Skills and Characteristics of Successful Cybersecurity Advocates

Julie M. Haney
University of Maryland, Baltimore County
1000 Hilltop Circle
Baltimore, Maryland
jhaney1@umbc.edu

Wayne G. Lutters
University of Maryland, Baltimore County
1000 Hilltop Circle
Baltimore, Maryland
lutters@umbc.edu

ABSTRACT
Cybersecurity advocates attempt to counter the tsunami of cyber attacks by promoting security best practices and encouraging security technology adoption. However, little is known about the skills necessary for successful advocacy. Our study explores the motivations, characteristics, and practices of cybersecurity advocates. Preliminary analysis of 19 interviews reveals that effective advocates must not only possess technical and soft skills, but also customer service orientation and context awareness. However, little cybersecurity training is available to develop these non-technical skills. Additionally, the cybersecurity profession neglects to frame the field as service-oriented, a theme identified repeatedly in our interviews. We discuss implications of these findings for recruitment and greater workforce diversity.

1. INTRODUCTION
Cyber attacks are on the rise, and companies, government agencies, and individuals are being exploited at an alarming pace [38] [39]. A 2016 survey conducted by a major telecommunications provider found that over 60% of the businesses surveyed had an information technology security breach in 2015, with 42% of those reporting that the breach resulted in significant negative impact [1]. Despite real and evolving cyber threats, organizations and individuals are falling behind in defending their systems and networks [7]. They often fail to implement and effectively use basic cybersecurity practices and technologies.

Further contributing to the problem is the shortage of cybersecurity professionals to address these challenges. Despite significant government and industry partnership efforts to increase the quantity and quality of the pipeline for future security professionals, there will be an estimated gap of 1.8 million information security workers by 2022, a 20% increase from the 1.5 million shortfall forecasted in 2015 [10].

How, then, can we make the most of the workforce we have? We argue that a critical role and force-multiplier in security adoption is the security professional who not only has technical skills, but also possesses the ability to promote best practices, educate, persuade, and serve as change agents for cybersecurity adoption. We call these professionals *cybersecurity advocates*.

Cybersecurity advocates promote security to a variety of individuals, including home users, office workers, students and faculty, technical staff and developers, and executives. They are rarely identified as advocates by their official job title, although some have more explicit titles such as "security evangelist." Many find themselves having to perform advocacy tasks in parallel to their information technology (IT) or security-related jobs. A complicating factor is that while some advocates have formal education in computer and security-related disciplines, others may come into the profession from non-technical disciplines such as policy, legal, business, and the humanities. This makes it difficult to establish a clear career track for these advocates.

There is an abundance of training, education curriculum, and skills assessment resources for traditional security professionals [8] [19] [23] [25] [32]. A quick review of these resources reveals that much of cybersecurity education is viewed through a technical lens, with little to no mention of "soft skills" such as communication, teamwork, and relationship building. These skills are critical to the work of cybersecurity advocates who have a social and organizational focus and impact. Currently, there are few resources for educating professionals on how to be good cybersecurity advocates. In addition to the bias towards technical skills, this gap is likely due in part to the fact that we have little understanding of the work practices and characteristics that lead to successful advocacy.

In this paper, we present preliminary findings from an in-progress interview study of 19 participants in which we explored the characteristics and motivations of cybersecurity advocates. By examining these characteristics, we begin to discover a set of skills and dispositions rarely emphasized in traditional and continuing information security education. By revealing the characteristics of these professionals, we hope to begin a dialogue about how the cybersecurity community can augment current security and education efforts to develop these advocates. We also see an opportunity to rebrand cybersecurity as a people-oriented, service profession, perhaps increasing the currently under-staffed security workforce by attracting a new demographic of individuals who may otherwise not consider cybersecurity as a career.

2. RELATED WORK
Limited research has been dedicated to the study of security professionals. Efforts have aimed to define needed security

Workshop on Security Information Workers, Symposium on Usable Privacy and Security (SOUPS) 2017, July 12 -- 14, 2017, Santa Clara, California.

professional skills [35][37] and to understand personality characteristics of those drawn to cybersecurity competitions [5]. Two significant field studies sought to illuminate the characteristics and challenges of security professionals to inform the design of more effective tools. The HOT Admin project [6][15] identified security practitioner skill sets and challenges in security practitioner work such as having to continually promote security and having to balance security and usability. IBM's study [14] focused on how the work of security administrators differs from non-security IT administrators, for example, the need to address greater technical and organizational complexity and having to be both proactive and reactive in their approach.

Hoffman et al.[16] recognized the importance of building a multi-disciplinary cybersecurity workforce. Bagchi-Sen et al. [4] identified a gap between purely technical training geared towards early career professionals, and the interpersonal, communication, and business-oriented skills required to progress in the field.

Although not cybersecurity specific, other studies echoed these findings by identifying essential skills for related information IT and information systems (IS) professions. Huang et al. [18] categorized IT job skills into three groups: technical, business, and humanistic. Noll and Wilkins [27] proposed a skills matrix and development model to guide IS curriculum based on study results indicating that soft skills, such as teamwork, collaboration, and presentation and writing skills, were important success factors within the field. Multiple research efforts focused on understanding the impact, roles, and characteristics of change agents who play an important role in information technology adoption [22][31][41].

This body of related work illuminates a need for technical personnel to possess non-technical skills and a void within current curricula to support this. Other than elements of one industry training program [33], we have yet to find comprehensive training resources that specifically supports the work practices of security professionals whose primary task is the promotion of security practices. This is a gap our study begins to address by identifying the skills and qualities that effective security advocates possess.

3. METHODOLOGY

We conducted 19 semi-structured interviews lasting on average 45 minutes. Interview questions addressed several areas: work practices, professional motivations and challenges, characteristics of successful advocacy, and communication approaches. Participants also completed a short, online demographic survey that collected information about years of experience in the field, current position, and sectors in which they have worked.

Using researcher contacts, internet searches, and snowballing, we recruited a purposeful sample of participants based on their roles as cybersecurity advocates. Interviews were audio recorded and transcribed. We then performed iterative, inductive coding and analysis on the data to identify core concepts [12].

4. FINDINGS

We focus here on a subset of our preliminary findings that describe the characteristics and skills of cybersecurity advocates. We start with an overview of participant demographics. We then progress from the technical credibility that the advocates must have to the soft skills and service-orientation noted as requirements of success by our participants.

4.1 Diverse Backgrounds and Roles

Our participants had diverse educational and career backgrounds. See Table 1 for a subset of participant demographic information. To avoid uniquely identifying any participants, we generalized some position titles and categorized formal education into technical (e.g., computer science, information systems, engineering, cybersecurity) and non-technical fields of study.

Interestingly, nine participants had at least one degree in a non-technical field, with six of those having no formal degrees in a technology discipline, but rather in areas such as policy, communications, history, law, business, English, and philosophy. These individuals often remarked about how they brought different perspectives and talents to the cybersecurity field. For example, one participant who had a law background found her niche within cybersecurity:

> *"They needed a translator to translate law to geek…And I learned that I sort of have a unique aptitude in this area where law and information security policy intersect." (P15)*

Our participants clustered in age from 35-44 (5 participants), 45-54 (6), and 55+ (7). They were a veteran group, with all but two having more than 10 years in the security field. Participants had worked in a variety of government, private industry, higher education, and non-profit organizations, most having experience in more than one of these sectors.

4.2 Technical Skills

Cybersecurity is most often viewed from a technical perspective, with innovative technology and highly technical workers seen as the path to solving to security problems. Not surprisingly, our participants confirmed that effective cybersecurity advocates must possess strong technical knowledge to gain credibility with their target audiences. One participant, who is a veteran in the field, emphasized the need for an advocate to have a solid understanding of the technical aspects:

> *"This is a business that is very technology oriented, and full of people…who want to one-up you. So if you can't kind of deal with that, it's going to be hard for you to be an effective advocate because people will kind of eat you up unless you're pretty convincing." (P04)*

4.3 Soft Skills

Technical knowledge is important, but those trained only in traditional computing disciplines may not have all the skills to be an effective advocate. The interviews clearly revealed that having a well-rounded approach and addressing social and organizational factors may be more imperative than the technical solutions alone. One of our government participants summed up this sentiment:

> *"If you're a computer scientist, and all you know is the computer science, and you don't have the empathy, you don't have the skills to listen,…you don't have that psychological side, I don't think you can make it work." (P03)*

The remainder of our findings focus on the less conventional, non-technical skills identified as important for security advocacy.

Table 1. Participant Demographics

	Gender	Years Security Experience	Current Position	*Current* & Past Sector(s) G=Government, E=Education, N=Non-profit, I=Industry	Formal Degrees T=Technical, N=Non-technical
P01	M	10+	Cybersecurity Expert	***G***	T, N
P02	M	10+	Professor	***E*****,** G, I	T, N
P03	F	10+	Computer Scientist	***G***	T
P04	M	10+	Security Evangelist	***N***, G	T
P05	M	10+	Cybersecurity Researcher	***I***, G	T
P06	M	10+	Non-profit President	***N***, G, E, I	N
P07	F	10+	Senior Technologist, Professor	***E***, ***G***, I	T
P08	M	5-10	Attorney, Consultant	***I***	N
P09	M	10+	Training Program Director	***E***, G	N
P10	M	10+	Instructor, Consultant	***E***, ***I***, G	T
P11	M	10+	Non-profit Director	***N***, I	N
P12	M	10+	Security Engineer	***I***, ***E***, G	T
P13	M	--	--	***I***	--
P14	M	5-10	Security Awareness Director	***E***, G	N
P15	F	10+	Non-profit Director	***N***, ***E***, I	N
P16	M	10+	Computer Scientist	***G***, E, I	T, N
P17	M	10+	Researcher	***I***	T
P18	M	10+	Vice-President IT	***E***	T
P19	F	10+	Senior Architect	***I***	T

Many of these skills are often referred to as "soft skills." These consist of personal attributes such as likeability and a positive attitude; career and collaborative attributes such as critical thinking, adaptability, and teamwork; people skills such as empathy and relationship building; and communication skills [30]. Unfortunately, these soft skills are not typically associated with cybersecurity professionals even though participants felt these were critical for effective security advocacy. One participant in a non-profit security advocacy group lamented this weakness within the security community, saying, *"We are terrible at soft skills. We're very mono-cultured and bring technical solutions." (P11)*

In this section, we discuss the soft skills our participants recognized as critical in their roles as advocates. We observe that while communication skills are typically recognized as an essential business skill, the soft skills needed by security advocates extend far beyond these.

4.3.1 Communication Skills

Our findings support past research on the importance of communication skills within related business, information systems, and IT fields [18][27]. As several participants remarked, they must be able to "sell" security. They use a variety of communication approaches tailored to their audience, for example, newspaper or television interviews, videos, training classes, presentations, or blogs. They attempt to engage and motivate their audiences, sometimes using imagery, metaphors, or pop culture references to explain technical concepts to less-technical audiences and overcome commonly held, negative perceptions of security.

A good advocate also must frame her communications for diverse audiences. For example, one participant who has extensive experience communicating security to both the general public and within organizations remarked, *"Being able to translate complicated things very simply is crucial to…advocating security."* (P02)

4.3.2 Personal Attributes

Arrogance among highly technical people was commonly observed by our participants and noted as an ineffective way to promote good security decision-making. Effective security advocates must exhibit humility, which was reflected in comments by P10, a consultant and security educator, who stated, *"Whenever I walk in the room, I assume I'm the stupidest one there, and everything works out great." (P10)*

Despite the challenges in the field, participants emphasized the need to portray a positive attitude. P01, who has worked as an

advocate within the U.S. federal government for over a decade, echoed this sentiment when he commented, *"One of the things I read and believe to be true…is…walk in smiling." (P01)*

Participants also talked about the need to maintain optimism that they could make some traction towards solving security problems. When asked what he finds most rewarding about his role as a security educator, P02 expressed this as:

> *"Probably the hope…Hope that I can leverage my lessons learned and recent internet history to help educate people about the technology society we live in and the risks there inside, so they don't make the same mistakes we made. So, sometimes it's a futile act, exercise in futility, but I do have hope." (P02)*

4.3.3 Career and Collaborative Attributes

Career attributes repeatedly mentioned by participants include critical thinking, adaptability, and innovativeness. The ability to be flexible in the face of changing circumstances and new information was emphasized by one participant:

> *"I have a base set of things that I know to be true…and a base set of procedures and policies that I have to follow. But once we get above that baseline, then…my every move is guided by constant course corrections based on what I'm seeing and what I'm feeling." (P01)*

Another recurring topic was that security advocacy cannot be an individual effort due to the diversity and interconnectedness of technologies, networks, and organizations. Our participants especially recognized the importance of cultivating partnerships and building consensus. In a complex, dynamic field, they themselves do not have all the answers, so they often must rely on collective expertise and the establishment of shared security goals. P11, who works with non-tech industries, recognized the need to come to common understandings before his clients would be receptive to security change: *"The goal is to surface beliefs, combine them with other beliefs, come to a set of shared beliefs." (P11)*

4.3.4 People Skills

Advocacy work requires an alignment towards people: an understanding of human behaviors, biases, and limitations and an ability to build relationships, in other words, "people skills." This idea of being people-oriented was repeatedly referred to in our interviews. When asked about the qualities or characteristics that make security advocates successful, several participants noted the ability to build relationships with others by establishing rapport and gaining trust. P12, a consultant who has worked with many different customers over his long career, commented,

> *"To me, trust is the most important thing that I have. If they trust that what I'm telling them and what I'm doing is the right thing, then I am much more successful." (P12)*

Empathy was specifically mentioned by several participants as a critical component in relationship building. P18, a vice president of IT at a university, commented:

> *"I think people have to have a high emotional intelligence and especially empathy. Part of being successful in this is being able to have a conversation and put yourself in the place of the person that you're working with, and then be able to give effective advice that is not preaching, is trying to be helpful, and is letting them know that they're not stupid because they may not know how to do certain things." (P18)*

4.4 Context Awareness

In addition to technical and soft skills, successful cybersecurity advocates must be context aware, recognizing that unique groups will have different sets of values, challenges, and strengths. One participant said quite simply, *"context is king" (P02)*.

Our participants had experience advocating to diverse audiences, both internal and external to their own organizations. Multiple participants commented that a good advocate needs to be aware of the environment, including the technology, people, and social and cultural structures. One participant who regularly performs security consultation discussed this importance:

> *"You need to translate technical findings into the need for business action. And to do that, you have to understand the business at some level." (P10)*

Participants said that successful cybersecurity advocates must also understand and communicate the "why" behind security recommendations and how security can be beneficial rather than detrimental. P02, who is a former Chief Information Security Officer, supported this focus on security being framed not as an obstacle, but as a contributor to the organization's success:

> *"When advocating for security funding or more authorities internally, I always framed in the context of 'We're here to help you. We're mission enablers, not mission constrainers.'" (P02)*

Several participants also specifically commented that they felt the responsibility to look at the bigger context and provide accurate and sensible technical guidance. P07, who has experience in higher education, government, and private industry, commented,

> *"I think in the security area there's a lot of mythology and a lot of things we do because we heard it's the right thing to do, and we have no idea why, but everybody else seems to be doing it, so we should do it, too. And so, trying to get people to stop and think it through, and figure out what's actually going to be effective and look at the threat models." (P07)*

An important aspect of context awareness is a recognition and understanding of the barriers customers face when trying to make decisions about implementing security practices. These barriers may come from any number of economic, social, political, or structural issues. For example, in cybersecurity, as opposed to other technology areas, the economic value can be difficult to calculate. P05, a security researcher and former government security professional, discussed this difficulty:

> *"It's hard to prove that [security is] working for you. Is it working because you've done such a good job and you've invested in all the right places, or is it working because you're just not the target today?" (P05)*

However, emphasizing the impacts of poor security is critical. Advocates must maintain a delicate balance of eliciting enough

concern to motivate, but not enough to overwhelm and paralyze. They also try to devise ways to overcome these barriers while remaining oriented towards the concerns of the organization. For example, P10 described his approach when consulting for financial service companies:

> *"Their biggest concern is compliance and regulatory scrutiny by government agencies. So you talk to them about that. 'You know, you've got this vulnerability, and if somebody hacked this...there's going to be an investigation by the government, and from a regulatory and compliance perspective, then you have issues.'" (P10)*

4.5 Service Orientation

While technical and soft skills may be expected competencies of advocates within the cybersecurity realm, our most surprising finding was the participants' strong sense of service orientation in helping others to protect themselves, safeguard their information, and ultimately work towards a *"common good"* (P15). Hogan, et al. [17] defined service orientation as the willingness to treat customers with courtesy, consideration, and tact; perceptiveness to customer needs; and the ability to communicate accurately and pleasantly. Although prior service orientation research has been mostly conducted in a commercial customer service business context, our data leads us to believe it has implications for cybersecurity advocacy as advocates' audiences can ultimately be viewed as "customers" of security information and guidance.

Service orientation was exhibited by our participants not only in how they approached and performed advocacy-related tasks, but also in their own reflective perceptions of themselves and their work. For example, P06, the head of non-profit security advocacy group, simply stated, *"I think we're making the world a better place."* (P06)

Accompanying this sense of service was a deep passion for the work. Even though security problems may seem intractable in the midst of dynamic and often sophisticated threats, participants reflected that the job has too much importance, and that the economic, physical, and national security consequences may be too dire for them *not* to do something. One participant commented,

> *"It's important because of the implications of not doing it… the significance and the potential of loss of dollars, of information, of man hours, of intellectual property, sensitive information." (P01)*

Passion did not just originate from the service component, but also from the intellectual stimulation of addressing hard problems. One participant, who has had diverse professional experience across multiple sectors, echoed this finding:

> *"Security is like a puzzle. It's like a puzzle that never goes away. And unlike the crossword puzzle…there's positive societal benefit for doing it." (P16)*

Participants saw a gap in security knowledge among individuals and organizations and were doing their best to remedy that by serving in education and awareness roles. Our participants also felt they have a responsibility to serve as mentors to the current and next generations of security professionals. P12, who teaches at local colleges in addition to his consulting job, commented,

> *"I'm not going to be in this forever, so I really want to make sure that I kind of bring in that education piece and try to help the next group." (P12)*

5. IMPLICATIONS

The strong evidence of the importance of non-technical skills for cybersecurity advocacy accentuates the lack of explicit emphasis of those skills within cybersecurity education curricula. We discuss potential implications of our findings toward improving educational resources for advocates to enhance the workforce we have now. Additionally, rebranding cybersecurity towards non-technical proficiencies and motivations may serve to attract a new cohort of individuals to the cybersecurity field in the future.

5.1 Cybersecurity Advocate Education

Advocates tend to be more advanced in their careers, having built on prior real-world experience. Therefore, we contend that there should be continuing education efforts to aid in the progression from security technologist to advocate. Some of these efforts might encourage the development of a change agent skill set. Change agents work to convince their intended audience that there is a need for change, build a solid information exchange relationship, aid in the deployment of the technology, and attempt to ensure long-term adoption of the technology [31]. In 1996, Markus and Benjamin [22] suggested an information systems change agent course that includes units on change agent approaches, personality characteristics, how to cope with challenges, ethical considerations, and awareness of organizational and structural conditions. Building on this foundation, future work may include modernizing and tailoring this course to the specific needs of cybersecurity advocates.

Additionally, as evidenced by the diversity in our participants' formal training, there appears to be a need for educational opportunities to facilitate the transition from working in non-security professions to cybersecurity advocacy. Several participants commented that more discipline diversity would be beneficial to augment proficiency gaps, such as business acumen and soft skills, among security professionals. Furthermore, security applies to all industries and sectors, but the security contexts of these may vary widely. Individuals working within a particular work setting have an intimate knowledge of that environment that an external advocate may not. Change agents are more successful with their clients when they exhibit homophily, the tendency of an individual to bond with others who have similar characteristics [31]. Therefore, it's logical to increase the reach and effectiveness of security advocacy by encouraging the development of cybersecurity advocates who are trusted insiders within diverse fields, for example, law, policy, finance, banking, and health.

5.2 Reframing Cybersecurity

To enhance the future cybersecurity workforce pipeline, we call on the cybersecurity education community to consider incorporating and emphasizing non-technical skills as critical components of the advancement and success of security professionals. Current curricula are largely technology-focused, and fail to include many of the soft skills highlighted in our study.

Additionally, our interviews suggest that there is a failure of the cybersecurity community as a whole to market security as a

service profession versus a technology-dominated field. U.S. Government organizations seem to do a better job of this, for example U.S. Army Cyber Command [39] encourages prospective employees to "Join the team that makes a difference." Yet there is opportunity for improvement in other sectors, including outreach programs for youth and college students.

Reframing cybersecurity may aid in attracting currently under-represented populations, such as women, and reducing the current workforce shortfalls. Despite rising numbers of women in STEM fields such as social sciences, mathematics, and engineering, women's participation in the U.S. computer technology field has been falling [20]. Women now make up only 24% of the overall computing workforce [1] and only 14% of the North American and 11% of the global cybersecurity workforce [10]. This population is often deterred by the perception of security as a male-dominated hacker culture, a lack of mentors, and the belief that only those with highly technical skills can work in the field [13][36].

According to the National Science Foundation [26], Hispanics make up 17% and African-Americans, 13% of the U.S. population; however, they are only 6% and 5% of STEM workers, respectively. Minorities make up an increasingly larger segment of the younger U.S. generations, often referred to as "Millennials" and "Generation Z" [2][9]. These generations are the largest potential source of new cybersecurity professionals, as they are close to 50% of the U.S. population [9][10]. The portrayal as a service profession may be critical in appealing to the values of these generations. Millennials want to positively impact their organization and have a job with meaning and purpose [24][29]. Generation Z are digital natives, having been exposed to technology from a young age. They self-identify as compassionate, open-minded, and determined, also with a desire to positively impact the world [34]. These are all important qualities identified by our study participants. Additional research needs to be conducted to investigate whether framing security as service and people oriented might be more appealing to under-represented groups and younger generations, as well as professionals in other disciplines.

6. CONCLUSION

Cybersecurity advocates serve as force-multipliers in security adoption. However, little has been done to encourage development of additional advocates or attract individuals with the interests and skills to be effective in this role. Our study suggests that a paradigm shift in cybersecurity education and branding may be necessary to keep pace with the dynamic nature of the field, foster more effective advocacy, and help address the workforce shortage. We recommend moving away from a predominantly technical emphasis toward a more holistic view, with the security community supporting non-technical competencies and discipline diversity in both professional development and recruitment efforts.

7. REFERENCES

[1] Accenture. 2016. "Cracking the Gender Code." Retrieved from https://www.accenture.com/t20161018T094638__w__/us-en/_acnmedia/Accenture/next-gen-3/girls-who-code/Accenture-Cracking-The-Gender-Code-Report.pdf

[2] Arthur, R. (2016). "Generation Z: 10 Stats From SXSW You Need To Know," *Forbes* (Mar 16, 2016). Retrieved May 19, 2017 from https://www.forbes.com/sites/rachelarthur/2016/03/ 16/generation-z/#3a8a0fe62909

[3] AT&T. 2016. "The CEO's guide to cyberbreach response: What to do before, during, and after a cyberbreach," *AT&T Cybersecurity Insights*, Volume 3. Retrieved May 19, 2017 from https://www.business.att.com/cybersecurity/docs/cyberbreachresponse.pdf

[4] Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). "Women in cybersecurity: A study of career advancement," *IT professional, 12(1)*.

[5] Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). "An examination of the vocational and psychological characteristics of cybersecurity competition participants," *In 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education*: *3GSE '15*.

[6] Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). "Towards understanding IT security professionals and their tools," *In Proc. of the 3rd Symposium on Usable Privacy and Security*: *SOUPS '07*, 100-111.

[7] Clinton, L. (2014). "Cyber-Risk Oversight," Director's Handbook Series. National Association of Corporate Directors.

[8] Department of Homeland Security. "National Initiative for Cybersecurity Careers and Studies." Retrieved May 19, 2017 from https://niccs.us-cert.gov

[9] Frey, W. "Diversity defines the millennial generation," Brookings Institute (Jun 28, 2016). Retrieved May 19, 2017 from https://www.brookings.edu/blog/the-avenue/2016/06/28/diversity-defines-the-millennial-generation/

[10] Frost & Sullivan. (2017). "The 2017 Global Information Workforce Security Study: Women in Cybersecurity." The Center for Cyber Safety and Education and Executive Women's Forum on Information Security, Risk Management & Privacy. Retrieved May 19, 2017 from https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf

[11] Fry, R. (2016). "Millennials Overtake Baby Boomers as America's Largest Generation," Pew Research Center (Apr 25, 2016). Retrieved May 19, 2017 from http://www.pewresearch.org/fact-tank/2016/04/25/millennials-overtake-baby-boomers/

[12] Glaser, B. G. & Strauss, A. L. (2009). *The Discovery of Grounded Theory: Strategies for Qualitative Research*: Transaction Publishers.

[13] Gonzalez, M. D. (2015). "Building a Cybersecurity Pipeline to Attract, Train, and Retain Women," *Business Journal for Entrepreneurs*, *2015(3)*.

[14] Haber, E. & Kandogan, E. (2007). "Security administrators: a breed apart," *In Workshop on Usable IT Security Management (USM'07) held with the ACM Symposium on Usable Privacy and Security*: *SOUPS '07*.

[15] Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagné, A., & Beznosov, K. (2008). "Human, organizational, and technological factors of IT Security," *In CHI '08 Ext. Abstracts on Human Factors in Computing Systems*, 3639-3644.

[16] Hoffman, L., Burley, D., & Toregas, C. (Mar 2012). "Holistically building the cybersecurity workforce," *IEEE Security & Privacy*, *10(2),* 33-39.

[17] Hogan, J., Hogan, R., & Busch, C. M. (1984). "How to measure service orientation," *Journal of Applied Psychology 69(1)*.

[18] Huang, H., Kvasny, L., Joshi, K. D., Trauth, E. M., & Mahar, J. (2009). "Synthesizing IT job skills identified in academic studies, practitioner publications and job ads," *In Proc. of the SIGMIS Conference on Comp. Personnel Research*, 121-128.

[19] International Information System Security Certification Consortium. https://www.isc2.org

[20] Landivar, L. C. (2013). "Disparities in STEM Employment by Sex, Race, and Hispanic Origin," U.S. Census Bureau. Retrieved May 19, 2017 from https://www.census.gov/prod/2013pubs/acs-24.pdf

[21] LeClair, J. ed. (2015). *Protecting Our Future, Volume 2: Educating a Cybersecurity Workforce (Vol. 3).* Hudson Whitman/ECP.

[22] Markus, M. L. & Benjamin, R. I. (Dec 1996). "Change agentry – the next IS frontier," *MIS Quarterly 20(4*), 385-407.

[23] McGettrick, A. (2013). "Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training," Association for Computing Machinery. Retrieved May 19, 2017 from https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf

[24] Myers, K. K., & Sadaghiani, K. (2010). "Millennials in the workplace: A communication perspective on Millennials' organizational relationships and performance," *Journal of Business and Psychology*, *25*(2), 225-238.

[25] National Centers of Academic Excellence in Cyber Defense. https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

[26] National Science Foundation. (2017). "Women, Minorities, and Persons with Disabilities in Science and Engineering." Retrieved May 19, 2017 from https://www.nsf.gov/statistics/2017/nsf17310/digest/about-this-report/

[27] Noll, C. L. & Wilkins, M. (2002). "Critical skills of IS professionals: A model for curriculum development," *Journal of Information Technology Education, 1(3)*, 143-154

[28] Pusey, P., Gondree, M., & Peterson, Z. (2016). "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations," *IEEE Security & Privacy*, *14(6)*, 90-95.

[29] PwC. "Engaging and Empowering Millennials." Retrieved May 19, 2017 from http://www.pwc.com/gx/en/hr-management-services/publications/assets/pwc-engaging-and-empowering-millennials.pdf

[30] Robles, M. M. (2012). "Executive perceptions of the top 10 soft skills needed in today's workplace," *Business Communication Quarterly, 75(4)*, 453-465.

[31] Rogers, E. (2003). *Diffusion of Innovations* (5th ed.), New York, NY: Simon and Schuster.

[32] SANS Institute. https://www.sans.org

[33] SANS Technology Institute. "Information Security Master's Degrees: MSISM." Retrieved May 19, 2017 from https://www.sans.edu/academics/masters-programs/msism

[34] Seemiller, C. & Grace, M. *Generation Z Goes to College.* Jossey and Bass.

[35] Shoemaker, D., Kohnke, A., & Sigler, K. (2016). "A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (2.0, Vol. 3)." CRC Press.

[36] Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., Sande, C., Acholonu, G., Bace, R., & Hall, L. (2013). "Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation," *In Proc. of the Conference on Innovation and Technology in Comp. Science Education: ITiCSE* '13, 1-14.

[37] Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). "Cyber education: a multi-level, multi-discipline approach," *In Proc. of the ACM 16th Annual Conference on Information Technology Education*, 43-44.

[38] Symantec. (2016). "2016 Internet Security Threat Report." Symantec Corporation. Retrieved December 18, 2016 from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[39] U.S. Army Cyber Command. http://www.arcyber.army.mil/Pages/ArcyberHome.aspx

[40] Verizon. (2016). "2016 Data Breach Investigations Report." Retrieved December 18, 2016 from http://www.verizonenterprise.com

[41] Winston, E. R. (Oct 1999). "IS consultants and the change agent role," *ACM SIGCPR Comp. Personnel, 20(4)*, 55-74.