it is more noticeable when women leave. Selection of current position level, with multiple steps in the career ladder, as an independent variable may help confirm the increasing impact of these retention barriers as women rise in level in the cybersecurity industry.

2.7.3 NICE cybersecurity workforce framework category

In 2008, The Federal Chief Information Officers Council began working on a framework to describe the different cybersecurity roles in the federal government. The Comprehensive National Cybersecurity Initiative, signed in 2008, required multiple agencies to develop a cybersecurity workforce framework, with a draft in September 2011 that became the first National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. Version 2.0 was released in 2014, and the current version of the Framework was released as NIST SP 800-181 in August of 2017 (Newhouse, Keith, Scribner, & Witte, 2017). The goal of the NICE Cybersecurity Workforce Framework is to provide “...organizations with a common, consistent lexicon that categorizes and describes cybersecurity work” (p. 2).

The NICE Cybersecurity Workforce Framework is composed of 3 tiers: Work Roles, Specialty Areas, and Categories (in ascending order). Work Roles are described in terms of tasks and requisite knowledge, skills, and abilities. There are 52 work roles in the Framework that support 33 Specialty Areas, which support 7 Categories. The 7 Categories (and 33 underlying Specialty Areas) are:

- Securely Provision
 - Risk Management

- Software Development
- Systems Architecture
- Technology R&D
- Systems Requirements Planning
- Test & Evaluation
- Systems Development
- Operate and Maintain
 - Data Administration
 - Knowledge Management
 - Customer Service and Technical Support
 - Network Services
 - Systems Administration
 - Systems Analysis
- Oversee and Govern
 - Legal Advice and Advocacy
 - Training, Education, and Awareness
 - Cybersecurity Management
 - Strategic Planning and Policy
 - Executive Cyber Leadership
 - Program/Project Management and Acquisition
- Protect and Defend
 - Cyber Defense Analysis
 - Cyber Defense Infrastructure Support
 - Incident Response
 - Vulnerability Assessment and Management
- Analyze
 - Threat Analysis
 - Exploitation Analysis
 - All-Source Analysis
 - Targets
 - Language Analysis
- Collect and Operate
 - Collection Operations
 - Cyber Operational Planning
 - Cyber Operations
- Investigate
 - Cyber Investigation
 - Digital Forensics

These categories were selected and refined by the authors of the framework to represent the widespread of different roles within the cybersecurity industry.

The NICE Cybersecurity Workforce Framework Category was selected as an independent variable in order to investigate whether the selected retention barriers

discussed below affect women differently based on the type of work that is done in the cybersecurity industry. For example, do women working in training experience the same impact of a hostile work environment as women working in a security operations center or as part of a penetration testing team? Similarly, do women working in digital forensics experience Impostor Phenomenon at the same level as women working in security awareness programs? Regardless of the industry (e.g., health, manufacturing, financial, government), the NICE Cybersecurity Workforce Framework Categories are relevant, and respondents from any industry will be able to determine the appropriate category.

2.8 Dependent Variables

The dependent variables of this study are selected factors affecting retention of women in the cybersecurity industry. Cybersecurity is part of Information Technology, which is part of STEM. This section presents research supporting various factors that have demonstrated impact on retention of women in STEM, IT, and cybersecurity.

2.8.1 Lack of mentorship

In addition to impacting the pipeline of women coming into the cybersecurity industry, lack of mentors for women in the industry is widely cited in extant literature as an important factor in the low retention rate of women in STEM and the cybersecurity industry. This lack of mentors and mentoring, per Drew (2015) can be both formal and informal. Formal mentor programs may not be present so that the only real mentoring happening is the informal variety happening through “buddying systems” of men (p. 3). The frequent occurrence of buddy mentoring between men (and the lack between women due to the lack of women) is another factor that is examined under Hostile Work Environment.

Johnson (2013) created a model that includes mentoring as well as other factors discussed in this literature review (see Figure 2), and stated that mentors showing interest and providing

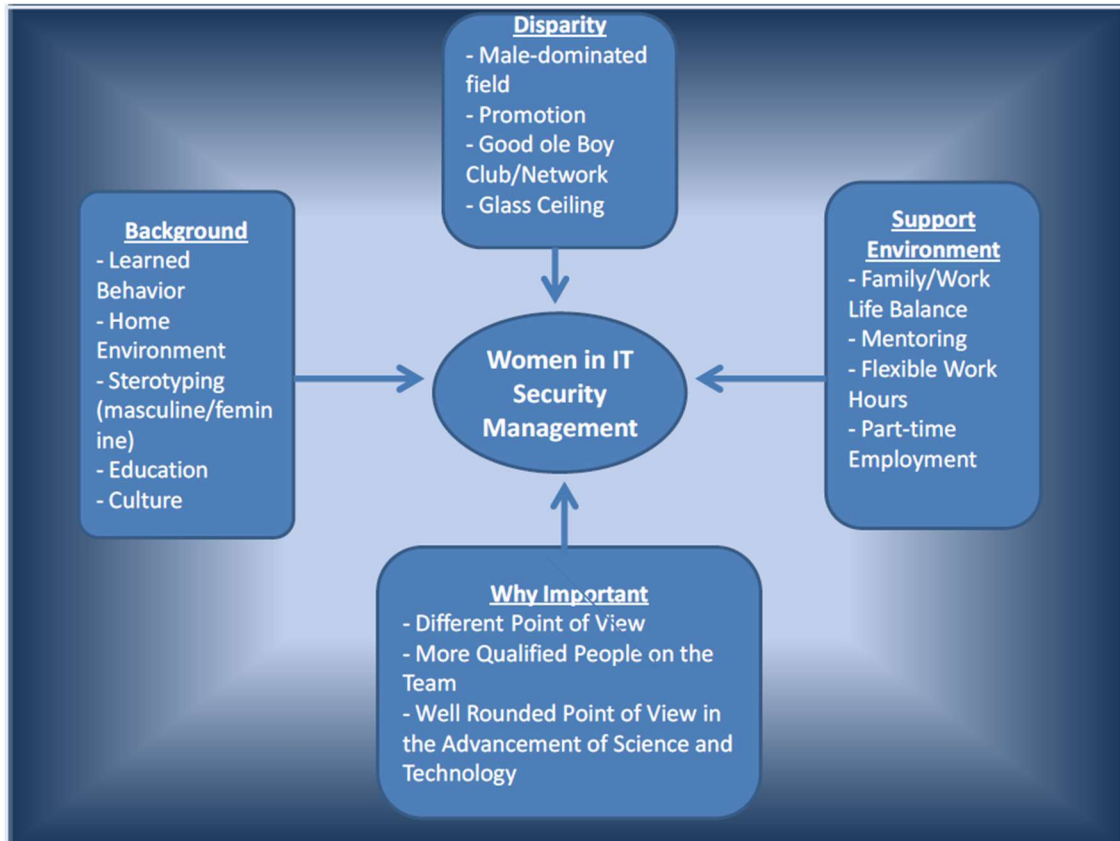


Figure 2: Johnson's model for the low numbers of women in STEM senior management (2013, p. 13).

role models help women succeed at work. The lack of women in the cybersecurity industry hurts the chances of women to get female mentors. Men may be good mentors, but men cannot as effectively fill in as role models. Female executives interviewed by Johnson point out "...how sad it was to attend IT security conferences and professional

IT security organization chapter meetings with so few females in attendance” (p. 56). Johnson’s study was to examine why there are so few women in executive roles in the cybersecurity industry. As women climb the corporate ladder, there are fewer women on the rungs above them to provide career mentoring, which becomes a self-feeding problem. Those women that are in a position to mentor other women may be hesitant for fear of being seen as mothering the mentee, which could harm the perceived professionalism of the mentor. In Johnson’s study, respondents overwhelmingly chose lack of mentoring as a major factor leading to fewer women in cybersecurity leadership positions.

LeClair, Shih, and Abraham (2014) point out that while equal pay and advancement paths are important for the retention of women in cybersecurity, mentoring is more important. The point made is that the mentor does not have to be female but must take an interest in the mentee’s success. Littlejohn (2016), studying women that have risen in the ranks of corporate security, found that women do not require women as mentors, just mentors that are active and interested in helping. While some of the respondents advocated for more women as mentors (relating that to success), the majority of the respondents said that the gender of the mentor was not an issue. Drury, Siy, and Cheryan (2011) found equal efficacy in recruiting women into STEM between male and female mentors but conclude that women role models and mentors are more effective for keeping women in STEM fields. The researchers go so far as to say that “...female role models are key to the retention of women in STEM fields” (p. 268). Kaspersky (2017a) found that only 42% of respondents felt that gender mattered in choosing role models in the workplace.

The Society of Women Engineers study (Holmes, 2016) explored company culture as a potential cause for high female attrition in STEM professions. The authors found that coaching/mentoring was one of the top priorities that women leaders found missing from the STEM workplace. Another top ten missing priority is leadership development. The study did not specify if the gender of the coach or mentor was important, just that the coaching or mentoring was missing.

Delmont (2016) found in researching women in leadership positions in Information Technology, that some of the female study participants had male sponsors or mentors, while others had female sponsors or mentors, without an indication of any difference in effectiveness. Delmont did find that more women were mentoring women than were men mentoring women. One important finding is that:

Some women in lower level positions in IT fields do not feel comfortable approaching women in IT executive positions. Too few women are seen in IT executive position in organizations, and as a result the few women that exist are oftentimes stretched, stressed and pressed for time, which can prevent them from reaching out to other women. This sends a negative message that women in executive positions are too busy to help them... (p. 142)

This finding magnifies the impact of having fewer women in upper echelons of industry and reduces the probability of entry-level women being mentored by senior women.

The research is divided on whether the gender match between mentor and mentee significantly affects the success and effectiveness of the mentor/mentee relationship but agrees on the importance of mentoring in industry retention. Female mentors are difficult to find due to the gender gap in the cybersecurity industry (female mentors become even harder to find as women rise in management level), and there may be an issue with men wanting to mentor women. Drew (2015) sees a lack of men willing to mentor women as a side effect of the 'good old boy' network, discussed later in this chapter. Drew also

sees the lack of women in senior management positions as impacting the advancement of women, due to lack of role models in senior management. Some interviewees reported being told by other women that “you could only succeed in this business by behaving like a man” (p. 5).

Lack of mentorship can impact a woman’s career in many ways, including interrelations with other dependent variables such as impostor phenomenon. Having a strong mentor might reduce the impact of one’s feelings of inadequacy or lack of technical skill. Additionally, having a strong female role model or mentor may ameliorate some of the impact of a hostile work environment, another of the dependent variables in this study. Including lack of mentorship as a dependent variable, whether due to needing more female mentors or due to the ineffectiveness of male mentors, may provide valuable guidance for the need and design of mentor programs.

2.8.2 Impostor Phenomenon

Neureiter and Traut-Mattausch (2016) define Impostor Phenomenon as “...an internal experience of intellectual and professional incapability despite objective evidence to the contrary” (p. 1). One interesting finding in this research is that employees suffering from Impostor Phenomenon tend to fear success at work because being promoted (while not feeling qualified) would lead to greater friction with co-workers, who are perceived to know that the employee is not suited for the promotion. The self-perception that the individual is not worthy of the success directly impacts career planning, as those employees affected by Impostor Phenomenon and fearing success did not conduct significant career planning.

As Figure 1 shows, the Fear of failure, Fear of success, and Low Self-esteem combine to form the Impostor feelings, which lead to career impacts. Lack of career planning, career striving, and motivation to lead could result in lower retention in the job or the industry, as the individual is not planning or preparing.

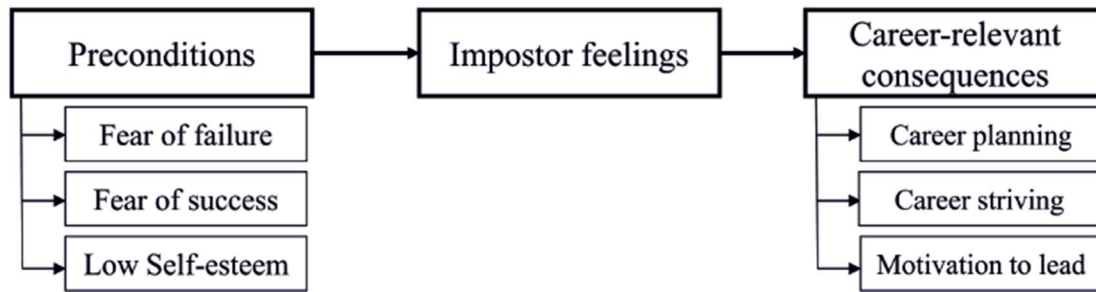


Figure 1: Neueiter & Traut-Mattausch (2016) model of Impostor Phenomenon and impact on career (p. 3).

Early seminal research into Impostor Phenomenon (Clance & Imes, 1978) found that the feeling of being an impostor can be implanted early in life via two sources. One source is the communications that the young girl is the socially adept sibling while the brother is the smart sibling. The female sibling grows to doubt comparative innate intellectual capabilities, which impacts future attitudes towards any effort demanding intellectual capacity. This source may not be an overt effect. The other source is communications that the young girl has all the attributes needed to be anything or do anything in life. Upon discovering that there are achievements that cannot be attained, self-doubt begins to grow. One finding of Clance and Imes is that while men are more likely to attribute success to internal traits, women are more likely to attribute success to external factors or short-term (not inherent) internal factors. For example, while a man might think a promotion was attained due to a job well done, a woman might believe

promotion arrives because ‘a token woman was needed’ or ‘there was a temporary shortage of qualified candidates.’ Additionally, the researchers found that Impostor Phenomenon is rarer among men than women, and when it does occur in men, it is usually with lower intensity than with women.

Buse, Bilimoria, and Perelli (2013) performed a study regarding the retention of women in U.S. engineering careers. A small sample (31 women) qualitative study was performed with 21 ‘persistent’ engineers and 10 ‘out-opting’ engineers. Self-efficacy and confidence played a significant role in 100% of the persistent engineers, while self-doubt and lack of confidence played a significant role in 90% of the out-opting engineers. The researcher found that the persistent engineers were more likely to express work identity in terms of professional engineering, while the out-opting engineers expressed identities in terms inconsistent with professional engineering. While not directly addressing Impostor Phenomenon, this study tied self-efficacy and confidence to retention of women in STEM professions.

Cech et al. (2011) defined Professional Role Confidence as a person’s confidence in the ability to do what is demanded by a professional role. The researchers found that success in a role sprang from technical competence, self-confidence, and personal commitment regarding the profession. The researchers identified ‘expertise confidence’ (the technical confidence) and ‘career-fit’ confidence (the confidence that the career fits with one’s aspirations and personal values) as the two parts of Professional Role Confidence. The study found “...professional role confidence is cultivated more successfully in men than in women engineering students, leaving women less likely to

plan to complete the engineering major or pursue a career in engineering” (Cech et al., 2011, p. 7).

Drew’s (2015) study into why women do not progress into senior management at the same rate as men identified what is termed the “stretch factor” (p. 3):

Where a job specifies 10 desirable requirements – men will apply if they hold 3 or 4 of them, while women would feel uncomfortable applying without at least 8 - “*I’ll wait until I’m ready...*” whereas for men it is “*I’ll give it a go.*” (p. 3)

Men are more willing to stretch individual qualifications to meet a job’s requirements than are women. Drew goes on to point out that men move around in jobs more frequently than women (because of the stretch factor), with women showing more insecurity and lack of self-confidence, which ties to Impostor Phenomenon. The ability to move around in one’s profession can add to job satisfaction and increased retention. Drew lists lack of confidence and lower career goals as major inhibitors to success for women in STEM careers. The lack of women in senior management roles may also impact women in cybersecurity due to lack of mentorship, as discussed earlier.

Impostor phenomenon manifests in several different ways:

- Not applying for promotion because one does not feel personal skills meet enough of the requirements
- Shrinking from taking credit for success at work because one fears antipathy from co-workers who are perceived as believing the person is not deserving of accolades
- Not planning for the future of one’s career, leaving career progression to chance
- Self-doubt and lack of confidence at work
- Not identifying with one’s professional role

Singh et al. (2013) created a model (Figure 2) that combined organizational support and two psychological factors, self-efficacy (related to Impostor Phenomenon) and outcome expectations to predict intent to leave the organization.

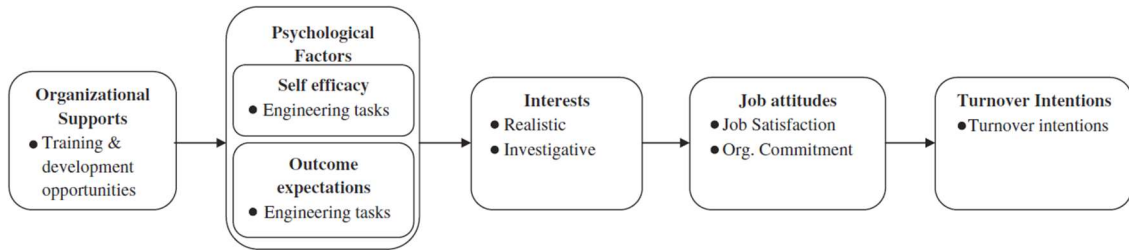


Figure 2: Predictive model for intent to leave organization (Singh, et al., 2013, p. 282).

Contrasting with other research, the researchers found that self-efficacy did not have a strong impact on intention to leave the organization. While there was a positive relationship between self-efficacy and job attitude, the real impact on turnover intention, outcome expectations stemming from organizational supports had a significant impact on turnover intention. Developmental experiences played an important role in positively impacting the outcome expectations of female engineers.

Most of the extant research found that Impostor Phenomenon has a significant effect on women in STEM fields. While research shows that men and women can be affected by Impostor Phenomenon, it is found in women more frequently and with more intensity. Including the Impostor Phenomenon as a dependent variable in this study may provide valuable information regarding the respondents' perceived impact of a psychological factor that is difficult to directly measure.

2.8.3 Hostile work environment

Studies of Science, Technology, Engineering, and Math (STEM) professions are included here, as cybersecurity falls under STEM and there is a lack of research specifically tied to cybersecurity. A hostile work environment encompasses many

elements, some active (such as harassment) and some passive (such as work/life balance). Both active and passive elements may contribute to women not staying in the cybersecurity industry. For example, Seron, Silbey, Cech, and Rubineau (2016), in a longitudinal study of engineering students during university and after graduation, found several underlying reasons for women leaving the engineering field. Female students experienced both dismissal and active sexual harassment. Some female students in internships were assigned more 'social' or administrative tasks such as communicating with customers or taking meeting minutes, where male students in internships were assigned more technical tasks. The perception was that engineers did not perceive the female students as serious engineers. Additionally, female students experienced active harassment, being propositioned or 'hit on' by more senior engineers. Internships are a chance for students to experience the real workplace, and female students saw a workplace that did not appeal to them.

A study commissioned by the Society of Women Engineers (Holmes, 2016) found that (referring to Engineering) "...30 percent of women who leave the profession cite workplace climate as the reason" (p. 10). The study had been commissioned due to the recognition that retention of women across all STEM professions is low. The major finding of the study is that women are willing to adapt to work/life balance issues and even withstand unfair evaluations and lack of promotion. What drives women away is the fact that organizations:

...tolerate persistent obstacles to attaining their company and career goals. The female leaders who participated in the study express this frustration as a lack of accountability. *Accountability* was their number one personal and desired cultural value, and the one they said was missing from their workplaces (p. 10).

The age group most likely to leave the profession, as shown by the study, is 31 to 50, which again demonstrates the lack of ‘settling’ described by Glass et al. (2013) and discussed in the earlier section on the independent variable ‘Time in Industry.’

Delmont (2016) found women adapting to working in male-dominated company culture. The most effective women leaders in the study found ways to manage cultural challenges in the workplace. As an example, some of the women studied used shortened names, using a more masculine-sounding version in order to fit into the culture. Delmont concludes that:

...gender and workplace cultural issues cause much frustration for women in IT fields, and supported by the literature regarding the obstacles facing women in IT fields. They are the primary contributors to why many women in IT fields leave their high paying jobs, and sometimes exit the IT field altogether (p. 143)

Discrimination

Reed et al. (2017) found that in the cybersecurity industry of North and Latin America, 51% of women reported discrimination compared to 15% of men. The types of discrimination reported included a mix of active and passive discrimination:

- Unconscious discrimination
- Unexplained lack of promotion
- Exaggerated reports of mistakes or errors
- Tokenism
- Overt discrimination

The United States had more women in cybersecurity reporting discrimination (53%) than any other country in the western hemisphere, with the closest being non-Mexico Latin America at 47%.

Discrimination can include being overlooked for input (Johnson, 2013) which can be unconscious or conscious. Respondents often reported being ignored, with inputs drowned out until providing some form of proof of competence and worthiness to male

co-workers. This was seen by respondents as an aspect of the male dominance of the cybersecurity industry, along with reports of women's ideas not being accepted without being transmitted via a male co-worker, Glass et al. (2013) found that "Because of the lack of a critical mass of women in STEM fields, especially at higher levels of authority, women entering STEM occupations are particularly vulnerable to the ideologies of gender-conservative men..." (p. 4)

This may describe a circular environment where the lack of women staying in cybersecurity leads to more discrimination, which may lead to more women leaving the industry. Not being asked for input in a male-dominated field is closely associated with the 'good old boy' network aspect, discussed later in this chapter. The researchers also hypothesize that the atmosphere in male-dominated STEM fields may interact negatively with the gender ideology of more liberal women, which results in increasing the probability of those women leaving the field.

Wage inequality

Wage inequality can be viewed as discrimination. Drawing parallels between the UK and the USA, Drew (2015) found a gender pay gap between comparable graduates in the UK within six months of graduation, largely because women do not negotiate for a higher starting salary as stringently as men. This is realized in that although women are more likely than men to earn honors degrees, women are half as likely as men to get a starting salary over €45,000. This disadvantage accumulates at each step of the ladder in the workplace, as a small gap becomes larger over a career. Drew also found that a lack of transparency in bonus programs contributed to a gender wage gap. Blau and Kahn (2017) found that while the gender wage gap narrowed overall by 2010, it narrowed more

slowly at the highest wage levels and the gap was larger for highly skilled positions. This finding brings in the independent variables such as Current Position Level and NICE Cybersecurity Workforce Framework Category. Per Reed et al. (2017) there is a real gender-based wage gap in cybersecurity. Between 2015 and 2017, the wage gap closed at the Executive level but is still at a 3% difference. The gap has worsened at the non-Managerial level, growing from 4% to 6% in the two years studied.

The literature is clear that a wage gap exists between men and women in STEM and specifically in cybersecurity. The gap is present at hiring and grows with each step of the career ladder, as women's wages fall farther and farther behind men's wage. While there is evidence of some success in narrowing the gap, there are differences based upon position level and the type of work being done. The literature supports the selection of time in industry, current position level, and NICE Cybersecurity Workforce Framework Category as independent variables.

Work/life balance

Work/life balance can be viewed as another passive aspect of a hostile-to-women work environment. Johnson (2013) found that most women interviewed for that study favored some kind of program that supported work/life balance for all employees (not just women) with the idea that these would help encourage women to stay in the cybersecurity industry. While work/life balance affects all employees, it tends to impact women more significantly as most women with children at home have the larger role in child rearing. Work/life balance programs include flexible working hours and telework. Glass et al. (2013) found that even if these programs are available women may be less willing to take advantage of them since male counterparts view using the programs as

demonstrating a lower commitment to the company. The researchers also found that having children was a strong predictor of women leaving the STEM fields due to a lack of work/life balance. Women who, in adolescence, expected to marry late in life and not have children were much less likely to leave the STEM field than young women expecting to marry early and raise children. The act of getting married led to an 84% increase in the odds that women would leave a STEM field. Parental leave as a work benefit reduced the chance of women leaving STEM by 39%.

Blau and Kahn (2013) conclude that, while work/life balance-friendly policies (e.g., family leave and part-time on demand) help encourage women to stay in the workforce, women that take advantage of the work/life balance policies may not be chosen for advancement. The researchers found that availability of these policies may even hurt all women since executive management cannot tell which women may take advantage of options such as shifting to part-time or flex-time, both of which are disadvantageous to holding a senior management position. Drew (2015) confirms that men and women that want to move up in the organizational hierarchy tend to eschew taking advantage of work/life balance programs, as those programs are viewed as incompatible with aggressive career climbing. Additionally, Drew found that many women opting out of STEM careers left because of the lack of work/life balance. The respondents emphasized that organizations need more than just a policy, organizations need to demonstrate that all employees at all levels saw the importance of work/life balance. Real work/life balance flexibility arose as an important prerequisite factor for women to consider rejoining STEM industries. Interestingly, Drew also found that

work/life balance was important to younger women with no existing (or plans for) family commitments.

Delmont's 2016 study found most respondents having work/life balance challenges. Factors that magnified the work/life balance challenge included marriage, children, and having significant others. Delmont states:

The participants in this study had family and personal responsibilities outside of work, which had a direct impact on their decision making, such as whether to take a higher-level position, or whether to take a job that required working excessive hours outside of normal work times (p. 146)

The research literature shows that work/life balance is an important factor in the decision to stay in STEM or cybersecurity fields. While not comparing women directly to men in this regard, there are indications that, due to the minority aspect, women are more affected by work/life balance factors than men. For example, the reluctance to take advantage of work/life balance programs may result in women being less happy about being in STEM fields.

'Good old boy' network

The 'good old boy' network is a form of benevolent discrimination in favor of men, where men benefit from discriminatory practices such as a higher frequency of networking and pre-selection for promotion, among others. Per LeClair and Pheils (2016), the 'good old boy' network is simply "...men taking care of their own" (Chapter 6, para. 6). Johnson (2013) found that men's networking extends beyond the work environment, such as attending sporting events or group outings such as golf (golf events generally tend to be gender separated). Women that are not interested in participating due to the nature of the work-external activities miss out on the stronger interpersonal

bonding that results from these activities and can be viewed even more strongly as outsiders.

Drew (2015) points to the concept of ‘homo-social’ behavior, which:

...reinforces the need to appoint/retain and progress ‘people like us’ and extends into dress/speech codes, social activities and general conformance to ‘what is acceptable.’ Underlying homo-social behavior is the phenomenon of unconscious bias that permeates human behavior and reinforces racial and gender stereotypes. (p.4)

Drew also found corporate culture dominated by male behavior and preferences, with managerial styles that leaned away from nurturing and collaboration.

The ‘good old boy’ network can also materialize simply as the perception of a ‘men only’ club. Warnert (2015), in a study regarding women in the Agile development community, points out two reasons for women feeling unwelcome. First, some women feel unwelcome in the Agile community because there were no women involved in writing and polishing the Agile Manifesto, the document that served as the foundation for the Agile movement. Second, women attending conferences and meeting do not see many other women attendees, which reinforces the idea that cybersecurity is a male-domain industry. Delmont (2016) describes women working within a gendered political system favoring men. As previously discussed in this chapter, women experience the same isolation in attending cybersecurity events. Women in this type of system are denied access to power and are outside the decision-making networks. This not only puts women at a disadvantage regarding decisions made, but also prevents them from being involved in making those decisions. Kabat-Farr and Cortina (2014) reinforce this concept, discussing gender harassment, which “...alienates and isolates women, reducing

their access to information and opportunities (typical effects of female underrepresentation)” (p. 60).

The ‘good old boy’ network is a strong example of a mostly passive effect of a hostile work environment. The actions, for the most part, are not taken directly against women, but in favor of men, resulting in a work environment that can be effectively stacked against women.

Sexual harassment

Kabat-Farr and Cortina (2014) describe two aspects of sexual harassment in the workplace, sexual-advance harassment and gender harassment. With sexual-advance harassment, women receive more sexual overtures than men in male-dominated workplaces, with one possible cause being sex role spillover theory (SRST), where men carry over sexual roles into the workplace so that some women are perceived as potential sexual partners rather than co-workers. This perception generates unwanted sexual advances or sexual coercion, which is the demand for sexual favors in return for positive employment actions or the avoidance of negative employment actions.

Gender harassment is not sexual but is gender-based and is aimed at the rejection of women working in a male-dominated area. With gender harassment, women experience “...interpersonal derogation, scorn, and rejection, which are common responses to women who violate gender stereotypes by doing “male” work” (p. 60). The researchers found a direct link between the underrepresentation of women in the workplace and elevated gender harassment, but not with elevated sexual harassment. The researchers conclude that the elevated harassment of women in male-dominated fields is due more to rejection than attraction.

Delmont (2016) found that women in Information Technology experienced multiple forms of harassment and discrimination, but rarely attempted formal resolution. Even though organizations have rules and policy in place regarding sexual harassment (as well as federal laws), organizations, in general, do not have an effective approach to manage sexual harassment claims. Women tend to not file formal complaints due to fear of some form of retaliation, enhanced by the knowledge that the organization is inept in dealing with that type of situation. With few examples, women do not know how to handle harassment and other gender issues in the workplace. Delmont notes that “A few of the participants confronted cultural and gender related issues head-on with the aggressor(s). However, most women ignored them and considered gender and cultural issues business as usual in the workplace” (p. 142-143).

Sexual harassment, whether sexual advance- or gender-harassment, is an active aspect of a hostile work environment, where men are actively acting against women. As such, it is an important component of a hostile work environment.

Including hostile work environment as a dependent variable in the study will help illuminate the impact on women working in the cybersecurity industry and may guide organizations working toward reducing gender imbalance.

2.9 Conclusion

There are two primary reasons for the gender gap in the cybersecurity industry: a lack of women in the educational pipeline and the low retention rate of women in the cybersecurity industry. This study focuses on factors affecting the low retention rate. Some of the most important factors for low retention of women in the cybersecurity industry are:

- Lack of mentorship (Johnson, 2013)
- Impostor Phenomenon (Buse, Bilimoria, & Perelli, 2013)
- Hostile Work Environment, which is comprised of multiple factors
 - Discrimination (Reed et al., 2017)
 - Wage inequality (Reed et al., 2017)
 - Work/life balance (Glass et al., 2013; Blau & Kahn, 2013)
 - ‘Good old boy’ network (LeClair & Pheils, 2016)
 - Sexual harassment (Kabat-Farr & Cortina, 2014)

2.10 Summary

This chapter began by providing the historical context for cybersecurity workforce development. The United States government recognized the need for the cybersecurity industry in the early 1960s (Warner, 2015). More recent developments, such as the NSA’s Centers for Academic Excellence program and the National Initiative for Cybersecurity Education, were put in place to aid in developing a pipeline of cybersecurity professionals entering college and proceeding into the workplace. The cybersecurity industry has an employment gap, with over 301,000 jobs currently open (Cybersecurity Supply and Demand Heat Map, n.d.), a number that has risen since 2015 (Setalvad, 2015).

The chapter also demonstrated a significant gender imbalance in the cybersecurity industry, with women only making up 10-15% of the industry workforce (LeClair, Shih, & Abraham, 2014). This imbalance is partly due to fewer young women being interested in joining the cybersecurity industry, the so-called ‘industry employment pipeline’, due to the image of the industry presented, the lack of awareness of the industry seen in younger women, the lack of mentors and role models for younger women, and the focus on competition rather than collaboration. The other major factor causing the gender gap is the lower retention rate of women in the cybersecurity industry (LeClair, Shih, & Abraham, 2014). In STEM, women exit the field at a 50% rate compared to 20% in non-

STEM fields (Glass et al., 2014). LeClair et al. (2014) found that 80% of men stay in the cybersecurity industry compared to only 60% of women. The chapter then discussed literature regarding multiple retention factors that affect the retention of women in Science, Technology, Engineering, and Mathematics (STEM), Information Technology, and the cybersecurity industry and some demographics that may provide insight into how those retention factors impact women and decisions to leave or stay in the cybersecurity industry.

The next chapter provides a discussion and rationale for the methodology and design selected to study the research questions. The research population, sample frame, and sample will be explained. The data collection instrument will be described along with how it will be employed/ implemented and why it is the correct instrument for the study. Chapter 3 also describes the statistical analyses that will be used, and the rationale for choosing those analyses. Discussions of the study's validity, reliability and limitations will also be provided. Demographics and retention factors discussed in this chapter make up the respective independent and dependent variables of the study.

The cybersecurity industry in the United States has a significant employment gap between the number of jobs open and the available qualified workforce. The current gap, per the Cybersecurity Supply and Demand Heat Map (n.d.) is over 301,000 job openings (with over 768,000 jobs filled). The number of job openings in cybersecurity in 2015 was estimated at 209,000 (Setalvad, 2015), indicating that the employment gap continues to grow. Government, academia, and industry are working to find approaches to closing the cybersecurity industry employment gap. The cybersecurity industry also has a gender gap. Women make up about 50% of the general workforce, but only make up 10-15% of

the United States cybersecurity workforce (LeClair, Shih, & Abraham, 2014). Closing the gender gap in the cybersecurity industry may also help close the employment gap by adding more qualified personnel to the existing cybersecurity labor pool. Recent efforts to close the gender gap have not had significant results (Reed, Zhong, Terwoerds, & Brocaglia, 2017).

The cybersecurity gender gap stems from two contributing factors, a weak pipeline of women into the industry and a low retention rate of women after joining the cybersecurity industry. A better understanding of why the retention rate for women in cybersecurity is significantly lower than the retention rate for men may help organizations keep more women retained in the industry, helping bolster the employment numbers and reduce the number of open positions.

Chapter 3 provides information regarding the specific research method and design and the appropriateness of the research method and design for studying the topic. The chapter also covers the research population, sample frame, sample, and data collection procedures. Examples from the survey instrument shall be provided along with a discussion on why the survey is an appropriate instrument for this research. The data analysis approach is discussed along with internal and external validity of the study.

Chapter 3: Methodology

3.1 Research Method and Design Appropriateness

The goal of this quantitative, correlational study was to investigate the nature (strength and direction) of the relationships between demographic factors and perceived impacts of barriers to retention among women in the cybersecurity industry. The demographic factors (independent variables) were *time working in the cybersecurity industry*, *current position level*, and *type of cybersecurity work* (as referenced by the NICE Cybersecurity Workforce Framework). The barriers to retention (dependent variables) were *lack of mentorship*, *impostor syndrome*, and *hostile work environment*.

Per Creswell (2012), the appropriate research methodology for studying the relationship between variables is the quantitative method. A qualitative study, per Cooper and Schindler (2011), is designed to "...tell the researcher how (process) and why (meaning) things happen as they do" (p. 160). Since the goal of this study is to determine the nature of the relationship between two sets of variables, qualitative research is inappropriate.

Regarding design, there are several choices within the quantitative methodology family. Descriptive Design is observational, with any hypotheses developed after data is collected ("Quantitative Approaches - Center for Innovation in Research and Teaching," n.d.). Experimental Design requires before and after measurements of two groups, with treatment applied to the test group (Creswell, 2012). Quasi-experimental Designs attempt to identify a causal relationship between variables. Correlational research, a subset of descriptive design (Cooper & Schindler, 2011) attempts to describe one or more

relationships between the research variables, with no attempt at causality. With the goal of this study being to investigate the nature of the relationships between the independent and dependent variables without identifying causality, a quantitative method with a correlational design was the correct approach.

3.2 Population, Sampling, and Data Collection Procedures and Rationale

There was no specific research site for this study. Multiple professional cybersecurity organizations were used to distribute the survey. Some of the organizations (e.g., Women in Security and Privacy, Women's Society of Cyberjutsu) cater specifically to female membership, while others (e.g., International Systems Security Association (ISSA)) have both men and women members. ISSA has a Special Interest Group for women in the cybersecurity industry. The organizations agreed to share and publicize the survey, and the survey was advertised via LinkedIn groups associated with professional organizations and via Twitter. Membership in these organizations includes women at all levels of management position (from Chief Information Security Officer to security analyst) and tenure in the industry. The cybersecurity industry organizations provided a channel for the distribution of the survey instrument.

3.3 Population

Three terms must be defined regarding respondents for a survey design, according to Creswell (2012): population, target population (sampling frame), and sample. Per Creswell, the population is a grouping of individuals with one or more characteristics that set them apart from other groups. The population for this study was women in the cybersecurity industry in the United States, regardless of the length of time in the industry, the type of cybersecurity work done, or the level of position held.

The sampling frame is the targeted subset of the total research population since it is typically unrealistic to be able to get every member of the research population to complete the survey. For this study, the sampling frame was ‘members of cybersecurity industry organizations.’ These organizations can be broadly categorized as catering either specifically to women in the cybersecurity industry (e.g. Women in Security and Privacy (WISP) and The Women’s Society of Cyberjutsu) or to all people working in the cybersecurity industry (e.g. Information Systems Security Association, Information Systems Audit (ISSA) and Control and Association (ISACA)). The general cybersecurity industry associations do not restrict membership to women, but many have special interest groups (SIGs) that are specifically oriented to women in the industry.

The research sample for this study was women in the cybersecurity industry working in the United States that self-selected by responding to the survey. The survey was advertised and communicated by the industry associations to membership, through the LinkedIn groups associated with the industry organizations, via Twitter, and by word of mouth. Leveraging an online survey approach allowed the administration of the survey access to a large set of geographically diverse women in the cybersecurity industry. As an incentive to participate in the study, five Amazon gift cards worth \$50.00 each were awarded to five randomly drawn respondents. The offer to participate in the drawing was on the last page of the survey, and respondents provided an email address for award notification purposes. Entering the email address was optional, and the instructions pointed this out. Email addresses were held separately from the other survey data and were used for the ‘thank you’ drawing. The email addresses were deleted immediately after the survey closed and the ‘thank you’ drawing was complete.

The survey site used encryption for data in transit (HTTPS, HyperText Transfer Protocol Secure). The survey data was held online in the researcher's password-protected account at the survey vendor, in the researcher's Microsoft OneDrive folder (protected by 2-factor authentication), or on the researcher's laptop (protected by password and encrypted with BitLocker whole drive encryption).

Based upon current employment numbers, there are about 768,000 cybersecurity professionals working in the U.S. (Cybersecurity Supply and Demand Heat Map, n.d.). Using recent estimates that women make up 10-15% of the cybersecurity workforce in the U.S. (LeClair, Shih, & Abraham, 2014) and 11% globally (Reed, Zhong, Terwoerds, & Brocaglia, 2017), this study used 12.5% of 768,000 (96,000) as the estimate for the total number of women working in the cybersecurity industry in the U.S.. Using a standard sample size calculator (<https://www.surveysystem.com/sscalc.htm>) with a confidence level of 95% and a confidence interval of 5%, the resulting recommended sample size was 383.

3.4 Data Collection

The study's data was collected using an online survey, with a survey instrument created by the researcher. A field and pilot test were administered before the release of the survey to the research sample population. The field test survey instrument was given to four respondents prior to Institutional Review Board (IRB) approval to check for clarity of instructions and questions. Comments were evaluated and incorporated to improve the survey instrument. Post-approval by the IRB, a pilot test was administered to four respondents to determine if the survey instrument was extracting the expected information (validation). Per Nardi (2013), respondents participating in the

field and pilot tests did not participate in the research survey as "...having them take the survey a second time could bias the results" (p. 100).

The first page of the survey had the information needed for informed consent by the respondent. The information on the first page included:

- Introduction
- Procedures
- Risks/Discomforts
- Benefits
- Confidentiality
- Compensation
- Participation
- Questions about the Research
- Consent

If the respondent consented to the study, she clicked an on-screen 'Next' button to continue into the survey (see Figure 3).

<p>Introduction</p> <p>Carl Willis-Ford at the University of Fairfax is conducting this research study to investigate the impact of barriers to retention of women in the cybersecurity industry.</p> <p><i>Please Note:</i> This survey is intended for women currently working in the cybersecurity industry in the United States.</p> <p>Procedures</p> <p>You will be asked to complete an online questionnaire. The questionnaire consists of 10 questions and will take approximately 7 minutes. Questions will include some demographic questions and questions about your perception of the impact of certain barriers to retention in your job.</p> <p>Email addresses are optional, all other questions are required. Incomplete surveys will be discarded.</p> <p>Risks/Discomforts</p> <p>There are minimal risks for participation in this study.</p> <p>Benefits</p> <p>There are no direct benefits to subjects. However, it is hoped that your participation will help researchers learn more about how to improve retention of women in the cybersecurity industry.</p> <p>Confidentiality</p> <p>All information provided will remain confidential and will only be reported as group data with no identifying information. All data, including questionnaires, will be kept in a secure location and only those directly involved with the research will have access to them. After the research is completed, the individual questionnaires will be disposed of, only the bulk data will be kept. Emails, if provided, will be deleted.</p> <p>Compensation</p> <p>Those participants that complete the questionnaire and provide an email address will be entered into a random 'Thank You' drawing for one of five \$50 Amazon gift cards.</p> <p>Participation</p> <p>Participation in this research study is voluntary. You have the right to refuse to participate entirely without jeopardy.</p> <p>Questions about the Research</p> <p>If you have questions regarding this study, you may contact Carl Willis-Ford at willis-fordc35@students.ufairfax.edu</p> <p>Consent</p> <p>Clicking 'Submit' at the end of this survey is your consent to participate in the research and including your email is consent to be in the 'thank you' drawing.</p>
--

Figure 3: Instruction page for the survey instrument.

Since it is an online survey, participation in the survey served as consent to participate in the study instead of a signature. The instruction page pointed out that the survey is intended for women working in cybersecurity. The survey instrument had a question (question number 1) to act as a qualifier for the survey. This question asked the respondent to verify that the respondent identifies as a woman and worked in the cybersecurity industry in the United States (see Figure 4).

1. I verify that I identify as a Woman and that I work in the cybersecurity industry in the United States *

Yes

No

Figure 4: Verification by respondent of fitness for survey.

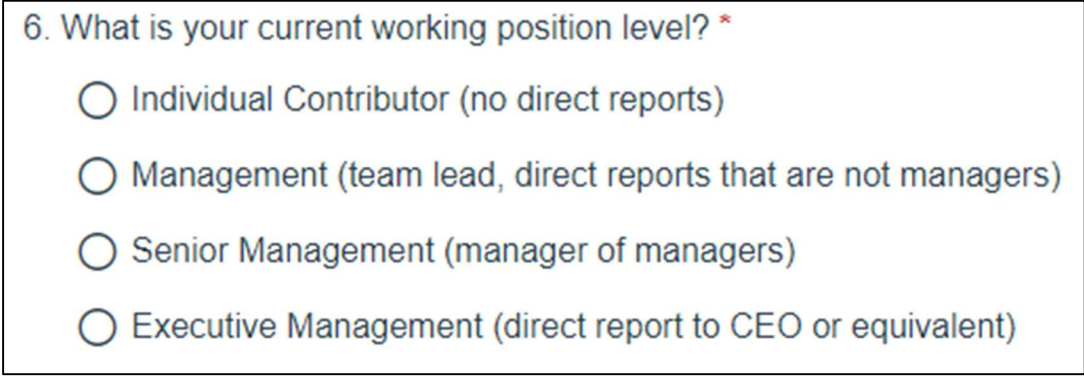
Any survey response with a response of ‘No’ to that question was discarded. Two general (non-research variable) demographic questions were asked, one regarding age and one regarding the level of education. These may contribute to further analysis combined with the other data collected. The survey instrument, for the independent variables (demographics), provided open text and radio button-style answer sets with pre-set choices for responses. For example, for ‘time in the cybersecurity industry’, the respondent was asked to enter a number, with instructions to round to the nearest whole year. Since Science, Technology, Engineering, and Math fields (STEM) are closely related to the cybersecurity industry, respondents were instructed to include time spent in a related STEM industry, but not to include employment time in other industries (see Figure 5).

4. How long have you worked in the cybersecurity industry? (include previous work in a Science, Technology, Engineering, or Math field). Please round to the nearest whole year. Do not count non-STEM work or internships. *

Figure 5: Capturing the Time in Industry independent variable.

For ‘current position level,’ the respondent chose one of the following selections:
individual contributor, management, senior management, or executive management.

There were short descriptions of each available to the respondent (see Figure 6).



6. What is your current working position level? *

- Individual Contributor (no direct reports)
- Management (team lead, direct reports that are not managers)
- Senior Management (manager of managers)
- Executive Management (direct report to CEO or equivalent)

Figure 6: Capturing the Current Position Level independent variable.

The individual contributor choice was targeted for respondents that have no direct reports. The management choice was for Team Leads and others whose direct reports are only individual contributors. Senior Managers are those whose direct reports are primarily managers, and Executive Managers are direct reports to the CEO or an equivalent position.

Lastly, for the NICE category, the survey instrument listed the categories (Analyze, Collect & Operate, Investigate, Operate & Maintain, Oversee & Govern, Protect & Defend, Securely Provision). Again, each choice had a description summarized from the NICE Cybersecurity Workforce Framework (see Figure 7).

For the dependent variables (perceived impact of retention barriers), the survey instrument used questions on a 5-point Likert-type scale. A true Likert scale (per Nardi, 2013) uses response categories that measure the respondent’s agreement with a statement,

such as ‘strongly agree,’ ‘agree,’ and the like. A Likert-type scale uses a similar ordinal arrangement, but different response categories. Fink (2003a) says “Current thinking suggests that 5- to 7-point scales are adequate for the majority of surveys that use ordered

6. What is the best fit of your *current* position in the NICE Cybersecurity Workforce Framework? (please see below for details on each choice)
 NOTE: If you work across several areas, please select the area where you spend most of your work time. *

- Analyze
- Collect & Operate
- Investigate
- Operate & Maintain
- Oversee & Govern
- Protect & Defend
- Securely Provision

Analyze: Threat Analysis, Exploitation Analysis, All-Source Analysis, Targets, Language Analysis
 Collect & Operate: Collection Operations, Cyber Operational Planning, Cyber Operations
 Investigate: Cyber Investigation, Digital Forensics
 Operate & Maintain: Data Administration, Knowledge Management, Customer Service & Technical Support, Network Services, Systems Administration, Systems Analysis
 Oversee & Govern: Legal Advice and Advocacy, Training/Education/Awareness, Cybersecurity Management, Strategic Planning and Policy, Executive Cyber Leadership, Program/Project Management and Acquisition
 Protect & Defend: Cyber Defense Analysis, Cyber Defense Infrastructure Support, Incident Response, Vulnerability Assessment and Management
 Securely Provision: Risk Management, Software Development, Systems Architecture, Technology R&D, Systems Requirements Planning, Test & Evaluation, Systems Development

Figure 7: Capturing the NICE Cybersecurity Workforce Framework independent variable.

responses. Self-administered questionnaires and telephone interviews should probably use 4- or 5-point scales.” (p. 57). Based on that assessment, this survey employed a 4-point scale. The response categories used in this research measured the respondent’s perceived impact of the retention barrier on how the respondent feels about staying in the cybersecurity industry. The perceived impact was measured as ‘none, somewhat, moderate, high.’ Some Likert-type scales include a neutral, ‘center’ choice between opposite extremes. Per Trochim, Donnelly, and Arora (2016) these are known as bipolar scales. The authors describe a ‘forced-choice’ response scale where there is no neutral or undecided response. A 4-point scale has no ‘neutral’ choice. See Figure 8.

Questions 7, 8, and 9 relate to factors that may or may not impact you individually, but that you may see elsewhere in the workplace. Please rate your perception of the impact of these factors on your desire to stay in the cybersecurity industry, regardless of whether you choose to stay or not.

7. What is your perception of the impact of Lack of Mentors on your desire to stay in the cybersecurity industry? *

None Somewhat Moderate High

8. What is your perception of the impact of the Impostor Phenomenon on your desire to stay in the cybersecurity industry?
 Note: Impostor Phenomenon is the feeling of inadequacy for the role even though there is objective evidence, such as certifications or job success, that you are qualified *

None Somewhat Moderate High

9. What is your perception of the impact of a Hostile Work Environment on your desire to stay in the cybersecurity industry?
 Note: Hostile Work Environment may include: Active or passive discrimination, wage inequality, lack of work/life balance, sexual harassment, or working in a 'good old boy network' *

None Somewhat Moderate High

Figure 8: Capturing the dependent variables.

Salkind (2012) provides guidance for questionnaires, which apply to surveys.

This guidance was taken into consideration for construction of the survey. The guidance is included as Table 1.

Table 1: Guidance for Questionnaires

<p>The Basic Assumption</p> <ul style="list-style-type: none"> • The questionnaire does not make unreasonable demands upon the respondent • The questionnaire does not have a hidden purpose • The questionnaire requests information that respondents presumably have
<p>The Questions</p> <ul style="list-style-type: none"> • The questionnaire contains questions that can be answered • The questionnaire contains questions that are straightforward
<p>The Format</p> <ul style="list-style-type: none"> • The items and the questionnaire are presented in an attractive, professional, and easy-to-understand format. • All questions and pages are clearly numbered

- The questionnaire contains clear and explicit directions as to how it should be completed and how it should be returned
- The questions are objective
- The questions are ordered from easy to difficult, and from easy to specific
- Transitions are used from one topic to the next one
- Examples are given when necessary

Note: Adapted from “Exploring Research” (8th Edition) by Neil J. Salkind, Upper Saddle River, NJ: Pearson, 2012, p. 149.

The survey was short. The first page provided information regarding informed consent, with the respondent being required to click a ‘Next’ button to continue. The second and third pages contained demographic (general and independent variable) questions. The survey was not be used to collect personally identifiable information, except optional email addresses for the ‘thank you’ drawing. The fourth page collected data for the barriers to retention (dependent variables). The bottom of the fourth page had the optional email address entry and the ‘submit’ button. The fifth and last page was a Thank You page, with no input required from the respondent. The survey was administered via the World Wide Web using a survey service (SurveyGizmo), with links to the survey posted in LinkedIn groups, on industry association websites, and on Twitter. The advantage of a web survey, per Trochim, Donnelly, and Arora (2016) is the ability to reach a large number of respondents very quickly. A recognized limitation of web surveys is that not all respondents may have easy access to computers or the internet. An assumption for this research is that women employed in the cybersecurity industry had access to both computers and the internet. The survey was available for four weeks.

Trochim, Donnelly, and Arora (2016) recommend limiting the number of ‘contingency’ or ‘filter’ questions as well as the number of ‘jump’ questions. Contingency or filter questions are questions that determine whether the respondent is qualified to respond to the survey or are used to guide the respondent to particular questions within the survey. Contingency or filter questions can lead to jump questions, where, based on the respondent’s answer, the respondent may be directed to skip one or more questions. This survey had no contingency questions and no jump questions. The instructions at the beginning of the survey (before the respondent clicking the assent button) noted that the survey is intended for women working in the cybersecurity industry. The first question on the survey was a filter question and asked the respondent to verify identification as a woman and current work in the cybersecurity industry in the United States. If the respondent provided a negative response to Question One, the survey response was discarded. The authors also recommend avoiding ‘double-barreled’ questions, which are questions containing conjunctions such as ‘and’ to package two questions into one. These kinds of questions confuse the respondents and result in answers that are difficult to interpret in that there is doubt as to which part of the conjunction the answer is referring. The only double-barreled question on the survey was Question One, which verified the status of the respondent in relation to the survey.

3.5 Validity – Internal and External

This section provides a discussion of the internal and external validity of the study. Creswell (2012) discusses validity within the context of experimental research. Since this study was non-experimental, other sources of discussion on validity were

referenced. Validity, in general, is described by Carmines & Zeller (1979) as having the quality of degree. Validity is not an all or nothing measure.

Additionally, Carmines & Zeller (1979) discuss validity as the quality of an indicator being fit for how it is being used. Thayer-Hart (2010) states that validity "...is the extent to which a survey question measures the property it is supposed to measure." Litwin (1995) provides an example that if an instrument is supposed to measure pain, it should not measure a related aspect, such as anxiety, instead. There are two broad types of validity typically presented: external and internal.

Internal validity, as described by Wiersma (2012), helps to show that what is intended to be measured is what is truly measured. Alternatively, as Fink (2003b) states, an internally valid design is "...free of nonrandom error or bias" (p. 60). Fink (2003b) lists several risks to avoid in order to maintain internal validity. Trochim, Donnelly, and Arora (2016) provide four approaches to rule out threats to internal validity: by argument, by measurement/observation, by analysis, and by preventative action. Table 2 lists Fink's internal validity risks and the approaches (by argument and by preventative action) used in this study to mitigate them.

Table 2: *Avoiding Risks to Internal Validity*

Internal Validity: Risks to Avoid		
Risk	Explanation	Mitigation
Maturation	Changes within respondents over time	The survey was non-experimental (i.e. there is no period for treatment) and was administered only once to each respondent
Selection	Bias in how respondents are chosen	The survey was available to all women in the cybersecurity industry in the United States and was widely advertised through industry organizations, special interest groups, Twitter, and LinkedIn groups
History	External events affecting respondents between surveys	The survey was only administered once and was a point-in-time survey
Instruments	Is survey instrument dependable?	The survey was field tested for usability, and then

		pilot tested to verify that desired data is collected
Statistical Regression	Regression toward the mean on re-test	The survey was administered once to each respondent, with no re-test
Attrition	Loss of study participants	The survey was administered once per respondent, so there was no loss of participants over time

The so-called ‘Interviewer Effects’ (Wiersma, 2012), where the presence of an interviewer influences the answers provided, was a non-factor for this study, as the surveys were performed in-person or over the telephone. Wiersma’s ‘Display Effect,’ which is a parallel to Interviewer Effect for online surveys, was mostly neutralized through the use of the survey service SurveyGizmo, which standardizes the display of the survey across devices. SurveyGizmo allowed the researcher to view the survey in three modes: desktop, tablet, and mobile. Wiersma’s concern for a respondent answering the survey multiple times was mitigated by an e-mail address being used only once for the ‘thank you’ drawing—there was no incentive for completing the survey multiple times.

Andres (2012, p. 118) says that external validity is “...the extent to which the findings of a study of a sample of individuals can be generalized beyond the study sample to its inferential population.” The survey was primarily advertised through cybersecurity

industry organizations. Word-of-mouth advertising will be encouraged, and the LinkedIn groups and Twitter accounts associated with the cybersecurity industry organizations were venues for messaging about the survey. Most LinkedIn groups for cybersecurity industry organizations allow non-members to join the groups and participate in discussions. While the primary venue for advertising was via the cybersecurity industry professional organizations, respondents were not limited to only those women that were members. Any woman working in the cybersecurity industry in the United States could be a respondent. This removed the chance of selection biases introduced by the researcher since the researcher did not determine who specifically received the survey. The respondent mix included all levels of position (e.g., individual contributor to executive management) and all categories of the NICE Cybersecurity Workforce Framework. This study had acknowledged limitations in that respondents were primarily drawn from cybersecurity industry professional organizations, which reduced the generalizability of the study.

3.6 Data Analysis

Both descriptive and inferential statistical analyses were performed in this study, and the SPSS statistical program was used for all analyses. Initially, descriptive statistics were computed for all of the study's variables. Per Howitt & Cramer (2000), a standard approach for summarizing data is to characterize the center, the spread, and the shape of the distribution. Ranges, means, and standard deviations were provided for the continuous variables and Likert-scale items (time working in the cybersecurity industry and the dependent variables of impact of lack of mentorship, impact of impostor phenomenon, and impact of hostile work environment, as well as a composite variable

computed as the sum of the responses to these three impact items). Frequencies and percentages were computed for current position level (executive management, senior management, management, or individual contributor) and the NICE categories (Analyze, Collect & Operate, Investigate, Operate & Maintain, Oversee & Govern, Protect & Defend, and Securely Provision).

Per Fink (2003c), when there is no expectation of which hypothesis (null or research) is valid, the two-tailed hypothesis test is appropriate. All inferential analyses were conducted using two-tailed tests and an alpha level of .05. Per Urdan (2017), the convention is to use an alpha level of .05 in social science research. The alpha level is the setpoint for determining whether a relationship is statistically significant or if the result could have happened by chance. If the probability of a given result happening by chance is less than the alpha level (set at .05), the conclusion is that the result is not by chance and is considered statistically significant. The first stage of the inferential analyses consisted of bivariate analyses that were used directly to answer the nine research questions of this study. Each research question addressed the relationship between one of the independent variables (time working in the cybersecurity industry, current position level, and NICE category) and one of the dependent variables (impact of lack of mentorship, the impact of impostor phenomenon, and impact of a hostile work environment). For time working in the cybersecurity industry (the first three research questions), Pearson correlations were computed. Per Urdan (2017), the Pearson correlation coefficient indicates whether "...the values on one variable are associated with the values on a second variable" (location 4841). If the coefficient is positive, it

indicates that the variables are associated with each other and that the variables move in the same direction (i.e., if one goes up, the other goes up, also).

Conversely, a negative correlation coefficient indicates that the variables are associated with each other but move in opposite directions. The strength of the relationship is indicated by the magnitude of the correlation coefficient, which can range from -1 to 1. The strongest relationships (positive and negative) would result in a coefficient of 1 or -1. As discussed above, the alpha level was set at .05, which means that a coefficient in the range of -.05 to .05 would show no statistically significant relationship.

Per Trochim, Donnelly, and Arora (2016), there are four major types of relationships that might be discovered in research:

1. No relationship: no correlation is found between the variables (i.e., a correlation coefficient in the range -.05 to .05)
2. Positive relationship: high values are associated with high values, low values with low values (i.e. a positive correlation coefficient greater than .05)
3. Negative relationship: Also called an inverse relationship, high values of one variable are associated with low values of the other variable (i.e. a negative correlation coefficient less than -.05)
4. A curvilinear relationship is not linear (as in positive or negative relationships). The nature of the relationship changes over the range of the variables (simple Pearson correlations provide insight into linear relationships between variables, curvilinear relationships typically have very small coefficient values)

These relationship types are shown graphically in Figure 9 below.

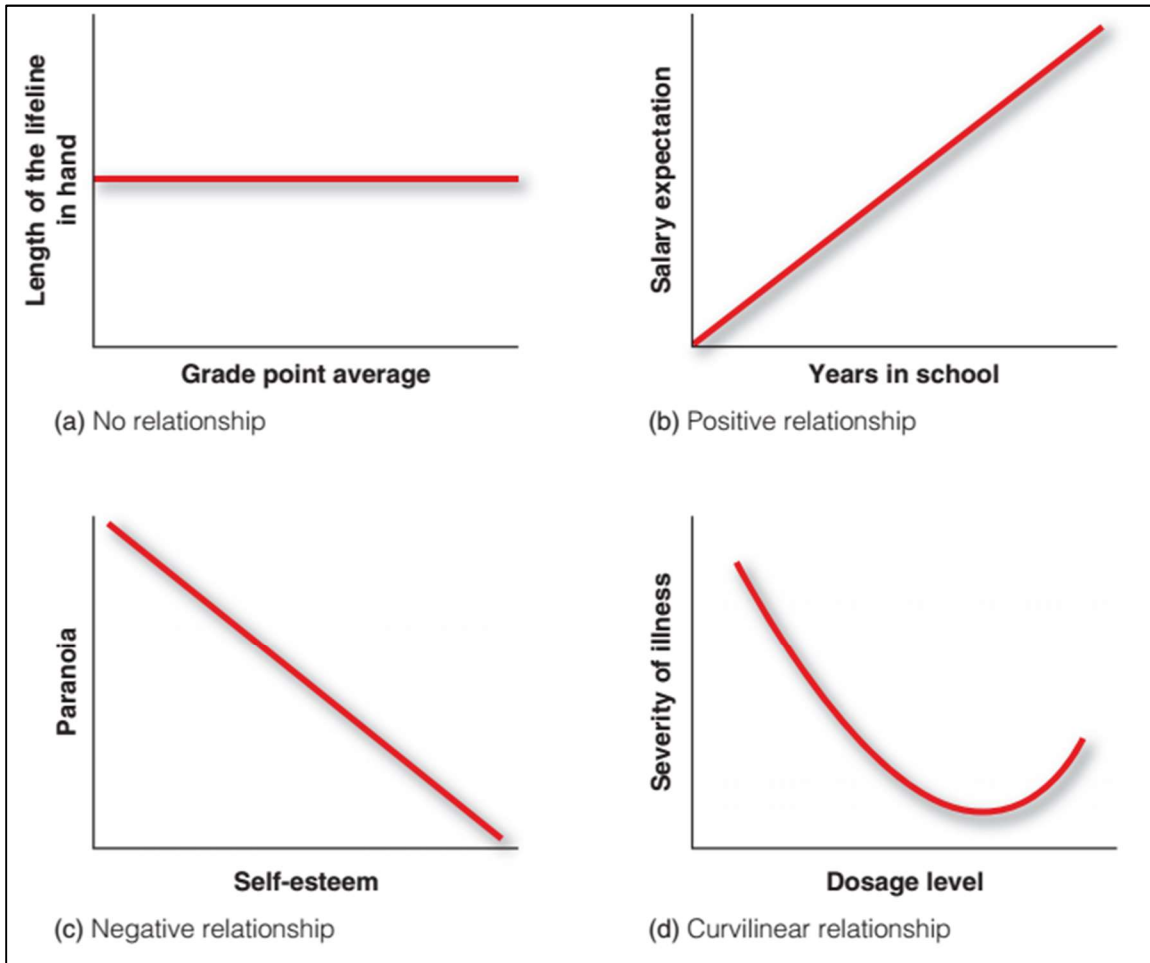


Figure 9: Types of relationships (Trochim, Donnelly, and Arora, 2016, p. 16).

One-way Analysis of Variance (ANOVA) tests provides a comparison of the means of two or more independent variables on one dependent variable. The next three research questions involve current position level (five categories), and three one-way ANOVAs were performed (one for each dependent variable). The final three research questions involve NICE category (seven categories), and three additional one-way ANOVAs were performed (again, one for each of the three dependent variables). For the one ANOVA test that showed a significant relationship, follow up tests were performed using Tukey's Honestly Significantly Different (HSD) tests to determine which groups

differed from which other groups. As each of the research questions is associated with one of the null hypotheses of this study, the answers to the research questions provided the basis for rejecting or not rejecting the null hypotheses (see Table 3).

Table 3: Null Hypotheses

Null Hypotheses	
H01	There is no significant relationship between time working in the cybersecurity industry and the perceived impact of lack of mentorship on retention
H02	There is no significant relationship between time working in the cybersecurity industry and the perceived impact of impostor syndrome on retention
H03	There is no significant relationship between time working in the cybersecurity industry and the perceived impact of a hostile work environment on retention
H04	There is no significant relationship between current position level and the perceived impact of lack of mentorship on retention
H05	There is no significant relationship between current position level and the perceived impact of impostor syndrome on retention
H06	There is no significant relationship between current position level and the perceived impact of a hostile work environment on retention

H07	There is no significant relationship between NICE Workforce Framework category and the perceived impact of lack of mentorship on retention
H08	There is no significant relationship between NICE Workforce Framework category and the perceived impact of impostor syndrome on retention
H09	There is no significant relationship between NICE Workforce Framework category and the perceived impact of a hostile work environment on retention

In the second stage of the inferential analyses, an exploratory analysis was conducted based on a composite dependent variable computed as the sum of the responses to the three dependent variables. As each of the individual dependent variables addresses the impact of one particular barrier, the composite variable represented the total barrier impact. The analysis was conducted in which each of the three independent variables was used simultaneously to predict scores on the composite dependent variable. A general linear model framework was used with the two categorical independent variables (current position level and NICE category) and one continuous independent variable (time in current position). The purposes of the exploratory analyses were first to assess the relationships between the independent variables and the overall perceived impact (rather than impact in each of the three areas individually) and to determine if

there is overlap in the prediction of perceived impact among the three independent variables.

3.7 Chapter Summary

Chapter Three provided a detailed description of the methodology and design used by this research. The chapter provided a short description of quantitative and qualitative methodologies, and the reasoning for choosing quantitative rather than qualitative methodology is provided. Several quantitative designs are described, and the rationale provided for choosing a correlational design.

Details of the research population, sample frame, and sample are provided along with the data collection process. The research population is described as women working in the cybersecurity industry in the United States. The sample frame is professional organizations in the cybersecurity industry, and the sample itself will be women that self-select by choosing to respond to the survey. The survey will be advertised through the cybersecurity industry organizations and social media groups associated with them. The survey is described as well as the types of questions that will be used to collect the data for the independent and dependent variables. Procedures for confidentiality and security of the collected data have been provided, including for data in transit and data at rest.

Validity is defined, and internal and external validity are differentiated. Risks to internal validity are described along with steps taken by the researcher to manage those risks. Field and pilot tests of the survey instrument, to ensure external validity, are described.

The data analysis process is thoroughly described, with various types of statistical tests to investigate relationships between the independent and dependent variables. Tests

also determined the nature of the relationships and the statistical significance of the results.

Chapter 4: Results and Findings

Chapter 3 provided a detailed explanation of the analysis performed upon the collected data. The focus of this chapter is to provide the results of the analysis and a review of the findings. The objective of this research was to understand better what factors lead to the lower retention rate of women than men in the U.S. cybersecurity industry.

4.1 Population Demographics

The study population was women in the cybersecurity industry working in the United States. There were 244 respondents, with 146 respondents filling out the survey completely. 98 respondents did not respond to the three questions (#7, #8, #9) that comprise the dependent variables. Five respondents who completed the survey indicated they did not identify as women (question #1). These five were eliminated from the sample. The final sample was 141 respondents who completed the survey and indicated that they identified as women.

4.2 Data Collection Procedures

A survey was created and field tested with four respondents from the researcher's employer. Feedback was collected and incorporated. Post-approval by the Institutional Review Board (IRB), a pilot test was conducted with four colleagues of the researcher who did not work at the same company. Again, feedback was collected and incorporated. These respondents were directed to not participate in the research survey, and they agreed to the restriction. The survey was created and released through SurveyGizmo, an online survey service. Upon release of the survey, notices were posted in the researcher's

personal LinkedIn feed (with tags to Women in Security and Privacy and Women in Cybersecurity) as well as other locations on LinkedIn:

- Information Security Community
- Information Systems Security Association (ISSA) Discussion Forum
- Computer Security Institute
- National Cybersecurity Student Association

Three more notices were posted in LinkedIn using the same tags over the following three weeks and a personal message was sent to 23 first-degree connections that were women working in the cybersecurity industry.

Additionally, the day the survey was released, a tweet was sent out from the researcher's account advertising the survey and tagging Women in Security and Privacy, ISSA, ASIS International, ISACA and Women in Cybersecurity. Two more tweets were sent in the following three weeks with the same tags. Direct messages were sent to Women's Society of Cyberjutsu, Women in Cybersecurity, Women in Security and Privacy, and #Infosec Women | Gender Diversity, asking for assistance in advertising the survey. The survey was available online from 26 August 2018 to 19 September 2018.

4.3 Sample Size

Recent estimates are that women make up 10-15% of the cybersecurity workforce in the U.S. (LeClair, Shih, & Abraham, 2014) and 11% globally (Reed, Zhong, Terwoerds, & Brocaglia, 2017). This study used 12.5% of the 768,000 currently employed U.S. cybersecurity professionals (Cybersecurity Supply and Demand Heat Map, n.d.), resulting in an estimated 96,000 women in the U.S. cybersecurity industry. Using a standard sample size calculator (<https://www.surveysystem.com/sscalc.htm>) with a confidence level of 95% and a confidence interval of 5%, the resulting recommended sample size is 383 respondents.

The collected sample was 141 respondents. Using a confidence level of 95% and a population of 96,000, the resulting confidence interval is 8.25%.

4.4 Demographic Data

Questions 2 through 6 collected demographic data about the respondent.

Questions 4 through 6 collected data for the independent variables of the research study.

4.4.1 Age (question 2)

Respondents were asked to indicate what age range included their age. The ranges were:

- 18 to 24
- 25 to 34
- 35 to 44
- 45 to 54
- 55 to 64
- 65 or older

The majority of the respondents (Table 1 and Figure 1) were between 25 and 54 years old (n=117, 83.0%) followed by 55 years and older (n=20, 14.2%) and 24 years or younger (4, 2.8%).

4.4.2 Highest level of education (question 3)

Respondents were asked to indicate their highest level of education. The majority of the respondents (Table 1 and Figure 2) hold graduate degrees: Master's, PhD., or M.D. (n=71, 50.4%), followed by Bachelor's degrees (n=56, 39.7%), with 12 holding either an Associate degree or have attended some college courses (8.5%). Two respondents (1.4%) had a high school or less education.

Table 4: Sample Personal Demographics, n = 141

Variable	n	%
	Gender	
Female	141	100.0%
	Age	
18 to 24 years	4	2.8%
25 to 34 years	55	39.0%
35 to 44 years	33	23.4%
45 to 54 years	29	20.6%
55 to 64 years	16	11.4%
65 years or older	4	2.8%
	Education	
Master's, Ph.D., M.D.	71	50.4%
Bachelor's degree	56	39.7%
Associate degree	3	2.1%
Some college, no degree	9	6.4%
High school/GED	2	1.4%
	Country	
Europe	5.0	3.6%
United States	133.0	94.3%
Other	3.0	2.1%

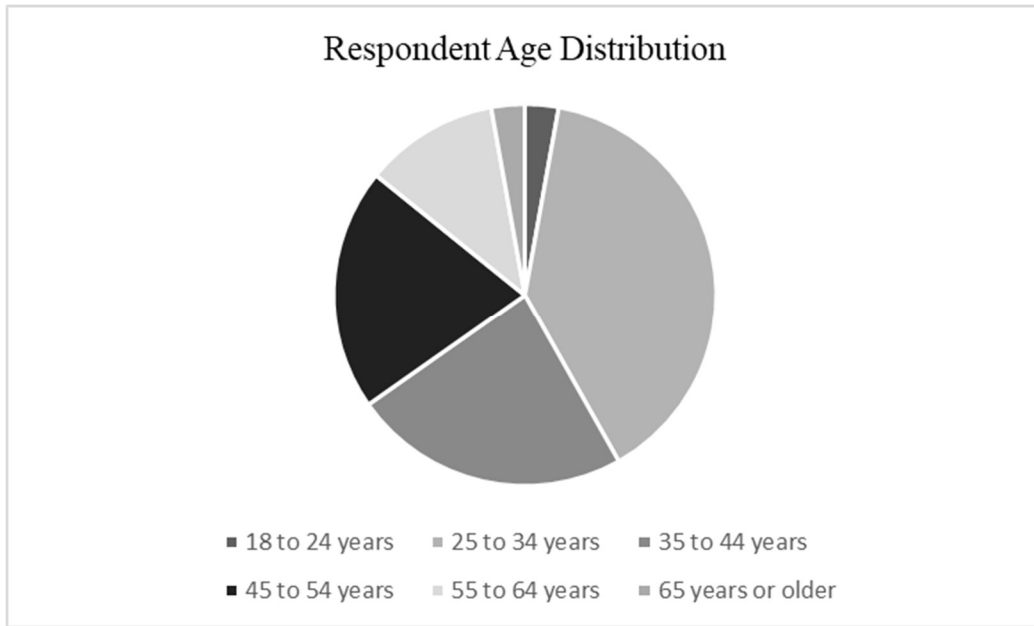


Figure 11: Respondent Age Distribution.

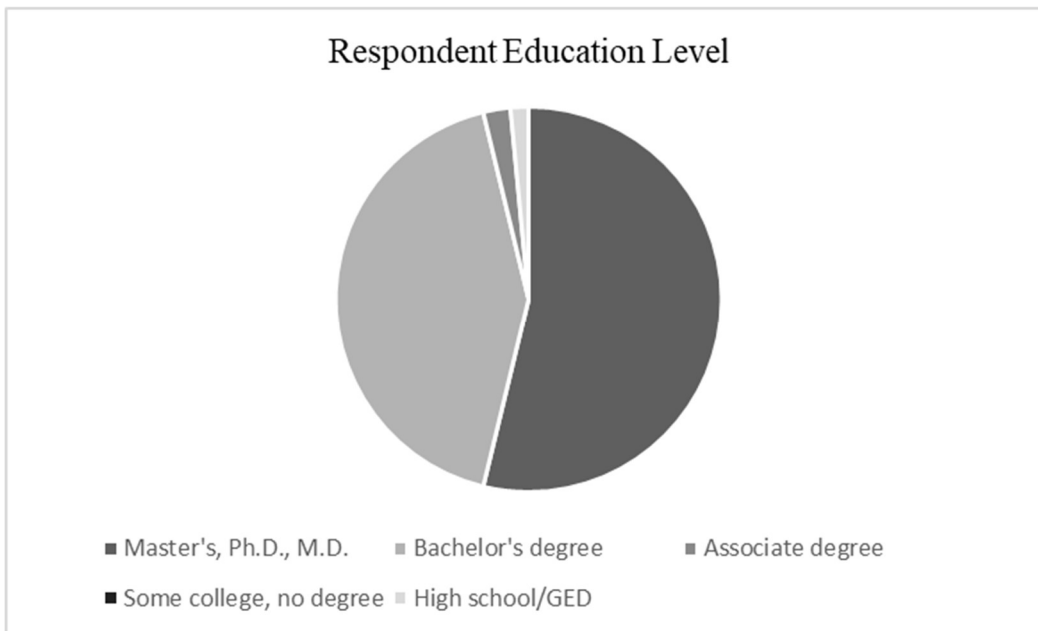


Figure 10: Respondent Education Level.

4.4.3 Time working in the cybersecurity industry (question 4)

Respondents were asked to input how long they had worked in the cybersecurity industry, rounded to the nearest whole year. Time spent in a related Science, Technology, Engineering, or Math industry was to be included, but time in non-STEM fields or internships was excluded. The mean for responses (Table 2 and Figure 3) to this question was 11.6 years (standard deviation = 9.9 years), with a minimum of less than one year and a maximum of 48 years.

4.4.4 Current working position level (question 5)

The majority of the respondents (Table 2 and Figure 4) chose Individual Contributor – no direct reports (n=81, 57.5%). Management (team lead, direct reports that are not managers) was the second most frequent level by number (n=37, 26.2%). Fewer respondents indicated they were senior management (manager of managers) (n=14, 9.9%) and executive management (direct report to CEO or equivalent) (n=9, 6.4%).

4.4.5 NICE Cybersecurity Workforce Framework category (question 6)

The majority of the respondents (Table 2 and Figure 5) selected the Oversee & Govern category (n=63, 44.7%), then Operate & Maintain (n=19, 13.5%), Protect & Defend (n=19, 13.5%), Analyze (18, 12.8%), and Securely Provision (n=14, 9.9%). Fewer of the respondents chose Investigate (n=6, 4.2%) and Collect & Operate (n=2, 1.4%). All seven of the NICE Cybersecurity Workforce Framework categories were represented in the responses.

Table 5: Sample Professional Demographics, n = 141

Variable	n	%
Position		
Executive Management (direct report to CEO or equivalent)	9	6.4%
Individual Contributor (no direct reports)	81	57.5%
Management (team lead, direct reports that are not managers)	37	26.2%
Senior Management (manager of managers)	14	9.9%
NICE Specialty Areas		
Analyze	18	12.8%
Collect & Operate	2	1.4%
Investigate	6	4.2%
Operate & Maintain	19	13.5%
Oversee & Govern	63	44.7%
Protect & Defend	19	13.5%
Securely Provision	14	9.9%
Years of Experience		
Mean = 11.6 years, standard deviation = 9.9 years,		
Minimum = <1year, Maximum = 48 years		



Figure 12: Time Working in the Cybersecurity Industry.

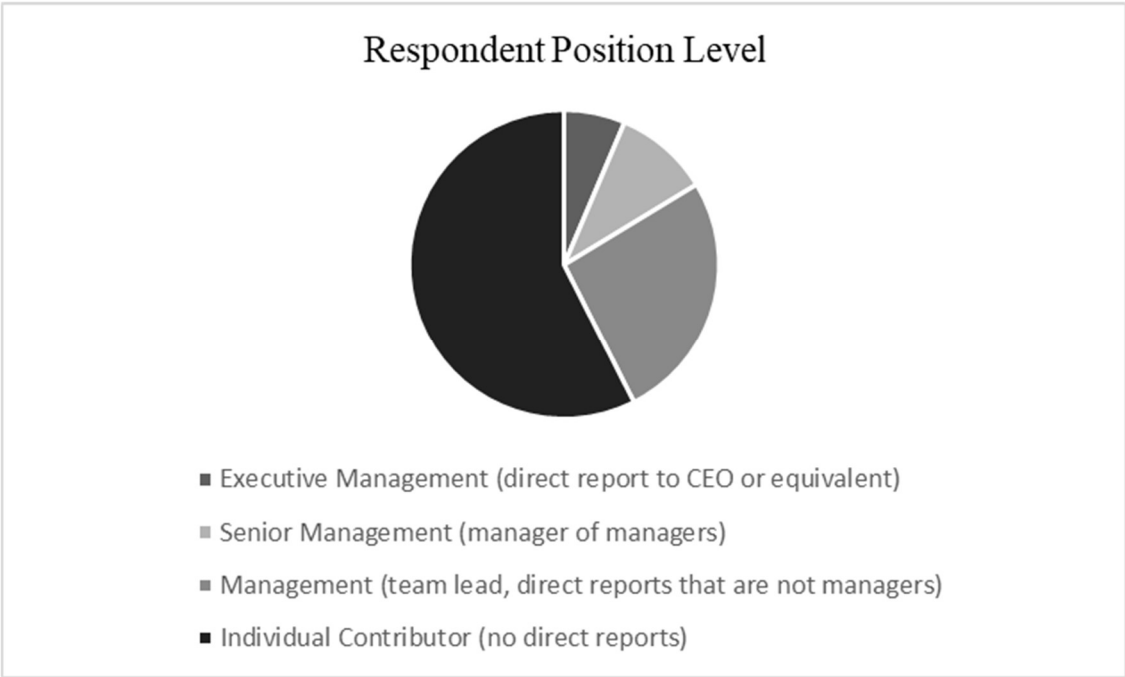


Figure 13: Respondent Current Working Position Level.

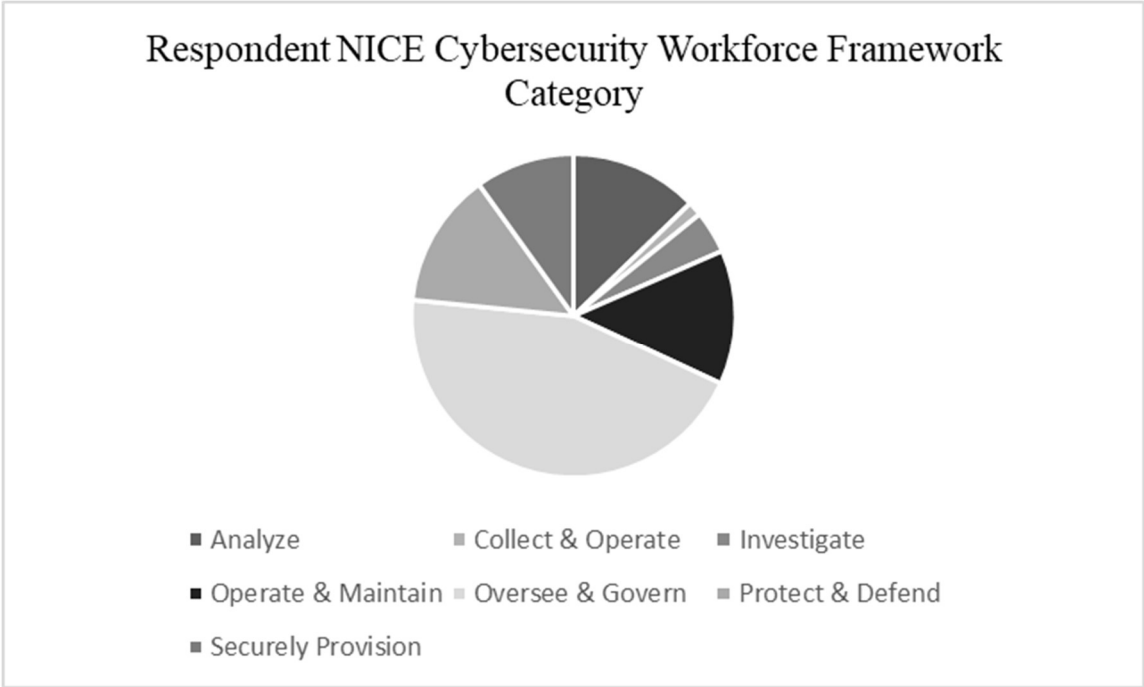


Figure 14: Respondent NICE Cybersecurity Workforce Framework Category.

4.5 Dependent Variable Descriptive Information

Questions 7 through 9 collected data for the dependent variables, asking respondents to indicate their perception of the impact of various retention factors on their desire to continue working in the cybersecurity industry.

4.5.1 Lack of mentorship (question 7)

Question 7 asked the respondent to indicate their perception of the impact of lack of mentorship on their desire to stay in the cybersecurity industry. The response scale was 0 = none, 1 = somewhat, 2 = moderate, and 3 = high. The responses (Table 3 and Figure 7) to this question ranged from 0 (none) to 3 (high) with a mean of 1.5 (falling between somewhat and moderate).

4.5.2 Impostor phenomenon (question 8)

Question 8 asked the respondent to indicate their perception of the impact of impostor phenomenon on their desire to stay in the cybersecurity industry. The response scale was 0 = none, 1 = somewhat, 2 = moderate, and 3 = high. The responses (Table 3 and Figure 8) to this question ranged from 0 (none) to 3 (high) with a mean of 1.7 (falling between somewhat and moderate, closer to moderate).

4.5.3 Hostile work environment (question 9)

Question 9 asked the respondent to indicate their perception of the impact of a hostile work environment on their desire to stay in the cybersecurity industry. The response scale was 0 = none, 1 = somewhat, 2 = moderate, and 3 = high. The responses (Table 3) ranged from 0 (none) to 3 (high) with a mean of 1.9 (between somewhat and moderate, but very close to moderate).

4.5.4 Composite

The composite is measured as the sum of responses to the perceptions of impact of the three retention factors. Since the response to an individual factor has a range of 0 – 3, the composite could range from 0 to 9. The mean responses (Table 3 and Figure 9) for the composite ranged from 0 to 9, with a mean of 5.1, which translates to a response of 1.7 (between somewhat and moderate, closer to moderate).

Table 6: Dependent Variable Descriptives, n = 141

Barrier	Mean	Std. D	Minimum	Maximum
Lack of mentorship	1.5	1.0	0	3
Impostor phenomenon	1.7	1.1	0	3
Hostile work environment	1.9	1.1	0	3
Composite	5.1	2.4	0.00	9.00

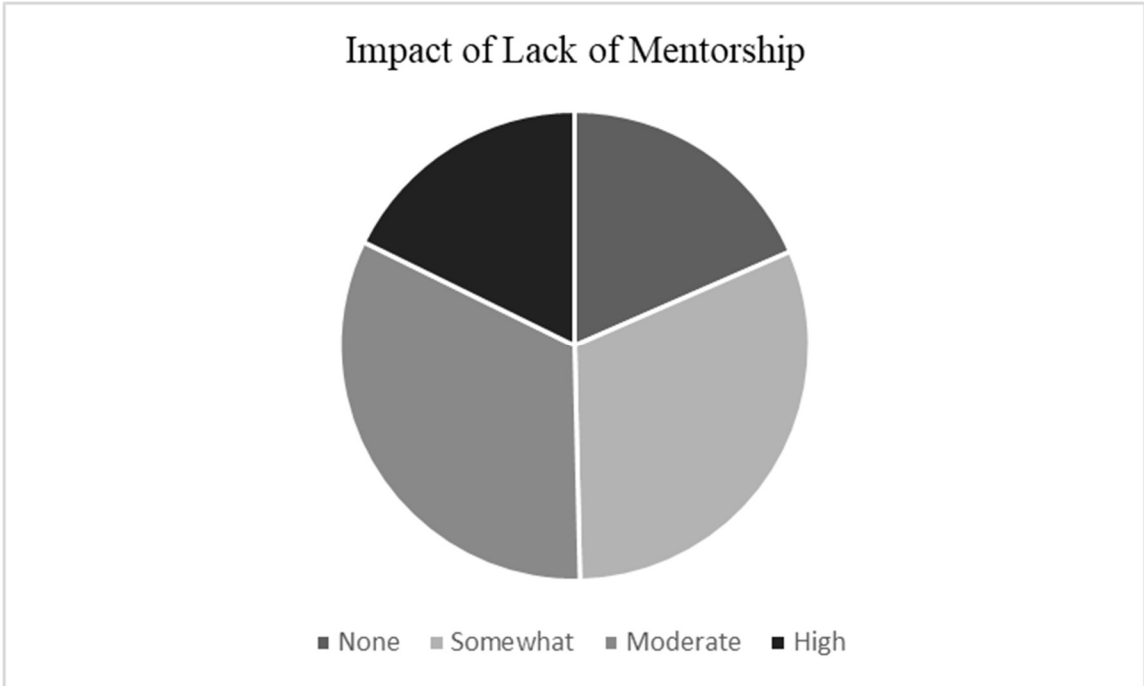


Figure 15: Impact of Lack of Mentorship.

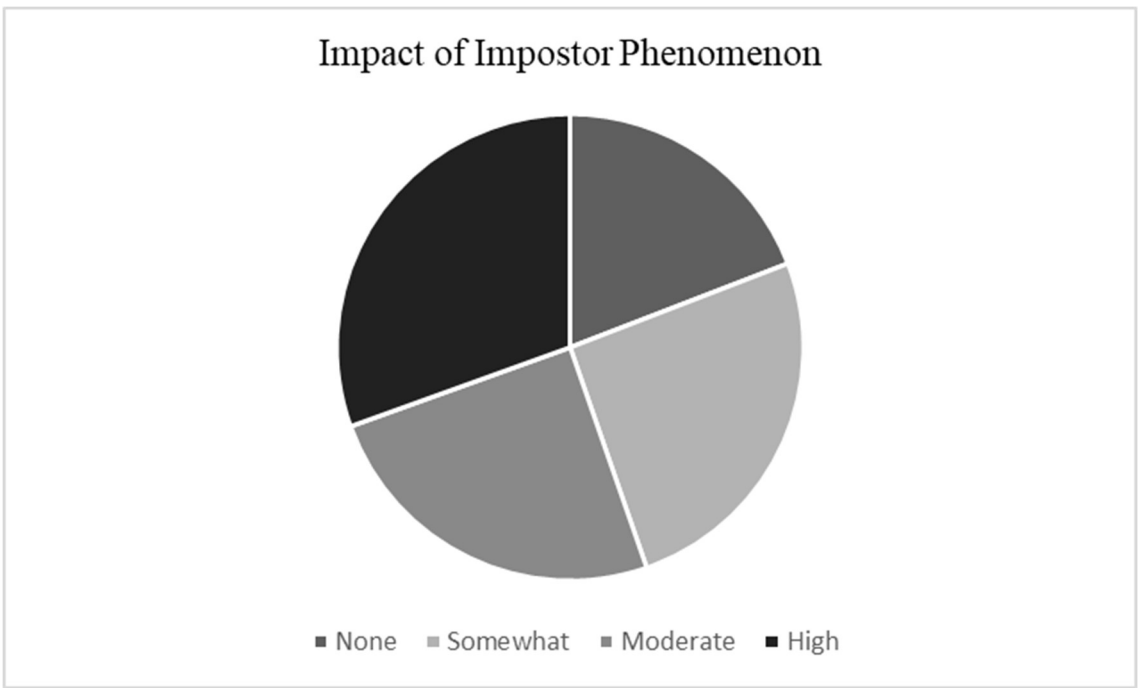


Figure 16: Impact of Impostor Phenomenon.

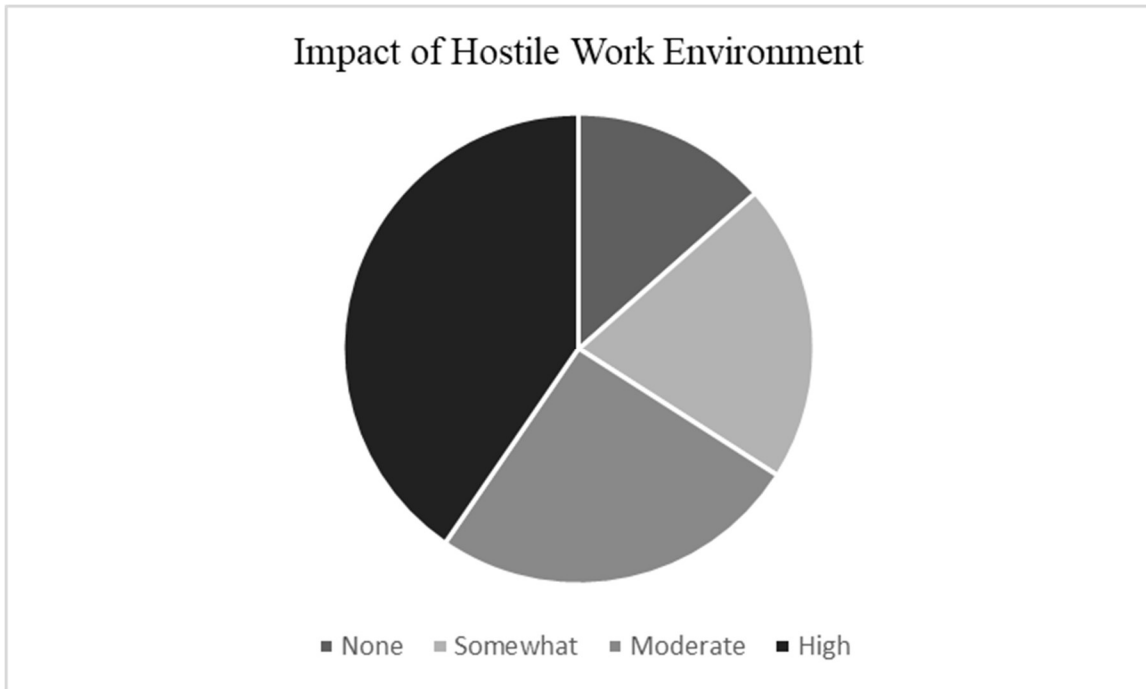


Figure 17: Impact of Hostile Work Environment.

4.6 Stage One of Inferential Analyses

The first stage of inferential analyses consisted of bivariate analyses directly answering the nine research questions of the study. Each research question addressed the relationship between one of the independent variables (time working in the cybersecurity industry, current position level and NICE Cybersecurity Workforce Framework category) and one of the dependent variables (impact of lack of mentorship, impact of impostor phenomenon, and impact of hostile work environment).

For research questions 1 – 3 (Table 4), regarding the relationship between time working in the cybersecurity industry and the three barriers to retention, a Pearson Correlation was used to determine whether there was a significant relationship. Two-tailed tests with an alpha level of .05 were used to test the hypotheses.

For research questions 4 – 6 (Table 5) and 7 – 9 (Table 6), One-way Analysis of Variance (ANOVA) tests were performed. Separate ANOVAs were conducted for each barrier being tested.

4.6.1 Research question one

RQ1: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of lack of mentorship?

H01: There is no significant relationship between *time working in the cybersecurity industry* and the perceived impact of lack of mentorship on retention.

HA1: There is a significant relationship between *time working in the cybersecurity industry* and the perceived impact of lack of mentorship on retention.

Test results show no significant relationship ($r = .042, p = .619$). The null hypothesis (H01) is retained. There is no significant relationship between *time working in the cybersecurity industry* and the perceived impact of lack of mentorship on retention.

4.6.2 Research question two

RQ2: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of Impostor Phenomenon?

H02: There is no significant relationship between *time working in the cybersecurity industry* and the perceived impact of Impostor Phenomenon on retention.

HA2: There is a significant relationship between *time working in the cybersecurity industry* and the perceived impact of Impostor Phenomenon on retention.

Test results show a significant relationship ($r = -.377, p = .000$). The null hypothesis is not retained. There is a significant relationship between *time working in the cybersecurity industry* and the perceived impact of Impostor Phenomenon on retention.

Correlations between .2 and .4 indicate a weak relationship, while the negative coefficient indicates a negative relationship. As time working in the cybersecurity industry increases, the perception of the impact of Impostor Phenomenon as a barrier to retention decreases.

4.6.3 Research question three

RQ3: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of a hostile work environment?

H03: There is no significant relationship between *time working in the cybersecurity industry* and the perceived impact of a hostile work environment on retention.

HA3: There is a significant relationship between *time working in the cybersecurity industry* and the perceived impact of a hostile work environment on retention.

Test results show no significant relationship ($r = .032, p = .703$). The null hypothesis is retained. There is no significant relationship between *time working in the cybersecurity industry* and the perceived impact of a hostile work environment on retention.

Table 7: Correlations of time working in the cybersecurity industry and Retention Barriers, $n = 141$

Retention Barrier	r	p
Lack of mentorship	.042	.619
Impostor phenomenon	-.377**	.000
Hostile work environment	-.032	.703

Note. r = Pearson correlation coefficient

* $p < .05$

** $p < .01$

4.6.4 Research question four

RQ4: What is the nature of the relationship between *current position level* and the perceived impact of lack of mentorship?

H04: There is no significant relationship between *current position level* and the perceived impact of lack of mentorship on retention.

HA4: There is a significant relationship between *current position level* and the perceived impact of lack of mentorship on retention.

Test results (Table 5) show no significant relationship, $F(1, 137) = 1.682$, $p = .174$. The null hypothesis is retained. There is no significant relationship between *current position level* and the perceived impact of lack of mentorship on retention.

Respondents rated lack of mentorship around 1.5, which indicates the impact of this barrier on retention (between *somewhat* and *moderate*).

4.6.5 Research question five

RQ5: What is the nature of the relationship between *current position level* and the perceived impact of Impostor Phenomenon?

H05: There is no significant relationship between *current position level* and the perceived impact of Impostor Phenomenon on retention.

HA5: There is a significant relationship between *current position level* and the perceived impact of Impostor Phenomenon on retention.

Test results (Table 5) show no significant relationship, $F(1, 137) = 2.242$, $p = .086$. The null hypothesis is retained. There is no significant relationship between *current position level* and the perceived impact of Impostor Phenomenon on retention. Respondents rated Impostor Phenomenon around 1.7, which indicates they rated this barrier's impact on retention between *somewhat* and close to *moderate*.

4.6.6 Research question six

RQ6: What is the nature of the relationship between *current position level* and the perceived impact of a hostile work environment?

H06: There is no significant relationship between *current position level* and the perceived impact of a hostile work environment on retention.

HA6: There is a significant relationship between *current position level* and the perceived impact of a hostile work environment on retention.

Test results (Table 5) show no significant relationship, $F(1, 137) = 2.104$, $p = .103$. The null hypothesis is retained. There is no significant relationship between *current position level* and the perceived impact of a hostile work environment. The respondents rated hostile work environment around 1.9, which indicates they rated this barrier's impact on retention close to moderate.

Table 8: ANOVA Results for Barriers to Retention by Current Working Position, $n = 141$

Lack of Mentorship				
Source	<i>df</i>	F	η^2	<i>p</i>
Position	3	1.682	.036	.174
Error	137	(.966)		
Impostor phenomenon				
Position	3	2.242	.047	.086
Error	137	(1.192)		
Hostile work environment				
Position	3	2.104	.044	.103
Error	137	(1.125)		

4.6.7 Research question seven

RQ7: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of lack of mentorship?

H07: There is no significant relationship between *NICE Workforce Framework category* and the perceived impact of lack of mentorship on retention.

HA7: There is a significant relationship between *NICE Workforce Framework category* and the perceived impact of lack of mentorship on retention.

Test results (Table 6) show no significance, $F(6, 134) = .341, p = .243$. The null hypothesis is retained. There is no significant relationship between the *NICE Workforce*

Framework category and the perceived impact of lack of mentorship. The respondents rated lack of mentorship around 1.5, which indicates they rated this barrier's impact on retention between somewhat and moderate.

4.6.8 Research question eight

RQ8: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon?

H08: There is no significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon on retention.

HA8: There is a significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon on retention.

Test results (Table 6) show a significant relationship, $F(6, 134) = 4.942, p = .000, \eta^2 = .607$. The null hypothesis is rejected. There is a significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon. Table 7 shows the descriptives of Impostor Phenomenon mean ratings by *NICE Cybersecurity Workforce Framework category*. The *collect and operate* category indicated the highest rating for the impact of Impostor Phenomenon (3, high). The categories of *analyze, operate, and maintain* and *protect and defend* rated the impact of Impostor Phenomenon as 2 (moderate). The categories of *investigate, oversee and govern*, and *securely provision* rated the impact of Impostor Phenomenon between 1 and 2 (somewhat to moderate).

Tukey's Honestly Significant Difference test used to determine where the differences were amongst the *NICE Cybersecurity Workforce Framework categories*. Oversee and Govern was significantly lower than Securely Provision (.014), Analyze

(.003), Operate and Maintain (.001) and Protect and Defend (.000). There were no other significant differences among the NICE Cybersecurity Workforce Framework categories.

4.6.9 Research question nine

RQ9: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of a hostile work environment?

H09: There is no significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact of a hostile work environment on retention.

HA9: There is a significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact of a hostile work environment on retention.

Test results show no significant relationship, $F(6, 134) = 1.323, p = .251$. The null hypothesis is retained. There is no significant relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of a hostile work environment. The respondents rated hostile work environment around 1.9, which indicated they rated this barrier's impact on retention close to moderate.

Table 9: ANOVA Results for Barriers to Retention by NICE Specialty Areas, $n = 141$

Lack of Mentorship				
Source	<i>df</i>	F	η^2	<i>p</i>
Position	6	1.341	.057	..243
Error	134	(.966)		
Impostor phenomenon				
Position	6	4.942**	.607	.000
Error	134	(1.047)		
Hostile work environment				
Position	6	1.323	.056	.251
Error	134	(1.136)		

Table 10: Descriptives for Impostor Phenomenon by NICE Specialty Area, $n = 141$

NICE Specialty Areas	Mean	SD	N
Analyze	2.00	1.029	18
Collect & Operate	3.00	0.000	2
Investigate	1.67	1.506	6
Operate & Maintain	2.11	0.994	19
Oversee & Govern	1.17	1.025	63
Protect & Defend	2.21	0.918	19
Securely Provision	1.93	0.997	14

4.7 Stage Two of Inferential Analyses

The purpose of this stage was to assess the relationship between the independent variables and the overall perceived impact (rather than the impact of each dependent variable individually). A Pearson Correlation test was performed *time working in the cybersecurity industry* and ANOVA tests were performed for *current working position* and *NICE Cybersecurity Workforce Framework category*. Additionally, this stage determined if there was overlap in the assessment of perceived impact among the three independent variables.

4.7.1 Time working in the cybersecurity industry

Test results (Table 8) show a significant relationship ($r = -.170$, $p = .044$). There is a significant relationship between *time working in the cybersecurity industry* and the overall composite of the perceived impact of the retention barriers. The correlation ($r = -.170$) less than .2 indicates a slight relationship. The negative coefficient indicates a negative relationship. As *time working in the cybersecurity industry* increases, the overall composite perceived impact of the retention barriers decreases.

Table 11: Correlations of Time Working in the Cybersecurity Industry and overall composite of the Retention Barriers, n = 141

Retention Barrier	<i>r</i>	<i>p</i>
	-	.0
Composite	.170*	44

Note. *r* = Pearson correlation coefficient

* $p < .05$

** $p < .01$

4.7.2 *Current working position*

Test results (Table 9) show no significant relationship, $F(3, 137) = 1.584$, $p = .196$. There is no significant relationship between *current position level* and the overall composite of the perceived impact of the retention barriers. The respondent composite rating was around 5.1 (average item response of 1.7) which indicates a rating between *somewhat* and *moderate*.

4.7.3 *NICE cybersecurity workforce framework category*

Test results (Table 9) show no significant relationship, $F(6, 134) = 1.676$, $p = .132$. There is no significant relationship between *NICE Cybersecurity Workforce Framework category* and the overall composite of the perceived impact of the retention barriers. The respondent composite rating was around 5.5 (average item response of 1.8) which indicates a rating between *somewhat* and *moderate*.

Table 12: ANOVA Results for the Composite of the Barriers Retention by Current Working Position and NICE Specialty Areas, n = 141

Current working position				
Source	<i>df</i>	F	η^2	<i>p</i>
Position	3	1.584	.034	.196
Error	137	(.966)		
NICE specialty area				
Position	6	1.676	.070	.132
Error	134	(5.677)		

Note: η^2 = eta squared, effect size

Value enclosed in parentheses represents mean square errors

* $p < .05$

** $p < .01$

4.8 Summary

Chapter 4 presented the results from the quantitative, correlational study of women in the U.S. cybersecurity industry. The goal of this research was to better understand the nature of the relationships between demographic factors and the perceived impacts of selected barriers to retention. The data was collected through an online, anonymous survey where the respondents were self-selected.

Chapter 5 will conclude this research by reviewing the research problem and questions, implications from the results, and recommendations for industry and for future research.

Chapter 5: Implications and Conclusions

This chapter contains a review of the quantitative correlational study, research problem, research questions, and the results from the online survey with 141 respondents, all women working in the U.S. cybersecurity industry. This chapter will also identify contributions of the research to the cybersecurity industry in improving retention of women in the cybersecurity industry. Implications for practitioners, policymakers, and for future research are also discussed.

5.1 Overview of the Research Problem and Questions

The U.S. cybersecurity industry has a significant employment gap, with over 301,000 job openings left unfilled (Cybersecurity Supply and Demand Heat Map, n.d.). In 2015, Setalvad (2015) reported 209,000 openings in the U.S. cybersecurity industry, which shows that the employment gap is growing. These unfilled cybersecurity jobs across all of the NICE Cybersecurity Workforce Framework categories and include:

- Cybersecurity Engineer
- Cybersecurity Analyst
- Network Engineer/Architect
- Cybersecurity Manager
- Systems Engineer
- Software Developer/Engineer
- Vulnerability Analyst
- Penetration Tester
- Systems Administrator
- IT Auditor

The demographics of the U.S. cybersecurity industry have a significant gender imbalance. While women make up about 50% of the U.S. general workforce, they only make up 10-15% of the U.S. cybersecurity workforce (LeClair, Shih, & Abraham, 2014). This imbalance is common across all position levels, as men are five times more likely to

hold C-level or managerial positions and six times more likely to hold non-managerial staff positions (Reed, Zhong, Terwoerds, and Brocaglia, 2017).

The low numbers of women in the U.S. cybersecurity industry are the result of two different issues. Firstly, the pipeline of women entering the cybersecurity industry from school is low (Shumba, et al., 2013; Pusey, Gondree, & Peterson, 2016). Secondly, the retention rate of women in U.S. Science, Technology, Engineering, and Math (STEM) industries (which includes the cybersecurity industry) is significantly lower than the retention rate of men. LeClair, Shih, and Abraham (2014) reported that women are retained in STEM at a 60% rate, while men are retained at an 80% rate. This goal of this study was to better understand the factors that may affect the retention of women in the U.S. cybersecurity industry.

In order to better understand the low retention rate of women in the U.S. cybersecurity industry, a literature review was performed to identify barriers to retention and demographic factors that were relevant to the retention of women in STEM or cybersecurity fields. Demographic factors chosen (independent variables) were: *time working in the cybersecurity industry*, *current position level*, and *NICE Cybersecurity Workforce Framework category* (used to identify the type of cybersecurity work the respondent is doing). The retention factors were presented as barriers to retention. The barriers to retention chosen were: *lack of mentorship*, *Impostor Phenomenon*, and *hostile work environment*.

5.1.1 Research questions

The high-level research question, derived from the research problem, was: What is the nature of the relationships between the demographic factors and the respondent's perception of the impact of the retention barriers? The specific research questions were:

RQ1: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of lack of mentorship?

RQ2: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of Impostor Phenomenon?

RQ3: What is the nature of the relationship between *time working in the cybersecurity industry* and the perceived impact of a hostile work environment?

RQ4: What is the nature of the relationship between *current position level* and the perceived impact of lack of mentorship?

RQ5: What is the nature of the relationship between *current position level* and the perceived impact of Impostor Phenomenon?

RQ6: What is the nature of the relationship between *current position level* and the perceived impact of a hostile work environment?

RQ7: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of lack of mentorship?

RQ8: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon?

RQ9: What is the nature of the relationship between the *NICE Cybersecurity Workforce Framework category* and the perceived impact of a hostile work environment?

5.1.2 Research hypotheses

The data collected from the online survey was used to test the following hypotheses:

H01: There is no significant relationship between time working in the cybersecurity industry and the perceived impact of lack of mentorship on retention

HA1: There is a significant relationship between time working in the cybersecurity industry and the perceived impact of lack of mentorship on retention

H02: There is no significant relationship between time working in the cybersecurity industry and the perceived impact of Impostor Phenomenon on retention

HA2: There is a significant relationship between time working in the cybersecurity industry and the perceived impact of Impostor Phenomenon on retention

H03: There is no significant relationship between time working in the cybersecurity industry and the perceived impact of a hostile work environment on retention

HA3: There is a significant relationship between time working in the cybersecurity industry and the perceived impact of a hostile work environment on retention

H04: There is no significant relationship between current position level and the perceived impact of lack of mentorship on retention

HA4: There is a significant relationship between current position level and the perceived impact of lack of mentorship on retention

H05: There is no significant relationship between current position level and the perceived impact of Impostor Phenomenon on retention

HA5: There is a significant relationship between current position level and the perceived impact of Impostor Phenomenon on retention

H06: There is no significant relationship between current position level and the perceived impact of a hostile work environment on retention

HA6: There is a significant relationship between current position level and the perceived impact of a hostile work environment on retention

H07: There is no significant relationship between NICE Workforce Framework category and the perceived impact of lack of mentorship on retention

HA7: There is a significant relationship between NICE Workforce Framework category and the perceived impact of lack of mentorship on retention

H08: There is no significant relationship between NICE Workforce Framework category and the perceived impact of Impostor Phenomenon on retention

HA8: There is a significant relationship between NICE Workforce Framework category and the perceived impact of Impostor Phenomenon on retention

H09: There is no significant relationship between NICE Workforce Framework category and the perceived impact of a hostile work environment on retention

HA9: There is a significant relationship between NICE Workforce Framework category and the perceived impact of a hostile work environment on retention

5.2 Contributions to Knowledge

Researchers (LeClair, Shih, & Abraham, 2014; Peacock & Irons, 2017) recognize the need for more research regarding the causes of the gender gap in the cybersecurity industry. Some researchers (Shumba, et al., 2013; Pusey, Gondree, & Peterson, 2016) demonstrate a low number of women entering the industry from school (the ‘pipeline’).

LeClair, et al. (2014) and Cech, Rubineau, Silbey, and Seron (2011) found a low retention rate among women in Science, Technology, Engineering, and Math (STEM) as well as in cybersecurity, which is a subset of STEM.

This study contributed to an improved understanding of how the impacts of certain barriers to retention are perceived by women in the U.S. cybersecurity industry. The three barriers selected for the study were selected based on extant literature. LeClair, et al. (2014) discuss the effects of lack of mentorship and gender discrimination (hostile work environment). Cech, Rubineau, Silbey, and Seron (2011) point to Impostor Phenomenon when they show that lack of confidence in work role by women negatively affects their intent to stay in their current position.

5.2.1 Lack of mentorship

The 141 respondents rated the combined impact on retention of *lack of mentorship* at a mean of 1.5 on a scale from 0 (no impact) to 3 (high impact). A 1.5 falls directly between ‘somewhat’ and ‘moderate’ regarding impact. This indicates that *lack of mentorship* is a noteworthy factor affecting retention of women in the cybersecurity industry.

5.2.2 Impostor Phenomenon

The 141 respondents rated the combined impact on retention of *Impostor Phenomenon* at a mean of 1.7 on a scale from 0 (no impact) to 3 (high impact). A 1.7 falls between ‘somewhat’ and ‘moderate’ regarding impact, but closer to ‘moderate’. This indicates that *Impostor Phenomenon* is a noteworthy factor affecting retention of women in the cybersecurity industry and could be a more important factor than *lack of mentorship*.

5.2.3 *Hostile work environment*

The 141 respondents rated the combined impact on retention of *hostile work environment* at a mean of 1.9 on a scale from 0 (no impact) to 3 (high impact). A 1.9 falls between ‘somewhat’ and ‘moderate’, but very close to moderate. This indicates that *hostile work environment* is a noteworthy factor affecting retention of women in the cybersecurity industry and could be a more important factor than *lack of mentorship* and *Impostor Phenomenon*.

All three barriers to retention were perceived by the respondents to be factors affecting the retention of women in the cybersecurity industry, aiding in confirming the results of the prior cited studies.

5.2.4 *Time working in the cybersecurity industry*

This study also provided information on the relationship between certain demographic factors and the perceived impact of the selected barriers to retention. Glass, Sassler, Levitte, and Michelmore found that women did not experience the ‘settling effect’, where the longer a person is in an industry, the less likely the person is to leave. They found little connection between higher age or skill levels and a lower retention rate for women in STEM. Buse, Bilmoria, and Perelli (2013) concluded that women found ways to adapt to workplace issues rather than leave as they stayed longer in a male-dominated industry. This contrast between the two studies suggested *time working in the cybersecurity industry* as a demographic for the study.

Time working in the cybersecurity industry is the independent variable for the first three research questions. The results of the data analysis showed no significant relationship between *time working in the cybersecurity industry* and the perceived impact

on retention or lack of mentorship (Research Question One) or the perceived impact on retention of a hostile work environment (Research Question Three). While lack of mentorship and hostile work environment are noteworthy barriers to retention, their perceived impact on retention does not change as women spend more time in the cybersecurity industry.

Data analysis showed a significant relationship between *time working in the cybersecurity industry* and the perceived impact on retention of Impostor Phenomenon (Research Question Two). Since the relationship is negative, the indication is that as women stay longer in their cybersecurity career, the negative impact of Impostor Phenomenon on retention is reduced. Women staying in cybersecurity experience reduced self-doubt about their ability to meet the needs of their cybersecurity positions.

The test of a significant relationship between *time working in the cybersecurity industry* and the overall composite of the perceived impact of the retention barriers demonstrated a slight negative relationship. As women spend more time in the cybersecurity industry, the retention barriers as a whole have lower perceived impact. As with other results, this shows that women early in their cybersecurity career are more susceptible to the impacts of these retention barriers.

5.2.5 Current position level

Johnson (2013) found that women perceived a greater impact from factors such as lack of mentorship and work/life balance (hostile work environment) as they climbed the corporate ladder. Reed, Zhong, Terwoerds, and Brocaglia discovered an increased impact of hostile work environment as women moved up in position level in their companies. These study results suggested the use of *current position level* as a demographic variable.

Current position level is the independent variable for the middle three research questions (4 – 6). The results of the data analysis showed no significant relationships between *current position level* and the perceived impact on retention of lack of mentorship (Research Question Four), Impostor Phenomenon (Research Question Five), or hostile work environment (Research Question Six). While all three are noteworthy barriers to retention, their perceived impact on retention does not change as women move up the corporate ladder. There may be fewer available mentors for women as they move up in a company, as reported by Johnson (2013). The lack of significant relationship means there is no greater or less impact on retention from lack of mentorship at higher management levels.

Similarly, there may be more occurrences of hostile work environment at a higher management level, but with no significant relationship with perceived impact on retention, it may be that women become inured to the effects as they move up in the company. The lack of significant relationship between *current position level* and Impostor Phenomenon seems counterintuitive since there was a significant relationship between *time working in the cybersecurity industry* and Impostor Phenomenon. It is possible that this contradiction is caused by women not moving up in the industry very quickly, so that *time working in the cybersecurity industry* has a larger effect than *current position level*.

5.2.6 NICE Cybersecurity Workforce Framework category

The *NICE Cybersecurity Workforce Framework category* was selected as an independent variable to investigate whether the perceived impact of the barriers to retention varied based upon what type of work was being performed by the respondent.

For example, does a woman working as an analyst in a security operations center experience Impostor Phenomenon with the same impact as a woman working in training? Since the *NICE Cybersecurity Workforce Framework categories* cut across all industries, respondents were able to identify which applied to them.

The *NICE Cybersecurity Workforce Framework category* is the independent variable for the last three research questions (7 – 9). The results of the data analysis showed no significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact on retention of lack of mentorship (Research Question Seven) or hostile work environment (Research Question Nine). While lack of mentorship and hostile work environment are noteworthy barriers to retention, their perceived impact does not change in relation to the type of work being performed within the cybersecurity industry.

Data analysis showed a significant relationship between *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon on retention (Research Question Eight). The post-hoc test to identify the differences showed that the category *Oversee and Govern* rated Impostor Phenomenon having a significantly lower perceived impact on retention than the categories *Securely Provision, Analyze, Operate and Maintain, and Protect and Defend*. The categories have the following underlying specialty areas:

- *Oversee and Govern*
 - Legal Advice and Advocacy
 - Training, Education, and Awareness
 - Cybersecurity Management
 - Strategic Planning and Policy
 - Executive Cyber Leadership
 - Program/Project Management and Acquisition
- *Securely Provision*

- Risk Management
- Software Development
- Systems Architecture
- Technology R&D
- Systems Requirements Planning
- Test & Evaluation
- Systems Development
- Analyze
 - Threat Analysis
 - Exploitation Analysis
 - All-Source Analysis
 - Targets
 - Language Analysis
- Operate and Maintain
 - Data Administration
 - Knowledge Management
 - Customer Service and Technical Support
 - Network Services
 - Systems Administration
 - Systems Analysis
- Protect and Defend
 - Cyber Defense Analysis
 - Cyber Defense Infrastructure Support
 - Incident Response
 - Vulnerability Assessment and Management

It can be argued that work within the Oversee and Govern category (in general) requires a lower level of technical knowledge and skill than the other categories listed. While Training, Education, and Awareness may require deep technical skills, the other specialty areas are not specifically tied to deep technical knowledge. Women in those specialty areas may have come up the ranks from technical positions but no longer exercise their technical knowledge to the same extent as they did previously. The experience that women gain as they move up and into Oversee and Govern positions may ameliorate the impact of Impostor Phenomenon. This may be the reason that the perceived impact of Impostor Phenomenon is lower for Oversee and Govern than for the other categories.

5.3 Limitations of the Study

The initial goal of the study was to investigate the relationships between certain demographic factors (*time working in the cybersecurity industry, current position level, and NICE Cybersecurity Workforce Framework category*) and selected barriers to retention (lack of mentorship, Impostor Phenomenon, and hostile work environment). Based upon sample calculations, the desired sample size was at least 383 respondents. The actual collected sample size was 141 respondents. This had the effect of changing the confidence interval from 5% to 8.25%.

5.4 Implications for Practitioners

Managers are those practitioners that implement policy within their organizations. There are several implications for managers and individual contributors stemming from this research.

5.4.1 Barriers to retention

The barriers to retention in this study (lack of mentorship, Impostor Phenomenon, and hostile work environment) are noteworthy and need to be considered when leading and managing women in the cybersecurity industry. To create an improvement in the retention of women in the cybersecurity industry, managers should be attentive to ensuring women have opportunities to get mentored, which may also help offset the impact of Impostor Phenomenon, which this research shows is more important early in the career (Research Question Two). Drew (2015) showed that lack of mentorship could be both formal and informal. Management attention is required to ensure that opportunities for receiving mentoring are appropriately distributed. This attention can take the form of formal mentoring programs with appropriately balanced mentee

assignments. Managers can encourage informal mentoring by senior employees and, again, ensure balanced implementation. The hostile work environment is made up of many factors and is a known concern among women. Some factors such as work/life balance and wage inequality may not be within a manager's purview, as these are typically set at the corporate level. Per Blau and Kahn (2013), women that take advantage of work/life balance policies such as family leave and flex-time may be penalized via lack of promotion, since they are seen as not career-oriented. If the organization has policies friendly to work/life balance, it is important that managers ensure no penalties are attached to anyone, including women, that take advantage of those policies. Other factors such as discrimination, 'good old boy' network, and sexual harassment are largely within a manager's control. This study demonstrates that managers in the cybersecurity industry need to be aware that it is an issue and take effective steps to stop it when seen if there is to be an improvement in retention of women in the cybersecurity industry.

At the individual contributor level, a significant implication regarding Impostor Phenomenon is seen. Impostor Phenomenon, per Neureiter and Traut-Mattausch (2016), is the feeling that one is incapable of performing in a professional role even if there is objective evidence to the contrary. If early-cybersecurity career women are aware of the effects of the Impostor Phenomenon (Research Question Two), especially in the most affected NICE Cybersecurity Workforce Framework categories (Research Question Eight), they may be able to self-actualize and manage the impact. While organizational support (such as communities of interest, special interest groups, or women-mentoring-

women programs) would help, it is possible that merely being aware of the potential impact of Impostor Phenomenon may reduce attrition.

5.5 Implications for Policy-Makers

Policy-makers, such as those in Human Resources that set organization-wide policies, can make significant positive impacts on the retention of women in the cybersecurity industry in relation to the results of this research. Looking at the researched retention barriers, all three are noteworthy for the impact on retention of women in cybersecurity, and all three can be positively affected by policy.

5.5.1 Lack of mentorship

Johnson (2013) discusses how powerful mentors can be in retaining women in STEM fields. Mentoring programs can be either formal or informal (or both). A formal mentoring program has trained mentors and either self- or company-assigned mentor/mentee pairings. The organization has oversight to ensure that the program follows diversity guidelines and that the mentors have appropriate training and are following the guidelines and policies. That oversight flows down to managers, as discussed above. Informal mentoring programs can still have mentor/mentee pairings or can be peer-to-peer, or other configurations. Training is sometimes a requirement, but the organization does not formalize the mentor/mentee relationships. Oversight is still possible to ensure that the program stays balanced. As pointed out by Drew (2015), informal mentoring can easily become imbalanced with respect to gender in a male-dominated industry like cybersecurity. Truly informal mentoring programs (those with no organizational oversight), per Drew, tend to exclude women.

5.5.2 Impostor Phenomenon

Organizations can set up support for women, particularly early in their careers (Research Question Two) and in the most susceptible NICE Cybersecurity Workforce Framework categories (Research Question Eight), to reduce the impact of Impostor Phenomenon. There are several options for organizational programs. Peer-support groups, such as early career women's groups, can help mitigate the impact of Impostor Phenomenon without taking significant organizational resources. The critical aspect is recognition that Impostor Phenomenon has a noteworthy impact on retention of women in the cybersecurity industry, as supported by this research. Without that recognition, establishing organization-sponsored programs will not make as much difference to the effect of Impostor Phenomenon.

5.5.3 Hostile work environment

For the purposes of this research, hostile work environment included several factors:

- Discrimination
- Wage inequality
- Work/life balance
- 'Good old boy' network
- Sexual harassment

Each of these factors can be positively affected by organizational policy. Policy alone is not enough, in that the organization must also ensure that managers implement the policies.

Reed, Zhong, Terwoerds, and Brocaglia (2017) found a mix of active and passive discrimination against women in cybersecurity. Established policies requiring equal

treatment and training for managers so that they can identify and stop discriminatory practices are needed to manage this subset of the hostile work environment.

Wage inequality exists in many industries, including cybersecurity.

Organizational policy, by establishing equivalence requirements and reviews, can narrow the gap. It is important to note that per Blau and Kahn (2017), wage inequality exists at all wage levels and is larger for highly skilled positions.

Work/life balance programs, per Glass et al. (2013) are a double-edged sword. Johnson (2013) found that women, due to having the larger role in child rearing, benefit most from work/life balance programs. Programs like telework and flex-time can help women, but many women fear taking advantage of such programs, as it can impact their probability of advancement. Policy makers need to establish work/life balance programs as a measure to aid retention of women in cybersecurity, but they also need to establish a policy to ensure that taking advantage of those programs does not result in any overt or covert punishment.

The 'good old boy network' crosses boundaries into other factors mentioned here, from passive discrimination to mentoring. LeClair and Pheils (2016) describe the good old boy network as men watching out for each other, and not watching out for women. This can be problematic from a policy point of view, as most of the manifestations are not overt and possibly even not with intent. By establishing formal mentoring programs, or informal programs with oversight, organizations can avoid some of the impacts of the good old boy network. Training managers and senior personnel in meeting protocol will help ensure that input is received from more than just the outspoken men at the table. The good old boy network is not necessarily against women but is men favoring men in

the workplace. Policies that encourage and enforce inclusion and diversity will help mitigate these effects.

While there are state and federal statutes against sexual harassment, it exists in the workplace and is significant in male-dominated industries such as STEM. Sexual-advance harassment, as described by Kabat-Farr and Cortina (2014) is more publicized, especially in the current #MeToo environment, where women are becoming more likely to speak out about it. Organizational policies likely exist regarding sexual-advance harassment, but policymakers need to ensure that women have easy access to reporting channels, the reports are confidential, and that there will not be reprisals against the women reporting incidents. The other side of sexual harassment, gender harassment, is more prevalent per Kabat-Farr and Cortina, and has a greater impact on reducing the number of women in male-dominated industries. Gender harassment is typified by derogatory remarks, rejection, and scorn as women are seen trying to do ‘male’ work. This type of harassment first needs a policy, and then needs managers that clearly implement that policy to ensure all understand that gender harassment is not allowed.

5.6 Implications for Future Research

This research has several implications for the high-level research objective of achieving a better understanding of retention of women in the cybersecurity industry. Starting with retention barriers in general, this research showed that lack of mentorship, Impostor Phenomenon, and hostile work environment are noteworthy retention barriers for women in the cybersecurity industry. Each of these retention barriers affords opportunities for further research.

5.6.1 Lack of mentorship

While no significant relationship was shown between the selected demographic factors (*time working in the cybersecurity industry, current position level, and NICE Cybersecurity Workforce Framework category*) and lack of mentorship, it was still shown to be a noteworthy retention barrier. Further research could be done to refine the understanding of the importance of female mentors or female role models. Additionally, research into the effectiveness of formal or informal mentoring programs on the retention of women in the cybersecurity industry would be informative.

5.6.2 Impostor Phenomenon

Significant relationships were found between *time working in the cybersecurity industry* and *NICE Cybersecurity Workforce Framework category* and the perceived impact of Impostor Phenomenon on retention of women in the cybersecurity industry. Further research can be done to understand better how *time working in the cybersecurity industry* affects the perceived impact of Impostor Phenomenon. For example, the relationship could be related to the settling effect observed by Glass et al. (2013) in that the longer a woman is in the industry, the more settled they are and the less likely they are to leave. Alternatively, it could be related to time in a position, as a woman would become more comfortable with the skill set required. Similarly, further research can be performed related to *NICE Cybersecurity Workforce Framework category* to better understand why respondents in different categories perceived different impact levels of Impostor Phenomenon.

5.6.3 Hostile work environment

While no significant relationship was shown between the selected demographic factors (*time working in the cybersecurity industry, current position level, and NICE Cybersecurity Workforce Framework category*) and hostile work environment, it was still shown to be a noteworthy retention barrier. In this research, hostile work environment was made up of five subfactors. Further research can be done upon the separate subfactors to investigate which have higher perceived impact and to see if there are significant relationships between each of the subfactors and relevant demographic factors. For example, it is possible that sexual harassment as a retention factor has a significant relationship with *NICE Cybersecurity Workforce Framework category* even though it did not have a significant relationship as part of the larger hostile work environment. Additionally, there are research opportunities investigating the different subfactors of hostile work environment related to current position level.

5.7 Conclusions from the Study Results

The high-level purpose of this study was to understand better factors affecting the retention of women in the cybersecurity industry, specifically the relationship of demographic factors to the perceived impact of specific barriers to retention.

The first conclusion is that all three of the barriers to retention (lack of mentorship, Impostor Phenomenon, and hostile work environment) are noteworthy as barriers to retention. Secondly, there were two significant relationships discovered regarding Impostor Phenomenon. The first is that the perceived impact of Impostor Phenomenon is reduced as women stay longer in the cybersecurity industry. The second is that the *NICE Cybersecurity Workforce Framework categories* of Securely Provision,

Analyze, Operate and Maintain, and Protect and Defend experience higher perceived impact of Impostor Phenomenon than the category of Oversee and Govern.

5.8 Assessment of Research Objectives

The initial research objective was to investigate relationships between certain demographic factors (*time working in the cybersecurity industry, current position level, and NICE Cybersecurity Workforce Framework category*) and selected barriers to retention (lack of mentorship, Impostor Phenomenon, and hostile work environment). All relationships were investigated, and two significant relationships were discovered. A third significant relationship was discovered when looking at relationships between the demographic factors and a composite of the barriers to retention. Lastly, the proposed barriers to retention were verified to be important as having noteworthy perceived impact upon the retention of women in the cybersecurity industry.

5.9 Summary

Chapter Five reviewed the research study questions and hypotheses and reviewed the contributions of this research to the body of knowledge. Chapter Five also presented the implications of the research to practitioners and policymakers and provided recommendations for further research. Chapter Five concluded with an assessment of the research objectives.

Appendices

Appendix A: Definition of Terms

Current Position Level: Describes the respondent's level in the work organization hierarchy. For the purposes of this study, the levels are defined as:

- Executive management: a Chief Executive Officer (CEO) or a direct report to a CEO
- Senior Management: a manager of managers, with budgetary and strategic planning responsibilities
- Middle Management: responsible for budgetary and planning for a business function, having direct reports that are not managers
- Individual Contributor: not having budgetary and strategic planning responsibilities, may have several direct reports (i.e. Team Lead)

Hostile Work Environment: U.S. Federal Code defines harassment as unwelcome conduct based on a set of personal characteristics, one of which is gender. One of the conditions where harassment becomes unlawful is "...such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment." (Labor, 2017). For this study, a hostile work environment is a work environment in which gender-based harassment exists to a level where the respondent feels it is intimidating, hostile, or abusive.

Impostor Phenomenon: Sakulku and Alexander (2011) define impostor phenomenon as successful women "...believing that they were intellectual frauds and feared being recognised as impostors" (p. 75).

NICE Cybersecurity Workforce Framework Category: The NICE Cybersecurity Workforce Framework provides a taxonomy of work within the cybersecurity industry. The framework consists of seven categories split into 33 specialty areas, which are further divided into 52 work roles (Newhouse, Keith, Scribner, & Witte, 2017). This study will use the seven categories.

Appendix B: Survey Instrument

Retention Factors for Women in Cybersecurity

Consent to be a Research Subject

Introduction: Carl Willis-Ford at the University of Fairfax is conducting this research study to investigate the impact of barriers to retention of women in the cybersecurity industry.

Please Note: This survey is intended for women currently working in the cybersecurity industry in the United States.

Procedures: You will be asked to complete an online questionnaire. The questionnaire consists of 10 questions and will take approximately 7 minutes. Questions will include some demographic questions and questions about your perception of the impact of certain barriers to retention in your job. Email addresses are optional, all other questions are required. Incomplete surveys will be discarded.

Risks/Discomforts: There are minimal risks for participation in this study.

Benefits: There are no direct benefits to subjects. However, it is hoped that your participation will help researchers learn more about how to improve retention of women in the cybersecurity industry.

Confidentiality: All information provided will remain confidential and will only be reported as group data with no identifying information. All data, including questionnaires, will be kept in a secure location and only those directly involved with the research will have access to them. After the research is completed, the individual questionnaires will be disposed of, only the bulk data will be kept. Emails, if provided, will be deleted.

Compensation: Those participants that complete the questionnaire and provide an email address will be entered into a random 'Thank You' drawing for one of five \$50 Amazon gift cards.

Participation: Participation in this research study is voluntary. You have the right to refuse to participate entirely without jeopardy.

Questions about the Research: If you have questions regarding this study, you may contact Carl Willis-Ford at willis-fordc35@students.ufairfax.edu

Consent: Clicking 'Submit' at the end of this survey is your consent to participate in the research and including your email is consent to be in the 'thank you' drawing.

Next

0%

Retention Factors for Women in Cybersecurity

Demographics

1. I verify that I identify as a Woman and that I work in the cybersecurity industry in the United States *

- Yes
 No

2. What is your age range? *

- 18 to 24
 25 to 34
 35 to 44
 45 to 54
 55 to 64
 65 or older

3. What is your highest level of education? *

- Less than high school
 Graduated high school/GED
 Some college, no degree
 Associate degree
 Bachelor's degree
 Advanced degree (Master's, Ph.D., M.D.)

4. How long have you worked in the cybersecurity industry? (include previous work in a Science, Technology, Engineering, or Math field). Please round to the nearest whole year. Do not count non-STEM work or internships. *

Back

Next

Retention Factors for Women in Cybersecurity

Demographics, Page 2

5. What is your current working position level? *

- Individual Contributor (no direct reports)
- Management (team lead, direct reports that are not managers)
- Senior Management (manager of managers)
- Executive Management (direct report to CEO or equivalent)

6. What is the best fit of your **current** position in the NICE Cybersecurity Workforce Framework? (please see below for details on each choice)
NOTE: If you work across several areas, please select the area where you spend most of your work time. *

- Analyze
- Collect & Operate
- Investigate
- Operate & Maintain
- Oversee & Govern
- Protect & Defend
- Securely Provision

Analyze: Threat Analysis, Exploitation Analysis, All-Source Analysis, Targets, Language Analysis
Collect & Operate: Collection Operations, Cyber Operational Planning, Cyber Operations

Investigate: Cyber Investigation, Digital Forensics

Operate & Maintain: Data Administration, Knowledge Management, Customer Service & Technical Support, Network Services, Systems Administration, Systems Analysis

Oversee & Govern: Legal Advice and Advocacy, Training/Education/Awareness, Cybersecurity Management, Strategic Planning and Policy, Executive Cyber Leadership, Program/Project Management and Acquisition

Protect & Defend: Cyber Defense Analysis, Cyber Defense Infrastructure Support, Incident Response, Vulnerability Assessment and Management

Securely Provision: Risk Management, Software Development, Systems Architecture, Technology R&D, Systems Requirements Planning, Test & Evaluation, Systems Development

[Back](#) [Next](#)

Retention Factors for Women in Cybersecurity

Questions 7, 8, and 9 relate to factors that may or may not impact you individually, but that you may see elsewhere in the workplace. Please rate your perception of the impact of these factors on your desire to stay in the cybersecurity industry, regardless of whether you choose to stay or not.

7. What is your perception of the impact of Lack of Mentors on your desire to stay in the cybersecurity industry? *

- | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|
| None | Somewhat | Moderate | High |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

8. What is your perception of the impact of the Impostor Phenomenon on your desire to stay in the cybersecurity industry?

Note: Impostor Phenomenon is the feeling of inadequacy for the role even though there is objective evidence, such as certifications or job success, that you are qualified *

- | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|
| None | Somewhat | Moderate | High |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

9. What is your perception of the impact of a Hostile Work Environment on your desire to stay in the cybersecurity industry?

Note: Hostile Work Environment may include: Active or passive discrimination, wage inequality, lack of work/life balance, sexual harassment, or working in a 'good old boy network' *

- | | | | |
|-----------------------|-----------------------|-----------------------|-----------------------|
| None | Somewhat | Moderate | High |
| <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

10. If you would like to participate in the 'Thank You' drawing for one of 5 \$50 Amazon Gift Cards, please enter your email address (email@email.com)

Note: You are not required to respond to this question

[Back](#) [Submit](#)

75% 

Retention Factors for Women in Cybersecurity

Thank You!

The survey is complete.

Thank you for taking this survey. Your response is important to building a better understanding of retention of women in cybersecurity.

100% 

Appendix C: IRB Certification of Approval



CERTIFICATION OF IRB APPROVAL

Candidate's Name: Carl D. Willis-Ford

Date Submitted: 8/19/18

Title of Study: THE PERCEIVED IMPACT OF BARRIERS TO RETENTION ON WOMEN IN CYBERSECURITY

Date of Review: 8/21/18

Classification of Research: Exempt Minimal Risk Potential Risk

Approval Status:

Approved as Submitted

Approved, subject to the following conditions:

Denied, for the following reasons:

Expiration Date for the approved study 2 years

Annual Review is required no

Whether a Close Out Report is required no

This certifies that the research study submitted has been reviewed by the Institutional Review Board.

Chair, Institutional Review Board Committee (Signature)

Danielle Rowell, PhD
Dean of Doctoral Research
IRB Institutional Chair
Danielle.Rowell@ufairfax.edu

References

- Aitoro, J. R. (2008, August). National Cyber Security Initiative will have a dozen parts. Retrieved March 18, 2018, from <http://www.nextgov.com/cybersecurity/2008/08/national-cyber-security-initiative-will-have-a-dozen-parts/42299/>
- Andres, L. (2012). *Designing & Doing Survey Research*. Thousand Oaks, CA: Sage Publications, Inc.
- Aspray, W., & Cortada, J. W. (2016). Before it was a giant: The early history of Symantec, 1982-1999. *IEEE Annals of the History of Computing*, 38(4), 26–41. <https://doi.org/10.1109/MAHC.2016.12>
- Baker, M. (2016). Striving for effective cyber workforce development. Carnegie-Mellon Software Engineering Institute CERT.
- Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). An examination of the vocational and psychological characteristics of cybersecurity competition participants. *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*.
- Bedding, K., & de Jongh, M. (2017). Federal workforce: Attracting and retaining talent in the field of cybersecurity.
- Blau, F. D., & Kahn, L. M. (2013). Female labor supply: Why is the United States falling behind? *American Economic Review*, 103(3), 251–256. <https://doi.org/10.1257/aer.103.3.251>
- Buse, K., Bilimoria, D., & Perelli, S. (2013). Why they stay: Women persisting in US engineering careers. *Career Development International*, 18(2), 139-154.
- Carmines, E. G., & Zeller, R. A. (1979). *Reliability and Validity Assessment*. Thousand Oaks, CA: Sage Publications, Inc.
- Cech, E., Rubineau, B., Silbey, S., & Seron, C. (2011). Professional role confidence and gendered persistence in engineering. *American Sociological Review*, 76(5), 641–666. <https://doi.org/10.1177/0003122411420815>
- Chen, G., Ployhart, R. E., Thomas, H. C., Anderson, N., & Bliese, P. D. (2011). The power of momentum: A new model of dynamic relationships between job satisfaction change and turnover intentions. *Academy of Management Journal*, 54(1), 159–181. <https://doi.org/10.5465/AMJ.2011.59215089>

- Cheryan, S., Siy, J. O., Vichayapai, M., Drury, B. J., & Kim, S. (2011). Do female and male role models who embody STEM stereotypes hinder women's anticipated success in STEM? *Social Psychological and Personality Science*, 2(6), 656–664. <https://doi.org/10.1177/1948550611405218>
- Claggett, G. P. (2016, March). The perception of women contending for first place in the information technology world: A qualitative case study. Capella University.
- Clance, P. R., & Imes, S. A. (1978). The imposter phenomenon in high achieving women: Dynamics and therapeutic intervention. *Psychotherapy: Theory, Research & Practice*, 15(3), 241–247. <https://doi.org/10.1037/h0086006>
- Cobb, S. (2016). Mind This Gap: Criminal Hacking and the Global Cybersecurity Skills Shortage, a Critical Analysis.
- Computer Security Online. (2017). *The 2017 U.S. state of cybercrime survey*. Retrieved from https://images.idgesg.net/assets/2017/09/idg_presentation_07202017.pdf
- Cooper, D. R., & Schindler, P. S. (2011). *Business Research Methods* (11th ed.). New York, NY, USA: McGraw-Hill Irwin.
- Creswell, J. (2012). *Educational Research* (6th ed.). Boston: Pearson Education, Inc.
- Cybersecurity Supply and Demand Heat Map. (n.d.). Retrieved June 24, 2018, from <http://cyberseek.org/heatmap.html>
- Delmont, M. (2016, August). The Lived Experiences of Women in the Information Technology Field as they Transition from One Leadership Level to the Next: A Phenomenological Study. University of Nevada, Las Vegas.
- Drew, E. (2015). Mitigating the fallout of women in the workplace: Dynamics of the first executive role, and what employers can do.
- Drury, B. J., Siy, J. O., & Cheryan, S. (2011). When do female role models benefit women? The importance of differentiating recruitment from retention in STEM. *Psychological Inquiry*, 22(4), 265–269. <https://doi.org/10.1080/1047840X.2011.620935>
- Fink, A. (2003a). *How to Ask Survey Questions* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.
- Fink, A. (2003b). *How to Design Survey Studies* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.
- Fink, A. (2003c). *How to Manage, Analyze, and Interpret Survey Data* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.

- Frost & Sullivan. (2017). 2017 Global information security workforce study: Benchmarking workforce capacity and response to cyber risk. Retrieved from <https://iamcybersafe.org/wp-content/uploads/2017/06/N-America-GISWS-REPORT.pdf>
- Fuller, C. R. (2016). *Shortening the skills gap: An exploratory study of cybersecurity professional experience*. Capella University. Retrieved from <http://search.proquest.com/openview/360e28e817ead249fd876729338c6fbd/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Glass, J. L., Sassler, S., Levitte, Y., & Michelmore, K. M. (2013). What's so special about STEM? A comparison of women's retention in STEM and professional occupations. *Social Forces; a Scientific Medium of Social Study and Interpretation*, 92(2), 723–756. <https://doi.org/10.1093/sf/sot092>
- Holmes, M. (2016). Why Women Leave Engineering: The SWE Gender Culture Study. *Society of Women Engineers*, 10–12.
- Howitt, D., & Cramer, D. (2000). *First Steps in Research and Statistics: A Practical Workbook for Psychology Students*. Philadelphia: Routledge.
- Johnson, M. L. (2013). Gender differences in the field of information security technology management: A qualitative, phenomenological study. Capella University.
- Kabat-Farr, D., & Cortina, L. M. (2014). Sex-based harassment in employment: New insights into gender and context. *Law and Human Behavior*, 38(1), 58–72. <https://doi.org/10.1037/lhb0000045>
- Kaspersky Lab. (2017a). Beyond 11%: A study into why women are not entering cybersecurity. Retrieved from <https://d1srlirzdlmpew.cloudfront.net/wp-content/uploads/sites/86/2017/11/03114046/Beyond-11-percent-Futureproofing-Report-EN-FINAL.pdf>
- Kaspersky Lab. (2017b). *Kaspersky Security Bulletin: OVERALL STATISTICS FOR 2017*. Retrieved from https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf
- Labor, 29 C.F.R. §1604.11 (2017). Retrieved from <https://www.gpo.gov/fdsys/pkg/CFR-2017-title29-vol4/pdf/CFR-2017-title29-vol4-sec1604-11.pdf>
- LeClair, J., & Pheils, D. (2016). *Women in cybersecurity*. BookBaby.

- LeClair, J., Shih, L., & Abraham, S. (2014). Women in STEM and cyber security fields. *Proceedings of the 2014 Conference for Industry and Education Collaboration, Savannah, Georgia* (pp. 5–7). Retrieved from http://www.indiana.edu/~ciec/Proceedings_2014/ETD/ETD355_LeClair.pdf
- Libicki, M. C., Senty, D., & Pollak, J. (2014). H4cker5 wanted: An examination of the cybersecurity labor market. RAND.
- Littlejohn, R. (2016). *Stories of women in corporate security who have risen through the leadership ranks*. University of Phoenix. Retrieved from <http://search.proquest.com/openview/8c3e407e2b5259f95d31a0808c869d78/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Litwin, M. S. (1995). *How to Measure Survey Reliability and Validity*. Thousand Oaks, CA: Sage Publications, Inc.
- Misa, T. J. (2016). Computer security discourse at RAND, SDC, and NSA (1958-1970). *IEEE Annals of the History of Computing*, 38(4), 12–25. <https://doi.org/10.1109/MAHC.2016.48>
- Nardi, P. M. (2013). *Doing Survey Research: A Guide to Quantitative Methods* (3rd ed.). Boulder: Paradigm Publishers.
- National Centers of Academic Excellence in Cyber Defense - NSA.gov. (n.d.). Retrieved March 18, 2018, from <https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/>
- Neureiter, M., & Traut-Mattausch, E. (2016). An inner barrier to career development: Preconditions of the impostor phenomenon and consequences for career development. *Frontiers in Psychology*, 7. <https://doi.org/10.3389/fpsyg.2016.00048>
- Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (No. NIST SP 800-181). Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-181>
- Peacock, D., & Irons, A. (2017). Gender inequality in cybersecurity: Exploring the gender gap in opportunities and progression. *International Journal of Gender, Science and Technology*, 9(1), 25–44.
- Petersen, R. (2015, June). *NICE Update to NIST ISPAB*. Presented at the NIST Information Security and Privacy Advisory Board. Retrieved from [https://csrc.nist.gov/presentations/2015/national-initiative-for-cybersecurity-education-\(n](https://csrc.nist.gov/presentations/2015/national-initiative-for-cybersecurity-education-(n)

- Pierce, A. O. (2016). *Exploring the cybersecurity hiring gap* (Ph.D. Thesis). Walden University.
- Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented populations. *IEEE Security & Privacy*, 14(6), 90–95.
- Quantitative Approaches - Center for Innovation in Research and Teaching. (n.d.). Retrieved June 16, 2018, from https://cirt.gcu.edu/research/developmentresources/research_ready/quantresearch/approaches
- Raytheon Company. (2016). *Securing our future: Closing the cybersecurity talent gap*. Retrieved from https://www.raytheon.com/cyber/rtnwcm/groups/corporate/documents/content/rtn_335212.pdf
- Reed, J., Zhong, Y., Terwoerds, L., & Brocaglia, J. (2017). *The 2017 global information security workforce study: Women in cybersecurity*. Retrieved from <https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf>
- Rogers, V. L. N. (2015). Women in IT: The endangered gender (pp. 95–98). ACM Press. <https://doi.org/10.1145/2815546.2815558>
- Ross, R., Katzke, S., Johnson, L. A., Swanson, M., Stoneburner, G., & Rogers, G. (2005). *Recommended security controls for federal information systems and organizations* (No. NIST SP 800-53). Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-53r1>
- Sakulku, J., & Alexander, J. (2011). The impostor phenomenon. *International Journal of Behavioral Science (IJBS)*, 6(1).
- Salkind, N. J. (2012). *Exploring Research* (8th ed.). Boston: Pearson Education, Inc.
- Seron, C., Silbey, S. S., Cech, E., & Rubineau, B. (2016). Persistence is cultural: Professional socialization and the reproduction of sex segregation. *Work and Occupations*, 43(2), 178–214. <https://doi.org/10.1177/0730888415618728>
- Setalvad, A. (2015, March 31). Demand to fill cybersecurity jobs booming. Retrieved January 13, 2018, from <http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/>

- Shine, L. R. (2016). Quantitative analysis of the gender differences in learning styles of IT professionals and the impact on leadership outcomes: Implications for STEM. Capella University. Retrieved from <http://search.proquest.com/openview/4889eef74b888f9371fb0b2f37641377/1?pq-origsite=gscholar&cbl=18750&diss=y>
- Shumba, R., Hall, L., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., & Bace, R. (2013). Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation (pp. 1–14). ACM Press. <https://doi.org/10.1145/2543882.2543883>
- Silbey, S. S. (2016). Why do so many women who study engineering leave the field? Retrieved January 20, 2018, from <https://hbr.org/2016/08/why-do-so-many-women-who-study-engineering-leave-the-field>
- Singh, R., Fouad, N. A., Fitzpatrick, M. E., Liu, J. P., Cappaert, K. J., & Figueredo, C. (2013). Stemming the tide: Predicting women engineers' intentions to leave. *Journal of Vocational Behavior*, 83(3), 281–294. <https://doi.org/10.1016/j.jvb.2013.05.007>
- Thayer-Hart, N. (2010). Survey Fundamentals: A Guide to Designing and Implementing Surveys. University of Wisconsin System Board of Regents. Retrieved from http://oqi.wisc.edu/resourcelibrary/uploads/resources/Survey_Guide.pdf
- Tobey, D., Pusey, P., & Burley, D. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*, 5(1).
- Trochim, W. M., Donnelly, J. P., & Arora, K. (2016). *Research Methods: The Essential Knowledge Base* (Second Edition). Boston, MA: Cengage Learning.
- Turner, G. E., Deemer, E. D., Tims, H. E., Corbett, K., & Mhire, J. (2014). Cyber Value and Interest Development: Assessment of a STEM Career Intervention for High School Students, 15.
- U.S. Department of Education. (2016). *Digest of Education Statistics 2016*.
- Urdan, T. (2017). *Statistics in Plain English* (4th ed.). New York, NY, USA: Routledge.
- Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal*, 4(2), 32.
- Warner, M. (2015). Notes on the evolution of computer security policy in the US government, 1965-2003. *IEEE Annals of the History of Computing*, 37(2), 8–18. <https://doi.org/10.1109/MAHC.2015.25>

Warnert, N. A. (2015). Increasing women's involvement in the agile community, 106.

Wee, J. M. C., Bashir, M., & Memon, N. (2016). Self-efficacy in cybersecurity tasks and its relationship with cybersecurity competition and work-related outcomes. Presented at the USENIX Security Symposium.

Wiersma, W. (2012). The Validity of Surveys: Online and Offline. Retrieved October 14, 2017, from http://wybowiersma.net/pub/essays/Wiersma,Wybo,The_validity_of_surveys_online_and_offline.pdf

Biography

Carl D. Willis-Ford is a former U.S. Navy nuclear reactor operator on fast attack submarines. Since leaving the Navy, he has over 30 years' experience including technical training, database administration, data security, technical project management, solution architecture, security policy/compliance/awareness, and public speaking on Insider Threat and the intersection of Human Experience and security programs. He currently works for General Dynamics Information Technology as a Senior Principal – Solution Architect. He has taught Technical Project Management and Network Security at George Mason University.

Carl holds a B.S. in Computer Science from Chapman University, a M.S. in Network Security from Capitol Technology University, and a M.S. in Technology Management from George Mason University.

Carl is active in cybersecurity workforce development:

- Technical Working Group member, NIST-sponsored Federal Information Systems Security Educators Association
- Planning Committee, Colloquium for Information Systems Security Education
- Planning Committee, Community College Cyber Summit
- Industry Board Member, National Cybersecurity Student Association

Carl has spoken on Insider Threat at George Mason University, and ISSA Chapter meetings, at national Dept. of Energy security conferences, and at the New York City Technology Forum. He currently resides in Lynden, WA.