FACTORS THAT INFLUENCE STUDENTS TO CHOOSE CYBERSECURITY CAREERS: AN EXPLORATORY STUDY

BY

GERALD JOHN EMERICK

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Education in Education Policy, Organization and Leadership
with a concentration in Learning Design and Leadership
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2020

Urbana, Illinois

Doctoral Committee:

Professor Bill Cope, Chair
Professor Mary Kalantzis
Associate Professor Matthew Montebello, University of Malta
Professor Yoon Pak

Abstract

Despite the strong, global demand for talented workers, higher than average salaries, and relatively low education requirements (bachelor’s degree) for computing fields such as cybersecurity, there continues to be a pipeline issue with graduating enough workers educated in cybersecurity to fill the demand in the United States and globally (Information Security Analysts, 2019; Morgan, 2017). At the same time, while there is significant literature related to factors that influence students to choose STEM careers more generally, there appears to be a lack of literature that addresses factors that influence students to choose a career in cybersecurity. This lack of literature limits our understanding of what interventions and programs may improve the cybersecurity pipeline issue.

This study utilized a mixed-methods case study approach with the goal of providing insight into what factors influenced students in an accredited university cybersecurity program to choose cybersecurity as their career. The study also sought to better understand what aspects of cybersecurity the students found most and least interesting. Twenty-nine new cybersecurity students and 10 information systems students completed a mixed-methods survey, and five faculty at the Midwestern university were interviewed. Key findings suggest strong themes of factors that influence students to choose cybersecurity careers and these students’ interests in traditional computing subjects as well as subjects specific to cybersecurity. Differences in influencing factors, interests, barriers, and obstacles amongst female and minority students suggest unique considerations and challenges.

Acknowledgements

There are many people to thank and acknowledge for influencing and supporting me to complete this educational journey. I want to thank my wife of 27 years for her patience, love, and support throughout this process. Your unwavering support and love during this time cannot be overstated, and I am deeply appreciative. I would also like to thank my three beautiful daughters for their love, support, and inspiration to continue my educational journey later in life.

My parents instilled the importance of education at an early age as a means to independence. My older brothers provided an example and role model of what hard work, persistence, or educational success looked like, which can not be understated when living and growing up in a rural community where educational attainment was not always a visible priority within the community.

Finally, I would like to thank my colleagues at my university and the professors and advisors at the University of Illinois for their encouragement, knowledge, advice, and support. Your approach that emphasizes support, flexibility, and encouragement without compromising integrity has forever influenced my personal approach to education. You inspire me and other students on a daily basis to reach higher. Let's continue to do what we can to make a positive, lasting difference in the world together.

Table of Contents

List of Tables v

List of Figures vi

Definition of Terms vii

Chapter 1 Introduction 1

Chapter 2 Literature Review 11

Chapter 3 Theory and Methodology 45

Chapter 4 Results 62

Chapter 5 Conclusions, Implications, and Recommendations 97

References 101

Appendix A – Student Participant Survey 106

Appendix B – Student Interview Guide 109

Appendix C – Faculty Interview Guide 110

Appendix D – Recruitment Emails 111

Appendix E – Participant Consent Form 113

Appendix F – Institutional Review Board 118

List of Tables

1. Descriptive Statistics for Faculty Participant Profile Data (N=5) 66

2. Descriptive Statistics for Cybersecurity Student Population (N=19) 70

3. Descriptive Statistics for Information Systems/Technology Student Population (N=10) 70

4. Cybersecurity Student ABET Topic Ranking (N=19) 72

5. Information Systems/Technology Student ABET Topic Ranking (N=10) 73

6. Cybersecurity Student NICE Topic Ranking (N=19) 74

7. Information Systems/Technology Student NICE Topic Ranking (N=10) 75

8. Cybersecurity Student Influencing Factor of College Major Choice Ranking (N=19) 76

9. Information Systems/Technology Student Influencing Factor of College Major Choice Ranking (N=10) 77

10. Female Student ABET Topic Ranking (N=5) 78

11. Female Student NICE Topic Ranking (N=5) 79

12. Female Student Influencing Factor of College Major Choice Ranking (N=5) 80

13. Faculty Interviews – Example Notes and Initial Coding 82

14. Faculty Interview Categories, Descriptive Codes and Occurrences (N=5) 84

15. Faculty Interview Data and Codes Summary Table 85

16. Student Surveys – Example of Notes and Initial Coding 88

17. Cyber Student Categories, Descriptive Codes and Occurrences (N=19) 89

18. Information Systems/Technology Student Categories, Descriptive Codes and Occurrences (N=10) 90

19. Female Student Categories, Descriptive Codes and Occurrences (N=3) 91

List of Figures

1. Social Cognitive Career Theory 6

2. Periodic Table of STEM Occupations 2019..15

Definition of Terms

1. ABET – Accrediting Board of Engineering Technology
2. ABET-CAC - Computer Science-Cybersecurity Accreditation
3. Cybersecurity – "The ability to protect or defend the use of cyberspace from cyber attacks" (Kissel, 2013, p. 58)
4. Cyber Defense – "Actions taken to defend against unauthorized activity within computer networks" (Kissel, 2013, p. 41)
5. Cyber Operations – "Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations" (Kissel, 2013, p. 41)
6. KSA – Knowledge, Skills, Abilities
7. NICE – National Initiative for Cybersecurity Education
8. NSA CAE – National Security Agency Center of Academic Excellence
9. SCCT – Social Cognitive Career Theory
10. STEM – Science Technology Mathematics Engineering

Chapter 1

Introduction

Significance and Statement of Purpose

Organizations, businesses, and individuals are increasingly dependent on secure technology within their workplace, at home, and anywhere outside their home when considering ubiquitous Internet-connected mobile technology such as cell phones, laptops, tablets, and automobiles. At the same time, cyber-attacks targeting organizations, businesses, and individuals continue to increase in frequency and sophistication. These attacks are not limited to technology but involve attacks such as phishing, a social attack, ranking number one and number two on the list of cyber threats that resulted in an incident or breach of data in 2020. Cybersecurity threats are a global phenomenon targeting small to large organizations and businesses across all industry sectors (2020 Data Breach Investigations Report 2020).

There is a global shortage of educated and skilled cybersecurity professionals. Morgan (2017) predicts a 3.5 million global worker shortage in cybersecurity by 2021. The United States Bureau of Labor Statistics ranks the Information Security Analyst number one in all STEM occupations in terms of a projected positive employment change of 31.6% from 2018 through 2028. Only one other STEM occupation, Statistician, was in the 30-percentile range and ranked at number two (U.S. Bureau of Labor Statistics, 2019).

Furthering the challenges cybersecurity threats present to society, there is a lack of qualified high school teachers in computer science let alone the more recent but related discipline of cybersecurity (Shein, 2019). As a consequence of this and other factors such as core curriculum requirements that do not require computer science, there is likelihood that students have little or no exposure to computer science curriculum or cybersecurity education within traditional middle school and high school curriculum and environments (Shein, 2019).

Compounding the potential lack of cybersecurity career awareness and educational opportunity presented to students, Mountrouidou et al. (2019) posits that too few students enter the cybersecurity profession that represent our diverse society while at the same time there are not enough cybersecurity educational opportunities for all students. Diversity in the cybersecurity workforce is important, considering the worker shortage and evolving policies within organizations to represent all genders and groups. The current cybersecurity workforce is not diverse with only “11% represented as female, 6% African American, and 7% Hispanic” as of 2019 (Mountrouidou, et al., 2019, p. 158).

Despite these daunting cybersecurity workforce and educational challenges, cybersecurity curriculum standards are progressing within higher education. Within higher education, cybersecurity curriculum and accreditation standards are emerging and providing guidance to curriculum designers and programs seeking accreditation. These standards also provide differentiation to more traditional computing programs such as computer science and information systems in terms of topics and subjects unique to cybersecurity. The Accreditation Board of Engineering and Technology (ABET) is an organization that accredits college and university programs in science, computing, and engineering. New college degree programs in cybersecurity have emerged with eight programs in the last two years at the time of this writing fully accredited in Computer Science - Cybersecurity by ABET (Criteria for Accrediting Computing Programs, 2019 – 2020). The National Security Agency (NSA) Center of Academic Excellence (CAE) designation in cyber defense is another organization and program that accredits university programs related to computing and cyber defense. Over 300 college and university programs have achieved one or more levels of cybersecurity academic center of excellence status by the National Security Agency Center of Excellence (NSA/DHS National CAE in Cyber Defense Designated Institutions). It is presumed that these recognized accreditation standards and program designations influence what topics educational institutions teach to cybersecurity students since they provide essential accreditation for the programs.

The literature review has revealed minimal insight into what factors influence students to choose cybersecurity as a higher education major and career. This should not be surprising due to the relatively new nature of the cybersecurity career, emerging education standards, and the small number of accredited cybersecurity programs that could offer participants for a study.

My interest in factors that influence career decisions has been with me personally for quite some time. As a high school student, I recall struggling to choose a college major and potential career given my limited exposure to the “real world” and the vast number of options before me. I have often found myself contemplating just how and why I have chosen the careers and employment opportunities that now liter my resume. As a father of three children that have now either recently graduated from a university, are finishing their university studies, or are just beginning the process of deciding on a career and college major, I see again first hand just how difficult it is to decide on a career direction as well as the multitude of factors that influence these decisions. As a professor teaching and advising in an accredited cybersecurity program, I have often wondered why students make a choice to pursue cybersecurity and what interventions could potentially be effective towards increasing the number of students pursuing cybersecurity. Considering the wide range of job roles, skills, exceptional employment opportunities, and the global need for workers to protect our privacy and digital assets, I often wonder if many students are missing an incredible opportunity due to lack of awareness or other misconceptions. More specifically, as I pursued my doctoral research and became more aware of the current literature, I found myself asking the following questions:

1. What and who will inform and inspire students who are contemplating their college major and careers to consider cybersecurity? How will students become aware of the career and the opportunity that cybersecurity offers?
2. Of the students who are enrolled in post-secondary cybersecurity programs, why are they there? What were the factors that influenced their decision to pursue cybersecurity as a college major and career?
3. Considering the wide array of subjects within cybersecurity, what aspects of cybersecurity education and careers are students attracted to and interested in the most and least?

The hypothesis of this dissertation is that if we better understood influencing factors and cybersecurity student interests, interventions and programs could be designed to make high school students more aware and interested in these educational and career opportunities. It is presumed that such increased awareness and knowledge could potentially address the cybersecurity worker shortage, which is both an issue of economics and national security (U.S. Congress Joint Economic Committee, 2012).

Research Questions

Central Research Question

- What factors have influenced current cybersecurity students to choose cybersecurity as a college major and career?

Sub-questions

- What technical and non-technical characteristics of cybersecurity, as defined by the leading curriculum standards, are student participants most and least interested in?
- How does background and context, such as gender, influence cybersecurity career choice, such as gender?
- Why do some students choose to major in a computing-related major that is not cybersecurity, such as information systems?

Hypothesis

There is currently not a clear understanding of the factors that influence cybersecurity career choice. By better understanding these factors, interventions and programs can be designed and implemented to increase awareness and interest in cybersecurity leading to more students choosing cybersecurity as a higher education major and career. The increased interest could improve the current pipeline issues that contribute to a shortage of cybersecurity workers.

Overview of Theory

The Social Cognitive Theory and Social Cognitive Career Theory (SCCT) are prominent in the literature as theoretical frameworks that are utilized to evaluate career choice, academic program choice, and general factors of influence on these choices. The SCCT has been used in similar studies such as Kier et al. (2014) to evaluate student career choice and interest. The theory aligns well with this study's research question and provides a theoretical structure for evaluating the research question. The figure below illustrates the SCCT model. This model is the overarching framework and influence for designing the survey and interview questions used in this study with qualitative and quantitative questions designed to address key aspects of the SCCT model. The SCCT model will also provide a lens through which the study's data can be analyzed and presented. The SCCT theory can be used to examine career choice influencing factors using five primary components: self-efficacy, outcome expectations, background context, social supports and barriers, and personal inputs such as gender, race, ethnicity, and predispositions. These five components may interact to influence interests, goals, learning experiences, and actions (Lent, et al., 1994).

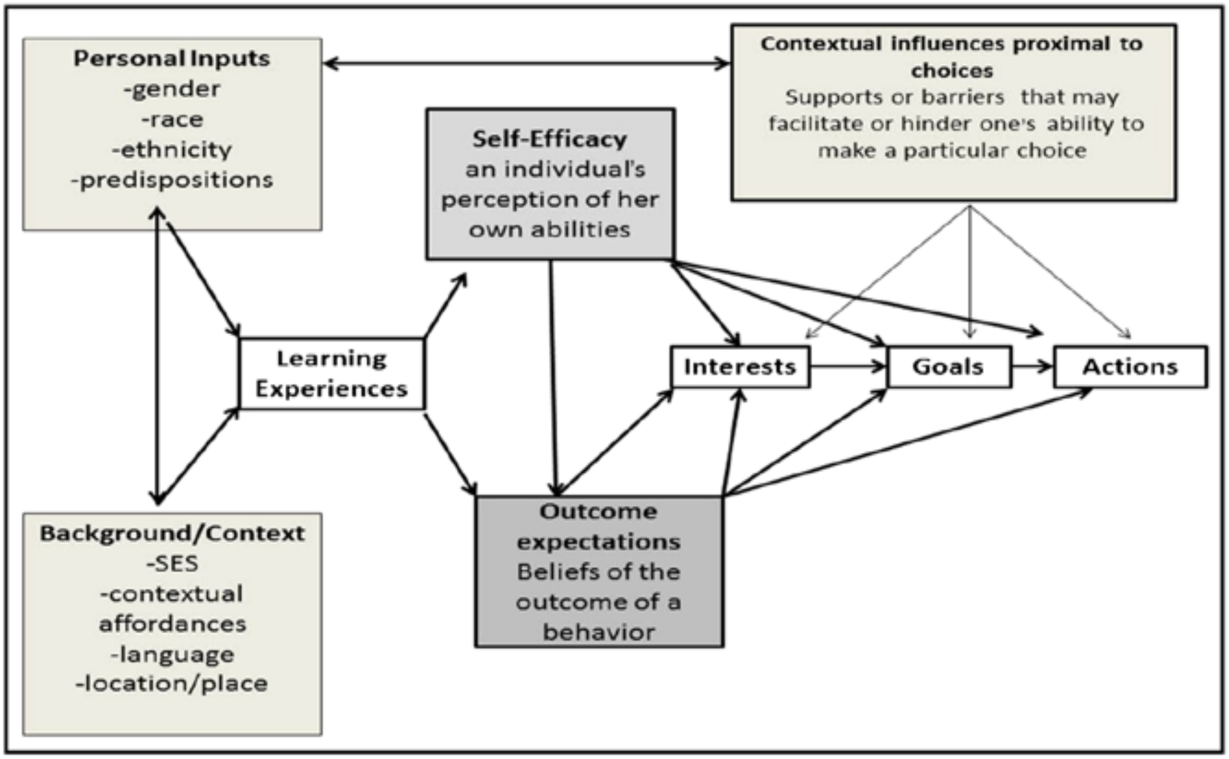

Personal Inputs
-gender
-race
-ethnicity
-predispositions
Contextual influences proximal to choices
Supports or barriers that may facilitate or hinder one's ability to make a particular choice
Self-Efficacy
an individual's perception of her own abilities
Learning Experiences
Interests
Goals
Actions
Background/Context
-SES
-contextual affordances
-language
-location/place
Outcome expectations
Beliefs of the outcome of a behavior

Figure 1
The Social Cognitive Career Theory (Lent et al. 1994)

Referencing the figure above, a student has personal attributes such as their gender or race and characteristics of their background. These personal attributes may include whether they live in a rural, suburban, or urban environment. Personal attributes and background influence their learning experiences in terms of courses they may be encouraged to take or perceptions they may have about appropriate courses. These learning experiences influence a student's self-efficacy and outcome expectations. For example, a student who performed well in math and science courses may have a higher level of self-efficacy such as believing they will succeed in STEM careers. High achievement in STEM-related learning experiences might also increase their outcome expectations, such as believing they will be positively rewarded for additional work within STEM. Self-efficacy and outcome expectations may influence interests, goals, and actions. For example, someone with a high level of self-efficacy and outcome expectations as relates to STEM may have an increased interest in STEM careers, set a goal to obtain a degree in a STEM field, and apply and enroll in a STEM major at a higher-education institution. This study doesn’t seek to understand the interplay of the SCCT components further but instead utilizes this framework and model as a means to design this research study to better understand why students specifically chose cybersecurity as a career and how they were influenced to do so.

The researcher will apply the SCCT theory within a pragmatic philosophical worldview. According to Creswell (2019), pragmatism is typical in social science research. It places the focus on the research problem or questions while affording the researcher the freedom to choose the methods and techniques that best address the research question or problem. Pragmatism often uses pluralistic or mixed method approaches to solve the problem or answer the question. Pragmatism is aligned well with the mixed methods research techniques utilized within this study as it allows for multiple approaches for collecting and analyzing data.

Approach to the Literature Review

The general field literature review was a journey of discovery to understand why students choose STEM education and careers, the pipeline challenges that have been present in STEM for quite some time, and the challenges related to attracting and retaining a diverse population of educated STEM workers. The literature was reviewed to discover essential research in the area of not only STEM pipeline challenges and potential solutions but also in regards to what factors may influence students to pursue a career in a STEM field within the larger context of career exploration. The constructs of the Social Cognitive Career Theory (SCCT) are frequently used in STEM career choice studies to measure student interest and influencing factors. Therefore, literature and findings that explore SCCT were included in this literature review.

The special field literature review focused more specifically on the relatively new educational and professional discipline of cybersecurity, which while typically categorized as STEM and computing, has many unique characteristics outside of traditional computer science and information systems that may be worthy of more focused research and exploration. As Mau et al. (2019) conclude in their study that assessed high school student STEM career interest using the Social Cognitive Framework: "given the range of academic majors and occupations organized under the STEM umbrella, there is a need to go beyond STEM as a uniform domain to more specialized considerations" (p. 8). The literature was explored to locate research studies that specifically focused on cybersecurity pipeline issues and factors that influence students to pursue cybersecurity as a major and career.

Current educational standards within cybersecurity higher education were also reviewed to provide a foundation for a better understanding of the specific characteristics of cybersecurity education and professional cybersecurity careers. These standards may help inform subsequent research design related to factors that influence students to choose cybersecurity education and careers. For example, some students may be attracted to the investigative aspects of cybersecurity while others are attracted to more "soft skills" such as risk analysis, compliance, and governance. In contrast to STEM when viewed broadly, neither of these aspects of cybersecurity requires high degrees of math or computer programming, which are characteristics that researchers and society often associate with STEM and computing-related disciplines.

Investigation, risk, compliance, and governance are also characteristics that are not traditionally associated with more traditional computing degrees such as computer science or information systems but are central to cybersecurity education and careers (NICE Cybersecurity Workforce Framework, 2019).

Summary of Methods and Research Plan

The questions and hypotheses presented in this study aligned well with qualitative methods due to the exploratory, inductive nature of the questions. Therefore, there was an emphasis on qualitative methods within this study's methodology. To improve the reliability and validity of the study, a mixed-methods survey instrument was included in the research design such that more participants could be efficiently included. The survey instrument allowed the researcher to more efficiently collect qualitative and quantitative data from the entire population of student participants within the case that volunteered to participate. The survey approach was more efficient and practical than interviewing each student individually while also allowing for the research to capture some quantitative data. The survey consisted of qualitative questions with some quantitative questions that allowed for further analysis, segregation, and descriptive statistics methods. The research plan utilized a case study approach. The case was bounded by new students in a cybersecurity or information systems major. The new cybersecurity students were enrolled in a 100-level, introductory cybersecurity course within a cybersecurity accredited bachelor's degree program. The faculty within this cybersecurity program further bounded the case as key informants and subject matter expert participants. The students completed a survey followed by interviews of selected student participants where clarification or elaboration of the survey data was deemed necessary and beneficial. Faculty participants were interviewed. Faculty participants were experts in the cybersecurity field as represented by their academic credentials, industry certifications, research publications, work experience, and experience teaching and advising cybersecurity students.

The researcher reviewed the qualitative data, coded the data, and pulled the themes and categories from the survey and interviews to address the research questions in both a qualitative and descriptive manner. In the interest of time and feasibility of access to participants, this study was limited to a single university. Considering the small number of accredited cybersecurity programs and current restrictions due to the COVID-19 pandemic, this study represented a significant number of current cybersecurity college students.

As you can see in Appendix A, the quantitative and qualitative survey questions are categorized by the components of the SCCT. By collecting SCCT personal inputs and demographic information, the qualitative data may be segmented and further analyzed, potentially offering more insights into influencing factors of cybersecurity career choice.

Chapter 2

Literature Review

Organization of the Literature Review

This review investigates foundational, working definitions of STEM, the current demand for STEM workers, and the relationship of STEM education and careers to national and global issues. The state of the STEM pipeline is also interrogated. Current literature is presented and analyzed related to STEM career predictors and influencing factors as relates to educational and career choice. This includes examining the factors that influence students to choose STEM careers, including demographic issues. The literature review also examines theoretical frameworks and debates related to career choices. The review then shifts focus to the more specific STEM discipline of cybersecurity.

Theory

Social Cognitive Career Theory (SCCT)

The Social Cognitive Theory and Social Cognitive Career Theory are prominent in the literature as theoretical frameworks that are utilized to evaluate career choice, academic program choice, and general factors of influence on these choices. A relatively new theoretical model, the Cybersecurity Engagement Model, may also provide structure and a lens to examine more specifically cybersecurity career influencing factors and choices.

Bandura's Social Cognitive Theory forms a basis for the Social Cognitive Career Theory that followed in Lent et al. (2008) that is prevalent in current literature related to STEM career choice and influence. Bandura (1986) presented the SCT theory with four key components that have an impact on motivation and obtaining goals: self-observation, self-evaluation, self-reaction, and self-efficacy. The self-efficacy component is especially prominent in the literature and can be partially described as a person's belief in themselves to be successful even if they have to work hard, persist, and apply themselves. Lent et al. (2008) expanded on SCT with an emphasis on self-efficacy with the Social Cognitive Career Theory (SCCT) and the potential to use the theory to predict student interest in STEM computing disciplines. Related studies that existed before Lent's 2008 study had primarily focused on engineering disciplines in a small geographic region. Lent's study was much broader, including 1208 participants from 42 universities with significant representation of genders, race, and academic standing. There were 21 predominantly white and 21 predominantly black universities included in the study. The survey instrument included aspects of the SCCT, such as students' self-efficacy, outcome expectations, interests, social supports and barriers, and educational goals, which were influenced by the SCT. The results suggested that the SCCT model generalized well within computing disciplines across gender, environment, and university. Two aspects of self-efficacy were a focal point. These self-efficacy aspects included the student's confidence in their ability to be successful in their major and their perceived ability to overcome barriers and obstacles such as lack of support from faculty or advisors.

Following Lent's SCCT research, Kier et al. (2014) examined whether a new survey instrument, STEM-CIS, based on key aspects of the SCCT, could be effective at measuring middle school students' interests and goals related to STEM subjects and potential career interests. The participants for this study were middle school students from rural areas in the United States with high poverty levels (80%) and a high level of minority students (85%). The STEM-CIS is a 44-item instrument that measures a student's interests in STEM subjects and careers. The STEM-CIS survey was found to be valid for predicting student interest in STEM when utilizing the SCCT framework. The survey was tested in a pilot project and subsequently modified to align with STEM and primary characteristics of the SCCT. The authors suggest that the survey will be useful to future researchers when evaluating student STEM interest beyond middle school as well as evaluating STEM programs.

Desired increase in STEM education is not just a United States initiative and problem but one of a global nature. Mau et al. (2019) utilized an instrument to assess psychometric factors that may influence Taiwanese student interest in specific STEM disciplines when applying an extension of Social Cognitive Career Theory (SCCT), STEM-CIS. This study's findings present strong support for using the STEM-CIS model to assess career interests of the Taiwanese high school student participants using a Chinese version of the STEM-CIS instrument. The study sought to expand beyond basic math, science and engineering disciplines and also address cultural aspects of STEM career interest assessments and counseling. Mau et al. stated in their findings that "given the range of academic majors and occupations organized under the STEM umbrella, there is a need to go beyond STEM as a uniform domain to more specialized considerations" (Mau, 2019, p. 8). This broadly supports expanding the analysis and applicability of the SCCT to more recent majors and disciplines such as cybersecurity, which is the focus of my dissertation study.

Cybersecurity Engagement Model

Although theories have been located in the literature that have been utilized to primarily study STEM career interest, such as the SCCT, there has been a lack of theoretical models located in the literature related to cybersecurity or specifically designed to examine factors that influence cybersecurity career choice. However, Lingelbach (2018) conducted a recent research study that examined the factors that attract females to the cybersecurity profession. A new theoretical model emerged from Lingelbach's study: the Cybersecurity Engagement Model. The theoretical model suggests that strategies, engagement, and a “cybersecurity profile mindset” will likely enable a successful career in cybersecurity (Lingelbach, 2018, p. 73). The model suggests that a cybersecurity career choice is heavily influenced by engagement factors such as awareness, which includes subcategories of exposure and education. Support from family and mentors, having a natural interest in cybersecurity, attractive salary potential, sense of contribution, and a perceived sense of pride and belonging were also found to be very influential strategies and engagement factors within this model.

The third, primary component to the cybersecurity engagement model, cybersecurity mindset, consists of personal characteristics such as self-efficacy, analytical mindedness, assertiveness, and technical savviness. The importance of personal characteristics is further supported by Lent et al. (2008) whose study suggested that self-efficacy and other personality traits have a significant influence on career choice. The cybersecurity engagement model may indicate that if the strategies, engagement factors, and a cybersecurity mindset are present, a successful career in cybersecurity may be more likely. Linglebach’s study was limited to female cybersecurity professionals currently working in a cybersecurity role within the defense industry. Lingelbach suggested future research using this model that may help to determine if the study’s results and theoretical model can be generalized and applied to other industries, genders, and to students.

What is STEM and Why is it Important?

The STEM acronym stands for Science, Technology, Engineering, and Mathematics. Occupations such as mechanical engineers, computer scientists, and statisticians are commonly categorized as STEM, as their occupation name would suggest. However, these four areas of the STEM acronym represent a very large array of educational fields of study and related careers beyond traditional engineering and science careers. For example, Langdon et al. (2011) presented within a recent U.S. Department of Commerce, Economics, and Statistics Administration report that there is not a standard, global definition for which specific occupations are classified as STEM. Another U.S. federal department, the U.S. Bureau of Labor Statics (BLS), did classify specific occupations as STEM, as seen in the Periodic Table of Science, Technology, Engineering and Math Occupations (2019). This BLS "periodic table" singled out 23 occupations specifically as STEM, including job descriptions, average salaries, education requirements, and projected growth.

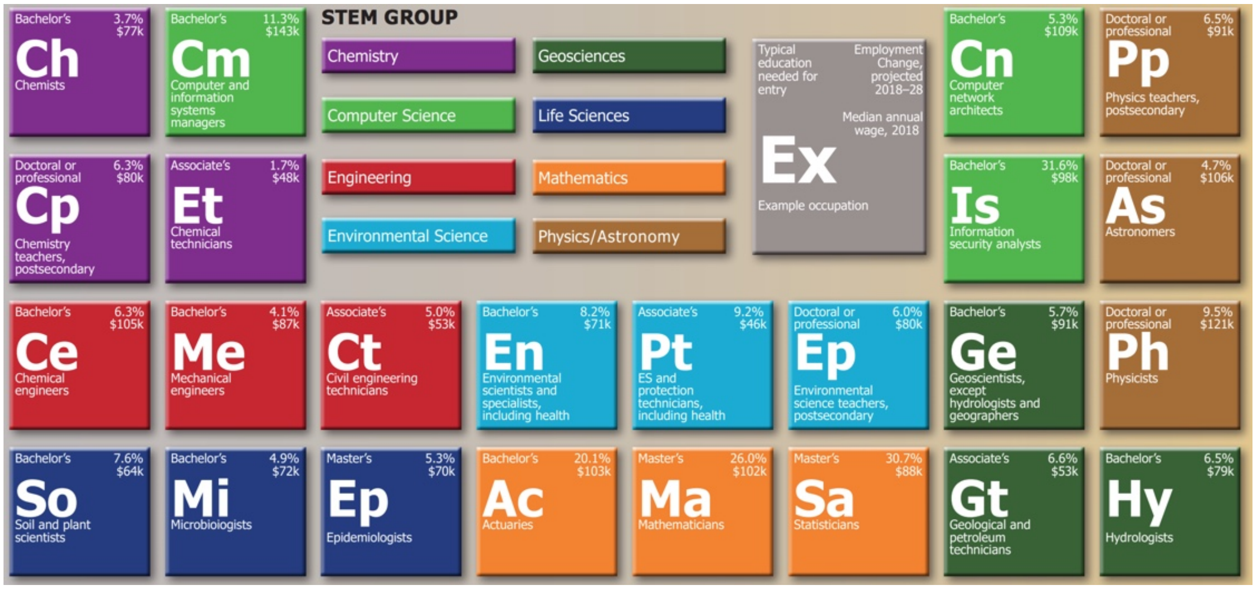


Figure 2
Periodic Table of STEM Occupations - 2019 (U.S. Bureau of Labor Statistics, 2019)

Noonan (2017) added to this lack of a STEM standard discussion by representing that there is no consensus on whether to include professions such as STEM educators, managers, technicians, health-care professionals, or social scientists within STEM. To further illustrate the broad range of disciplines within STEM and the varying aspects of STEM within each discipline, one can look to the Accrediting Board of Engineering and Technology's recent accreditation criteria of college computing programs specifically deemed “cybersecurity.” These cybersecurity accreditation requirements include only six college credits of math, which is typically two college courses, of fundamental (not advanced) math in the areas of discrete mathematics and statistics (Criteria for Accrediting Computing Programs, 2019 – 2020).

Education requirements for STEM careers typically require a bachelors degree or higher. According to Langdon et al. (2011), “68% of STEM workers have a bachelor’s degree or higher compared to 31% of non-STEM workers,” which emphasizes the importance of education within STEM careers (Langdon, 2001, p. 6). Noonan (2017) presented similar findings as “nearly three-quarters of STEM workers have at least a college degree compared to just over one-third of non-STEM workers” (Noonan, 2017, p. 2). The demand for STEM workers in industry and STEM education requirements presents an opportunity for those evaluating career and educational options in terms of low unemployment, high wages, and innovative work (Morgan, 2017). This employment opportunity also presents an economic and national security challenge when the demand for STEM workers is not met. The demand for STEM workers is projected to outpace the demand for non-STEM through at least 2028 and likely beyond if history repeats itself. During this time period, STEM occupations are expected to grow by almost 9%, whereas non-STEM careers are expected to grow by 5%. The annual salary for STEM careers is projected to average $84,880 with no-STEM careers averaging a salary of $37,020 (Employment in STEM Occupations, 2019). One STEM discipline, cybersecurity, is projected to have a 3.5 million-worker shortage globally by 2021 (Morgan, 2017).

Langdon et al. (2011) writing on behalf of the U.S. Department of Commerce, Economics, and Statistics Administration emphasized that STEM is very important to the future of the United States, stating that STEM workers “are essential for developing our technological innovation and global competitiveness" (Langdon, 2001, p. 6). Noonan (2017) addressed the innovation aspect as well, stating that STEM workers drive U.S. innovation, as they are more likely to apply for, receive, and commercialize patents. The United States is also not leading many global competitors in graduation rates for STEM workers with Germany, Canada, and Mexico graduating more students as a percentage of degrees granted (U.S. Congress, 2012). The 2012 U.S. Congress report on STEM Education also emphasized the criticalness of technology innovation as a primary driver of U.S. economic growth, stating that "over half of the economic growth in the U.S. over the past 50 years being attributed to improved productivity through innovation" (U.S. Congress, 2012, p. 1).

STEM Career Predicators and Influencing Factors

Understanding factors that might predict and influence students to choose STEM education and careers is critically important towards improving the STEM pipeline problem, or, in other words, increasing the number of students studying STEM and pursuing STEM careers. By better understanding influencing factors and predictors, society and government can invest in programs and interventions that may influence students that may not have otherwise considered STEM opportunities. These interventions could come in many forms, from teacher and counselor training and awareness, mentor programs, curriculum standard changes, outreach programs, workshops, camps, and general awareness.

The majority of the literature that has been located and reviewed to date consists of quantitative studies that attempt to correlate student interest in STEM primarily with: personality traits such as levels of self-efficacy; achievement in traditional STEM courses such as math and science; outcome expectations; level of STEM awareness such as employment, earning potential, and perceived job characteristic compatibility; and analysis of demographic factors such as race, gender, and socio-economic factors. Many of these studies utilized the constructs of Social Cognitive Career Theory as a theoretical framework to guide the design of the research and analysis of the results.

Hall et al. (2011) examined factors that influenced students to pursue opportunities in STEM fields by utilizing multiple quantitative survey instruments across four groups of participants from the southeast United States. Participant groups included high school students, parents of the high school students, school personnel, and engineering college students. Hall sought to determine factors that influenced the high school students' career decisions, the level of STEM awareness amongst the parents and school personnel, and the factors that influenced the engineering college students' career choice and timing of their major decision. The high school and college student survey questions focused on influencing factors such as friends, peers, parents, teachers, counselors, earning potential, affordability of education, and other media influences. The parent survey questions probed at the parent's college aspirations for their children, familiarity with STEM, and general college environment awareness. College students enrolled in a low-level engineering course were given the same survey as the high school students. The school personnel survey included teachers of math and science as well as school counselors.

The results of the Hall et al. (2011) study and the analysis of the data presented an interesting perspective in the literature given the breadth of the participants and potentially unique, yet related, perspectives of the participants. The high school and college survey results were similar, with both groups ranking the following influencing factors in the following order: personal interest, earning potential, parents, and teachers. The second and third factors were flipped between the high school and college students, with high school students ranking earning potential higher. Most college students did not choose their major until high school. These results highlight a diverse set of influencing factors. The parent and high school personnel survey indicated a high level of interest in STEM careers but a relatively low level of awareness, which is problematic given that parents and teachers were two of the top four high school and college student influencing factors. For example, 60% of the high school personnel indicated that they "did not feel knowledgeable about career options in science fields" (Hall et al., 2011, p. 39).

Malgwi et al. (2005) also examined influencing factors of major selection and change of major with college student participants at a large northeastern United States university. Malgwi et al. analyzed factors that may be different between traditional and transfer students as well as factors that may differ by gender. Similar to Hall et al. (2011), the results indicated that the highest-rated influencing factor of career choice or major selection was student interest. Malgwi's study segmented the data by gender, which resulted in a difference in the second highest-rated factor. Female students rated aptitude perception second while male participants rated potential for career advancement and opportunity second. This also correlates well with Hall's study, with earning potential (opportunity) rated very high at number three for high school students and number two by college students (Hall et al., 2011). In Malgwi's study, women were significantly more likely to be influenced by their "aptitude for the subject than the earnings potential" (Malgwi et al., 2005, p. 277). When looking at those students that changed majors and the factors that influenced the change, there were no differences in the top four factors between male and female respondents. This may suggest that over time, influencing factors by gender may become more similar amongst college students.

Both the Hall et al. (2011) and Malgwi et al. (2005) studies suggest that there are many influencing factors as relates to career choice by both high school and college students, but the most important, highest-ranked factor in both studies was student interest. Masnick et al. (2010) also researched high school and college students. Masnick et al.'s study focused on interests, attitudes, understandings, and misconceptions as relate to occupations in science. Masnick et al.’s study sought to determine how students’ positively and negatively perceive science careers and how these perceptions compare to non-science related careers. The authors hypothesized that high school students associate what are traditionally considered negative attributes, such as complex mathematics, lack of creativity, and limited social skills, with scientific careers. This study had high school and college student participants rate occupations relative to one another based on a set of characteristics such as scientific, creative, and artistic. The results were then analyzed to determine which occupations were perceived by the participants to have certain characteristics, which may help to explain why some students are drawn to some occupations and not others based on their interests and perceptions of the occupation. The results of Masnick’s study were similar across the high school and college participant groups. A key finding in this study was that science was perceived to be the opposite of the creative characteristic. Participants also did not strongly associate the people-oriented characteristic with scientific careers. Male and female participants had very similar perceptions of the science occupations within this study. Since other studies, including Hall et al. (2011) and Malgwi et al. (2005), have shown that student interest is an important influencing factor of career choice, if social and creative aspects of scientific career perceptions can be improved, then scientific occupation career choice may also improve as a result.

Falco (2017) also addressed influencing factors of career choice with a focus on the influence of the school counselor. This study sought to better understand how secondary school counselors could maximize student engagement in STEM by better understanding the factors that influence student success in STEM courses and subsequently implementing interventions that increase student interest and success in STEM courses. Falco presented that outcome expectations from family members and peers are an influencing factor. The author cited studies that indicate that parent, institution, and teacher "gender and race stereotypes do exist" and are likely an influencing factor in terms of "STEM encouragement and student perceptions of successful outcomes in STEM careers" (Falco, 2017, p. 364). Falco suggests that secondary school counselors need to monitor the "course taking patterns" of their students and "encourage advanced courses in mathematics and science for those students that show aptitude in those subjects" (p. 365). In addition, support may be needed towards a growth-oriented approach in the form of tutoring or study groups for those students that need additional assistance to be successful in these STEM courses. Falco also suggested that counselors should highlight the benefits of enrolling in advanced STEM courses such as the "potential to earn a higher salary" and "better preparation for college coursework" (Falco, 2017, p. 365). High earning potential was presented in the top three influencing factors within the Hall et al. (2011) study for both the high school and the college participants, which adds additional support to Falco's findings.

Women and Minority Underrepresentation in STEM

There is a focus in much of the literature related to STEM pipeline issues and career choice related to the underrepresentation of women and minorities in both STEM education and careers. Much of the literature attempts to provide insight into why females make different career and educational choices than men and whether this is actually by choice or by some form of discrimination or influence.

Eccles (1994) explored why women choose particular occupations and why so fewer women choose STEM education and careers than men. With some similarities to aspects of SCT and SCCT frameworks, Eccles focused on motivational factors such as “goals, career aspirations, course selection, persistence on difficult tasks, and how participants chose to allocate their effort” (Eccles, 1994, p. 587). Eccles's participants consisted primarily of adolescent and high-school students. The findings suggest that women and men tend to choose stereotypical occupations based on their gender, such as women having a tendency to choose nursing while men may have more of a tendency to pursue engineering fields. The author suggests policy and culture changes that may make male-dominated occupations more attractive to women, such as providing better support for families, like easier access to child care services. A theoretical model, Model of Achievement Related Choices (MARC), was developed that provides a framework for linking educational, vocational, and other achievement-related choices to beliefs about expectations for success and the importance or value that individuals place on a particular option.

The Eccles (1994) study suggested that MARC can be used to predict whether students are more or less likely to enroll in a course based on influencing factors such as past success, parents, teachers, counselors, peers, and other social influences. It is also suggested that many options are never considered due to a lack of awareness or inaccurate information. The aspect of lack of awareness may have a robust application to the field of cybersecurity as it is a relatively new profession and educational field. Therefore, there is likely a general lack of awareness not just among students but also among those that influence students. Other significant findings in the Eccles study are related to gender. According to Eccles, “gendered socialized practices at home, in the schools, and among peers play a major role in shaping individual differences in self-perceptions and subjective task values” (Eccles, 1994, p. 605). In addition, the study suggested that “more equitable treatment and more family-sensitive social policies and supports would likely facilitate women’s willingness to consider a wide variety of occupational choices” (Eccles, 1994, p. 605).

Rosenbloom et al. (2008) investigated hypotheses for why women were underrepresented in STEM technical careers, such as information technology (IT). These hypotheses focused on three areas: discrimination, differences in ability, and choice. Participants were working professionals in the United States and included information technology occupations as well as non-IT occupations. Rosenbloom et al. presented that when accounting for measures of interest and personality, gender is not a statistically significant factor when determining the career choice between IT and non-IT professions. In other words, if two people of different genders have similar personality traits, gender is not a factor regarding IT career choice. The authors interpreted these results to mean that women are making the choice not to be part of the IT profession based on actual or perceived job characteristics (as opposed to other factors such as discrimination). Holland’s General Occupation Themes Model was utilized in the Rosenbloom study. Holland (1996) analyzed how environmental characteristic compatibility with personality type influences career aspirations and persistence. Holland’s models have been used to demonstrate or predict whether someone will persist in the same job or have a tendency to change occupations. Holland (1996) concluded that people are happier and tend to change careers less if they work in environments that are compatible with their personality type. Rosenbloom et al. (2008), using Holland’s model, presented that men scored higher than women on average in the “Realistic” and “Investigative” themes and lower on the “Artistic” and “Social” themes. “Realistic” theme people prefer activities that “involve mechanical manipulations or repairs and construction” while “Investigative” themes involve “gathering information, uncovering new facts or theories, and analyzing and interpreting data” (Rosenbloom et al., 2008,

p. 6). These themes traditionally represent characteristics of IT-related work much more than “Artistic” and “Social” themes. The authors emphasized that “occupational personality is not an inherent characteristic,” and therefore other influencing factors such as parents, education, and social pressures should be a focus of future studies (Rosenbloom et al., 2008, p. 13).

Wang et al. (2013) conducted a longitudinal study where math and verbal skills of high school 12th graders were analyzed as potential predictors of STEM career choice and persistence by age 33. The results of Wang’s study indicate that students with high levels of math and high levels of verbal skills are less likely to choose STEM occupations than those with high math skills but moderate verbal skills. In addition, the high math/high verbal group included more women than men. The author suggested that females consider a wider range of occupations, including non-STEM fields, due to their high verbal skills in addition to their high math skills. This is significant because it supports, as have many other studies in this bibliography, that math ability by itself is not the only or even necessarily the most significant factor to consider when analyzing STEM career choice. This study also suggested that math and verbal ability factors are more significant than “interests, occupation and lifestyle values, family education, and income” (Wang et al., 2013, p. 773).

Frome et al. (2006) collaborated with Eccles and others on a subsequent study that analyzed why more women do not maintain their career aspirations in male-dominated fields from adolescence to early adulthood. This longitudinal study found that female adolescents who held aspirations for a male-dominated career were unlikely to persist. Seven years after the initial survey, 80% of the participants were working in neutral or female-dominated occupations. This suggests that not only are women less likely to choose a male-dominated field to begin with but that they are also unlikely to persist in that field when they do. Interventions to improve persistence were presented, including providing real role models to encourage females while still in high school and improving employer family support such as child care that traditionally falls as the female spouse's primary responsibility.

Mau (2003) also examined factors of gender-related to persistence in student STEM interest. This study analyzed six years of data from the National Educational Longitudinal Survey of 1988 through the lens of SCCT. Participants were male, female, Asian, Black, Hispanic, and White. Math performance and self-efficacy were found to be two of the strongest predictors of persistence in science and engineering careers before adding race or gender to the analysis. Of the initial 24,599 eighth-grade students, 827 students aspired to science and engineering careers. Of the 827 students, "176 continued with the same aspirations in science and engineering 6 years after they had been identified (persisters), whereas 583 changed their aspirations to non-science and engineering careers (switchers)" (Mau, 2003, p. 238). The study concluded that men were more than twice as likely than women to persist in a STEM career. Falco (2017) emphasized that school "counselors need to be aware of stereotypes that could impact their ability to influence underrepresented groups" and need to encourage applications to scholarships for STEM education to mitigate disadvantages (Falco, 2017, p. 368).

Many STEM studies and some specific to computing and cybersecurity had female aspects of the study as part of a key question or hypothesis or had significant data analysis using gender as a focal point. Those cited in this research include Bashir et al. (2015), who sought to better understand if a larger number of females attending cybersecurity competitions would translate into an increase in diversity in the profession; Dunn and Merkle (2018), who suggested that female participation in cyber competitions resulted in a greater increase in cybersecurity interest than males; Lingelbach, whose study specifically examined female's characteristics in the cybersecurity profession' McEwan and McConnell (2013), who suggested that teenage females were less likely to express interest in learning more about computing; and McGill et al. (2016), who found that 16 to 17-year-old females feel welcome in computing but are influenced very little by computing activities prior to college, which is counter to some of the other studies, such as Shumba et al. (2013), which revealed that many females did not feel welcome. In addition to these studies, Shumba et al. (2013) presented work performed by an ACM conference working group in 2013 focused on women and minorities in the cybersecurity profession.

Shumba et al. (2013) stated that past studies have found barriers to women and minorities in computer science and summarized the findings as "misconceptions about what computer science is and who can do it" (Shumba et al., 2013, p. 5). Barriers cited in the authors' literature review could be categorized as the perception of a male-dominated work environment, primarily male-dominated faculty that may be less welcoming, females not being encouraged in middle and high school levels, and misunderstandings or narrow understanding of what the field entails or could be for those that choose it to pursue it. The Shumba et al. (2013) working group categorized initiatives that can improve female and minority participation in the categories of recruitment, education, and career development. Additional barriers that were identified by this working group included the perception of "strong alignment with the hacker community and military" (Shumba et al., 2013, p. 5). Specifically related to cybersecurity, the author noted the male-dominated "hacker culture" characterized by late nights at the computer lab and working weekends may not be welcoming to females or provide an environment where females feel safe. Shumba's study recommends camps, competitions, and workshops designed to be welcoming to women and minorities starting at least as early as high school and middle school. The study's results also emphasized changing the current perception of a hacking culture and military image.

Additional points of emphasis included having women and minorities lead initiatives in education, professional organizations, and mentoring.

Computing and Cybersecurity Career Predicators and Influencing Factors

The literature located to date related to student cybersecurity career choice influence is largely related to community college or university outreach programs to secondary schools, clubs, workshops, or nation and state-sponsored events, such as cyber competitions. These programs and events are designed to increase student interest and awareness in cybersecurity. In the absence of a standard and ubiquitous cybersecurity curriculum, it appears that special events and outreach programs are the primary instruments to stimulate student interest and awareness.

Outreach Programs and Their Influence

In a broad study focused on computing outreach activities and their potential effect on student college major selection, McGill et al. (2016) evaluated whether high school student participation in university computing outreach activities impacted the selection of students' current college major. The study also emphasized the underrepresentation of females in computing-related fields and how increasing female participation can help provide a solution to the shortage of workers in computing. Undergraduate students from six different universities were recruited to participate. A little over half of the survey participants indicated that involvement in a computing activity prior to college did not affect their decision to major in a computing-related field. More than one-fifth of respondents indicated that participating in a computing activity before college did affect their decision. There was a very strong relationship between participating in a computing activity before college and deciding to major in a computing field amongst male participants, especially if the activity had voluntary participation. The results indicated that female students feel welcome in computing activities, but females not previously interested in computing will be influenced very little by computing activities prior to college.

In a study three years earlier than McGill's, McEwan and McConnell (2013) examined the interest and perception among 16 and 17-year-old United Kingdom students towards computing-related degrees. This study also had mixed results in terms of increasing student interest as a result of the program. The study found "pronounced" and "entrenched" attitudes in the student participants (McEwan & McConnell, 2013, p. 3). Only 14 of the 111 students indicated that they would (7) or might (7) pursue a computing career. Sixty-five percent had already decided on a career choice with family (22), media (17), or an acquaintance that currently does the job (17) being the most influential. Teachers (6) and career advisors (4) were the least influential in student career choice. Almost 50% indicated they knew very little or nothing about computing careers. Over 67% were not sure or did not want to learn more about computing careers. Females were much less likely to indicate they wanted to learn more about the computing careers. These findings are discouraging since they suggest that not only are students, especially females, generally unaware of computing careers, they have little interest in learning more about the career. However, most of the participants had already indicated a career choice. When compared with the other literature in this review, this study's results are more negative in terms of the influence a program or event can have on increasing students' interest and awareness.

More recently, Nakama and Paulett (2018) presented a case study involving a community college that partnered with a high school in a rural community in Hawaii, which provided an opportunity for students to engage in cybersecurity education. The case study explores what "does and doesn't work" and the potential of online technologies to enable the education. More specifically, the program within the study was designed to increase the number of women and minorities in cybersecurity education by offering a community college, four-course, online certificate program to high school students. Through student and other stakeholder surveys as well as observation, the author presented many insights related to successes, challenges, and student perceptions. There were two cohorts of 41 and 43 students, respectively, included in the study. Survey questions included why the student chose to enter the program and what activities or experiences would increase their interest in cybersecurity. Nakama and Paulett's study also captured data from those students that withdrew from the program. The students indicated the following top three items that could increase their interest in cybersecurity: first, "more information about what the job would entail," second, "access to more relevant classes," and third, "reassurance they would earn a good living" (Nakama & Paulett, 2018, p. 44). The potential influences of friends and family were ranked last. Open-ended responses indicated current teachers and counselors, followed by an opportunity to receive free college credit, as reasons why students were interested in the program. Those students that withdrew still indicated an interest in cybersecurity and cited other reasons for withdrawing from the program, such as time management and other activities competing for their time.

Turner et al. (2014)) also conducted a study of an outreach program where university faculty partnered with high school teachers and teams of high school sophomores to solve challenges in a variety of disciplines, including cybersecurity. The program was in the form of a camp program designed to foster interest in cybersecurity among high school students and high school teachers. More specifically, the study analyzed investigative interests as a predictor of student self-efficacy and provided specific analysis in regards to impact on female students. Turner hypothesized that the intervention would significantly increase interest in cybersecurity amongst female students. The study utilized pre and post-testing of 60 students from 10 high schools in the southeast United States. Over half were female, with the majority of both male and female participants identified as Caucasian. Faculty on each team were a mix of STEM and liberal arts faculty.

Turner et al. (2014) suggested that cybersecurity requires a broader definition than an "engineering centric" approach and that cybersecurity is more of a natural science with aspects of liberal arts as well. Examples cited were the policy, ethical, and social aspects of cybersecurity (Turner et al., 2014, p. 2). The study measured occupational interest using occupational themes, including science, self-efficacy, and perceived value of the cybersecurity activities. The results also suggest that female perceptions of cybersecurity value can increase when integrating STEM and liberal arts skills. In addition, learning the actual value of the tasks can lead to an increase in interest. Male student participants reported a decrease in interest. The authors hypothesized that the male participant expectations for the camp were not met, resulting in lower survey scores or the low scores representing the males protecting their self-worth. Increases in self-efficacy and confidence in cybersecurity were present in the results for all participants.

In another university outreach program utilizing a camp format, Ladabouche (2016) sought to evaluate the effectiveness of the GenCyber program, a National Security Agency and National Science Foundation (NSA/NSF) grant-funded program initiated in 2014 that provides funding for cybersecurity summer camps to both students and teachers at the K-12 levels. The goal of the program is to increase diversity and interest in cybersecurity careers to help address the shortage of skilled cybersecurity workers. Additional goals of the program include raising awareness of safe, online behavior and improving teaching of cybersecurity content in K-12 levels. The camps are free of charge, typically hosted at public universities, and are organized as student, teacher, or student and teacher camps. GenCyber provides the camp organizers with goals and guidelines, but the camp organizers determine the detailed curriculum and delivery. This design allows a fundamental, common foundation of each camp while allowing each camp to be unique. In 2014 and 2015, the program served 240 teachers and 1300 student participants, half of whom were female. Survey results of student participants indicated strong overall interest and improved interest in cybersecurity careers as a result of the program. A survey of teachers that had attended the program in 2015 presented that 62% of the teachers had implemented a cybersecurity curriculum. The program has grown substantially with an almost 70% increase in student participation and a 75% increase in teacher participation between 2015 and 2016.

Competitions, Camps, Workshops, and Interventions

Cybersecurity competitions are a somewhat popular means of attracting high school and college students to the field of cybersecurity as well as older adults and professionals. There are many cyber competitions sponsored by universities, federal agencies, state organizations, and private organizations that are designed to recruit talent to the cybersecurity field. In addition to GenCyber, CyberPatriot is another program targeting high school students with a goal of increasing student interest in cybersecurity. The program was initiated by the Air Force Association with a goal to increase the number of workers in the field of cybersecurity. Manson et al. (2012) presented how one university worked with a high school district to help increase participation in the CyberPatriot program.

Manson et al. (2012) conducted a study that involved a partnership between a local university and high school. The university assisted the high school with preparing for the CyberPatriot cybersecurity competition by offering classroom sessions designed to prepare the students. The research utilized a mixed-methods approach of both quantitative survey data and qualitative data from interviews. There were 146 participants. The research provided quantitative demographic information from the survey that included grade level, ethnicity, gender, and overall interest in the field of computing. Four interviews were conducted that represented the university, industry, high school faculty, and one student participant. Eight qualitative questions presented open-ended questions related to awareness and motivation, whether the participant's experience was positive or negative, and their interest in future programs. Manson found that student motivation for participation did not include the desire to win the competition but rather an interest in learning more about computing and security, as the participants already had an interest in computing. Manson presented that participants had an overall positive view of the CyberPatriot competition in terms of increasing interest in learning cybersecurity skills. The participants in general had many desires for improvement, including desire for growth in the CyberPatriot program, more training for the event, improvements to the technical environment, and better educational feedback to the participants to increase the value of the event. All participants expressed a desire for a stronger relationship between the university and the high school with more online resources to reduce the need to commute from the high school to the university to practice for the competition. One very significant limitation of this study is that only one student was interviewed, with the remaining student participants completing the survey.

The Cybersecurity Awareness Week event is a large cybersecurity training and competition event where students can participate in workshops and cybersecurity competitions. Bashir et al. (2015) conducted a quantitative study of the participants that attended this event. Bashir sought insight into why participants chose to attend Cybersecurity Awareness Week and whether competition participants' expectations were met. Bashir also examined variation between race and gender groups. Bashir found that 15% of participants were women, which is “more than twice that were currently represented professionally in the workforce” (Bashir et al., 2015, p. 75). In terms of racial diversity, the competitions “included more racially diverse participants than were currently represented professionally in the cybersecurity workforce” (Bashir et al., 2015, p. 75).

The Bashir et al. (2015) results indicate that students attend the competition because the events are fun, enjoyable, and students wanted to learn new skills. These reasons were consistent across genders and racial groups. Most students did not attend the competition because they wanted to win. Bashir’s study measured whether the competitions met participants’ expectations by determining if students attended more than one competition per year. A significant percentage of high school, undergraduate, and graduate students attended more than one competition a year with the number per year increasing per student as the students progress from high school to undergraduate to graduate programs. The study also represented that a significant number of students indicated that they learned new skills and would recommend competition participation to others. This further supports that competitions met participant expectations.

Bashir et al. (2015) found that the progression from high school to graduate school was aligned with the progression at which participants indicated they were more likely to pursue cybersecurity as a career, with high school students the least confident in their decision. Regardless of educational level, the study showed that cybersecurity competitions can positively influence a participant’s decision to pursue a career in cybersecurity, even though some demographic groups were more influenced than others. A limitation of the study is that the surveys were conducted, in many cases, years after the competition experience as opposed to a timely pre and post-survey data collection design.

In a subsequent study of Cybersecurity Awareness Week (CAW), Bashir et al. (2017) analyzed the psychological profile of participants that attended CAW and the effectiveness of the events over a ten-year period. The study cites unique job characteristics for cybersecurity professionals that emphasize a need for a separate personality profile, although the author did hypothesize there would be similarities to other STEM disciplines. These personality characteristics included “investigating failures, enacting contingencies, and defending against intrusion” (Bashir et al., 2017, p. 155). The researchers focused on identifying specific personality traits, determining if participation in competitions affected cybersecurity career decisions, and comparing personality traits amongst self-reporting and non-self reporting participants that identified as computer hackers. There were 588 survey participants in the study from a sample size of 8000. Approximately 50% of the participants were undergraduate students, 29% were high school students, and the remaining had completed graduate or other professional degrees. The study resulted in a profile of cybersecurity participants that can be utilized to inform cybersecurity competition design to attract participants. The profile determined by this study indicates that participants showed that “they tend to be high in openness, investigative interests, and rational decision-making styles” (Bashir et al., 2017, p. 162). Competition designers are urged to “include more logic-based tasks that require research, investigation, and deduction” (Bashir et al., 2017, p. 162). The researchers also recommended more reinforcement and rewards during competitions not just for the winners of the competition to increase participants’ sense of competency. They believed incorporating these suggestions into future events may attract more participants to cybersecurity competitions and thus result in more participants pursuing cybersecurity as a career. Limitations of the study that were highlighted included the retrospective nature of the study, which can result in years between the survey and when the subject participated in the competition. This significant amount of time could lead to changes in participant characteristics and profiles.

Dunn and Merkle (2018) also assessed the impact of CyberPatriot competitions on participants' interest in cybersecurity careers. The results indicate that participant interests increase as a result of the competition with a greater increase in females than males, which is a unique aspect of this study. Dunn conducted a quantitative statistical analysis of post-survey data from participants in the CyberPatriot program. The surveys evaluated students' interest and perceptions in cybersecurity before and after the competition, even though the survey was only conducted post-competition. The survey questions also inquired about perceived gender biases in terms of how accessible and welcoming the competition was to women. The survey was sent to all participants in 2016 and 2017. Dunn presented that students reported that they had greater knowledge of cybersecurity careers and improved perception of their abilities as a result of the competition. The study followed through with CyberPatriot alumni and found that over 59% of those in higher education were majoring in cybersecurity or a computer science related field and 82.4% of graduates were employed or seeking work in a cybersecurity or computer science related field. These percentages were very similar for males and females.

In terms of female participants, the Dunn and Merkle (2018) study data showed that 23% of participants were female in 2016 while 11% of the current workforce was female. The survey data indicated a lower female self-perception of ability than male participants. However, the positive change in response was higher on every question for females than males, indicating that the cybersecurity competition had even more of a positive influence on female participants.

Within a university setting, across upper and lower level computing courses, Jeneja et al. (2016) conducted a study to determine if peer interactions across lower-level information technology and upper-level cybersecurity courses in higher education may encourage students to explore cybersecurity careers. One of the interesting aspects of this study is that the participants were much further along in their educational careers than most other studies' participants, which have been most often in high-school within literature located to date. In Jeneja's study, students were placed in mentor groups across the upper and lower courses. Groups met once a month in classroom settings where upper course mentors led discussions and gave presentations. The findings suggest that peer mentoring of students in lower-level information technology (IT) courses by students in upper-level cybersecurity courses may encourage more students to pursue careers in cybersecurity. The results indicate a 68% increased interest in cybersecurity, and 82% of participants found the peer interactions to be positive. In addition, over 54% of participants indicated that the interactions with peers improved confidence when discussing cybersecurity.

From these studies, it appears as if the majority of outreach programs and events can increase overall student interest and awareness in cybersecurity and that there can be some differences in results based on the design of the study, participants, student demographics, and gender. There are a number of factors of influence cited by the participants in these studies that range from personal interest, more information about the actual job responsibilities, whether the program was informative and fun, family and friend influences, and participant personality traits.

Cybersecurity Education Standards and Trends

Compared to more traditional educational topics such as math, science, language, and arts, computer science and cybersecurity are relatively new subject areas. Educational standards and qualified teachers to both structure and deliver computing and cybersecurity curriculum are still emerging. Recognized accreditation standards as well as national and state initiatives to increase certified teachers, provide standards, accreditations, and designations influence what topics educational institutions teach to K-12, cybersecurity college students, and adult learners studying cybersecurity. These initiatives and standards can greatly influence, inspire, and increase interest among future cybersecurity college majors and professionals as they make their way into the educational systems at all levels.

As an example of how these relatively new disciplines of computer science and cybersecurity are still emerging, according to a report by Shein (2019), only 36 computer science teachers graduated from universities in the United States in 2017 compared to 11,157 math teachers. However, Shein did report a positive trend towards improving the number of teachers in computing disciplines. In 2018, 27 states offered teacher certification in computer science, with an increase to 33 states in 2019. Shein attributed a recent increase in computer science majors at universities in the United States to the improvement at the middle and high school levels in terms of the number of teachers and states now offering computer science courses. In addition, Shein also stated that only 19 states currently have policies that require K-12 to provide all students access to computer science courses. According to Shein and code.org, an organization with over 42 million registered students and 1 million registered teachers, 90% of parents desired that their children have an opportunity to study computer science, yet only 45% of high schools currently teach the subject. Organizations such as the Computer Science Teachers Association (K-12 Computer Science Standards, Revised 2017, 2017) and the Association for Computer Machinery have also authored frameworks and standards for K-12 computer science curriculum and teaching practices (K12 Computer Science Framework, 2016). There are two advanced placement computer science courses and exam standards that afford students the ability to complete a standard exam for college credit. Both of these advanced placement computer science courses emphasize computing concepts and computer programming. There are no advanced placement exams for cybersecurity at this time (AP Central, 2020).

Cybersecurity shares several characteristics and educational curricula with computer science. Still, it is very unique, as evidenced by the Accrediting Board of Engineering and Technology (ABET) Computer Science-Cybersecurity Accreditation (ABET-CAC), that began accrediting programs in cybersecurity in 2019 (Criteria for Accrediting Computing Programs, 2019 – 2020). The ABET-CAC accreditation standard includes five of six criteria from the ABET Computer Science program accreditation plus an additional 45 credit hours of specific cybersecurity coursework. This supports the uniqueness of cybersecurity education curriculum and requirements. The additional 45 credit hours in cybersecurity include topics such as risk, adversarial thinking, systems thinking, data security (at rest and in transit), human security, and organization security. Some of the areas that ABET Computer Science and ABET Cybersecurity have in common include algorithms, programming, computer architecture, and computer networking (Criteria for Accrediting Computing Programs, 2019 – 2020).

In addition to ABET-CAC, there are other influential cybersecurity-focused education initiatives, such as the National Initiative for Cybersecurity Careers and Studies (Cybersecurity in the Classroom, 2020), that is focused on K-12 cybersecurity education; the National Security Agency Academic Center of Excellence designations (National Centers of Academic Excellence); and the National Initiative for Cybersecurity Education framework (NICE Cybersecurity Workforce Framework, 2019, May 18). The Cybersecurity Careers and Studies (2018) program supported by the United States Department of Homeland Security provides a program for K-12 teachers to provide cybersecurity curricula and education tools. This is accomplished through a federal Cybersecurity Education Training Assistance Program (CETAP) grant supporting the National Integrated Cyber Education Research Center (NICERC) in Louisiana. The curriculum includes a library of materials to build awareness of cybersecurity issues, cybersecurity education, and cybersecurity careers. The materials include posters, brochures, lesson plans, workbooks, instructor support materials, and assessments. NICERC provides workshops for K-12 teachers to assist with integrating cybersecurity, computer science, and STEM into their classrooms. Post-secondary education opportunities and scholarships are also part of the awareness program. The Cybersecurity Careers and Studies program also defines eight cybersecurity job profiles that outline education requirements, median salary, job growth, soft skills, and common job duties. The job profiles are titled "Encryption Expert, Incident Responder, Cyber Forensics Expert, Legal Advisor, Security Engineer, Multi-Disciplined Language Analyst, Software Developer, and Vulnerability Assessment Analyst" (Cybersecurity Careers and Studies, 2018).

The National Security Agency supports and promotes two types of academic guidelines and accreditations that can guide cybersecurity higher education: Cyber Defense and Cyber Operations. The Cyber Defense (CAE-CD) program goals are to promote higher education and research in cybersecurity while increasing the number of cybersecurity professionals. The program provides opportunities for Center of Academic Excellence designations to accredited higher education programs that offer associate, bachelor's, master's, or doctoral programs that meet the program criteria. The Cyber Operations (CAE-CO) program supports the National Initiative for Cybersecurity Education (NICE) with a goal of increasing the number of educated cybersecurity professionals. Universities and colleges can apply for designations in both CAE-CO or CAE-CD. These designations are influential in that they can influence curriculum standards, which may influence factors that attract students to cybersecurity educational programs and professions (National Centers of Academic Excellence). The National Security Agency has designated over 300 college and university programs as achieving and maintaining one or more levels of cybersecurity academic center of excellence (NSA/DHS National CAE in Cyber Defense Designated Institutions).

The National Initiative for Cybersecurity Education (NICE) Framework defines an educational framework that can be used to structure the knowledge, skills, and abilities (KSA) for the cybersecurity profession. The framework includes seven categories of cybersecurity, 33 specialties grouped under the categories, and over 100 professional work titles grouped in 53 work roles. The NICE framework is intended for employers, professionals, technology providers, and educators. Educators can design and develop curriculum based on the KSA structure and definitions, while employers can use the KSA to structure, assess, and train their cybersecurity workforce. This framework provides insight into the types of jobs and skills that exist within the discipline of cybersecurity. The KSAs are organized under seven categories: "operate and maintain, protected and defend, investigate, collect and operate, analyze, securely provision, and oversee and govern" (NICE Cybersecurity Workforce Framework, 2019).

As an example of a more local initiative, the Michigan Initiative for Cybersecurity Education (MICE) was founded in 2017 with a mission is to expand cybersecurity and computer science education throughout the United States. MICE provides an online and face-to-face curriculum that was designed through a collaboration of K-12 and post-secondary information technology educators. Their goals include addressing the lack of training available to both students and teachers. The curriculum is aligned with professional information technology certifications and includes numerous forms of curriculum that teachers can utilize. The group also advocates for cybersecurity and computer science education standards adoption in Michigan (Michigan Initiative for Cybersecurity Education, 2019).

Dawson and Thomson (2018) sought to better understand the knowledge, skills, and abilities that are needed within the cybersecurity discipline to be successful. More specifically, Dawson and Thompson examined to what extent people that work within cybersecurity need a combination of technical skills, domain-specific knowledge, and social intelligence to be successful. Their results suggested that people who are drawn to cybersecurity require "systemic thinking, team orientation, passion for continued learning, strong communication skills, a sense of civic duty, and blend of social and technical skills" and that those who are drawn to the field may have social and psychological traits that are somewhat uniquely compatible with a career in cybersecurity (Dawson & Thomson, 2018, p. 1). Dawson and Thompson's study is critical of both the National Security Agency Centers for Academic Excellence criteria and the Cybersecurity Workforce framework for lacking proper emphasis in social and communication skills. Lingelbach (2019) also conducted a study that examined the skills necessary to succeed in cybersecurity, emphasizing soft skills categorized as a "cybersecurity mindset" that consists of personal characteristics such as self-efficacy, analytical-mindedness, assertiveness, and technological saviness.

Gaps and Limitations

The literature identified and reviewed is focused on more traditional STEM careers in engineering, mathematics, and science, with few studies in more specific degree programs such as cybersecurity or information systems. Some literature, such as Mau et al. (2019), suggested a need to conduct studies that focus on specific occupations or programs. Lent et al. (2008) also recommended further research and interventions in more specific fields, such as particular computing majors, in addition to more aggregate studies of STEM. This may be important due to the unique aspects of specific STEM programs. For example, some STEM programs, such as cybersecurity, do not necessarily require advanced mathematics or science (Criteria for Accrediting Computing Programs, 2019 – 2020). Therefore, studies focused on these traditional STEM aspects may be missing some or all of the key influencing factors for specific career and education choices, which may have significant implications for intervention programs that attempt to increase STEM career choice in these more focused occupations. Lent et al. (2008) also suggested that future studies may benefit from looking at choice actions as opposed to choice intentions. My study includes participants who have made the choice of a cybersecurity career, not just expressed an intention to pursue a computing-related career.

There appears to be a lack of studies on cybersecurity that integrate the unique, more detailed aspects of the cybersecurity discipline as opposed to only looking at cybersecurity as a whole or cybersecurity as part of more traditional computer science or information systems program. Future studies could be designed around standard job descriptions and characteristics as well as emerging standard curriculum for specific programs and occupations. The NIST NICE Cybersecurity Framework and the ABET Computer Science-Cybersecurity accreditation course requirements could be examined with key aspects and skills found in these standards influencing survey or interview questions that may identify specific occupation characteristics and influencing factors. In addition to these standards and frameworks, personality, values, and social and communication skill aspects should also be considered for future studies, as suggested by Dawson (2018) and Lingelbach (2019).

There was not a single study located in the literature that included student participants from a program accredited in ABET-CAC or any other program that was specifically focused on cybersecurity as opposed to a program with a concentration or a few courses in cybersecurity. Furthermore, there were no studies located that stated the participants were from an NSA-CAE designated program. This leads us to believe that the programs in the study were traditional computer science or information systems programs that may have a limited aspect of cybersecurity in the curriculum.

There has been limited research identified that utilized qualitative methods that explore influencing factors in STEM career choice or more specifically cybersecurity major or career choice. Most of the literature attempted to correlate personality traits, academic performance in traditional STEM subjects such as math and science, and environmental factors such as parents, teachers, counselors, and socio-economic influences. While this literature is insightful, it may be incomplete. There may be other factors that researchers do not represent in their quantitative surveys that could be discovered through open-ended, exploratory surveys or interviews with student participants. Instead of quantitatively surveying large groups of students, studies could be more focused on smaller groups of students in accredited cybersecurity programs. This may allow for deeper discovery of identification and ranking of influencing factors that are associated with specific programs and occupations such as cybersecurity.

Conclusion

The literature identified and reviewed in this work demonstrates that the demand for workers and pipeline problems in STEM persist and are projected to persist into the future, creating a need for more research into factors that influence students to choose STEM occupations. The literature cited many factors that influence students to study STEM with some common themes emerging. There are also some studies that highlighted somewhat unique factors or a significant difference in factor ranking by participants, resulting in a lack of consensus. An inclusive and more focused approach to the STEM problem will be needed to effectively close the worker shortage gap in STEM. Gender and race factors should not be overlooked, as the literature highlights some key differences within these demographics.

Simply identifying an interest in math and science or personality factors as predictors of STEM career choice may oversimplify the problem. This is worthy of highlighting, as many of the STEM studies that are included in this review seem to have focused on aspects of mathematics more than any other aspect of STEM as a potential predictor of a student's choice to pursue a STEM educational program or career. The implications start to come in to focus if one imagines a high school counselor encouraging or discouraging students to pursue a STEM career based on their experience and skills in mathematics, which may or may not be very relevant depending on the specific STEM choice. This is not to say that traditional STEM subjects such as science and math cannot be predictors of a student's interest in STEM fields, but they could be too narrow of a focus.

As Mau et al. (2019) suggested, more focused research on specific occupations is needed. One such field appears to be the cybersecurity occupation, as there may be significant differences between specific STEM occupation characteristics and perceptions. More research is needed into what can be done to improve the pipeline issues as relates specifically to cybersecurity. I have a very strong hunch through my own experiences that most cybersecurity students do not choose the cybersecurity program where I teach because of their interest in mathematics or science, which seem to be the two main subject areas that much of the current literature is focused on. Why do these students choose cybersecurity? What factors influenced them?

Chapter 3

Theory and Methodology

Theory

Career choice decisions and influences will vary based on many factors. Career choice theories can provide a lens and framework for examining what influences career choice. However, generalizations about influencing factors can lack meaning and be overly simplistic to the point that the results may not be actionable. For example, some studies cited in chapter 2, such as Hall et al. (2011) and Masnick et al. (2010), partially conclude that students who like math or science may be more likely to choose STEM careers. STEM is incredibly broad. Math and science are not necessarily an emphasized aspect of many careers classified as STEM. My dissertation research focuses on identifying the factors that influence students to choose a specific career, cybersecurity, which while categorized as STEM, has many unique characteristics (beyond math and science) that are worthy of investigation.

The Social Cognitive Theory and Social Cognitive Career Theory (SCCT) are prominent in the literature as theoretical frameworks that are utilized to evaluate career choice, academic program choice, and general factors of influence on these choices. The SCCT has been used in similar studies to evaluate student career choice and interest, such as Kier et al. (2014). The theory aligns well with this study's research question and provides a theoretical structure for evaluating the research question. Per Lent et al. (1994), the SCCT theory can be used to examine career choice influencing factors using five primary components: self-efficacy, outcome expectations, background/context, social supports and barriers, and personal inputs such as gender, race, ethnicity, and predispositions. These five components may interact to influence interests, goals, learning experiences, and actions. According to Lent et al. (1994), goals and actions are heavily influenced by self-efficacy. Lent’s theory also suggests that self-efficacy interactions with outcome expectations may influence interests. As a potential example of these components’ interaction, if a student believes their success in cybersecurity courses will make their parents happy (outcome expectation), they may work harder (self-efficacy) to achieve a good grade. This successful good grade may then influence future interest in cybersecurity-related subjects. Kier et al. (2014) used the SCCT to develop survey questions categorized by key aspects of the SCCT to examine general STEM career interest of high school students who had not yet entered college with a chosen major. This study utilizes the SCCT, similar to Kier et al. (2014), to design mixed-methods survey and qualitative interview instruments to evaluate the more specific STEM discipline of cybersecurity. Lent et al. (2008) used the SCCT theory to examine interest and career choice in more general computing disciplines. In further alignment with this study, Lent found that the SCCT model fits well with “both relatively new as well as advanced students” (Lent et al., 2008, p. 59). Figure 1 illustrates the components of the SCCT and their potential interaction.

Researcher Role and Ethical Considerations

My interest in career influencing factors dates back to my own struggle as a recent high school graduate with deciding which career I would like to pursue and what major in college to declare. Creswell (2018) and Scheurich (n.d.) stated the importance of the researcher being transparent with their past experiences and how these past experiences may shape the researcher’s interpretation. Patton (2002) also emphasized the importance of recognizing bias and taking measures to make any predisposition clear by acknowledging the researcher’s experiences and orientation. Liu (2106) emphasized that quality is established by the researcher clearly stating: “researcher motivation, sufficient description of research methods, clear strategies to establish rigor, and the researcher's role in data analysis" (p. 129). I was an undecided major my freshman and sophomore years of college even though I did have two primary interests in STEM fields: Computer Science and Biology/Chemistry. I found choosing a career and major to be a difficult and somewhat stressful task given my limited experience with and exposure to the many choices a student entering university studies typically has and the long-term implications of career choice including financial and job security aspects. Growing up in a rural, blue-collar, lower middle-class setting, I felt disadvantaged compared to what I perceived to be broader and richer experiences of those surrounded by family and friends that were more connected to the professional world in more populated geographical areas. I also often wondered how some high school and college freshman peers could be so confident of their career and college major choice given everyone's limited exposure to influencing factors at that point in their lives.

My role as a researcher will be as an insider as I am currently an associate professor within the cybersecurity program at a midwestern university. Within this role, I teach and provide academic advising to the students enrolled in the cybersecurity program. I have been employed as full-time, tenure track faculty at the midwestern university since 2011. During this time, I have taught and designed many of the courses within the cybersecurity program that partially defines this case study. The program is currently one of eight Accreditation Board of Engineering and Technology – Computing and Cybersecurity programs in the United States (Criteria for Accrediting Computing Programs, 2019 – 2020). I often ask my advisees or prospective students why they are interested in studying cybersecurity. I also see this topic expressed within student admission application essays to our program. While there are some themes and insights from these brief student conversations or statements within student application essays, there is much room for exploration and further understanding of what has influenced students' career choice of cybersecurity. These past experiences with students may inform the research design to some extent, but the researcher is also aware that remaining unbiased is critically important. My past experiences cannot influence the outcomes of the study but rather let the data lead to the proper conclusions and discussions.

I will not be the instructor for any of the student participants in this study; therefore, there will be no direct power influence present. It is possible that I will be the assigned advisor for one or more of the participants. As an insider, as their future professor, and potential academic advisor, I hold a position of some power in relation to the student participants in this study. Perceived power issues will be mitigated by clearly communicating to participants that participating in the research is voluntary and that lack of participation will in no way impact their status or treatment within the university or its programs. To put a finer point on the responsibility of the researcher, Morse et al. (2002) argued that qualitative validity and reliability should remain the primary responsibility of the researcher utilizing verification strategies throughout the research and not shift responsibility or rely on the reviewers of the research.

Merriam and Tisdell (2016) advised that researchers must take an approach that is sensitive, respectful, and non-judgmental towards participants. The nature of the questions in this study should not lead to sensitive information being disclosed but rather a safe reflection that will not jeopardize the participant's future relationship with me or anyone else at the university. In addition, the Institutional Review Board will review the research design, and the research will strive to not place any participant at risk. IRB approval and all IRB processes are critical since the research will involve human subjects. According to Butin (2010), IRB approval reduces the risk to participants and helps to ensure that a study is conducted in an ethical manner. Other ethical considerations include the confidentiality and privacy of sensitive information obtained through the survey or interviews. It is possible that responses to survey or interview questions are sensitive, as the researcher cannot control a participant's sharing of personal or private information in response to open-ended questions. Participants need to know that they are part of a study and that their responses, while anonymous, may be included in the results. Anonymity and privacy are further described in the Data Collection section. If interview audio and video are recorded, IRB and participant permission is required, and guidelines should be followed to make the interviewee comfortable with the recording process.

Another ethical aspect is that the researcher could benefit from the study's results as they could be used to design interventions that increase enrollment within the program that the researcher teaches within. However, the project's larger purpose is to protect our nation and citizen's privacy and data by helping to solve the problem of a growing shortage of cybersecurity workers. In addition, the results will be published and freely available to any institution or organization that wishes to utilize the results to recruit and grow enrollment in cybersecurity studies and programs, which is the overarching goal of the research.

Study Overview

The study aims to provide insight into what factors influence cybersecurity career choice. The central and subquestions of this study are:

Research Questions

Central Research Question

- What are the factors that have influenced current cybersecurity students to choose cybersecurity as a college major and career?

Sub-questions

- What technical and non-technical characteristics of cybersecurity, as defined by the leading curriculum standards, are student participants most and least interested in?
- How does background and context influence cybersecurity career choice, such as gender?

Factors that influenced cybersecurity career choice will be examined through the lens of the Social Cognitive Career Theory and current cybersecurity curriculum standards. Participants will include current students enrolled in an introductory cybersecurity course as well as new information systems/technology students at a public, midwestern university. Faculty within this program will also be included in the study to provide additional perspective and contrast to the student data. A mixed-methods survey instrument will be designed for the student participants. Faculty participants will be interviewed. Follow-up interviews with selected student participants based on the need to clarify or elaborate their survey data may also occur. The student survey will be designed primarily for qualitative analysis and descriptive statistical analysis.

Mixed-methods, Exploratory Case Study Design

The research questions in this study aligned well with exploratory methods, given the limited research that currently exists in cybersecurity career choice and the immaturity of the field of cybersecurity relative to other STEM fields. This study implemented a methodology that utilized a mixed-methods, exploratory case study approach. Merriam and Tisdell (2016) recommended a qualitative method when the researcher seeks to understand how people interpret their experiences, how people construct their worlds, and what meaning people attribute to their experiences. One of the overarching goals of the research in this study was to uncover and interpret the meanings, patterns, and themes related to factors that influence career choice and to do so in an exploratory and inductive manner. Creswell (2018) also suggested that a qualitative method be used when the research question is exploratory in nature. Qualitative research allows for open-ended questions that can be presented to participants in the form of interview or survey questions (Kelley et al., 2003). A survey instrument with both quantitative and qualitative questions was utilized to effectively and efficiently include the entire population of students within the case. The survey questions were categorized by alignment with the components of the SCCT. Creswell (2018) recommended a quantitative or mixed methods approach when there are a larger number of participants and when the study seeks to analyze data using descriptive statistics. This study preferred to include all student participants within the case. Given the number of student participants, a mixed-methods survey instrument was more practical than individual interviews for all student participants. Including all students within the case also allowed the researcher to capture demographic information, influential factors, and interest information more efficiently.

Within this case study research setting, most cybersecurity freshman majors were enrolled in a 100 level, introductory cybersecurity course that served as the main boundary of this case. The position of the researcher, as well as the timing of the research, afforded the researcher the opportunity to select qualified participants from an intrinsically bounded system or case: an introductory cybersecurity course section, within an accredited cybersecurity program at a midwestern university in which all incoming freshman to the cybersecurity program enroll. Merriam and Tisdell (2016) described a case study as a bounded system, unit of analysis, and with a finite number of participants. A course section of an introductory cybersecurity course with students that have made their career choice recently met these characteristics. The bounded system was the course section itself, with the finite number of participants in the course set at a maximum of 25 student participants, assuming all students in the course met the participant requirements. To further bound the case study, there were five full-time faculty in the cybersecurity program, excluding the researcher, that might also have served as key informant and subject matter expert participants, offering an alternative perspective to influencing career choice factors through their experience engaging with cybersecurity students in both a teaching and advising capacity. A second student group, the information systems/technology students, were also part of this case. This second student group was included to offer a perspective from students that chose a computing major but did not choose cybersecurity. Yin (2014) suggested that a case study has qualities of a contemporary phenomenon within a natural context. This study fit both of those criteria, as cybersecurity is a relatively new occupation and field of study. In addition, this research was conducted within the context of academia, where students and faculty naturally engage and participate.

Strengths

A mixed-methods approach was chosen to maximize the discovery of the factors that influence students to choose cybersecurity and to maximize participation. According to Creswell (2018) and Kelley et al. (2003), a qualitative approach that utilizes inductive, open-ended survey and interviewing techniques allows for rich, thick descriptions of participant responses. This approach also allowed the researcher the flexibility to alter their questions and techniques during the study to maximize the data collected. Instead of being limited by numerical analysis of the data with a quantitative approach, the researcher could instead build insightful, rich narratives while parsing the data and discovering themes and patterns. The qualitative approach could also yield rich data primarily from the participant's perspective, not the researcher's perspective.

Access to qualified participants within a qualified case is also a strength of this study. There were only eight fully accredited cybersecurity programs per the Accrediting Board of Engineering Technology – Computer Science and Cybersecurity at the time of this writing (Criteria for Accrediting Computing Programs, 2019 – 2020). The researcher was positioned within one of these programs with access to student and faculty participants. The student participants were selected such that their graduation from high school and entry to a university major occurred within a relatively short period of time, which may have increased the accuracy of their data due to limiting the time to "forget" the factors that led to their career choice. This student participant profile, faculty profile as key informants, and the accredited academic program status should have improved the credibility and validity of the participants and the case.

Limitations

Time, thoroughness, and voluntary participation of participants that ensured validity and reliability were constraints of the study. The study was conducted in the context of an academic dissertation, whose time and budget constraints did not allow for a large number of participants over a long period of time. Participant sample selection was limited to a single university, primarily due to logistical and budgetary reasons. The recent COVID-19 pandemic was also a limiting factor in terms of broadening the study to other universities. The number of participants selected for follow-up interviews needed to be within reason, as each qualitative interview requires significant time and data analysis. This could have lead to concerns regarding validity and reliability if the number of and mix of participants was not considered sufficient saturation by the researcher or dissertation committee.

The study included student participants that chose to pursue a career in cybersecurity. What about those students who considered cybersecurity and then chose a different, related major such as information systems? There are many majors that include aspects of computing and therefore it was difficult or perhaps impossible to include all computing related majors in this study. To mitigate this limitation, a second of group students that chose information systems as a major was invited to participate in the study. A group of students that was not represented in the study were non-traditional students that chose to pursue cybersecurity careers through self-study or alternative education to a traditional four-year higher education program.

Setting

The setting was a midwestern state university. According to the university's fall enrollment summary, the university had enrollment of over 12,000 students with enrollment in the undergraduate cybersecurity program of approximately 150 students. Forty-six percent of students at the university were male, 54% female, and 76% of students identify as White. The university was a career-oriented university offering degrees at the associate, bachelor's, master's, and doctorate levels. There were six tenure track faculty and one full-time adjunct teaching and advising within the cybersecurity program. The cybersecurity program was designated as a center of excellence through the National Security Agency and was accredited by the Accrediting Board of Engineering Technology – Computer Science and Cybersecurity. Participant surveys and interviews were originally planned to be conducted at a midwestern university. However, due to the COVID-19 pandemic, virtual interviews using technologies such as Zoom were utilized to adhere to university policies or social distancing guidelines.

Participants

Patton (2002) suggested that the researcher must define the essential attributes for the participants and the site(s) and then find those people and sites to conduct their research. Participants included student participants and faculty participants. Faculty participants were selected from the faculty that were within the cybersecurity program faculty group. Student participants were selected as a case defined by enrollment in the 100 level, introductory cybersecurity course or new information systems/technology students. Freshman or sophomore status was important to ensure that a minimal amount of time had passed since the student was a high school student working through decisions related to a university, major of study, and career choice. This may have eliminated influencing factors that might have been considered non-traditional, such as full-time work experience, other university experiences, or coursework outside of the cybersecurity major.

Participant Sampling and Recruitment

Patton (2002) described purposeful sampling as a method based on maximizing what can be learned, discovered, and understood in depth. Patton also stated that qualitative research seeks rich information from a small, qualified group of participants. Creswell (2018) suggested convenience sampling when there are constraints of time, money, location, and availability. This study utilized a convenience, two-tier sampling method for the student participants. According to Merriam and Tisdell (2016), when conducting a two-tier sampling case, the researcher first selects the case and then a sample within the case. A convenience sample is one in which participants are chosen based on their availability and convenience. Therefore, a sample of student participants were selected from within the university, which was the outer boundary of the case

The researcher evaluated, with feedback from the dissertation committee, options that involved interviewing a sampling of students in the case versus providing a mixed-methods survey to all student participants in the case with optional follow-up interviews as necessary. The student participant sample included all freshman and sophomore transfers in the cybersecurity and information systems/technology majors. Kelley et al. (2003) suggested that larger samples give a better estimate of the population and that the sample size needed for qualitative surveys is smaller than quantitative surveys. Faculty participants included all faculty that teach and advise in the cybersecurity program. These sample sizes were likely to far exceed dissertations with similar research designs such as those from Leonard (2016) and Lingelbach (2018) as well as recommendations from Creswell (2018) for qualitative studies that utilize qualitative data collection and have time and budget constraints.

A solicitation for participation email was sent to the qualified students with a link to the student survey that included a confirmation of consent. Faculty participant sampling was based on years of experience teaching and advising in cybersecurity as well as availability. Faculty with more years of teaching and advising experience were sought to participate first. As seen in Appendix D, an email was sent to qualified student and faculty participants who met the criteria. The email described the study and participation requirements.

Consent Procedures

Recruitment and consent followed the procedures and guidelines of the Intuitional Review Board at both a midwestern university and the University of Illinois. The midwestern university determined that the study would not require additional IRB oversight since the IRB from the University of Illinois was overseeing the project as part of doctoral course requirements. The letter from the midwestern university IRB is found in Appendix F. Each participant was presented with a voluntary consent form before the survey or interview, as seen in Appendix E.

Data Sources and Collection

Data was collected utilizing a survey instrument that included mixed-methods questions, followed by purposefully selective qualitative interviews. All selected student participants within the case were sent the survey. Selected faculty participants were interviewed in the role of subject matter experts and key informants. According to Merriam and Tisdell (2016), when we cannot observe a behavior or feelings such as past events or experiences, it may be necessary to conduct interviews.

Mixed-methods surveys were chosen as the primary instrument over interviews due to time and budget constraints, as there were 25 or more student participants. Creswell (2018) generally described this approach as a mixed-methods, explanatory sequential approach. With this approach, data was collected in the first phase (surveys) and then survey results were utilized to plan a potential second phase (interviews) with the intent being additional qualitative data in the second phase, further explaining the data obtained in the first phase. Kelley et al. (2003) suggested that qualitative surveys are “well-suited for descriptive studies” and can be used to “explore aspects of a situation” (Kelley et al., 2003, p. 261). Kelley et al. (2003) described this type of descriptive research as research involving important factors, behaviors, experiences, knowledge and associations as opposed to analytical studies which “tend to examine the effect of one set of variables on another set of variables” (Kelley et al. 2003, p. 261-262).

Survey questions (Appendix A) were designed primarily as neutral, open-ended questions and were influenced by studies from Kier et al. (2014) and Lent et al. (2008), who both used the SCCT theoretical framework in their studies related to career choice. Kier et al. (2014) used the SCCT to develop survey questions categorized by key aspects of the SCCT to examine general STEM career interest and intent of high school students who had not yet entered college with a chosen major. In addition to open-ended questions, the survey collected contact information and demographic data for each participant, including age, gender, high school GPA, and SAT scores. A ranking of favorable to least favorable cybersecurity knowledge, abilities, and skills (KSA) per the ABET-CAC and the NICE Framework was also included. Examples of these KSAs include verbs such as protect, defend, govern, investigate, automate, and administer (technology). The KSA ranking added some quantitative data to the results that provided further insights into student interests and opportunities to analyze the data using descriptive statistics methods. The SCCT aspects that were examined are:

- interests
- self-efficacy
- outcome expectations
- learning experiences
- contextual supports and barriers
- personal inputs
- background

Interests have been shown in a number of studies that evaluate career choice to be one of the top influencing factors, including the studies from Hall et al. (2011) and Malgwi et al. (2005). The literature reviewed in this dissertation also presented a strong theme of focusing on understanding or increasing student interest in order to increase student enrollment in STEM fields. Therefore, interests, in the context of cybersecurity curriculum standards such as ABET-CAC and the NSA NICE Framework, were further represented in the survey. These interests were ranked or scored by the student participants. The students also ranked interests in KSA topics such as:

- Software Security (ABET)
- Data Security – at rest and in transit (ABET)
- Human Behavior and Organizational Security (ABET)
- Computer Programming (ABET)
- Computer Networking and Architecture (ABET)
- Mathematics (ABET)
- Digital Forensics and Cyber Investigations (NICE)
- Cyber Operations (NICE)
- Vulnerability Analysis and Threat Assessment (NICE)
- Systems Administration and Defense (NICE)
- Governance, Leadership, and Management (NICE)

Selected student participants were potentially scheduled for a follow-up interview with the researcher. Creswell (2018) suggested follow-up interviews when clarification or elaboration is needed from survey data. Participant interviews were recorded for subsequent analysis with participant approval and anonymity provisions. The interview questions followed a semi-structured format. The semi-structured interview format was selected to allow the interviewer to have a guide during the interview process while also allowing the flexibility to have follow-up questions or ask questions that aren't in the guide or script. According to Alsaawi (2014), this approach gives the interviewer the opportunity to elaborate while not hindering the depth and richness of the discussion. The researcher was careful to ask only one question at time and avoid compound questions in both the survey and interviews as suggested by Turner (2010). Turner also suggested avoiding showing emotion when listening to participant responses. Turner cautioned that notetaking should be conducted in a calm manner so as not to distract or cause participant concerns regarding why notes are being taken. The interviewer should free themselves of distractions, such as mobile phones, and give the interviewee their full attention. Questions should be asked in a calm manner and the interviewee should not feel rushed or stressed (Turner, 2010).

Privacy

Participants were assigned a pseudonym to maintain anonymity after the survey or interview. The pseudonym key was kept in a safe place during the research and then destroyed afterward (Saldana, 2016). Recordings were encrypted. Survey data and interview notes were kept in a secure environment.

Data Analysis

Survey and interview data were coded and analyzed to identify prominent themes and factors that influence students to choose a cybersecurity career. The survey questions were categorized by alignment with the components of the SCCT. Saldana (2016) recommended multiple rounds of coding of the survey and interview data in addition to the initial set of codes such that themes that can be refined in subsequent rounds of coding. Saldana (2016) recommended that initial codes and themes be preserved to demonstrate transparency in the process and the researcher's thoughts and findings. Saldana posited that additional rounds of analysis of the data, coding, categorization, and theme identification are effective at identifying the primary themes and categories from the data. Narrative text and summary tables were also utilized to describe the codes, themes, data, and findings.

Descriptive statistics were used to present qualitative and quantitative findings such as rankings, averages of student interests, and occurrence of factors based on codes or themes that emerged. Data was segmented using demographic data provided by the student participants. Data was further segmented based on student and faculty responses to identify common themes and potential gaps in perceptions and understanding between these two participant groups.

Reliability and Validity

The thoroughness of coding and analysis of the data was critical. The researcher utilized structured coding methods and analytic memos to document their methods and thought processes. Researcher memos included date and title. This added validity and reliability to the study by providing evidence of the researcher's detailed methods and thoughts (Saldana, 2016). The researcher also created artifacts that demonstrated the process by which the data was coded and analyzed. For example, the first round of coding artifact with a draft codes and categories was preserved. Additional artifacts and memos illustrated how coding evolved into a final set of themes, categories, codes, and concepts.

All qualified student participants within the case were included in the sample. This increased validity due to a very large sample size in relation to the population within the case. Faculty interviews were considered key informant and subject matter expert interviews, which represented years of experience teaching and advising hundreds of cybersecurity students. Faculty interviews added validity and potential triangulation of data.

Timeline

June-July 2020	Methodology Review and Feedback
July-August 2020	IRB Approval
July-August 2020	Prelim and Study Approval
September 2020	Student Surveys Sent, Faculty Interviews
Sept. - Oct 2020	Data Analysis of Surveys
November 2020	Data Analysis, Results, Discussion
December 2020	Dissertation Defense

Chapter 4

Results

Overview

This mixed-methods research study utilized interview and survey techniques from three different participant groups to address the research questions that were designed to explore factors that influence high school students to choose a major in cybersecurity. This chapter presents a profile of these participant groups, how data was collected, how data was analyzed, and the data analysis results. In addition to the central question, sub-questions were also explored. A journal was utilized during the entire data collection and analysis process. This journal served as a historical record of all activities from the time surveys were sent and interviews were scheduled through the data collection analysis process. This journal assisted the researcher with organization and focus and served as a means to provide transparency to the researcher's thoughts and process. According to Saldana (2016), utilization of a journal adds validity and rigor when conducting qualitative research.

Data collection utilized a mixed-method survey instrument delivered to two groups of student participants and individual interviews with a group of faculty. The faculty served as key informants and subject matter experts. Data analysis and coding commenced as soon as possible after interviews were completed and surveys were returned. Transcripts from interviews were preserved for later analysis. A series of rounds of coding occurred for both the interview transcripts and surveys. What emerged from these rounds of coding were initial codes and themes. More in-depth analysis revealed prominent themes and categories. These themes and categories were then analyzed and compared using demographic data as well as cross-group comparisons.

The central question and sub-questions are restated in this section from Chapter 1 for convenience and to refocus the reader on the questions under investigation.

Central Research Question

- What factors have influenced current cybersecurity students to choose cybersecurity as a college major and career?

Sub-questions

- What technical and non-technical characteristics of cybersecurity, as defined by the leading curriculum standards, are student participants most and least interested in?
- How do background and context, such as gender, influence cybersecurity career choice?
- Why do some students choose to major in a computing related major that is not cybersecurity, such as information systems?

Participants

Participants in this study were members of one of three groups:

1. New cybersecurity students within a 100-level cybersecurity course with a chosen major of cybersecurity
2. Cybersecurity faculty: professors/advisors
3. Freshman or Sophomore transfer students from the information systems major (not cybersecurity)

Participant Group 1 - New Cybersecurity Students

These students were recruited from the 100-level cybersecurity course to participate in the study. The students were either new freshman admits or sophomore transfers that recently graduated from high school. The criteria were selected such that participants that had recently made their college major choice as traditional college students were included. These criteria align with the central research question focused on high school student career choice. The survey was sent via email to 27 students in this participant group. The survey was also announced in class. Nineteen students responded with complete surveys, which represented a 70% response rate from this group. The participants completed the survey outside of class and were incentivized with a gift card and a small amount of extra credit in the 100-level cybersecurity course if they completed the survey. E-gift cards were sent to each participant who completed the survey within a few days of completion. Students were recruited to participate in the survey the first week of class, reminded twice via email in subsequent weeks, and the survey was closed after three weeks such that data could be analyzed. Approximately eight students in this group combined with Participant Group 3 started the survey but did not complete it in a meaningful manner. The survey instrument is found in Appendix A.

Participant Group 2 - Cybersecurity Professors and Advisors

The program serving as the case for this study includes five full-time tenure track professors teaching cybersecurity, including the researcher, and one full-time adjunct teaching cybersecurity. Other part-time adjuncts serve the program but were not available during this study's time frame. The faculty were selected as key informants and subject matter experts with responsibilities in teaching, advising, and research within the cybersecurity industry and the cybersecurity academic program. Some faculty members have also served as faculty advisors to cybersecurity student organizations, program directors, and department heads offering many years of experience and multiple perspectives of their work and interactions with students. Interviews were scheduled and conducted with five faculty members the second and third week of the semester.

Each faculty participant was interviewed individually for approximately 30 minutes using structured interview techniques remotely over Zoom with audio and video enabled for the interviewer and interviewee. An interview guide was followed consistently during each interview. This guide is found in Appendix C. Each interview was recorded, reviewed, analyzed, and initially coded within no more than two weeks of the interview.

The faculty participant group collectively represents over 36.5 years of teaching, 32.5 years teaching cybersecurity, and 31 years of advising students. Four years of faculty RSO advising, 13 years of program director experience, and two years of information systems department head experience are also represented in this faculty group. The researcher served as the interviewer and possesses over 10 years of cybersecurity teaching and advising experience in higher education. The entire faculty in this participant group, including the interviewer, has many years of industry experience and multiple top industry certifications in cybersecurity or a computing discipline. All of the tenure track participants have earned their PhD and all faculty participants, including the adjunct faculty, possess one or more degrees in a computing field including cybersecurity, information assurance, computer science, or information systems.

Table 1

Descriptive Statistics for Faculty Participant Profile Data (N=5)

Participant	Level	Highest Degree	Gender	Years Full-Time	Years Part-Time	Years Advising
P1	Associate	PhD	Male	6	1	5
P2	Full	PhD	Male	21	12	20
P3	Assistant	PhD	Male	4	4	4
P4	Adjunct	Masters	Female	3	2	0
P5	Assistant	PhD	Female	2.5	3.5	2

Participant Group 3 - New Information Systems/Technology Students

During the preliminary defense phase of this dissertation it was determined that the researcher should include students who did not choose cybersecurity as a major to address the question of why some students interested in computing do not choose cybersecurity as a major. A list was obtained of freshman admits and sophomore transfers majoring in information systems/technology at the same university as the cybersecurity students that had recently graduated from high school. The criteria were selected such that participants that had recently made their college major choice as a traditional college student were included. These criteria align with the central research question focused on high school student career choice. The survey was sent to 24 students in this participant group. Ten students responded with complete surveys, which represented a 42% response rate from this group. Three of these ten students were seniors. These seniors obtained the survey because they were also enrolled in the 100-level cybersecurity course with cybersecurity freshmen as part of a minor or as an elective. Since there were only 10 respondents including these seniors, the researcher chose to include the seniors' survey data in the study. Removing these three seniors from the study does not impact the themes that emerged from the qualitative data but rather strengthens the themes as these seniors reported similar influencing factors as the freshman in the study. While this is much lower participation than

Participant Group 1, the data provided was rich enough to yield valuable insights and themes. The participants completed the survey outside of class and were incentivized with a gift card to complete the survey. E-gift cards were sent to each participant who completed the survey within a few days of completion. The researcher could not offer extra credit, in addition to the gift card, as was done in Participant Group 1. Students were recruited to participate in the survey the first week of class, reminded twice via email in subsequent weeks, and the survey was closed after three weeks such that data could be analyzed.

Data Collection - Survey Instrument

The survey was created and administered using a private Survey Monkey account. A link was generated from Survey Monkey and sent via email to the student participants. Students were required to read the consent form and acknowledge that the consent form was read and agreed to before proceeding with the survey.

The design of the survey included questions that were demographic, open-ended, or numerical ranking. Demographic questions included age, graduation year, gender, race/ethnicity, environment (rural, city, suburb), GPA, college major, and standard test scores. Standard test scores were not required questions, as some students may not have taken a standardized college entrance exam. All other questions were required. The remaining questions were open-ended or ranking and related to the SCCT, such as background, context, outcome expectations, learning experience, and self-efficacy. Two other questions asked students to rank their interest in the main curriculum components of the ABET-Cybersecurity accreditation standards such as "software security," "digital forensics," "computer network," and "mathematics." A ranking of the NICE Framework category names and descriptions were also presented and included items such as "analyze," "investigate," and "protect and defend." Additional questions were influenced by the literature as prominent factors in career choice. These questions focused on influencing factors of people such as family, teachers, counselors or friends, admission requirements, technical and non-technical aspects of the major that were of interest, and the students' perceptions of what they envisioned themselves doing in their chosen career. The last question of the survey asked students to rank 10 potential influencing factors. These factors were derived as the most prominent in the literature related to career choice influencing factors.

Faculty Interviews

An interview guide was developed, as seen in Appendix C, and utilized to conduct structured interviews with five faculty members. The interview guide was closely followed such that all participants in the faculty group were represented equally. There were seven open-ended questions that allowed the faculty interviewee to express the experiences and observations of influencing factors that they believe contribute to students selecting cybersecurity as their major and career. Common personality traits and skillsets of students were also explored. Some questions investigated barriers and obstacles to students choosing cybersecurity with a focus on obstacles and barriers for women and minorities.

During each interview, the interviewer took some brief notes of the primary points from the interviewee's responses. This was primarily as a backup in the event that the recording or transcript failed for a technical reason. Each faculty interview was recorded, including both audio and video. The audio of each interview was automatically transcribed by software and preserved as a text file. These interview artifacts allowed for a detailed review of each interview.

Descriptive Statistics of Student Participants

Before qualitative analysis and coding of the student data, quantitative data from the survey instrument were gathered in the form of descriptive statistics. This data included student demographic and academic data. The demographic data indicate a predominance of white males in the student participant groups. Fourteen of the 19 cybersecurity students chose to report both SAT Scores. In comparison, only two information systems/technology students chose to report the SAT Math score, and four chose to report the SAT Composite score. This lack of reporting of scores made a comparison of this data between these groups difficult. However, the data indicate a slightly higher level of prior academic achievement within the cybersecurity student group than the information systems/technology group. While only five females completed the survey, this represents a significant percentage of the 11 females in the student population who were invited to complete the survey. The average age of the students within both student groups was 19.

Table 2

Descriptive Statistics for Cybersecurity Student Population (N=19)

Characteristic	N	Percentage (%)
Gender/Race/Ethnicity		
Female	3	16%
Male	16	74%
White	18	95%
Multiracial or Multiethnic	1	5%
HS Environment		
City	1	5%
Rural	8	42%
Suburb	10	53%
Academic Standing		
Freshman Admit	17	89%
Sophomore Transfer	2	11%
Academic Scores	**Average**	
HS GPA	3.6	
SAT Composite (N=14)	1260	
SAT Math (N=14)	616	

Table 3

Descriptive Statistics for Information Systems/Technology Student Population (N=10)

Characteristic	N	Percentage (%)
Gender/Race/ Ethnicity		
Female	2	20%
Male	8	80%
White	9	90%
Multiracial or Multiethnic	1	10%
HS Environment		
City	1	10%
Rural	5	50%
Suburb	4	40%
Standing		
Freshman Admit	7	70%
Senior	3	30%
Academic Scores	**Average**	
HS GPA	3.3	
SAT Composite (N=4)	1157	
SAT Math (N=2)	560	

Quantitative Analysis of Interest and Influence Factor Ranking Data

Both student groups were asked to rank their interest in standard cybersecurity curriculum topics and common career influencing factors derived from the literature and, to a lesser degree, the researcher's experience teaching and advising students. Students ranked 10 influencing factors, 12 ABET topics, and seven NICE topics. A ranking is intended to determine which choices are more and less preferred overall. Each ranking was counted and weighted such that "1" had the most weight and the last ranking had the least weight. This number ranking was emphasized in the survey question as "1 is the highest.". The results indicate a clear cybersecurity student interest in two unique topics to cybersecurity: "vulnerability and threat analysis" and "digital forensics investigation". These two topics were ranked closely with a significant drop in ranking after these top two topics. Also of interest is that "mathematics" was ranked last, yet as the literature illustrated, is often a point of emphasis for those students who are perceived to be a good "fit" for STEM careers. It is also interesting that computer programming was ranked 11th by cybersecurity students, as computer programming was the most referenced prior computing coursework in the qualitative data.

The ranking of ABET topic by the information systems/technology participants varied greatly from the cybersecurity student rankings. The topics that the cybersecurity students ranked 11th and 8th out of 12, "computer programming" and "computer hardware and architecture" were the two highest ranked topics for the information systems/technology students. However, "mathematics" again ranked last at 12th as it did with the cybersecurity students. Another interesting finding is that "computer networking" ranked behind two security topics of "data security" and "software security" indicating that this group of students, while interested most in traditional computing topics such as programming and hardware, also have a high interest in security topics. The two highest ranked topics by cybersecurity students were ranked seventh and ninth by the information systems/technology student group representing a significant difference in interests between these two groups.

Table 4

Cybersecurity Student ABET Topic Ranking (N=19)

ABET Topic	Average Ranking
Vulnerability and Threat Analysis	9.21
Digital Forensics Investigation	8.95
Data Security	7.63
System Administration and Defense	7.47
Software Security	7.32
Risk Analysis	6.89
Computer Networking	5.58
Computer Hardware and Architecture	5.53
Human Behavior and Organization Security	5.42
Governance, Leadership, and Management	5.32
Computer Programming	5.26
Mathematics	3.42

Table 5

Information Systems/Technology Student ABET Topic Ranking (N=10)

ABET Topic	Average Ranking
Computer Programming	8.6
Computer Hardware and Architecture	8.5
System Administration and Defense	8.3
Data Security	8
Software Security	7.9
Computer Networking	7.2
Vulnerability and Threat Analysis	6.3
Governance, Leadership, and Management	5.6
Digital Forensics Investigation	5.2
Risk Analysis	5.1
Human Behavior and Organization Security	3.9
Mathematics	3.4

The second ranking question on the student survey asked students to rank their interests in computing and cybersecurity topics as defined by the NICE Framework. The results are shown in the tables below. Once again, in a similar manner to the ABET cybersecurity topic ranking, the top three cybersecurity student topics were ranked much lower by the information systems/technology group, indicating significant differences in interests between these two student groups. “Investigate” was a strong number one ranking for the cybersecurity students. The top four rankings by the information systems/technology student group did not have much separation in average ranking, as there was a tie between third and fourth and only a tenth of a point separating second and third. The second and third topics for the cybersecurity students were also very close, and there was a tie in the ranking of the bottom two topics. The cybersecurity student number one ranking of “Investigate” was ranked second to last by the information systems/technology students.

Table 6

Cybersecurity Student NICE Topic Ranking (N=19)

NICE Framework Topic	Average Ranking
Investigate - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	5.47
Protect and Defend - Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	4.95
Collect and Operate - Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	4.84
Analyze - Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	4.05
Oversee and Govern - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	3.21
Operate and Maintain - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	2.74
Securely Provision - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	2.74

Table 7

Information Systems/Technology Student NICE Topic Ranking (N=10)

NICE Framework Topic	Average Ranking
Oversee and Govern - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	4.6
Operate and Maintain - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	4.5
Analyze - Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	4.4
Protect and Defend - Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	4.4
Securely Provision - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	3.7
Investigate - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	3.6
Collect and Operate - Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	2.8

The third ranking question on the student survey asked students to rank their least and most influential factors from a list of 10 factors that were prominent in the literature and the SCCT model. The resulting ranking of these factors between the two student groups is similar, much more similar than the rankings of ABET and NICE topic interests across the two groups. The top two influencing factors are the same between the student groups. Teachers and counselors were in the bottom three within both student groups. The difference in average ranking between the top three to five influencing factors is relatively small when compared to the bottom three or four ranked factors in both groups.

Both student groups were more influenced by the technical rather than the non-technical aspects of their majors, as well as the high demand for their majors. This is reflected in a prevalent outcome expectation of job security and employability that both groups ranked second. This may be an opportunity, as the breadth of both majors includes many non-technical aspects as seen in the ABET and NICE framework topics, to increase awareness in both majors in students that may be more interested in non-technical topics.

Prior learning experiences in extracurricular workshops, camps, or programs ranked much higher for the cybersecurity students. Learning experiences in previous courses ranked near the middle for both groups. However, interest in technical aspects of their college major ranked number one for both. The SCCT suggests that prior learning experiences influence interest. This corresponds well to the qualitative data analysis that suggests prior computing courses in high school is one of the top influencing factors (McGill et al., 2016).

Table 8

Cybersecurity Student Influencing Factor of College Major Choice Ranking (N=19)

Influencing Factor of College Major Choice	**Average Ranking**
Interest in technical aspects of college major	7.95
Job security and employability	7.84
Learning experiences in prior courses	6.68
Learning experiences in extracurricular workshops, camps, or programs	6.53
Salary and earning potential	6.53
Parents or family member	4.74
Interest in non-technical or people aspects of college major	4.58
Teacher	4
School counselor	3.11
Friends	3.05

Table 9

Information Systems/Technology Student Influencing Factor of College Major Choice Ranking (N=10)

Influencing Factor of College Major Choice	Average Ranking
Interest in technical aspects of college major	8
Job security and employability	7.6
Salary and earning potential	7.1
Learning experiences in prior courses	5.7
Parents or family member	5.7
Friends	5.7
Learning experiences in extra curricular workshops, camps, or programs	4.9
Interest in non-technical or people aspects of college major	4.2
Teacher	4
School counselor	2.1

Female Interest and Influence Factor Ranking Data

There were only two racial minority participants across both student groups, limiting analysis of this demographic segment. This furthers what the literature suggested in terms of a lack of minority representation in STEM and computing occupations (Shumba et al., 2013). Females were represented between 16% and 20% within the student groups with five female students participating in the survey. Due to the lower number of female participants, the female rankings for interest and influencing factors were combined into one population representing both student groups to increase validity by representing a larger number of participants. There were three cybersecurity and two information systems/technology female participants, which may skew the rankings in favor of the cybersecurity female student participants. “Digital forensics” and “vulnerability and threat analysis” were ranked first and second with “computer programming” ranked as a close third place. The slight imbalance of female representation between the two student groups may explain why the top two cybersecurity ABET topic rankings slightly out weighed the information systems/technology group's top ranking of "computer programming." The top two rankings varied slightly from the full cybersecurity student group with rankings number one and two flipping in favor of "digital forensics investigation." It is also interesting that "computer networking" dropped to last, even below the consistently last place ranked "mathematics" topic.

Table 10

Female Student ABET Topic Ranking (N=5)

ABET Topic	Average Ranking
Digital Forensics Investigation	9
Vulnerability and Threat Analysis	8
Computer Programming	7.4
Governance, Leadership, and Management	7
Data Security	7
Risk Analysis	6.8
Human Behavior and Organization Security	6.6
System Administration and Defense	6.2
Software Security	5.4
Computer Hardware and Architecture	5.4
Mathematics	5
Computer Networking	4.2

The ranking by female participants of the NICE topics was significantly different in numerous areas when compared to each student group as whole. When ranking NICE topics, the female students chose "investigate" as their top ranking, as did the entire cybersecurity student group. "Investigate" was ranked second-to-last by the information systems/technology student group. "Analyze," ranked second for the female students, was a significant change from fourth of seven by the information systems/technology group. “Collect and operate,” ranked second by the cybersecurity student group, dropped significantly to fifth out of seven for the female students.

Table 11

Female Student NICE Topic Ranking (N=5)

NICE Framework Topic	Average Ranking
Investigate - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.	5.6
Analyze - Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.	5.2
Oversee and Govern - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.	4.6
Operate and Maintain - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.	4.2
Collect and Operate - Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.	3.2
Protect and Defend - Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.	3
Securely Provision - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.	2.2

Female participants’ ranking of influencing factor of college major choice revealed some similarities and differences compared to the cybersecurity student and information systems/technology student groups. Interest in technical aspects of college major remained at the top with job security and employability remaining in the top three. Teacher and school counselor influence remained in the bottom three when compared with both full student groups. A significant difference in ranking exists with parents and family member with the females ranking this second while the student groups ranked these items more in the middle, at number five and six out of 10.

Table 12

Female Student Influencing Factor of College Major Choice Ranking (N=5)

Influencing Factor of College Major Choice	Average Ranking
Interest in technical aspects of college major	7.6
Parents or family member	7.2
Job security and employability	7.2
Salary and earning potential	6.8
Learning experiences in prior courses	6.4
Interest in non-technical or people aspects of college major	6
Learning experiences in extra curricular workshops, camps, or programs	5.8
Teacher	4.6
Friends	2.2
School counselor	1.2

Qualitative Data Analysis of Faculty Interviews

Soon after each interview, the researcher downloaded the audio and video of the interview and the interview transcript as artifacts to be preserved and analyzed as soon as possible. The audio and video were played back, paused where necessary, analyzed, and initially coded as soon as possible after each interview. This review and analysis occurred for all faculty interviews no later than two days after the interview. Since there were five interviews of less than 30 minutes each, the researcher was able to spend time carefully reviewing and analyzing each audio/video recording. During the interview recording review, the researcher summarized the key points for each interviewee and began to perform descriptive coding where the researcher summarizes with nouns or short phrases the main topic or key points of the conversation (Saldana, 2016, p. 102). Saldana (2016) suggested that descriptive coding is applicable to most qualitative studies. Saldana likens the process to using hashtags on social media to annotate or link similar content.

During the playback of the recording, summary notes and descriptive codes were written in the margins of the interview guides that were used for note-taking during the interview. These notes and descriptive codes were then added to an Excel spreadsheet for better organization and analysis capabilities, as seen in Table 13. Each spreadsheet row represented a participant and each column an interview question. Each cell contained notes and descriptive codes. This format allowed the researcher to capture, organize, and look across the interview data horizontally and vertically for similarities and differences in the data. Counting occurrences of codes to objectively determine which codes were least and most prevalent across the interview data also occurred.

There were several similarities across faculty participants that began to emerge from the data with "lack of awareness" and "lack of prior computing coursework opportunity" being prominent themes as obstacles and barriers to choosing a career in cybersecurity. Similar personality traits were described across the faculty data such "natural curiosity," "intelligent," and "analytical" as well some common influencing factors such as the "opportunity for prior computing coursework" and "influential family member."

Table 13

Faculty Interviews – Example Notes and Initial Coding

Participant	Experience	Factors	Personality
P2	17 years cybersecurity, 2 years department head, 13 years program director	Parent, family member, prior coursework, external - TV, media, movies, news, job demand, salary	Introvert, problem-solving, not necessarily a math background or interest, analytical
P3	2 years WICS advisor	HS courses in computing, extracurricular camps, workshops, conference, personal impact of cyber attacks (phishing), teacher, family member	Intelligent, high achiever, natural Curiosity, gamer
P5	2 years WICS RSO	Piques interest, salary, career potential, media - TV, movies, news	Analytical, intelligent, make a difference, desire to learn, job that involves change, investigative mindset

After the first round of descriptive coding and organization, code mapping was performed. Saldana (2016) suggested the code mapping process as a method to further organize and display qualitative findings after the first cycle of coding is complete. During the code mapping process, the list of descriptive codes began to be organized into categories and themes through multiple iterations of organization, categorization, and consolidation. With the data in Excel, the codes were easily sorted, categorized, and counted for occurrence across the data and by participant.

Below is the table of categories, codes, and occurrences that emerged after at least two iterations of code mapping. Wherever possible, more detailed and infrequently occurring descriptive codes were combined with similar codes to form a higher level of abstraction or inclusion of the factor that was more meaningful yet accurate. An example might be a personality trait coded as “quiet” and “introverted” or “problem solving” and “determination.” Not all codes with low occurrences were removed if they were unique or could not be consolidated with similar codes. An example of this is “availability of college programs,” which while only occurring once, appeared to be a very significant and specific barrier and therefore remained included as a unique code. One concern that emerges from this coding is that COVID-19 has caused many outreach and extracurricular opportunities to be canceled. “Prior computing coursework or extracurricular” had the highest occurrence as a code overall and as an influencing factor. COVID-19 may also impact or worsen the top-rated barrier or obstacle by occurrence as high schools may have less opportunity to participate in face-to-face outreach programs that could heighten awareness of the cybersecurity occupation for students, teachers, counselors, and administrators.

Table 14

Faculty Interview Categories, Descriptive Codes and Occurrences (N=5)

Category / Code	No. of Occurrences	Participants
External or Contextual Factor		
Prior Computing Coursework or Extracurricular	5	P2, P1, P3(2), P4
Family or Mentor	3	P2, P1, P3
Media (TV, Movies, News)	3	P2, P1, P5
Salary	3	P2, P3, P5
Job Demand	2	P2, P5
Personality Trait or Interest		
Curiosity/Desire to Learn	4	P1, P2, P4, P5
Technology Interest	3	P1, P3, P4
Intelligent	3	P2, P3, P5
Helping Others	3	P2, P3, P4
Gamer	3	P2, P1, P3
Problem Solving	3	P2, P4, P5
Analytical	2	P2, P5
Introvert	2	P2, P4
Barriers and Obstacles		
High School Occupation Awareness	4	P1, P2, P4, P5
Availability of Prior Computing Course	3	P2, P1, P5
COVID-19	2	P3, P5
Availability of College Programs	1	P2
Female or Minority Barriers and Obstacles		
Lack of Role Model or Mentor	3	P2, P1, P3
Lack of Women in Leadership Positions	3	P3, P1, P2
Portrayal of White Hacker Males in the Media	2	P2, P4
Information Systems/Technology Majors		
Student Occupation Awareness	4	P2, P3, P4, P5
Different Interest (Programming, Systems Analysis)	2	P2, P4

As a final process of analyzing and presenting the faculty interview results and data, a code summary table was created. The purpose of this table is to summarize and compare each participant's primary data set (Saldana, 2016, p. 229).

Table 15

Faculty Interview Data and Codes Summary Table

Interview Summary	Primary Codes
P1 - Faculty Participant Prior computing course experience as well as a mentor, teacher, counselor, or role model are influencing factors. High School influencers are not aware of cybersecurity careers or cannot accurately represent and differentiate between different careers in computing. Cybersecurity students are naturally curious, inquisitive, and may identify with a hacking or gaming culture. Lake of role model or mentor is an obstacle to female and minority students choosing cybersecurity. Media such as TV and movies may contribute to piquing a student's curiosity or interest in a cybersecurity career.	Prior Coursework or Extracurricular Family or Mentor Media Curiosity/Desire to Learn Technology Interest High School Occupation Awareness Lack of Role Model or Mentor Student Awareness of Occupation
P2 - Faculty Participant Parents, family members, and prior coursework are the top influencing factors. Media such as TV and movies may contribute to increasing a student's interest or could also place cybersecurity in a negative context. Job demand and salary tend to attract many students. Student personality traits typically include introversion, strong problem solving, analytical, enjoy learning, helping others, and not necessarily an interest in mathematics. Awareness and understanding of the occupation are barriers to everyone including females and minorities. Availability of high school courses, programs, and university programs are barriers and obstacles. History of a white, male-dominated field may be intimidating and unwelcoming to female and minority students.	Prior Coursework or Extracurricular Family or Mentor Media (TV, Movies, News) Salary Job Demand Curiosity/Desire to Learn Helping Others High School Occupation Awareness Availability of College Programs Availability of Prior Computing Course Lack of Women in Leadership Positions

Table 15 (cont.)

P3 - Faculty Participant Prior computing courses, extracurricular, teacher or family members are significant influencing factors. Cybersecurity students are intelligent, curious, and may have a gaming or other technical interest. Lack of awareness of cybersecurity occupation may cause students to choose an alternative computing major or career. Females may perceive the occupation as male-dominated and only technical. Females may not be aware of non-technical roles within the occupation. COVID-19 is slowing or preventing awareness through programs designed to build awareness. Women are lacking in positions of authority and as role models in the occupation.	Prior Coursework or Extracurricular Family or Mentor Intelligent Curiosity/Desire to Learn High School Occupation Awareness Lack of Women in Leadership Positions Lack of Role Model or Mentor COVID-19 Student Awareness of Occupation
P4 - Faculty Participant Students are drawn to cybersecurity in part due to a desire to help and protect themselves and other people from cyber attacks. Cybersecurity students demonstrate a strong desire to learn but are often quiet and reserved. Many have technical interests but possess a broader view of computing than other computing who may have a limited awareness of cybersecurity occupations. Prior learning and courses are a significant influence and a barrier as most high schools that do not offer courses in cybersecurity. Cybersecurity can be intimidating to females and minorities if they lack the self-confidence to pursue an occupation that is currently dominated by white males.	Curiosity/Desire to Learn Helping Others Technology Interest Prior Coursework or Extracurricular Student Awareness of Occupation
P5 - Faculty Participant Different forms of media may pique a student's interest as well as salary and career potential. Students are analytical, intelligent, have a strong desire to learn and make a difference, and possess an investigative mindset. Students may choose other computing majors or careers due to a lack of awareness or limited understanding. Awareness of programs in cybersecurity is an obstacle. High schools may push females to non-STEM roles or traditional female occupations early. COVID has halted many outreach programs such as camps and competitions. Minority and rural schools may not be funded to offer courses in computing.	Media (TV, Movies, News) Salary Job Demand COVID-19 Student Awareness of Occupation Intelligent Analytical High School Occupation Awareness Availability of Prior Computing Course

Qualitative Data Analysis of Student Surveys

As surveys were returned, the researcher began to read and review what each student participant had written within the open-ended, qualitative questions that would need analysis, coding, and interpretation. The researcher repeated this process for each individual survey and began summarizing the data and identifying initial codes through descriptive coding where the researcher summarizes with nouns or short phrases the main topic or key points of the qualitative data (Saldana, 2016, p. 102). Saldana (2016) suggested that descriptive coding is applicable to most qualitative studies. Saldana likens the process similar to the method of using hashtags on social media to annotate or link similar content.

The summary information and descriptive codes were organized in an Excel spreadsheet along with some demographic data for each student participant. Each row represented a participant and each column an open-ended question on the survey. The summary information and initial codes were placed in each cell. This organization of data allowed the researcher to begin to code and look across the data for similarities and differences in the content. An example of this initial organization is show in Table 16.

Table 16

Student Surveys – Example of Notes and Initial Coding

Participant	Admissions	Other Programs	Outcomes	Personal Attributes	People
P27	No Influence	Accounting	Job Demand, Critical Thinking	Determination, Love of learning	Family
P29	No Influence	Health Care	Job Demand, Salary		
P3	No Influence		Job Demand, Salary, Flexibility	Intelligent, Helpful, Resourceful	Family
P6	No Influence	Veterinary, Graphic Design, Software Engineering	Knowledge, Independence	Hard worker, creative	Family
P15	Contributed	Criminal Justice	Knowledge, Job Demand		Family

Some prevalent codes or themes emerged quickly from the initial, first pass of coding. These initial themes were influences of “prior course work,” “job demand,” “family members,” “curiosity,” “desire to help others,” “job security,” and “salary” in no particular order. All of these codes and themes were present in the faculty interview data as well. During the second round of coding and categorization, a list of codes and categories was utilized from the faculty interview data, and then codes were added to those categories as needed. There was not a need for additional categories, and only a few additional codes were added, with some faculty codes being removed from the student list of codes. The faculty and the student data had a lot in common in terms of influencing factors, personality traits, and interests, although the students were not as verbose as the faculty in terms of personality traits.

Table 17

Cyber Student Categories, Descriptive Codes and Occurrences (N=19)

Category / Code	**No. of Occurrences**
External or Contextual Factor	
Job Demand and Opportunity	16
Prior Computing Coursework	15
Family or Mentor	10
Extracurricular	6
HS Teacher	6
Salary	5
Media (TV, Movies, News)	4
Professor	4
Counselor	3
Friend	2
Personality Trait or Interest	
Technology	12
Helping/Protecting Others	9
Curiosity/Desire to Learn	7
Problem Solving	6
Programming	5
Determination	3
Intelligent	2
Gamer	1

The number of occurrences by code clearly indicates a theme of “job demand and opportunity,” “prior computing coursework,” and “family or mentor” as the top three influencers in response to major choice, with the number of occurrences dropping substantially after the third ranked code. In terms of personality trait or interest, “technology” was the most prevalent followed by “Helping/Protecting Others,” and “Curiosity/Desire to Learn.” “Problem Solving” ranked just behind these three personality traits or interests.

The information systems/technology ranking by number of occurrences was similar to the cybersecurity students, but there were also significant differences with “family or mentor” ranking much lower and “salary” ranking higher.

Table 18

Information Systems/Technology Student Categories, Descriptive Codes, and Occurrences (N=10)

Category / Code	No. of Occurrences
External or Contextual Factor	
Prior Computing Coursework	7
Job Demand and Opportunity	7
Salary	4
Family or Mentor	3
Extracurricular	2
Friend	2
Media (TV, Movies, News)	2
HS Teacher	1
Personality Trait or Interest	
Determination	5
Programming	4
Curiosity/Desire to Learn	3
Technology	3
Helping Others	3
Gamer	1
Problem Solving	1
Mathematics	1

Qualitative Data Analysis of Female and Minority Surveys

Similar to the quantitative data analysis for the female students, the female students were combined into one category code ranking across both student groups due to the lower number of female students across both groups. There was only one minority student in each student group that identified as male; therefore, a separate qualitative analysis was not performed on this subsection. The results were similar to the student groups as a whole, especially the cybersecurity student group. “Programming” interest did rank higher in the female group, as did “extracurricular,” with four of the five female students describing a “summer camp” as an influencing factor.

Table 19

Female Student Categories, Descriptive Codes and Occurrences (N=3)

Category / Code	No. of Occurrences
External or Contextual Factor	
Job Demand and Opportunity	4
Prior Computing Coursework	4
Family or Mentor	4
Extracurricular (Camp)	3
Salary	2
Media (TV, Movies, News)	2
HS Teacher	1
Professor	1
Personality Trait or Interest	
Programming	3
Technology	3
Helping/Protecting Others	2
Curiosity/Desire to Learn	2
Determination	2
Problem Solving	1
Intelligent	1

Similar to the cybersecurity and information systems/technology groups, the females were more influenced by “Job Demand and Opportunity” and “Prior Computing Coursework.” The third ranking, “family or mentor,” ranked third most influential as it was by the cybersecurity group. “Extracurricular (camp)” was specified as an influential factor by three of the five female students. This is a significant change when compared to the two other student groups, as the majority of the females were influenced by this factor. “Programming” was also prevalent in the female segment and occurred as much as “technology,” which was a clear leader amongst the cybersecurity student group.

Summary of Findings

Student Influencing Factors Findings

This dissertation’s central question was to determine the factors that influence students to choose cybersecurity as a career. This study’s data indicate that “Prior Computing Coursework,” “Job Demand and Salary,” “Family or Mentor,” and “Technical Interest” are the dominant influencing factors and themes. These themes were triangulated within the data and results, as they were strong themes both quantitatively and qualitatively across all three participant groups that included faculty and students. All but one of the 29 student participants, or 97% of the student participants, described a prior computing course as an influential factor toward their major choice. All but three of the 29 participants, or 90% of the students, described the demand for the occupation, salary, or career opportunity as an influencing factor. Technology interest, expressed as a result of prior computing coursework or family influence, was also very prevalent in the quantitative and qualitative data. It is also worth noting that only two of the 29 student participants indicated that college program admission requirements influenced their decision to choose a major.

Cybersecurity Topics of Interest Findings

A sub-question to the central question in this research sought to better understand which topics or subjects, as defined by leading cybersecurity curriculum standards, new cybersecurity students were most and least interested in. A second sub-question sought to better understand why students choose a computing major that is not cybersecurity, such as information systems.

Students were asked to rank their interest in computing topics and complete a series of open-ended questions on a survey. General STEM topics such as “science” and “mathematics” were largely absent within the quantitative and qualitative data for both student and faculty participant groups. Students participant groups ranked mathematics last or close to last when interests or influencing factors were ranked quantitatively. This may inform those in a position of influence, such as a high school teacher or counselor, to not solely utilize or heavily weight a student’s performance or interest in science or math as an indicator that they may have a capacity or interest for a subsequent course or career in computing or more specifically cybersecurity.

“Programming” was prevalent in the qualitative data across both student groups as an activity that influenced interest in a computing career. The information systems/technology student group ranked “programming” number two in terms of an interest and number one in the ABET topic ranking followed by “hardware and architecture.” This group also ranked “oversee and govern” and “operate and maintain” as number one and number two within the NICE topics. The cybersecurity students ranked computer programming and hardware much lower and instead represented top interests of “digital forensics investigation,” “vulnerability and threat analysis,” “investigate,” and “protect and defend.”

The top topics and bottom topics were close to an inverse between the two student groups. This is significant from a number of perspectives, including the need to educate and build awareness with students of specific computing occupations as opposed to limiting the experience to more traditional or generic computing topics like “programming,” “hardware,” and "networking." While these are certainly topics within cybersecurity, they offer a very limited perspective that may in turn limit student interest.

It appears that even though the cybersecurity students were not as interested in programming, prior programming course experiences helped to pique their interest in computing, which factored into their awareness and selection of cybersecurity. This leaves quite a bit of room for investigation and potential improvement in terms of building a more direct learning experience opportunity in cybersecurity prior to the student entering higher education. Furthermore, there is currently no advanced placement course for cybersecurity per the College Board organization (AP Courses and Exams, n.d.).

One could conclude that one of the other interests or influencing factors in combination with the "prior computing course" factor significantly influenced these students to choose cybersecurity, since their interest likely was not in programming as indicated by the cybersecurity student rankings of topics. According to the influencing factors rankings, this was likely a family member or the student becoming aware of the career potential and salary within the cybersecurity occupation.

Student Personality, Interests, and Self-Efficacy

There were several survey questions that sought to further understand why students choose cybersecurity or another computing major such as information systems. Some of these questions focused on personality, interests, and self-efficacy. Interest in technology, as well as a curiosity and desire to learn, were consistent themes within both student groups. Both faculty and students also describe personality characteristics related to determination, tenacity, self-confidence, and problem-solving. A desire to help others was a very strong theme within the cybersecurity student group that compliments curriculum topics that were rated very high such as "protect and defend." This theme, along with a lesser interest in programming and computer hardware, may help differentiate the cybersecurity student group from the information systems student group in terms of interests.

The SCCT model demonstrates that learning experiences can influence interests. This may be illustrated in these findings with strong representations of "prior computing coursework" and "technology interest." The computing coursework may be leading to an interest in technology as the SCCT model might suggest. Students also self-described their ability to problem-solve and demonstrate a determination to solve technical or complex problems. Referring to the SCCT model, their prior computing coursework learning experiences may be impacting their self-efficacy in terms of their positive beliefs to utilize determination to solve technical problems within a computing context.

Female and Minority Findings

This study also sought to understand better how influencing factors, interests, and potential barriers present for female and minority students. There were five female students and two minority students in the study. This represented a small percentage of the participants in the student participant groups overall, but this is not unlike their representation within the cybersecurity occupation itself. The lack of minority representation presented challenges with analyzing data for this demographic segment.

With five of the 11 or 45% of the females completing the survey, there was an opportunity for analysis and insight into this demographic segment. There were some divergent themes within the female segment when compared to their respective student participant groups as a whole. Females ranked "computer networking" last in terms of interest and "parent or family" member much higher as an influencing factor, as the female group ranked this second as opposed to a middle ranking of fifth or sixth out of 10 by the two student groups. The female group expressed similar interests to their student groups in terms of their ABET Topic rankings. However, "analyze" moved up substantially in the NICE topic ranking to number two.

One of the seven questions within the faculty interview guide asked each faculty member to address any obstacles or barriers to female and minority students that they have observed. Barriers and obstacles for females were well represented in the faculty interview data. Faculty pointed to a lack of awareness of the cybersecurity occupation as well as a poor understanding of the breadth of the occupation, the simply association of the occupation with a traditionally white, male computer science role. Lack of opportunity for specific courses or mentoring in cybersecurity occupation opportunity was also a strong theme amongst the faculty. The faculty questioned whether many high school counselors or high school teachers could accurately represent the cybersecurity occupation and differentiate it from computer science or information systems during discussions with students. Minority barriers and obstacles were largely absent from faculty interview data. Faculty responses gravitated towards addressing the lack of females when asked about barriers and obstacles for females and minorities or more generically referred to barriers for all genders, races, and ethnicities.

Chapter 5

Conclusions, Implications, and Recommendations

Conclusions

The literature review within this study demonstrated a pipeline problem related to educating enough talented workers in cybersecurity to address the global shortage of cybersecurity workers. The literature also indicated a lack of understanding of what may influence students, including female and minority students, to choose a career in cybersecurity and how these factors may differ from STEM generally and other computing occupations. It was hypothesized that by better understanding influencing factors and interests of cybersecurity students, interventions and programs could be designed and implemented towards increasing awareness and interest in cybersecurity. This increased awareness and interest could lead to more students choosing cybersecurity as a higher education major and career, improving the current pipeline issues that contribute to a shortage of cybersecurity workers.

This study has significantly contributed to the literature. This study suggests that there are gaps in awareness of the cybersecurity occupation among potential students and those that inform and influence those students. More specifically, the study suggests the current curriculum, teachers, and counselors that potentially influence students prior to higher education present a significant opportunity towards building additional awareness and educational opportunities in cybersecurity.

This study's data indicate that the following were the most influential factors of student cybersecurity career choice:

- Prior Computing Coursework or Extracurricular
- Job demand and Salary
- Technical Interest
- Family or Mentor

This study's data indicate topics of interest among students that have chosen cybersecurity as a college major differ from other computing majors. These topics center around themes of investigation and analysis of cybersecurity threats and included the following:

- Digital Forensics Investigation (ABET)
- Vulnerability and Threat Analysis (ABET)
- Investigate (NICE)
- Protect and Defend (NICE)

This study also suggests that new students who choose cybersecurity have interests that differ significantly from traditional information systems major students. In fact, the top and bottom-ranked interests between the groups were almost opposite of each other. For example, the information systems/technology student group ranked "programming" and "hardware and architecture" as their highest interests, while cybersecurity students ranked "programming" second to last and "hardware and architecture" in the bottom half of their interest rankings. This study suggests there is a need to further educate and build awareness amongst those that influence and inform students of the numerous occupations related to computing. This additional awareness should include the differences between the occupations and the depth/breadth of the roles and skills utilized within these occupations. This could lead to more students choosing computing-related careers and specifically choosing cybersecurity.

Recommendations

The study met its goal of answering the research questions through unique participation from faculty in an accredited cybersecurity program, new cybersecurity students within this program, and students that chose a computing major that was not cybersecurity. The prior coursework that is heavily influencing students to choose cybersecurity (programming), while a computing topic, is ranked near the bottom in terms of their interests amongst computing subjects. What if there were introductory cybersecurity courses, such as digital forensics, available at the high school level? What if there were high school programs that provided students, teachers, and counselors with an opportunity to become more aware of the depth and breadth of the cybersecurity occupation? How many more students might choose to pursue cybersecurity as a career not just through an interest sparked by a topic they really aren't interested in (programming) but rather a computing topic in which they are highly interested?

This study indicates that introducing a cybersecurity course prior to higher education could be highly influential, and as result of this study, we are better informed as to which topics students are and are not initially interested in at this stage of their educational journey. An advanced placement course in cybersecurity through the College Board could be a catalyst for introducing standard cybersecurity curriculum prior to higher education.

This study also suggests that female and minority students continue to be underrepresented in computing programs such as cybersecurity and information systems. This study provides insights into these barriers and the unique interests of female students. These results may help inform programs designed to increase female and minority awareness and interest in computing and cybersecurity prior to higher education. For example, this study suggests that representing or introducing cybersecurity as "computer networking" is likely to decrease female student interest.

It would have likely been insightful to directly obtain the minority and female students' perspectives on barriers and obstacles. However, gender and race/ethnicity were not a known demographic attribute prior to the student surveys, and this question was therefore not included in the survey. Follow-up interviews/surveys or a subsequent study focused on these students may provide further insight into this question. The study also suggests that there is room to expand faculty understanding of obstacles and barriers for this demographic, such that programmatic decisions can be informed towards increasing participation from these female and minority groups.

Implications for Future Research

There is much opportunity for subsequent studies of factors that influence students to choose cybersecurity and the interests of these students. Due to time and budget constraints, this study included students from a single university in a rural location. Future studies could expand to include additional cybersecurity programs as well as alternative computing majors at other universities. Future studies should also attempt to dig deeper into the barriers and obstacles faced by female and minority students, as these groups, while represented in this study, require further representation and research.

Asking students to rank their interests in computing and cybersecurity topics at the beginning of their college journey is valuable and insightful. However, how do these interests change as they become more aware and educated on the many subjects within cybersecurity? Future research could focus on how student interests change from their initial, perhaps somewhat uninformed interests in cybersecurity, to more mature, well-informed interests later in a cybersecurity program after completing an internship or upon graduation from the university.

Closure

The literature on this topic has now been enriched by this study's mixed-method, rich descriptions, and descriptive statistics from an essential and influential set of study participants. This investigation looked deep into the interests, influences, and experiences of both faculty and students and, as a result, has furthered the understanding of factors that influence students to choose a career in cybersecurity.

References

Alsaawi, A. (2014). A critical review of qualitative interviews. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.2819536

AP Courses and Exams. (n.d.). In College Board. Retrieved September 15, 2020, from https://apstudents.collegeboard.org/course-index-page

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

Bashir, M., Lambert, A., Guo, B., Memon, N., & Halevi, T. (2015). Cybersecurity competitions: The human angle. *IEEE Security & Privacy, Security & Privacy, IEEE, IEEE Security & Privacy, 13*(5), 74–79. https://doi-org.proxy2.library.illinois.edu/10.1109/MSP.2015.100

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

Butin, D. W. (2010). The education dissertation (4th ed.). Thousand Oaks, CA: SAGE.

Creswell, J. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.).* Thousand Oaks, CA: Sage.

Cybersecurity in the Classroom. (2020, January 18). In *National Initiative for Cybersecurity Careers and Studies.* Retrieved from https://niccs.us-cert.gov/formal-education/integrating-cybersecurity-classroom

Cybersecurity Worforce Assessment Act. (2014, December 18). In *Library of Congress.* Retrieved from https://www.congress.gov/113/plaws/publ246/PLAW-113publ246.pdf

Criteria for Accrediting Computing Programs, 2019 – 2020. (n.d.). In *ABET.* Retrieved from https://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-computing-programs-2019-2020/

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *FRONTIERS IN PSYCHOLOGY*, *9*. https://doi-org.proxy2.library.illinois.edu/10.3389/fpsyg.2018.00744

Dunn, M. H., & Merkle, L. D. (2018). Assessing the impact of a national cybersecurity competition on students' career interests. *Association for Computing Machinery (ACM)*, 62–67. https://doi.org/10.1145/3159450.3159462

Eccles, J. (1994). Understanding women's educational and occupational choices. *Psychology of Women Quarterly, 18*, 585-609. https://doi.org/10.1111/j.1471-6402.1994.tb01049.x

Employment in STEM Occupations. (2019, September 4). In *U.S. Bureau of Labor Statistics.* Retrieved from Statistics https://www.bls.gov/emp/tables/stememployment.htm

Falco, L. D. (2017). The school counselor and STEM career development. *Journal of Career Development, 44*(4), 359–374. https://doi.org/10.1177/08948453166564451603.

Frome, P. M., Alfed, C. J., Eccles, J. S., & Barber, B. L. (2006). Why don't they want a male dominated job? An investigation of young women who changed their occupational aspirations. *Educational Research and Evaluation, 12*, 359–372. https://doi.org/10.1080/13803610600765786

Hall, C., Dickerson, J., Batts, D., Kauffmann, P., & Bosse, M. (2011). Are we missing opportunities to encourage interest in stem fields? *Journal of Technology Education, 23*(1), 33–46. https://doi.org/10.21061/jte.v23i1.a.4

Holland, J. L. (1996). Exploring careers with a typology: What we have learned and some new directions. *American Psychologist, 51*(4), 397–406. https://doi.org.proxy2.library.illinois.edu/10.1037/0003-066X.51.4.397

Information Security Analysts. (2019, September 4). In *U.S. Bureau of Labor Statistics*. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

Janeja, V. P., Seaman, C., Kephart, K., Gangopadhyay, A., & Everhart, A. (2016). Cybersecurity workforce development: A peer mentoring approach. *2016 IEEE Conference on Intelligence and Security Informatics (ISI), Intelligence and Security Informatics (ISI), 2016 IEEE Conference On*, 267–272. https://doi-org.proxy2.library.illinois.edu/10.1109/ISI.2016.7745487

Kelley, K., Clark, B., Brown, V., & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research. *International Journal for Quality in Health Care, 15*(3), 261-266.

Kier, M. W., Blanchard, M.R., Osborne, J.W., Albert, J.L. The development of the STEM career interest survey (STEM-CIS). *Res. Sci. Educ. 2014, 44*, 461–481. https://doi.org/10.1007/s11165-013-9389-3

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

Langdon, D., McKittrick, G., Beede, D., Khan, B., & Doms, M. (2011). STEM: Good jobs now and for the future. (ESA Issue Brief No. 03-11). Washington, DC: U.S. Department of Commerce, Economics and Statistics Administration.

Lent, R. W., Brown, S. D., & Hackett, G. (1994). Toward a unifying social cognitive theory of career and academic interest, choice, and performance. *Journal of Vocational Behavior, 45*, 79–122.

Lent, R. W., Lopez, A. M., Lopez, F. G., & Sheu, H. B. (2008). Social cognitive career theory and the prediction of interests and choice goals in the computing disciplines. *Journal of Vocational Behavior, 73*(1), 52–62. https://doi.org/10.1016/j.jvb.2008.01.002

Lingelbach, K. K. (2018). Perceptions of female cybersecurity professionals toward factors that encourage females to the cybersecurity field [ProQuest LLC]. In *Croquet LLC*.

Liu, L. (2016). Using generic inductive approach in qualitative educational research: A case study analysis. *Journal of Education and Learning, 5*(2), 129-135.

Malgwi, C. A., Howe, M. A., & Burnaby, P. A. (2005). Influences on students' choice of college major. *Journal of Education for Business, 80*(5), 275–282. https://doi.org/10.3200/JOEB.80.5.275-282

Manson, D., Curl, S., & Carlin, A. (2012). CyberPatriot: Exploring university-high school partnerships. *Communications of the IIMA, 12*(1), 65.

Masnick, A., Valente, S., Cox, B., & Osman, C. (2010). A multidimensional scaling analysis of students' attitudes about science careers. *International Journal of Science Education, 32*(5), 653–667. https://doi.org/10.1080/09500690902759053

Mau, W. C. (2003). Factors that influence persistence in science and engineering career aspirations. *The Career Development Quarterly, 51*, 234 – 243. https://doi.org/ 10.1109/MCSE.2017.42

Mau, W. C., Chen, S. J., & Lin, C. C. (2019). Assessing high school students' stem career interests using a social cognitive framework. *Education Sciences, 9*(2). https://doi.org/10.3390/educsci9020151

McEwan, T., & McConnell, A. (2013). Young people's perceptions of computing careers. 2013 *IEEE Frontiers in Education Conference (FIE), Frontiers in Education Conference, 2013 IEEE*, 1597–1603. https://doi-org.proxy2.library.illinois.edu/10.1109/FIE.2013.6685108

McGill, M. M., Decker, A., & Settle, A. (2016). Undergraduate students' perceptions of the impact of pre-college computing activities on choices of major. *ACM Transactions on Computing Education, 16*(4), 1–33. https://doi.org/10.1145/2920214

Merriam, S. B., & Tisdell, E. J. (2016). *Qualitative research: A guide to design and implementation (4th ed.).* San Francisco, CA: Jossey-Bass.

Morgan, S. (2017, June 6). Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. In *CSO Online*. Retrieved from https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the human: A review of literature on broadening diversity in cybersecurity education. *Annual Conference on Innovation and Technology in Computer Science Education, ITiCS*E, 157–176. https://doi-org.proxy2.library.illinois.edu/10.1145/3344429.3372507

Nakama, D., & Paullet, K. (2018, August). The urgency for cybersecurity education: The impact of early college innovation in Hawaii rural communities. *Information Systems Education Journal, 16*(4), 41-52.

National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. (2017, August). In *NIST*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Noonan, R. (n.d.). STEM Jobs: 2017 Update. In *U.S. Department of Commerce*. Retrieved from https://www.commerce.gov/sites/default/files/migrated/reports/stem-jobs-2017-update.pdf

NSA/DHS National CAE in Cyber Defense Designated Institutions. (n.d.). In *National IA Education and Training Programs*. Retrieved from http://www.iad.gov/NIETP/reports/cae_designated_institutions.cfm

Patton, M. Q. (2002). *Qualitative research & evaluation methods (3rd ed.).* Thousand Oaks, CA: Sage.

Percentage of postsecondary degrees awarded to women, by field of study and country: 2016. (2019, May 23). In *National Center for Educational Statistics*. Retrieved from https://nces.ed.gov/programs/digest/d18/tables/dt18_603.60.asp

Rosenbloom, J. L., Ash, R. A., Dupont, B., & Coder, L. (2008). Why are there so few women in information technology? Assessing the role of personality in career choices. *Journal of Economic Psychology, 29*, 543–554. https://doi.org/ 10.1016/j.joep.2007.09.005

Saldana, J. (2016). *The coding manual for qualitative researchers (3rd ed.).* Thousand Oaks, CA: Sage.

Scheurich, J. J. (n.d.). A postmodernist critique of research interviewing. *International Journal of Qualitative Studies in Education, 8*(3), 239–252. https://doi-org.proxy2.library.illinois.edu/10.1080/0951839950080303

Shein, E. (2019). The CS teacher shortage. *Communications of the ACM, 62*(10), 17–18. https://doi.org/10.1145/3355375

Shumba, R., Acholonu, G., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., Sande C., Acholonu G., Bace R., Hall, L. (2013, March). Cybersecurity, women and minorities: Findings and recommendations from a preliminary investigation. *ITiCSE-WGR 2013 - Proceedings of the ACM Conference on Innovation and Technology in Computer Science Educatio*n, 1-13. https://doi-org.proxy2.library.illinois.edu/10.1145/2543882.2543883

Turner III, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. *Qualitative Report, 15*(3), 754–760.

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. *Electronic Journal of Science Education, 1*8(1).

U.S. Bureau of Labor Statistics. (2019). “Periodic table of science, technology, engineering, and math occupations.” Retrieved from https://www.bls.gov/k12/teachers/posters/pdf/periodic-table.pdf

U.S. Congress Joint Economic Committee. (2012, April). STEM education: Preparing for the jobs of the future. Washington, DC.

Wang, M. T., Eccles, J. S., & Kenny, S. (2013). Not lack of ability but more choice: Individual and gender differences in choice of careers in science, technology, engineering, and mathematics. *Psychological Science, 24*(5), 770–775. https://doi.org/10.1177/0956797612458937

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

2020 Data Breach Investigations Report (2020). In Verizon. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Appendix A – Student Participant Survey

The document can be found here: https://docs.google.com/spreadsheets/d/1H9CrD5fWKX1OJCbjApZxXa0krDBOj2-emTFNGTNP5ME/edit?usp=sharing

Item #	Question Type	SCCT Aspect	ABET or NICE Aspect	Item
1	Demographic	Background / Context	NA	What is your name?
2	Demographic	Background / Context	NA	What is your age?
3	Demographic	Background / Context	NA	What is your gender?
4	Demographic	Background / Context	NA	What is your current standing (Freshman, Sophomore, Junior, Senior)?
5	Demographic	Background / Context	NA	What was your high school GPA?
6	Demographic	Background / Context	NA	What was your overall SAT Score?
7	Demographic	Background / Context	NA	What was your SAT Math Score?
8	Demographic	Background / Context	NA	Were you primarily raised in a rural, suburb, or metropolitan environment?
9	Demographic	Personal Inputs	NA	What is your race?
10	Open-Ended	Learning Experiences	NA	How have prior courses influenced your decision to choose cybersecurity as a career?
11	Open-Ended	Contextual Influences	NA	How have the people in your life influenced your decision to choose a career in cybersecurity?
12	Open-Ended	Contextual Influences	NA	Describe any experiences outside of the classroom that have influenced your decision to choose a career in cybersecurity.
13	Open-Ended	NA	NA	Tell me about how you became aware of cybersecurity as a career and college major?
14	Open-Ended	Interests	NA	What other careers and college majors did you consider and why?
15	Open-Ended	Interests	NA	Describe the technical computing aspects of cybersecurity that influenced your decision to choose a career in cybersecurity?
16	Open-Ended	Interests	NA	Describe the non-technical aspects of cybersecurity that influenced your decision to choose a career in cybersecurity?
17	Open-Ended	Interests	NA	Describe the work activities you see yourself doing in a cybersecurity career.

18	Open-Ended	Outcome Expectation	NA	Tell me about any positive outcomes and benefits you expect as a result of earning a degree in cybersecurity.
19	Open-Ended	Self-Efficacy	NA	Describe how your personal attributes and characteristics will help you overcome barriers and obstacles that you may encounter in the cybersecurity program.
20	Open-Ended	NA	NA	Is there anything else you'd like to share about what influenced your decision to choose a career in cybersecurity?
21	Ranking	Interests	NICE, ABET	Rank the following in order of most to least interesting with "1" being the most interesting: 1) Computer Programming 2) Computer Networking 3) Mathematics 4) Digital Forensics Investigation 5) Vulnerability and Threat Analysis 6) System Administration and Defense 7) Governance, Leadership, and Management 8) Data Security 9) Software Security 10) Risk Analysis 11) Computer Architecture 12) Human Behavior and Organization Security
22	Ranking	Influential Factors	NA	Rank the following in order of most to least influential in your decision to choose your current college major with "1" being the most interesting. 1. Learning experiences in prior courses 2. Parents or family member 3. Friends 4. Teachers 5. School counselor 6. Learning experiences in extra curricular workshops or camps 7. Salary and wage potential 8. Job security and employability 9. Interest in technical aspects of cybersecurity 10. Interest in non-technical or people aspects of cybersecurity 11. Interest in protection and defense 12. Interest in investigation 13. Other – please specify

23	Ranking	Interests	NICE	Rank the following in order of most to least interesting with "1" being the most interesting: 1) **Analyze** - Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence 2) **Collect and Operate** - Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence. 3) **Investigate** - Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence. 4) **Operate and Maintain** - Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security. 5) **Oversee and Govern** - Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work. 6) **Protect and Defend** - Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks. 7) **Securely Provision** - Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development
24	Text	Incentive	NA	Please specify the email address so we can send you your e-gift.

Appendix B – Student Interview Guide

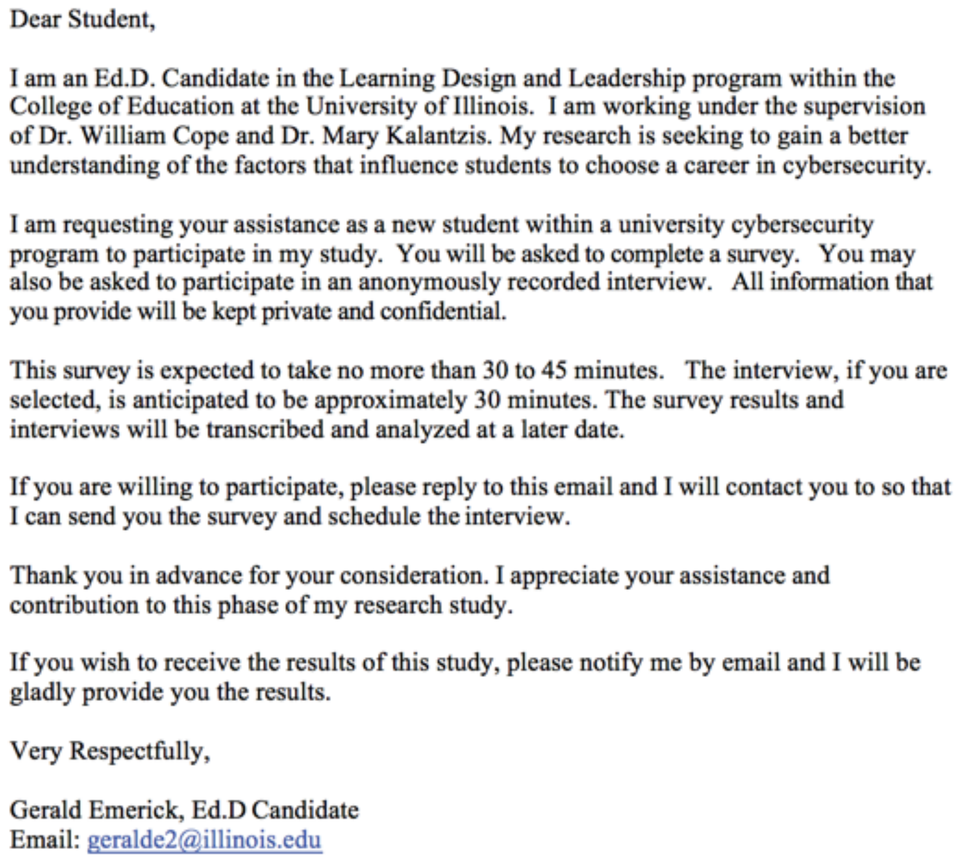
Student interview questions will be determined based on the analysis of the student surveys. Questions will be formulated to clarify and elaborate on the student survey response. Below is a list of potential questions for consideration.

1. What types job or positions have your parents and close family members held?
2. What college majors or degrees were obtained or pursued by your parents or close family members?
3. What process or steps did you use to decide on a major in cybersecurity?
4. Which classes and activities did you enjoy the most and least during high school?
5. How have family or friends influenced your career choice?
6. Describe a middle or high school teacher or counselor that may have been an influenced you in your decision to choose a career in cybersecurity.
7. What areas of cybersecurity interest you the most? Which areas or aspects interest you the least?
8. How have your personal attributes and characteristics helped you succeed in cybersecurity?
9. Is there anything else you would like to share regarding what influenced your decision to choose a cybersecurity career?

Appendix C – Faculty Interview Guide

1. Reflecting on your years of experience teaching and advising cybersecurity students, what do you believe are the primary factors that influence students to choose cybersecurity as a career?
2. Describe common personality characteristics that you have observed amongst students in cybersecurity.
3. What is the skill set that attracts cybersecurity students and enables them to succeed?
4. Describe barriers and obstacles you have observed that are preventing more students from choosing cybersecurity as a career.
5. Describe any barriers or obstacles you have observed that may prevent or discourage women and minorities from pursuing a career in cybersecurity.
6. Is there anything else you would like to share regarding what you have observed as an influence to choosing a career in cybersecurity?

Appendix D - Recruitment Emails



Dear Student,

I am an Ed.D. Candidate in the Learning Design and Leadership program within the College of Education at the University of Illinois. I am working under the supervision of Dr. William Cope and Dr. Mary Kalantzis. My research is seeking to gain a better understanding of the factors that influence students to choose a career in cybersecurity.

I am requesting your assistance as a new student within a university cybersecurity program to participate in my study. You will be asked to complete a survey. You may also be asked to participate in an anonymously recorded interview. All information that you provide will be kept private and confidential.

This survey is expected to take no more than 30 to 45 minutes. The interview, if you are selected, is anticipated to be approximately 30 minutes. The survey results and interviews will be transcribed and analyzed at a later date.

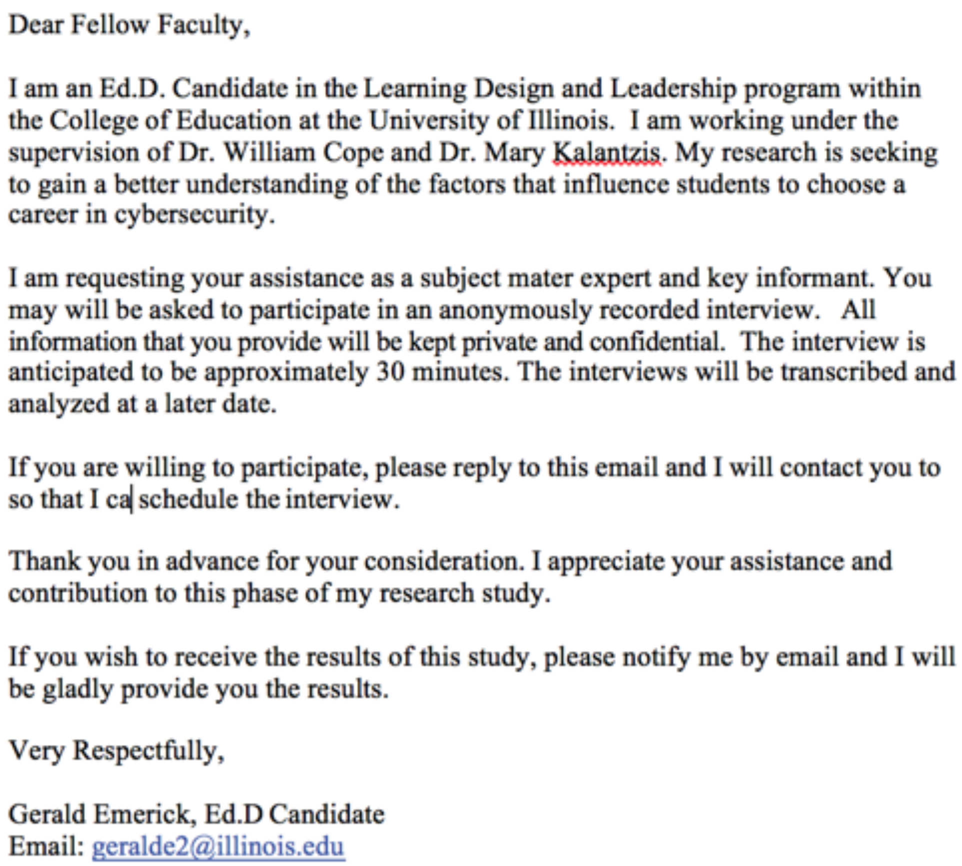
If you are willing to participate, please reply to this email and I will contact you to so that I can send you the survey and schedule the interview.

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

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

Very Respectfully,

Gerald Emerick, Ed.D Candidate
Email: geralde2@illinois.edu



Dear Fellow Faculty,

I am an Ed.D. Candidate in the Learning Design and Leadership program within the College of Education at the University of Illinois. I am working under the supervision of Dr. William Cope and Dr. Mary Kalantzis. My research is seeking to gain a better understanding of the factors that influence students to choose a career in cybersecurity.

I am requesting your assistance as a subject mater expert and key informant. You may will be asked to participate in an anonymously recorded interview. All information that you provide will be kept private and confidential. The interview is anticipated to be approximately 30 minutes. The interviews will be transcribed and analyzed at a later date.

If you are willing to participate, please reply to this email and I will contact you to so that I ca schedule the interview.

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

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

Very Respectfully,

Gerald Emerick, Ed.D Candidate
Email: geralde2@illinois.edu

Appendix E –Participant Consent Form

General Informed Consent Form
Consent to be in a Research Study Entitled

Factors that influence students to choose a career in cybersecurity: An exploratory study

Who is doing this research study?

College: College of Education, University of Illinois, Champaign-Urbana

Principal Investigator: Gerald Emerick, M.Sc., Ed.D Candidate

Faculty Advisor/Dissertation Chair: William Cope, Ph.D.

Site Information: Ferris State University, Big Rapids, MI. Virtual via Zoom or similar.

Funding: Unfunded

What is this study about?

This is a research study designed to investigate the factors that influence students to choose a career in cybersecurity. The study is important due to the global shortage of skilled workers in cybersecurity. There is a national shortage of educated and skilled cybersecurity professionals. One highly cited industry study predicts a 3.5 million global worker shortage in cybersecurity by 2021. The Bureau of Labor Statistics ranks the Information Security Analyst number one in all STEM occupations in terms of a projected positive employment change of 31.6% from 2018 through 2028. At the same time, there is a lack of qualified high school teachers in computer science let alone the more recent but related discipline of cybersecurity. As a consequence of this and other factors such as core curriculum requirements that do not require computer science, there is a threat that high school students have little or no exposure to computing science curriculum or cybersecurity education within traditional middle school and high school curriculum and environments.

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

You are being asked to be in this research study because you are a part of the sample group possessing the criteria needed to better understand what influences students to choose a career in the cybersecurity field. The criteria for participation for students are enrollment in the 100-level cybersecurity course, cybersecurity major, and freshman standing. Faculty participant criteria include being a faculty member in the cybersecurity program with significant experience teaching and advising cybersecurity students.

This study will include about 20 people.

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

While you are taking part in this research study, you will not be asked to participate in any risk or harm than you would have in everyday life. Risks to you are minimal, meaning they are not thought to be greater than any other risks your experience every day. Being recorded means that confidentiality cannot be promised. If sharing your opinions makes you anxious or stressful, we can refer you to someone who may be able to help you with these feelings.

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

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

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

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

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

.

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

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

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

Will it cost me anything?

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

How will you keep my information private?

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

Will there be any Audio or Video Recording?

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

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

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

Primary contact:
Gerald Emerick, M.Sc., Ed.D Candidate, can be reached at (616) 951-4676.

If primary is not available, contact:
William Cope, Ph.D. can be reached via email billcope@illinois.edu.

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

Institutional Review Board
University of Illinois
(217) 333-2670
IRB@illinois.edu

You may also visit the University of Illinois IRB website at https://oprs.research.illinois.edu/rights-consent for further information regarding your rights as a research participant.

Research Consent & Authorization Signature Section

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

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

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

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

Adult Signature Section

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

____________________ ________________________ __________

Printed Name of Participant   Signature of Participant   Date

____________________ ________________________ __________

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

Appendix F – Institutional Review Board

ILLINOIS

OFFICE OF THE VICE CHANCELLOR
FOR RESEARCH & INNOVATION

Office for the Protection of Research Subjects
805 W. Pennsylvania Ave., MC-095
Urbana, IL 61801-4822

July 8, 2020

Notice of Exempt Determination

Principal Investigator	William Cope
CC	Gerald Emerick
Protocol Title	*Factors that influence students to choose cybersecurity higher education and careers: An exploratory study*
Protocol Number	21015
Funding Source	Unfunded
Review Category	Exempt 2 (ii)
Determination Date	July 8, 2020
Closure Date	July 7, 2025

This letter authorizes the use of human subjects in the above protocol. The University of Illinois at Urbana-Champaign Office for the Protection of Research Subjects (OPRS) has reviewed your application and determined the criteria for exemption have been met.

The Principal Investigator of this study is responsible for:

- Conducting research in a manner consistent with the requirements of the University and federal regulations found at 45 CFR 46.
- Requesting approval from the IRB prior to implementing major modifications.
- Notifying OPRS of any problems involving human subjects, including unanticipated events, participant complaints, or protocol deviations.
- Notifying OPRS of the completion of the study.

Changes to an **exempt** protocol are only required if substantive modifications are requested and/or the changes requested may affect the exempt status.