Issues in Information Systems
Volume 24, Issue 3, pp. 83-96, 2023

DOI: https://doi.org/10.48009/3_iis_2023_108

A study of female cybersecurity professionals

Kembley Lingelbach, *Middle Georgia State University, Kembley.lingelbach@mga.edu*

Abstract

The purpose of this study is to explore what can be done to improve the number of qualified women working in cybersecurity and to investigate why there are so few of them. Twelve female cybersecurity experts were interviewed for this study using a grounded theory methodology to understand their perspectives on their views of the field. Participants shared ideas for encouraging more women to work in cybersecurity. The study's findings revealed four engagement elements and one unanticipated co-factor that are thought to affect individuals' inclinations to pursue careers in cybersecurity. The four factors—awareness, support, intrinsic and extrinsic values—were discovered. The intriguing discovery of the cybersecurity mindset profile component, which is thought to improve career trajectory success, calls for more investigation to learn the effects on the choice to enter the cybersecurity industry. Women now have a voice in suggesting ways to encourage other women to seek careers in cybersecurity as a result of the influence of this research. The study also aids in demystifying the components' complexity by categorizing and arranging them systematically to generate a theoretical model that will offer academics, and practitioners, a comprehensive understanding of how to educate future cybersecurity experts.

Keywords: cybersecurity, gender, grounded theory, profile mindset factors, cybersecurity engagement model

Introduction

The workforce in cybersecurity still suffers from the substantial underrepresentation of women. This contributes to the general labor deficit in the industry, which is becoming worse. Since there is a growing need for cybersecurity personnel, this issue needs to be thoroughly explored. According to the US Bureau of Labor Statistics, labor is scarce, with over a quarter of a million open positions in the US alone and a growth of 18% from 2014 to 2024. ISC2's 2015 Global Information Security Workforce Study found that supply lagged behind demand, with just around 10% of workers being women (Suby, 2015a; Suby2015b). In 2017, there was an increase to 11% however, continued to be underrepresented (Frost & Sullivan, 2017). Cyberseek.org indicated the demand increased by 534K to over 750K in 2022 (Cyberseek.org). However, by 2021, the ISC2 Workforce study found that women made up around 24% of the workforce, but that their salaries did not differ from those of their male colleagues (ISC2, 2021).

This study looked promising, however, beginning with the 2019 ISC Workforce study, the research methodology had been modified. ISC2 posits that "to fully understand cybersecurity needs and behaviors in the business sector,' the survey now includes "a global mix of certified professionals in official cybersecurity roles and IT/ICT professionals who spend at least 25% of a typical week handling responsibilities related to cybersecurity where the participants were now questioned whether they perform any type of security related skills based on a percentage of the work function (ISC2, 2019, p.4). This methodological change doubled the participation rate from 2018 (1,452) to 3,237 in 2019 as well included

those participants where a portion of the job skills were connected to security, rather than only cybersecurity is included in the 24% increase (ISC2, 2019, p.4).

Research Goal

The main goal of this research study is to investigate the reasons why few qualified females are not entering the cybersecurity workforce and determine what can be done to increase their numbers. Based on the development of a grounded theory from interviews with females in the cybersecurity field, the information gained provided the factors that can impact decisions to enter and stay in the cybersecurity field (Lingelbach, 2018). This investigation focused on qualified females who are not entering or are underrepresented in the cybersecurity workforce. Another goal, as a result of this research, is to provide holistic insight to academicians, and practitioners to develop programs that will help balance the gender disparity. Parts of this work have been submitted in partial fulfillment of the requirements for a Doctor of Philosophy degree, at Nova Southeastern University.

Research Questions

Main Research Question

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

Sub or probing interview questions

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

Relevance and Significance

According to D'Hondt (2016), the United States is struggling to find, keep, and train the future cybersecurity specialists needed to safeguard the country's vital infrastructure. It is believed that this study can provide strategies to encourage women to pursue careers in cybersecurity. Additionally, by comprehending the nature of female cybersecurity experts, one may get insight into the phenomena, and knowledge of the causes that affected their decision to work in the sector. According to Caldwell (2013) and Ingalhalikar et al. (2014), this type of study can help provide organizations, academia, and the government a framework for attracting, retaining, and developing female cybersecurity professionals who would then offer unique and innovative solutions from a female viewpoint.

With a theoretical framework based on the data that defines the wide range of elements reported in past studies, this research intends to expand the body of academic knowledge and develop a more insightful, succinct theory. Females in cybersecurity will not only close the gender gap but also widen the pool of future cybersecurity experts, and produce more creative solutions in the long run, which has important ramifications for the sector as a whole (Frost & Sullivan, 2017).

The workforce deficit and its implications for the cybersecurity industry can be detrimental to the defense of the country and its citizens. Professionals in cybersecurity are essential for resolving security issues when new information technologies are implemented in enterprises (LeClair et al., 2014). Women working in cybersecurity could mitigate gendered prejudices about science and improve future female cybersecurity employees' implicit affiliation with it (LeClair et al., 2014). Al-Alawi et al., 2023 suggests that women still

face challenges limiting their careers in the cybersecurity banking sector (p. 19). Some of these challenges include societal support, raising awareness that the cybersecurity field is not limited to only males, work-life balance, sufficient technical knowledge, and organizational support. They also suggest "the role of empowering women in the field is a continuous process of improvement, and with hard work and empowerment, women can contribute and have significant roles" (p.19).

Review of Literature

A review of the literature that has been pertinent to the issue of why women are underrepresented in the cybersecurity industry is offered. The limited research published in this field primarily focuses on self-efficacy and student motivation (Amo, 2016; Bashir, Wee, Memon, & Guo, 2017; Lishinski, Yadav, Good, & Enbody, 2016; Roach, McGaughey, & Downey, 2011), lack of encouragement from families (Ashcraft, Eger, & Friend, 2012; D'Hondt, 2016, Fisher, Lang, Craig, & Forgasz, 2015; Wang, Hong, Raviz, & Ivory, 2015), organizational culture and cultural barriers, knowledge, skills and abilities (KSAs) (Al-Alawi, Al-Khaja & Mehrota, 2023; Ashford, Koohang & Floyd, 2012; Bagchi-Sen et al., 2010; Huang & Bashir, 2015; Levy, 2005; Ramim & Levy, 2015; Smith, Koohang & Behling, 2010; Trauth & Quesenberry, 2007; 2023), the education system, and lack of female role models or mentors (Huang & Bashir, 2015; LeClair et al., 2014; Jethwani, Memon, Seo, & Richer, 2017), as well as conscious and unconscious discrimination and retention factors (Frost & Sullivan, 2017), were prominent in the list of factors and barriers limiting women in the cybersecurity field.

According to Trauth & Quesenberry (2007), it is difficult to pinpoint a single element as the fundamental cause of the underrepresentation of women in the field, making this a complicated, and difficult subject of research. To comprehend the gender gap in IT areas, they offered an overview of three theoretical perspectives: the essentialist theory, the social construction theory, and the individual differences theory. Trauth and Quesenberry (2023) focus on environmental or cultural, identity, and individual influences that may that determine a female's decision to pursue a STEM or IT career. They contend that essentialist and social constructionist theories lack the analytical rigor needed to consider more complex managerial suggestions. Additionally, they show how the individual differences theory of gender may greatly influence the reconfiguration of analytical understanding of the IT gender gap and inspire creative management strategies (Trauth & Quesenberry, 2007; 2023; Quesenberry & Trauth, 2007; 2012). In summary, Trauth and Queensberry's theoretical perspectives encompass essentialist theory, social construction theory, and individual differences theory. Here are the key points of each theory:

- **Essentialist Theory**
  - Assumes that there are inherent, fixed, and natural differences between individuals.
  - Attributed these differences to essential characteristics such as biological or genetic factors.
  - Emphasizes the stable and unchanging nature of these essential differences.
  - Argues that essential differences influence behavior, performance, and outcomes in various domains.
- **Social Construction Theory**
  - Views differences between individuals as socially constructed and influenced by societal norms, values, and beliefs.
  - Asserts that categories and classifications of people are created and maintained through social processes.
  - Emphasizes the role of cultural, historical, and social contexts in shaping individual identities and differences.
  - Recognizes that social constructions can change over time and vary across different societies or communities.

- **Individual Differences Theory**
    - Focuses on the uniqueness and variation among individuals.
    - Considers personal attributes, experiences, skills, abilities, and personalities that distinguish individuals from each other.
    - Recognizes that individual differences impact behaviors, attitudes, performance, and outcomes.

These theoretical perspectives provide differing views on the nature, and origins of differences among individuals. While essentialist theory emphasizes inherent and fixed differences, social construction theory highlights the influence of societal processes, and individual differences theory focuses on the unique characteristics of individuals. Understanding these perspectives helps in exploring, and explaining the complexities of human differences. However, according to other research, promoting female involvement in the information technology, and cybersecurity industries will be more successful if similarities rather than gender discrepancies are identified (Frieze & Quesenberry, 2015).

According to positivist studies on technology adoption, research on gender, and IT frequently focuses on gender disparities (Olbrich et al., 2015). A qualitative approach to methodology, according to Trauth, "will bring more richness in the data" and "present more nuances than just research in gender, and IT use research" (Olbrich et al., 2015, p. 37). Trauth contends that earlier gender research, and information systems were primarily quantitative and focused on gender differences, but over time shifted to focus only on women. There are many practitioner and industry research studies on STEM disciplines, which cover engineering and computer areas as a whole rather than the cybersecurity sector alone, according to a survey of practitioners, and academic literature. Frieze and Quesenberry (2015) and Olbrich et al (2015) both make significant contributions to promoting female involvement in information technology (IT), and emphasize the importance of qualitative research in the field. Frieze and Quesenberry (2015) focus on the barriers that hinder womens' participation, and highlight the significance of addressing these barriers to encourage, and support more women to pursue careers in IT. Their research sheds light on gender biases and stereotypes that exists in the IT industry and provides insights into strategies for overcoming them.

On the other hand, Olbrich et al (2015) emphasizes the importance of understanding the experiences and perspectives women in IT. They argue research alone may not capture the nuanced challenges and opportunities faced by women in the field, and that by using qualitative research methods, such as interviews and observations, would provide a deeper understanding of the factors that influence women's involvement in IT, and offer recommendations for fostering gender diversity in the industry.

Overall, both of these studies contribute to the advancement of female involvement in IT by identifying complex barriers and offering insights into the experiences of women in the field. They also highlight the importance of qualitative research in gaining a comprehensive understanding of the issues, and to provide effective strategies for promoting gender diversity in IT. The gaps in the literature indicate a lack of understanding of cybersecurity, and its complexities compared to other STEM fields, as well as a lack of qualitative research to give the depth and dimension of the concerns (Trauth & Quesenberry, 2007; Olbrich et al., 2015).

It may be that female students are unaware of the employment options available to them, since research on gender problems in cybersecurity is underdeveloped in terms of creating the domain's specific framework or theories, and increasing awareness of this relatively young sector. Women may be discouraged from entering the sector of cybersecurity due to their lack of awareness of the intricacies of the field itself. This would imply that a requirement for the understanding of the cybersecurity discipline exists.

Methodology

This study employed grounded theory to understand the perspectives of the participants, and explore the process in depth (Creswell, 2009, 2013). Grounded theory is best used for understanding, and describing the common meaning of the lived experiences of individuals who share similar experiences (Charmaz, 2014; Creswell, 2013). It also allows for the elaboration of perceptions, and views to emerge into patterns, and themes (Creswell, 2009, 2013). An Institutional Review Board (IRB) reviewed, and approved this grounded theory research project, which involves conducting interviews with female cybersecurity professionals.

After a thorough evaluation, the IRB has determined that there are no apparent risks to the participants involved in this research. The research complied with ethical guidelines, and ensured the confidentiality, and anonymity of the participants, as well as obtained informed consent prior to conducting the interviews. Recruitment was accomplished through the cybersecurity forums and seminars in the southeastern United States targeting female cybersecurity professionals in the defense industry, United States Air Force civilians, and military. Brochures and flyers announcing the research were distributed to attendees. Detailed recruitment letters with informed consent forms were sent to volunteers via email to those participants that responded to the flyers' call for participation.

The sample is a purposive sample type of 12 female cybersecurity professionals who have been in the cybersecurity field for at least one year, and is over the age of 18. Recorded face-to-face interviews were scheduled, and conducted in a public library for convenience. The interview protocol consisted of open-ended questions with numerous guiding, and probing questions. Validity, transparency, and rigor of the data analysis was employed through member checking. This process was accomplished by sending the participants their transcripts via email for review prior to data analysis .

Results

Data analysis begins with data collection of the 12 interviews, professionally transcribed. The interviews were gathered over 4 weeks, and were seven to 31 minutes in total recording time. The transcripts were the raw data which consisted of 112 transcript pages.

Demographic Analysis

The demographic analysis of the participants were the ages of mid-20s to 64 years of age, college education, and certifications, and all were either federal government or defense industry cyber security professionals. The data coding analysis results from classic grounded theory processes of open, selective, and theoretical coding. See Table 1. The demographic data were gathered during each interview, recorded in the transcript, and entered into a spreadsheet. Table 1 provides an understanding of the participant data set.

The ages of the participants ranged from 26 to 62, and over 75% were over the age of 40. 83% of the participants were federal government cybersecurity professionals, and 17% were defense contractors in the cybersecurity field. 75% of the participants possessed Security+ certifications, and all but two had more than one certification; only one participant did not possess a certification and was a mid-level manager of a cybersecurity office.

Table 1. Descriptive Statistics for the Population (N=12) (Lingelbach, 2018)

Age	*N*	Percentage (%)
25-34	2	17%
35-44	3	25%
45-54	3	25%
55-59	2	17%
60-64	2	17%
Academic Level	**N**	**Percentage (%)**
Undergraduate Degree	6	50%
Graduate Degree	6	50%
Security Certification	***N***	**Percentage (%)**
Security+	8	66%
CISSP	3	25%
CISM	1	8%
CAP	1	8%
Test Out Security Pro Certified Computer User	1	8%
Industry	***N***	**Percevntage (%)**
Federal Government	10	83%
Defense Industry Contractor	2	17%

Education levels varied from Associate's to Master's degrees and in varied fields. Fifty percent possessed a Master's degree and ranged from Master in Information Technology, Information Technology Management, Information Systems and Technology Management, Business Administration, Cybersecurity, and Business. The other six participants had undergraduate degrees ranged from fields such as Computer Science, Accounting, Chemical Engineering, Business Administration, Information Technology, Geology, and Pre-Med (Biology).

Thematic Analysis

The initial or open coding stage of analyzing data is where the data are coded for all possibilities (Glaser, 1978). In this phase, the data was analyzed line-by-line. The initial coding procedures generated 33 codes with 758 occurrences. These open codes were then categorized into 14 subgroups, and through axial coding further classified the open codes into 8 axial codes. The selective coding phase allows the researcher to code only the data that sufficiently relates to the core category, called inductive methodology. In this phase, the focus is on a core category (Glaser, 1978). The researcher continues to saturate the core category and related categories, delimiting data collection, and analysis to establish the boundaries of an emerging theory. Once theoretical saturation is reached, the researcher begins theoretical coding to outline a theory. Theoretical saturation was achieved by the 12th interview as data was found to be recurring with no new concepts noted.

Strategies and Engagement Factors

The factors that attract or draw females to the cybersecurity field are the main research issue. The

overarching themes across all participant perceptions were awareness, support, and intrinsic, and extrinsic factors. The following is an example of each theme and examples of participants' quotes to illustrate the findings are grounded in the data. Table 2 presents the selective codes, occurrences, and factors for attracting females to the field. This indicates that awareness, exposure, and support can affect negatively or positively the participation rate.

Table 2. Summary of Theoretical Codes – Attraction Factors (Lingelbach, 2018)

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

The themes that emerged from the coding process were considered strategies of attraction or engagement factors:

Awareness

The participants suggested an awareness that includes early exposure and education will increase confidence and interest in cybersecurity. One participant stated her idea of educating girls early: "Early education, like elementary age, having girls participate in computer-related activities". Another participant stated, " I would say, too—like you were saying earlier about the programs and stuff, the STEM programs for girls. They didn't have that when I was growing up. I think that would help increase females coming into the industry." Yet another participant suggests that awareness and exposure can benefit girls pursuing cybersecurity through programming programs: "I like the outreach programs that they have as Girls Can Code. I love that. So those types of things to start them [female students] when they are younger and develop them to get excited about cybersecurity and the computer industry."

Support

The support theoretical code includes groups such as networking groups, cybersecurity conferences, and industry conferences, STEM programs, family influences as well as role models and mentors were suggested to help young girls become aware of cybersecurity. For example, one participant believed that opportunities, and role models will help girls become engaged: "When I used to fence, my fencing coach said, 'If you want girls to do something, you provide them with a group to do it in and let them have fun, and they'll do anything. He was a world-class coach. And I think providing girls with that opportunity, and also providing them with role models, really helps a lot.' Another Participant believed support groups, mentoring, and visiting the schools will help: 'Support groups, mentoring, actually going to the schools, engaging early and letting them see a woman in the field". Another participant agreed that women mentors and role models are needed: 'And have women mentors and things like that. I think that seeing a woman is encouraging on its own, but to see a woman in the cybersecurity field and they may say, hey, I want to be like her.'

There was an overall consensus that family influence, and having a computer in the home affected attraction to the cybersecurity field. One participant suggested that how you were raised may have affected how she views herself and does not see that she is any different from a man: 'Okay, another thing I would say is that it is how you were raised. I was raised by my dad. My mom worked primarily all of the time, so it was my dad and my three brothers. So, I didn't see myself as being any different than them, so if something happened

along the way as far as some type of discrimination because I'm a female, I wouldn't even notice it because I was raised that anything a man can do, I can do better.'

Intrinsic

Several intrinsic factors were seen by the participants as being instrumental in attracting females to the cybersecurity field. Those factors include having a natural interest in the field and seeing cybersecurity as fun, exciting, challenging, and rewarding. Almost all participants agreed there must be an interest in technology, and computers. Having a natural interest and affinity to computers, networking, and cybersecurity is what led some of the participants to the cybersecurity field as stated: 'I guess that's what I grew up doing unconsciously, and then when I went to think about, well, what do I want to study? what do I want to do? I was well, cybersecurity. Here are two of my favorite things that I like to do. Yeah, I think some of the interest will be natural…'

Several other intrinsic factors were seen by the participants as being instrumental in attracting females to the cybersecurity field. Other factors include not only having a natural interest in the field, but also seeing cybersecurity as fun, exciting, challenging, and rewarding. One participant believed that cybersecurity is fun: 'It's not just a matter of numbers and coding and programming and knowing the hardware. It's a higher level of thinking that's, yeah, interesting and fun. So just continue putting it out there that this is something they [girls] can do and it is fun. If they like puzzles, like problem-solving, brain puzzles…then, it's a good place to be.'

Extrinsic

Extrinsic factors such as salary, opportunities, independence, and sense of contribution were discussed as being beneficial to engaging girls to pursue the cybersecurity field. One participant felt like she is contributing to something worthwhile: 'I feel like I get to contribute in a way that matters. I mean, you know, I've had some jobs that I felt like, you know, I'm not doing anything, you know, that's worth anything and I feel like, you know, in this way I feel like I'm contributing toward something.' Another participant thought cybersecurity is the best job and the salary is attractive: 'Pay scales are great, especially in the civilian world, for cyber, and I got into IT because I was 28 years old, about to be divorced, and I needed a job, and a career that would pay well. So, I flipped through college catalogs, and I thought this is what I want to do. And oddly enough, I've enjoyed every minute of it. It's the best job anybody could have.'

Cybersecurity Profile and Mindset

A contributing factor emerged that was an unexpected theme consisting of a cybersecurity profile mindset where the participants believed that a female would need to possess certain characteristics to be successful in the field (Lingelbach, 2018). Those personal characteristics were found to be assertiveness, analytically minded, technically savvy, and self-efficacy factors. Another personal characteristic the participants felt that may impact females' entrance into the field is profile fitness for the field. Participants felt that females that 'fit a profile' will provide successful entry and retention in the cybersecurity field (Lingelbach, 2018). Such profile characteristics include personal interests, knowledge, skills, and abilities, prior experience, assertiveness, personality, and self-efficacy factors.

Prior research indicates that if a person fits a certain profile, and possesses soft skills, not just technical skills, they may have a successful entry into the cybersecurity field (Dawson & Thompson, 2018; Merhout, et al., 2009; Wee, et al., 2016a, 2016b). See Figure 1. All participants believed that on some level, personal characteristics, and mindset will contribute to the engagement of females in the cybersecurity field. The cybersecurity mindset factors include personal characteristics, and factors that will make it possible to

succeed in the cybersecurity field. Other prior research suggests a certain work-role fit will enable successful access to cybersecurity (Bagchi-Sen et al., 2010; Dawson & Thomson, 2018). Cybersecurity professionals should be similar to the networks they operate; they must be reliable, trustworthy, and resilient (Dawson & Thomson, 2018).

Factors of Authentication - Something You Have, Something You Know, and Something You Are

Analogous to the three factors of authentication: something you have, something you know, and something you are, aligns neatly with the cybersecurity mindset perceived to be factors of a successful cybersecurity career trajectory (figure 1). Dawson and Thomson (2018) also suggest, "There exists a requirement for systemic thinkers, team players, a love for continued learning, strong communication skills, a sense of civic duty and a blend of technical skills, and social skills" (p. 1). They also suggest that researchers should focus on, not only the technical skills for the future cybersecurity workforce, but also the organizational fit, personality traits, and values. Penn and Lent (2018) also agree that self-efficacy, and personality have an impact on career decisions. This cybersecurity mindset construct emerged through the research on engaging females in the field, and suggests by the data that fitness of the cybersecurity profile will enable successful a cybersecurity path.

Figure 1 illustrates the personal characteristics, cognitive, and social skills as well as experience factors that play an important role in a successful journey to the cybersecurity field. All participants' perceptions indicate that some level of personal characteristics will contribute to engaging females in the cybersecurity field. One participant believed: "If I wasn't personally technically savvy, why would I choose to be in the [cybersecurity] field?"; while another stated that self-efficacy played a role in engagement: "If they want to say something they speak their mind. And I think that could be a barrier if a woman is not prepared and equipped to trust in herself and trust and be self-confident and just push forward, you know. But I believe if we start educating our girls early, they get the confidence, self-esteem, and knowledge, and then they're unstoppable. I just think they'll be unstoppable and they can go in any direction they want. Get confidence in them and tell them they're just more than, you know, just a female, and most of all you're just a female mind—I've heard that one as well! And so, yes, a powerful female mind. And take whatever that negative comment is, make it positive, make it work for you."

Another participant explained communication, awareness, and understanding the field are important: "I keep mentioning communication, understanding, awareness, and training. All those things to me are key". Other participants believed personality and physical appearance may affect pursuing the field: "I think, you know, sometimes if you have a meek, mild-mannered female, it might not bode well and they may go home crying at night". Another participant listed knowledge, skills, and abilities would result in successful cybersecurity professionals: "So, if we can, you know, track that somehow to what the KSAs are, what's your person's knowledge, skill, and abilities are, we may be more successful in the field".

One participant stated that because of the way a female looks, may affect how people view them: "Well, and it's like sometimes, you know—like I think one time, there was a pretty girl and they're like oh, yeah, she doesn't know anything about IT. So, sometimes I feel like, I do get taken advantage of—I mean, not taken advantage of but taken a little bit more seriously because I'm not, you know, super pretty". However, other factors include having experience, another participant indicated: "So, I mean, it [cybersecurity] does require you to have, especially the Government require[s] you to have certifications. And so that's a lot of training, especially if you don't have any hands-on IT background experience. I found having the hands-on experience to be probably one of my biggest challenges. I mean, I had to learn Linux commands and things that I—that wasn't something I had done before. But everything you look at [job listings] says they want you to have experience first."

Figure 1: Cybersecurity/Profile Mindset Authentication Factors (Lingelbach, 20218)

Theoretical Model

The resulting Cybersecurity Engagement Model (CEM) in Figure 2 is presented based on the evidence grounded in the data. The theoretical framework indicates strategies and engagement factors together with a cybersecurity profile mindset will enable a successful cybersecurity career trajectory.

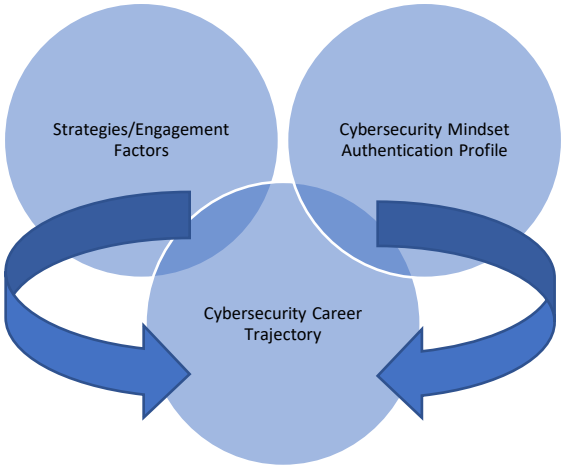

Figure 2: Cybersecurity Engagement Model (CEM) (Lingelbach, 2018)

Cybersecurity Career Trajectory

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

The model in Figure 2 indicates if the strategies, and engagement factors are in place along with the cybersecurity profile or mindset, then a successful cybersecurity career path is possible. Notice all three parts of the model overlap, this means that these three factors are interrelated and should be maintained throughout the career. In a technology career, one must keep abreast of current technology changes continuously or cease to be relevant. This model assumes the cybersecurity professional will be successful by utilizing the factors of the model throughout their career.

Implications and Conclusions

This study was a grounded theory research designed to discover insightful information from seasoned female cybersecurity professionals that will enable the advancement of females in the field. These findings contributed notably to the body of knowledge, and have several implications for providing other researchers and practitioners insight into the perceptions of female cybersecurity professionals and strategies to encourage them to pursue the field. The results make it evident, through the beliefs of 12 women, that women can do cybersecurity well. Generating an interest early in a girl's life can bring more women to the field, therefore, reducing the overall shortages in the United States and worldwide. Moreover, the results can be utilized to reduce the gender disparity in the cybersecurity field.

This study may have implications in other male-dominated career fields, as well, where the theoretical model can be applied to increase female participation rates. Future research is recommended in the area of validating the theoretical model with particular attention to the cybersecurity mindset profile characteristics. Other research recommended is completing studies of both male, and female participants in the field, and broader industries to determine if the conclusions with one group are representative of another group's experiences. In conclusion, the findings of this study have reinforced prior research that increasing an interest early in a young girl's life can bring more women to the cybersecurity field. While this research has provided a narrative of actual experiences, it most importantly has provided personally revealed reasons for females to pursue the field of cybersecurity. The results unveiled several areas for consideration for faculty, and higher education administrators, and practitioners when developing future cybersecurity professionals.

References

Al-Alawi, Al-Khaja, N. A., & Mehrotra, A. A. (2023). Women in Cybersecurity: A Study of the Digital Banking Sector in Bahrain. *Journal of International Women's Studies*, *25*(1), 1–20.

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

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

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

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

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

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

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

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

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

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

Cyberseek.org (2022). Hack the gap. Retrieved from https://www.Cyberseek.org

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

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

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

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

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

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

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

(ISC)2 Cybersecurity Workforce Study, 2019. Strategies for Building and Growing Strong Cybersecurity Teams. Retrieved from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482

(ISC)2 Cybersecurity Workforce Study, 2021. A Resilient Cybersecurity Profession Charts the Path Forward. Retrieved from https://iapp.org/media/pdf/resource_center/ISC2_Cybersecurity_Workforce_Study_2021.pdf

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

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

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

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

Lingelbach, K. K. (2018). Perceptions of female cybersecurity professionals toward factors that encourage females to the cybersecurity field (Doctoral dissertation, Nova Southeastern University).

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

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

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

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

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

Quesenberry, J. & Trauth, E. M. (2012). The (dis)placement of women in the IT workforce: An investigation of individual career values and organizational interventions. *Information Systems Journal*, *22*(6), 457-473. doi:10.1111/j.1365-2575.2012. 00416.x

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

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

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

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

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

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

Trauth, E. M., & Quesenberry, J. L. (Eds.). (2023). Handbook of Gender and Technology: Environment, Identity, Individual.

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

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

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

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