https://doi.org/10.48009/2_iis_2019_9-17

Issues in Information Systems
Volume 20, Issue 2, pp. 9-17, 2019

STUDENT PERCEPTIONS OF SKILLS AND COMPETENCIES NEEDED FOR CYBERSECURITY PROGRAMS AND CAREERS

Sushma Mishra, Robert Morris University, mishra@rmu.edu
Jamie Pinchot, Robert Morris University, pinchot@rmu.edu
Donna Cellante, Robert Morris University, cellante@rmu.edu
Karen Paullet, Robert Morris University, paullet@rmu.edu

ABSTRACT

The cybersecurity industry is facing a serious skills gap, with hundreds of thousands of positions left unfilled in the U.S. and projected estimates that the shortage of skilled workers will continue to increase. There is also a shortage of cybersecurity programs in academia that can adequately prepare students for the challenging needs of the profession. This paper investigates the perceptions of students in cybersecurity programs about the skills, competencies, and interests that are needed to succeed in the cybersecurity field, their motivations for choosing the field, and perceptions about the program in which they are enrolled. Three focus groups were conducted with students and thematic analysis was applied to the data. Themes relating to skills and competencies needed for cybersecurity professionals, motivations for choosing the field of cybersecurity, and perceptions about cybersecurity programs were derived from the focus groups. Recommendations are provided for academics for ways to improve recruitment, retention, and curriculum for cybersecurity programs based on these findings.

Keywords: cybersecurity, information security, digital forensics, focus group, qualitative, women in cybersecurity

INTRODUCTION

The complex and changing cybersecurity landscape requires the skills of talented information technology (IT) security professionals to prevent, detect, and handle cybersecurity incidents (NeSmith, 2018; Kauflin, 2017; Morgan, 2017). However, the cybersecurity industry is facing a serious and significant skills gap, with unfilled positions in many areas of the field (NeSmith, 2018). In 2017, approximately 780,000 people were employed in cybersecurity positions in the U.S., while 350,000 cybersecurity positions were left unfilled (Morgan, 2017). It is estimated that there will be 3.5 million unfilled cybersecurity jobs by 2021 (Morgan, 2017). It is critical to address this issue as the shortage of workers will leave corporate IT teams shorthanded while cyber attacks of all types are intensifying by increasing in both number and sophistication (Kauflin, 2017).

One of the issues surrounding the cyber skills gap stems from the shortage of cybersecurity programs in academia that can adequately prepare students for the challenging needs of the information security profession. The majority of cybersecurity degrees available today offer an outdated approach or struggle to keep up with changing technologies in the field ("The Cybersecurity Talent Shortage", n.d.). There is a critical need for cybersecurity programs that follow the rigorous guidelines of the National Cybersecurity Center of Excellence promoted by NIST ("National Cybersecurity", n.d.; "NIST Cybersecurity Framework", n.d.).

In addition, high schools have fallen short in promoting cybersecurity as a career choice. A majority of high schools do not make students aware of cybersecurity at all, offering no classes or programs in the discipline (Caldwell, 2013; "The Cybersecurity Talent Shortage", n.d.). Because of this, many students may not have a sense of the types of skills and competencies that they possess that might make them a good fit for a cybersecurity career. Cybersecurity should be promoted more heavily in high schools and could even be promoted earlier in primary school to foster interest in the field. The industry needs to do a better job of recruiting younger students by demystifying jobs in this area and showing that a career in this field can be interesting and rewarding as well as lucrative (Caldwell, 2013).

This study will attempt to address part of the cybersecurity skills gap by assessing the perceptions of students in a cybersecurity program about the skills, competencies, and interests that make them a good fit for the field.

Addressing these perceptions may help to guide future high school and university efforts at recruiting students into cybersecurity majors more effectively. In addition, the study will attempt to understand the perceptions of students about the cybersecurity programs at the researchers' university and their motivations for choosing one of these programs. This data will help to assess the programs and identify areas of improvement for both curriculum and recruitment. Three research questions were developed for exploration:

RQ1: What are students' perceptions of the skills, competencies, and interests that make them a good fit for the cybersecurity field?

RQ2: What motivated students to choose the Computer Forensics and Information Security (CFIS) or Information Security and Assurance (ISA) program?

RQ3: What are students' perceptions about the CFIS and ISA programs?

LITERATURE REVIEW

Cybersecurity Program Components

According to Dampier (2015), there are six essential elements needed to build a successful cybersecurity program which include faculty, courses, equipment and laboratories, students, budget, and credentials. The critical areas that must be covered in a cybersecurity degree come from several areas of computing including Security Policy and Law, Computer Security, Network Security, Digital Forensics and Cyber Physical Security (Dampier, 2015).
Included as part of the curriculum for Purdue University's Cybersecurity degree mimic those identified by Dampier (2015). The titles to the courses are slightly modified but they represent the same content: Network Security, Digital Forensics, Cybersecurity Policies, Cybersecurity Ethics and Law, and Information Systems Security (Purdue Global, 2018).

The National Cybersecurity Curriculum Program developed by the National Security Agency (NSA) has built a program which maps to the National Cybersecurity Workforce Framework which will prepare cybersecurity students for the workforce. In 2017, the NSA awarded 54 grants to universities that built recommended requirements into their cybersecurity curriculum. The NSA recommends courses in networking, forensics, national laws, regulations and policies, and classes on cyber threats and vulnerabilities among others (NSA, 2017).

Skills and Competencies

Haney and Lutters (2016) conducted a study to determine the skills and characteristics of successful cybersecurity advocates. The researchers conducted 19 semi-structured interviews which addressed work practices, professional motivations and challenges, characteristics of successful advocacy, and communication approaches. The outcome of the study concluded that successful cybersecurity professionals must possess innovative technical skills to help solve the problems associated with the field, along with soft skills so that they can address social and organizational factors.

A study on the future of the cybersecurity workforce suggests that the skills and competencies needed for successful cybersecurity experts go beyond technical skills. Those who hold jobs within the cyber realm need to have a combination of technical skills, domain specific knowledge, and social intelligence to be successful. Key traits determined from the study for those working in the cyber workforce include systemic thinkers, team players, possessing both technical and social skills, being loyal to the organization in which they belong, strong communication skills, and continual learners (Dawson & Thomson, 2018).

As listed in the cybersecurity workforce competencies report, leaders in cybersecurity, along with professionals and talent development leaders, were pulled together in a roundtable discussion to determine the competencies needed by cybersecurity professionals. The focus was to identify what academic institutions, employers, industry, and students can do to help bridge the gap in the workforce. The competencies were broken down into five tiers. Tier 1 is Personal Effectiveness Competencies which include interpersonal skills, integrity, lifelong learning, and professionalism. Tier 2 lists Academic Competencies such as writing, mathematics, science, communication, critical and analytical thinking, and IT user skills. Tier 3 is the Workplace Competencies which include teamwork, creative

thinking, problem solving, and working with tools and technology. Tier 4 is the Industry-Wide Technical Competencies which include cybersecurity, information assurance, risk management, incident detection and incident response, and remediation. Tier 5 is the Industry-Sector Functional Areas for those who have worked several years in the field. The skills identified are knowledge of operating and maintaining security, investigation, analysis skills, and the ability to oversee and govern the cybersecurity workforce (Phoenix, 2014).

Motivations for Students to Choose a Degree in Cybersecurity

Mavlik (2017) discusses the value of earning a cybersecurity degree, stating "the facts you can't ignore" about the value of a cybersecurity degree. The first reason is that cybersecurity jobs are on the rise. The U. S. Bureau of Labor Statistics (2019) projects an 18% increase in cybersecurity jobs through 2024. The second indicator is that cybersecurity professionals are needed in all industries. The third and fourth factors are companies are struggling to find qualified cybersecurity professionals, and employers are seeking candidates with cybersecurity degrees. The final three factors are that cybersecurity job opportunities increase with a person's level of education, cybersecurity professionals can expect above-average earnings, and that the field offers room for career advancement (Mavlik, 2017). The U.S. Department of Labor lists the median annual wages for cybersecurity professionals to range from $70,000 to $118,000. Students are attracted to the salary and career options in the field.

METHODOLOGY

Focus groups are a data collection method where the data is collected through a semi-structured group interview process. A focus group is a common qualitative research technique. It typically consists of a small number of participants, usually about 6 to 12, who share similar characteristics or common interests. Researchers use focus groups when they want to get more in-depth information on perceptions, insights, attitudes, experiences, or beliefs. It asks participants for open-ended responses conveying thoughts or feelings (Quain, 2019). The purpose of conducting a focus group is to listen and gather information. It is a way to understand how people feel or think about an issue, product, or service. They are used to gather opinions (Krueger & Casey, 2014). Exploratory research is an investigation into a problem or situation which provides insights to the researcher. It may use a variety of methods such as trial studies, interviews, focus groups, group discussions, experiments, or other tactics for the purpose of gaining information. Since we were exploring the perceptions of current students in cybersecurity degrees, we believe this method is a good fit for our study.

We conducted three separate focus groups, using the same structured protocol for all three groups. We asked 13 questions addressing our research questions to gather information about the Cyber Forensics and Information Security (CFIS) or Information Security and Assurance (ISA) major. We did audio record each of the sessions and detailed notes were taken as well. We conducted each focus group with at least one moderator and one note-taker. Each session was about 45 minutes long.

Students enrolled in the CFIS undergraduate major (approximately 159 students) and the ISA graduate program (approximately 30 students) were invited to participate in one of three focus groups in March 2019. The first focus group had four students (2 males, 2 females) participate. The second focus group had 10 students (8 males, 2 females) participate, and the third focus group had 11 students (9 males, 2 females) participate.

All of the data that was recorded was transcribed by a researcher on the team and checked by other members of the team for accuracy. Thematic analysis of the data was conducted. The first round of coding was done by each member of the team individually, both manually and using Dedoose software, and then came to a consensus. Next, teams of two developed the various themes. This was then verified together by all four members of the team.

RESULTS

RQ1: What are students' perceptions of the skills, competencies, and interests that make them a good fit for the cybersecurity field?

Our data analysis suggests four themes: Constant desire to learn, problem-solving skills, forensics mindset, and communications skills (see Table 1).

One of the major themes suggests that a desire to learn in an ever changing and constantly evolving world of information technology overall, and cybersecurity in particular, is important to succeed. The role of technology in business and society at large and its potential to impact business outcomes is growing exponentially and any professional who seeks a career in this area has to be agile, adaptive, and open to quick learning. Cybersecurity training does require and emphasize problem-solving skills. Students who are in the major have typically been interested in this major since high school. There have been many studies investigating beliefs and perceptions of students regarding the IT profession (Choudhury et al., 2010; Scott et al., 2009). Students described skills and competencies of IT professionals as technically oriented, critical thinkers, problem solvers, and good managerial skills (Warren et al., 2012).

Table 1. Perceptions of skills, competencies and interest for cybersecurity field

Research Question	Themes	Count	Participant Excerpts
RQ1: What are students' perceptions of the skills, competencies, and interests that make them a good fit for the cybersecurity field?	Constant desire to learn	9	"Look where we were 40 years ago, and look where we're at now. It's like, there's no stopping it. It's just taking over every little thing that we do. And I mean, the big challenge would be for any cyber forensics investigator – I don't care how good you are or not – you constantly have to learn new ways, because there are people out there that are finding new ways to do things."
	Problem-solving skills	6	"I think a lot of, especially in the IT world, you're going to come across a lot of situations and problems where you don't know exactly how to solve them and there's not just going to be here's this and it will tell you x, y, z and how to solve it."
	Forensics mindset	6	"I know how to look stuff up, but this aspect of the hacking thing is so completely foreign to me, so making that sort of mindset for me is a huge thing for me. I really, really want to learn that."
	Communications skills	3	"Definitely people skills. Working now in cybersecurity and seeing some people's ability, inability to speak to each other is one of the problems that I do see. We have a couple people from different schools that are just a completely different breed sometimes. And they don't know how to communicate their entire thought completely and thoroughly."

It is not surprising that "communication skills" has emerged as a theme in required skills for students to succeed in the cybersecurity field. The socio-technical nature of information systems requires a constant focus on the social aspects of any problem or solution in the field. Given that all controls and tools have to be effectively implemented to contain cybersecurity issues, it is imperative that soft skills, such as communication skills, play a critical role in the success of security programs (Dawson & Thomson, 2018).

RQ2: What motivated students to choose the CFIS or ISA program?

Focus group participants suggested the following reasons for choosing this program: Sense of job security, influence of social circle (friends, family, and colleagues), unique program with integrated option, and interest in field of security and forensics (see Table 2).

The number of available jobs in the cybersecurity and forensics area is greater than the supply of graduates who are trained to do these jobs. In this area, job security is strong for the incoming workforce as this growing field predicts more and more job additions in many years to come (Morgan, 2017). Cybersecurity has tremendous demand and growth and students feel drawn towards it as there is an abundance of opportunities professionally to grow.

Table 2. Motivations for choosing CFIS/ISA program

Research Question	Themes	Count	Participant Excerpts
RQ2: What motivated students to choose the CFIS or ISA program?	Sense of job security / Huge job opportunities	14	"I left because I was bored with my job, there wasn't anything left for me to learn. I knew I had to go back to school. And when I told everybody I was going into IT, one person told me that where the future is headed is IT security and that's the reason why I got into it."
	Influence of social circle (friends, family, colleagues)	13	"My sister also went here. She got her manufacturing and engineering degree here and also did track and field as well. She just had a phenomenal experience here and the job placement is just off the charts and they just do such a great job of just like shoving internships and job opportunities almost down your throat."
	Unique program with integrated option	12	"I actually sat down with the department head at the time and we had like a two hour long meeting and we kind of discussed the ABET accreditation, that was one huge factor in my decision of choosing this university. We talked about the fact that this university has the integrated program, making it easier for you to get your Master's in a shorter amount of time with the ability to use your scholarship."
	Interest in field of security and forensics	12	"..and I thought the modern way of the world is going toward everything cyber. I feel like if you don't know about it, you're already at a disadvantage, so and I also want to work for the government. So, knowing the cyber warfare and everything about that, that will just benefit me in the future."

The program has a strong presence in the local area and is perceived as a high quality school that delivers employment for its graduates. The placement rate of graduates from the computer information systems department have been above 90% for over a decade. The alumni and community strongly recommend the program to prospective students through a strong word-of-mouth promotion for the school.

The CFIS program offers a great mix of courses in the preventive and the investigative sides of security. One of the unique features of undergraduate program is the "integrated" option. This allows students who have earned 87 credits in undergraduate program and have a GPA of 3.0 or above to apply for a Masters' program in any of the six degrees offered through the department and get a discount of up to 6 credits on tuition. It allows any scholarship money that the student might have to be used towards the integrated option. The opportunity to be able to complete an undergraduate and a Masters' degree in a 4+1 years is attractive.

RQ3: What are students' perceptions about the Computer Forensics and Information Security (CFIS) and Information Security and Assurance (ISA) programs?

Participants had suggestions for improving the content offerings even though they did acknowledge that the strengths of the program outweigh the challenges, and they got quality education during their stay at this university. The themes that emerged from our data analysis for this question were: Need for more future-oriented course content and hands-on activities, different teaching styles of knowledgeable professors, focus on hands-on experience, and peers in major like family (see Table 3).

Table 3. Perceptions about CFIS and ISA programs

Research Question	Themes	Count	Participant Excerpts
RQ3: What are students' perceptions about the Computer Forensics and Information Security (CFIS) and Information Security and Assurance (ISA) programs?	Need for more future-oriented course content and hands-on activities	14	"And the problem is that I think, this university's classes and curriculum need to be geared more towards – I think these focus groups need to go on to determine – ok, what's going on in the real world, like I don't have a lick of Powershell scripting. Not. And that's like, it's being used every single day."
	Different teaching styles of knowledgeable professors	10	"But in terms of the program itself, the best teachers that I could ever ask for honestly, so all good stuff."
	Focus on hands-on experience	9	"And intro to computer forensics because we actually use software that they use in the real world like FTK, Splunk. So, I think that the program does a good job for preparing you for hands-on skills."
	Peers in major like family	5	"I can't tell you how many times I was struggling with an assignment and I just go to one of my peers, who isn't like a whiz at it, but we just like, put our minds together and trial and error and just figure it out. And when you do trial and error with a partner and you finally figure it out. Just the feeling is… like, you know what you're doing now. Just ok, this really makes sense and now you know what you're doing."

A major theme suggested the need to improve course offerings that are geared towards the organizations of the future. Students suggested that courses should be tailored towards what industry needs today and should have more hands-on activities associated with each course. The confidence level of students is boosted when they learn skills that fit into their expected jobs for the future. Participants did acknowledge that there are many courses that already use hands-on activities to learn concepts and they find those courses extremely useful. However, they do feel the need for more course work that simulates the real world environment in laboratories and helps them enter the workforce more prepared to do the job. Students seemed appreciative of professors' teaching styles and believed all professors were knowledgeable and were working towards making students' experiences better in the program. Another key strength identified for this program was the close bonding of students in the major due to their social organization.

DISCUSSION

There is tremendous media coverage about security breaches and cyber warfare, and this generates lots of interest in students about cyber-related topics. There is keen interest in students about everything cyber and there also exists a huge demand of jobs in this area. This state of demand-supply imbalance may have implications for years to come. It is critical that these implications for academic administrators, students, and industries be critically assessed and acted upon urgently. This study identifies student perceptions about skills, competencies, and interests for

cybersecurity. It also categorizes and prioritizes components of programs that work and do not work. Table 4 below presents prescriptive strategies for academic administrators to attract and retain students in cyber security related majors and develop outstanding cyber security professionals.

Table 4. Strategies Prescribed for Academic Administrators and Educators

RQ1: What are students' perceptions of the skills, competencies, and interests that make them a good fit for the cybersecurity field?	
Themes	**Recommendations (for academics)**
Constant desire to learn	Create course assignments that reflect current issues in the cybersecurity field; Strive to teach the tools and techniques used in the field
Problem-solving skills	Challenge students with applied problems in the field in form of case studies; Hold local and regional competitions
Forensics mindset	Provide opportunities for investigative work; Provide opportunities to be creative in analyzing situations
Communications skills	Provide group projects and presentation opportunities
RQ2: What motivated students to choose the CFIS or ISA program?	
Themes	**Recommendations (for academics)**
Sense of job security / Huge job opportunities	Show the supply gap for employment to guidance counselors, etc., to increase awareness; Provide opportunities to work together to create quality cyber security professionals
Influence of social circle (friends, family, colleagues)	Create strong reputation in local area; Maintain good alumni relations
Unique program with integrated option	Emphasize unique mix of security and forensics courses; Provide creative solutions to projects/assignments
Interest in field of security and forensics	Develop relationships with local school districts to promote awareness; Provide bridge courses at high school level
RQ3: What are students' perceptions about the Computer Forensics and Information Security (CFIS) and Information Security and Assurance (ISA) programs?	
Themes	**Recommendations (for academics)**
Need for more future-oriented course content and hands-on activities	Develop courses in latest technologies with emphasis on hands-on activities. Example: AWS and security, Blockchain, PowerScript, and Python
Different teaching styles of knowledgeable professors	Provide exposure to content through a variety of professors and teaching styles
Focus on hands-on experience	Provide more hands-on experience in software tools and techniques
Peers in major like family	Provide opportunities for students to bond and learn from each other; Group projects, clubs, and trips to relevant events could help to build a student community

The implications of this study are manifold. First, this exploratory study identifies components of cyber security programs that are attractive to students. This is a unique contribution to the body of knowledge in this domain. Second, it provides insights to academic administrators for tailoring their program offerings accordingly to recruit students from high schools. Third, it provides a unique set of strategies for administrators to utilize in understanding, retaining, and training current and future students that would prove critical in contributing to the work force of the future.

A major limitation of the study is that all the participants are from one university and do not necessarily reflect aspirations of students at other institutions. Also, in this qualitative study, researcher bias could be reflected as the researchers are the instruments used to conduct the data collection and analysis. However, a bias of this nature is

inherent to this method of research. Future studies with students from multiple universities participating and using variety of research methods is warranted.

CONCLUSION

Our results coincide with the literature on skills and competencies needed for successful cybersecurity professionals and reinforced the idea that communication skills are critical (Haney & Lutters, 2016; Dawson & Thompson, 2018). In addition, while the literature did also note critical and analytical thinking as well as problem solving as key skills for cybersecurity, our study found students using the term "forensics mindset" which implies many of the same qualities with more emphasis on an investigative approach. A deeper understanding of students' perceptions of the skills, competencies, and interests that will help them to succeed in the field of cybersecurity can also be insightful for recruiting for the field.

Based on the results of this study, some of the most important recommendations for building successful cybersecurity programs include an effort to teach with tools and techniques that are up to date and used in industry, to provide a plethora of hands-on activities in a variety of courses, to offer courses using different teaching styles, and finally, to foster a sense of community amongst students within the program.

REFERENCES

Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions). (2019). Statista. Retrieved from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security. 2013*(7), 5-10. Retrieved from http://www.firemon.com/wp-content/uploads/2013/09/Article_-_Plugging_the_cyber-security_skills_gap.pdf

Choudhury, V., Lopes, A. B. and Arthur, D. (2010) IT careers camp: An early intervention strategy to increase IS enrollments. Information Systems Research, 21, 1, 1-14.

De groot, J. (2019). The history of data breaches. Digital Guardian. Retrieved from https://digitalguardian.com/blog/history-data-breaches

Dampier, D. (2015). Building a successful cyber-security program. *Distributed Analytics and Security Institute, Mississippi State University.* Retrieved from http://www.dasi.msstate.edu/publications/docs/2015/06/13502Cyber_Security_Workshop_paper_-_Final.pdf

Dawson, J. & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology.* Issue 9: 744. Published 2018 June 12.

Finkle, J. (2018). Medtronic disables pacemaker programmer updates over hack concern. Retrieved from https://www.reuters.com/article/us-medtronic-cyber/medtronic-disables-pacemaker-programmer-updates-over-hack-concern-idUSKCN1ML2GR

Fruhlinger, J. (2018). The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the Internet. Retrieved from https://www.csoonline.com/article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Haney, J., M., & Lutters, W.G., (2016). Skills and characteristics of successful cybersecurity advocates. Retrieved from https://www.usenix.org/system/files/conference/soups2017/wsiw2017-haney.pdf

IBM. (2018). 2018 cost of a data breach study: Global overview. Retrieved from https://www.ibm.com/downloads/cas/861MNWN2

Kauflin, J. (2017). The fast-growing job with a huge skills gap: Cyber security. *Forbes*. Retrieved from https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#5b1a9d65163a

Krueger, R. & Casey, M.A. (2014). *Focus groups: A practical guide for applied research.* Washington, D.C.: Sage.

Mavlik, C. (2017). Is a cyber security degree worth it? The facts you can't ignore. Rasmussen College. Retrieved from https://www.rasmussen.edu/degrees/technology/blog/cyber-security-degree-worth-it/

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

National Security Agency (2017). National Cybersecurity Curriculum Program.

National Cybersecurity Center of Excellence. (n.d.). Retrieved from https://www.nccoe.nist.gov/

NIST Cybersecurity Framework (n.d.). Retrieved from https://www.nist.gov/cyberframework

NeSmith, B. (2018). The cybersecurity talent gap is an industry crisis. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#41efe27ca6b3

Purdue Global (2018). Bachelor of science in cybersecurity. Retrieved on April 15, 2019 at https://www.purdueglobal.edu/degree-programs/information-technology/bachelors-cybersecurity.pdf

Quain, S. (February 12, 2019). The focus group research method, from https://smallbusiness.chron.com/focus-group-research-method-17464.html

Scott, C., Fuller, M. A., MacIndoe, K. M., and Joshi, K. D. (2009) More than a bumper sticker: The factors influencing information systems career choices, Communications of Association for Information Systems, 24, 15, 7-26.

The cyber security talent shortage: What's academia got to do with it? (n.d.). Retrieved from https://onlinedegrees.sandiego.edu/education-and-cyber-security-talent-shortage/

U.S. Bureau of Labor Statistics (2019). Occupational outlook handbook: Information Security Analysts. Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

University of San Diego. 92019). 6 reasons why women should consider a career in IT https://onlinedegrees.sandiego.edu/women-cyber-security-reasons-to-enter-field/

University of Phoenix & ISC2, (2014). Cybersecurity workforce competencies: Preparing tomorrow risk-ready professionals. University of Phoenix Executive Summary Report. Retrieved from file:///C:/Users/Karen/Research/2019-2020/University-of-Phoenix-ISC2-cybersecurity-report.pdf

Warren, J., Young, D., and Williams, K. (2012). Personality, gender and careers in information technology. AMCIS 2012 Proceedings. 12. http://aisel.aisnet.org/amcis2012/proceedings/ISEducation/12