Promoting Skill and Discipline Diversity in Cybersecurity Advocacy

Julie M. Haney and Wayne G. Lutters

Department of Information Systems, University of Maryland, Baltimore County, USA
{jhaney1, lutters}@umbc.edu

Abstract. Cybersecurity advocates attempt to reduce exposure to 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 professional attributes of cybersecurity advocates. Qualitative analysis of 28 interviews reveals that effective advocates must not only possess technical acumen, but also interpersonal skills, communication skills, context awareness, and a customer service orientation. These non-technical skills are often missing from cybersecurity training, limiting career progression into the cybersecurity advocate role for existing security professionals and those from other disciplines. We discuss implications of these findings for improving professional development opportunities and encouraging greater workforce diversity within the cybersecurity advocacy field.

Keywords. cybersecurity education, security professionals, discipline diversity, advocacy

- Defines cybersecurity advocates as security professionals who promote security best practices and adoption as a major component of their jobs
- Presents evidence that, in addition to technical knowledge, cybersecurity advocates demonstrate strong non-technical competencies and service orientation
- Suggests a need for establishing a career track to aid in the progression to the cybersecurity advocate role from within the security field and from other disciplines

1 Introduction

The effects of cyber attacks can be devastating on personal, organizational, national, and global levels. However, people routinely fail to adequately protect their digital assets. In 2016, cybercrime and espionage cost the global economy over $450 billion, with more than two billion personal records stolen (Hiscox, 2017). The need for the cybersecurity community to encourage and equip everyone to better protect themselves is, therefore, clear. In this paper, we suggest that a critical role in this endeavor is the security professional who possesses the responsibility to promote best practices, serving as catalysts for cybersecurity adoption. We call these professionals *cybersecurity advocates*.

"Cybersecurity advocate" is an emerging term-of-art among practitioners, with most advocates not identified as such by their job title. These are security professionals for whom promoting, educating, and encouraging adoption of security are major components of their jobs, part of their personal identity, and integral to their career advancement. Advocates' audiences are diverse and may include home users, office workers, technical staff, and executives. Examples of advocates include: individuals designing and executing security awareness programs within their organizations; security researchers who promote the use of security technologies; non-profit security advocacy staff who develop security campaigns and publish guidance; consultants who work to convince their clients to implement security measures; and security educators who teach technical and non-technical audiences.

There is an abundance of education curricula for traditional security professionals, e.g., the National Initiative for Cybersecurity Education Framework, which outlines the knowledge, skills, and abilities for various cybersecurity work roles (Newhouse, Scribner, and Witte, 2017). These resources reveal that much of cybersecurity education is viewed through a technical lens, with little to no mention of non-technical competencies such as communication and relationship building. These skills are critical to the advocacy role, which has a social and organizational focus and impact. A complicating factor is that, while some advocates have formal computing education, others come into the profession from non-technical disciplines. Currently, there are few resources for educating professionals on how to be good cybersecurity advocates and no clear career track. In addition to the bias towards technical skills, this gap is likely due to there being little understanding of the work practices and characteristics that lead to successful advocacy.

In this paper, we begin to address this gap. Our findings are part of a first-of-its-kind, broader investigation of cybersecurity advocates' work practices (Haney and Lutters, 2018) and address one central research question from that study: What are the professional characteristics and skills that cybersecurity advocates employ in their work? By examining these traits, we discovered a set of skills and dispositions beyond the technical competencies usually emphasized in preparatory and continuing education programs.

Our research has several novel contributions presented in this paper. We are the first to define and enumerate competencies for the role of cybersecurity advocate which can be used to augment current professional development resources to prepare for advocacy. Additionally, we highlight the benefits of discipline diversity within the advocate community. Our work uniquely identifies service orientation as a core aspect of cybersecurity advocacy. Accordingly, we see an as yet unrealized opportunity to frame this role as a people-oriented service profession, perhaps attracting a more diverse demographic of individuals who may not otherwise consider cybersecurity as a career choice.

2 Related Work

The work of cybersecurity advocates has similarities to, but does not fall cleanly within, the boundaries of traditional security work roles, for example, those in Newhouse,

Scribner, and Witte (2017) and the Skills Framework for the Information Age Foundation (2018). However, by understanding the practices and challenges of traditional security professionals, similarities and differences in professional development needs for advocates can be discovered.

Various efforts sought to illuminate skills and work practices of security professionals. Two field studies, the HOTAdmin project (Botta et al., 2007) and IBM's system administrator study (Haber and Kandogan, 2007), found that security professionals' work differed from that of non-security technical staff in the complexity and diversity of tasks, the need to be up-to-date on the latest technologies and vulnerabilities, and having to continually promote security. These tasks necessitated skills such as pattern recognition, inferential analysis, communication, and collaboration. Paul (2014) supported these findings in a study of analysts in a network operations center, revealing that communication with external stakeholders was an important, but challenging, aspect of the job. Goodall, Lutters, and Komlodi (2009) investigated the work practices of network intrusion detection analysts, suggesting that developing support tools for their tasks required a holistic, sociotechnical perspective. Ben-Asher and Gonzalez (2015) found that both situated and domain knowledge contribute to a security analyst's ability to triage network events.

This body of literature highlights the complexity of cybersecurity jobs. Technical knowledge is foundational, but there are contextual, social, and organizational factors also at play. As a type of security professional, cybersecurity advocates often operate at the interfaces between the technical and the organizational. For example, they have to determine how best to "sell" security to stakeholders who do not have a shared understanding of risk. Yet not enough is understood about how they can be successful.

3 Methodology

From November 2016 to August 2017, we conducted interviews of 28 cybersecurity advocates. The study was approved by our institutional review board with informed consent but no compensation for participants.

Utilizing researcher contacts and internet searches, we recruited participants who performed cybersecurity advocacy as a significant component of their jobs. We initially recruited individuals who publicly self-identified as working primarily in this capacity. Our participant sampling strategy was grounded in a purposive approach to ensure suitability and maximize diversity, while considering snowballing recommendations that allowed interviewees to identify others like themselves. To account for the potential of different viewpoints and techniques, we sampled advocates with varying backgrounds and roles, working in a variety of sectors, and who served different types of audiences.

Table 1. Participant Demographics. **Sector** (***Current***, Past): E=Education, G=Government, I=Industry, N=Non-profit. **Edu** (Education): T=Technical degree, N=Non-technical degree, U=Unknown/not reported. **Audience**: I=Internal to own organization, E=External , B=Both internal and external. **Audience Description**: dev=developers, end=end users in an organization, fac=faculty, gen=general public, industry=industry partners, mgr=managers, non-tech=non-technical professionals, policy=public policy makers, stud=students, tech=technical staff

ID	Current Role	Sector	Edu	Audience	Audience Description
P01	Security analyst	***G***	T,N	B	tech, mgrs
P02	Professor	***E***,G,I	T,N	B	gen, stud
P03	Computer scientist	***G***,I	T	B	tech, mgr, gen
P04	Security evangelist	***N***,G	T	B	tech, mgr
P05	Security researcher	***I***, G	T	B	tech, mgr
P06	Director	***N***,G,E,I	N	B	policy, mgr
P07	Senior technologist	***G***,***E***,I	T	E	gen, mgr
P08	Security consultant	***I***	N	E	non-tech, mgr
P09	Training director	***E***,G	N	E	tech
P10	Instructor, consultant	***I***,***E***,G	T	E	tech, mgr
P11	Director	***N***,I	N	E	policy, tech, mgr
P12	Security engineer	***I***,***E***,G	T	E	tech, mgr
P13	not provided	***I***	U	I	tech, mgr
P14	Security awareness	***E***,G	N	B	stud, fac, tech, mgr
P15	Director	***N, E***, I	N	B	tech, mgr
P16	Computer scientist	***G E***, I	T,N	I	mgr
P17	Researcher	***I***	T	E	dev, tech
P18	CIO	***E***	T	B	stud, fac, tech, mgr
P19	Senior architect	***I***	T	I	dev
P20	Professor	***E G***	T	E	stud, tech, mgr
P21	Company co-founder	***I***,G	T	E	end, tech, mgr
P22	Security researcher	***I***,E	T	B	dev
P23	Security consultant	***I***,E	N	B	tech, gen
P24	Director	***N***	N	E	gen, tech, mgr
P25	Deputy CIO	***G***,I	N	B	end, tech, mgr
P26	CISO	***G***,I	T	B	end, tech, industry
P27	Director	***N***,I	N	B	tech, mgr
P28	Security awareness	***I***,E	N	B	end, tech, mgr

Table 1 summarizes participant demographics, with some information generalized to preserve anonymity. We interviewed 10 female and 18 male professionals. Overall, they were an experienced group, with all but six having more than 10 years in the security field, and the rest having at least five. From a formal education perspective, 14 participants had at least one degree in a non-technical field, with 11 of those having no formal tech degrees, but rather in areas such as communications, business, and law. Participants had worked in diverse roles in government, private industry, education, and non-profit organizations, most having experience in more than one of these sectors. When asked to describe their target audience, 10 said their audience was mainly external to their organization, three mainly focused within their organization, and 15 said they advocate both externally and internally.

Data collection and analysis followed a Grounded Theory approach. Grounded Theory is a type of qualitative research in which concepts are derived directly from the data and not from prior contributions. Data collection and analysis are tightly coupled and usually happen in parallel, with analysis of data informing subsequent data collection decisions (Corbin & Strauss, 2015).

Interviews lasted on average 45 minutes. Interview questions (Appendix A) addressed several areas: work practices, professional motivations and challenges, characteristics of successful advocates, and techniques. In this paper, we report on a subset of data focused on characteristics. Participants also completed an online demographic survey that collected information about education and experience in the security field (also in Appendix A). Interviews were audio recorded, transcribed, and assigned a participant code (e.g., P10) to protect confidentiality.

We interviewed until we reached theoretical saturation, the point at which no new ideas emerged from the data. Given that the goal of qualitative research is rich, holistic contextual understanding, and not predictive generalization, the attainment of theoretical saturation signaled that the appropriate number of interviews had been achieved (Corbin and Strauss, 2015). Maximizing for sample diversity helped us reach this saturation as did the semi-structured nature of the interviews, which allowed for follow-on questions and the elicitation of deep, rich data. Our semi-structured interview approach was ordered enough for cross-participant comparison, but open enough to let participants raise themes we had not imagined in advance.

We followed Grounded Theory data coding and analysis methods, which allowed for an organic emergence of core concepts. Both authors initially reviewed five interviews individually and performed inductive, open coding to label/categorize and look for meaning. We subsequently met multiple times to discuss concepts identified in those interviews. These discussions led to the development of a codebook, which the first author used to recode the initial five interviews to align with the codebook, and then deductively code the remaining interviews. We then progressed to the recognition of relationships among those codes (axial coding), wrote analytic memos to begin to capture emerging ideas, and employed selective coding (identification of core concepts/themes) (Corbin and Strauss, 2015). Table 2 shows this progression leading to the central concept of “skill and discipline diversity.” This theme was supported by participant demographics and interview data categorized in the following axial codes: non-technical competencies, technical knowledge, and service orientation. Appendix B provides more details on data analysis and development of the codebook.

Table 2. Code Progression

Open Coding	Axial Coding	Selective Coding
Interpersonal skills	**Non-technical Competencies**	**Skill and Discipline Diversity**
Communication/translation skills		
Context awareness		
Technical skills	**Technical Knowledge**	
Credibility - technical		
Staying relevant		
Service profession	**Service Orientation**	
Passion		
Perception of importance of the work		
Education & awareness		
Formal education	**Career Diversity**	
Career history		
Role		

4 Understanding Attributes of Cybersecurity Advocates

4.1 Non-technical Competencies

Cybersecurity is often viewed from a technocentric perspective. Not surprisingly, 19 participants asserted that effective cybersecurity advocates should possess technical knowledge to gain credibility with their target audiences. One security analyst noted, *"if you don't know what you're doing, that's going to become apparent very quickly" (P01).*

Technical knowledge is indeed important, but those trained only in computing and engineering disciplines may not have fully developed all of the skills to be an effective advocate. The interviews revealed that being able to address social and organizational complexity may be more imperative than technical solutions alone. All 28 participants discussed non-technical skills and abilities when asked to describe qualities of those successful in security advocacy, with interpersonal skills, context awareness, and

communication skills most frequently mentioned. As noted by nine participants, these skills may differentiate advocates from other security professionals: *"The majority of [security] professionals have a huge understanding of technical issues, but a very, very small percentage of them have any soft skills whatsoever" (P27).*

Interpersonal Skills. All participants noted that advocacy work requires an orientation towards people with strong interpersonal skills, including understanding human behavior and an ability to build trust. One participant reflected*: "people who are emotionally intelligent tend to be able to understand problems and frustrations much better than people who have not invested in that part of themselves. And they tend to be very good at problem and conflict resolution" (P23).* Another discussed the importance of relationship building when trying to influence security behaviors: *"There's the developing of the rapport with the people... so that they not only listen, but they trust you" (P01).*

Eight participants mentioned the need to maintain a positive attitude that progress could be made towards solving seemingly overwhelming security problems. A security consultant had hope that his work was fruitful*: "I think there are small things we can do on individual projects and individual tasks where we can make a difference and make things better. So, it's having that focused optimism" (P10).*

Other interpersonal skills mentioned as important included listening skills (6 participants), empathy (4), and humility (5). An advocate who works to influence the security practices of companies that produce safety-critical technologies (e.g., medical devices) remarked on the confluence of these qualities in his work:

> *"I focus on getting everyone to feel heard. Identity and empathy... Once they're heard, they're more likely to hear others. And once we know their belief structure, we can see which ones are good that we work on and foster, which ones are bad that we need to dampen" (P11).*

Context Awareness. In addition to technical and interpersonal skills, 22 participants commented that cybersecurity advocates must be context aware, recognizing that unique audiences have different strengths, values, and challenges. This awareness then guides how advocates tailor their message. One participant commented, *"context is king… it's not a one-size-fits-all approach" (P02).* A corporate consultant discussed the importance of understanding his audience's environment*: "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).*

Context awareness also aids in identifying root causes of poor security behaviors, which may be due to educational, economic, social, political, or structural issues. One participant lamented, *"we as a society have a tendency to treat symptoms and not causes" (P01).* When considering ways to change problematic security behaviors, a former security awareness director remarked, *"you need to ask yourself why aren't they doing it. And you need to keep asking why… to get to the root cause because you'll find the why is very different for groups, often for individuals, or teams" (P21).*

Ten participants said that successful advocates must also communicate the reasons behind security recommendations. Specifically, they must show how good security practices are fundamentally beneficial rather than just annoying or detrimental. A security researcher commented that advocates must possess *"an ability to make them understand why this is important to them or why this is the right thing to do or the best thing to do" (P05).* A former Chief Information Security Officer (CISO) discussed how, in the corporate world, security should be marketed not as an obstacle, but as a contributor to an organization's success: *"We're here to help you. We're mission enablers, not mission constrainers" (P02).*

Communication Skills. Our findings support past research on the importance of communication skills (mentioned by 23 participants) within the information technology field. As several participants remarked, they must be able to "sell" security. To do this, a good advocate must be context aware and frame her communications for diverse audiences, often serving as a translator between technical and non-technical audiences. A security awareness manager supported this notion: "*You have to be able to talk something that's not IT... but you also have to be willing to take the time to understand the IT side in order to make that translation, or it gets lost" (P28).* Unfortunately, being a translator can be particularly taxing for highly technical individuals because, according to one participant, they often "*struggle with something called 'curse of knowledge.' So they understand technology and problems so well, they have this assumption other people must understand it also… And as a result, they communicate in rather confusing terms" (P09).*

The advocates we interviewed used a variety of communication approaches tailored to their audience including: written materials (18), which include books, newsletters, papers, and frameworks; small group or individual face-to-face interactions (17); large forum/conference presentations (16), social media/blogs (12); and classroom training (9). Via these channels, advocates described attempts at engaging their audiences, sometimes using stories, imagery, metaphors, humor, or pop culture references to explain complex technical concepts.

4.2 Service Orientation

While technical and soft skills may be expected competencies of cybersecurity advocates, our most surprising finding was participants' strong sense of service in helping others to protect themselves and their information. Hogan, Hogan, and Busch (1984) 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 most prior service orientation research was conducted in a business context, our data leads us to believe it has implications for cybersecurity advocacy since advocates' audiences can ultimately be viewed as "customers" of security guidance.

Service orientation was portrayed by 25 participants not only in how they performed advocacy-related tasks, but also in their own self-reflective perceptions of their professional identity. A former lawyer now serving as a director at a non-profit considered how her security advocacy work aligned with her predispositions: *"I think fundamentally I am the type of person that likes to help other people. That's been pretty clear in my whole career" (P15).* Another participant, who mainly advocates to non-

technical audiences, remarked, *"There's so much stuff going on for people nowadays… If I can take a worry off the table for people, I'm happy to do that" (P08).*

Accompanying this sense of service was a deep passion for the work. Even though security problems may seem intractable, participants reflected that their job is too important to falter. One participant discussed his advocacy motivation: *"I primarily do it to fix society. I see that we have a lot of problems that are getting worse" (P16).* Another participant, who worked with U.S. government customers, 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).* An advocate who works for a non-profit also remarked on the societal impact of security: *"security is an enabler for us to do the things that we want to do... It's beyond critical" (P24).*

All participants saw a gap in security knowledge among individuals and organizations and were doing their best to remedy that through education. One talked about the rewards of serving as both a corporate consultant and a community educator:

> *"I always get really excited when I can just tell people have learned something… I know that I've done something good, and I know that I have done something that could impact millions of people, maybe not immediately, but in some significant amount of time" (P23).*

Five participants noted they felt a responsibility to serve as mentors to the next generation. An interviewee who taught at local colleges 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).* Three participants had positive experiences providing security education to youth. One remarked he enjoyed *"trying to influence a younger age because I think those people have an appreciation for the technology, but maybe not the security aspects of it" (P05).*

4.3 Discipline Diversity

Our findings reveal that while some participants trained solely in technical aspects of their job had a natural proclivity to non-technical competencies, many brought skills honed by formal education or prior careers in non-technical fields. We show how "discipline diversity," the incorporation of individuals with non-technical professional training/experience into the cybersecurity advocate capacity, was viewed by participants as beneficial.

Of the 14 participants with at least one non-technical degree, six had primarily worked in tech positions their entire careers, while eight worked in non-technical positions prior to their advocacy roles. They viewed their educations as advantageous in developing non-technical competencies important for security advocacy. One participant, who had worked in computer security his entire career without a formal technical degree, stated, *"As I stopped having imposter syndrome about it, I've really leveraged my undergraduate philosophy background, soft skills, instead of thinking they were a deficiency" (P11).*

Four participants had backgrounds in marketing or communications. One of them used prior experience studying interpersonal communications when influencing executives and government officials about cybersecurity policies: *"You need to be able to be flexible in terms of adapting your argument to their particular needs. And you need to be honest with them… So those basic skills, which also happen to work with interpersonal relationships, absolutely work in this space" (P06).*

A graphic designer saw the benefit of being an experienced marketer who could speak in terms understood by non-experts: *"because I'm not an IT person, all of this that I come in touch with I find interesting and scary, and realize that the rest of the population isn't getting this information" (P28).*

Three participants with law degrees became advocates because of their ability to understand the relationship between law, policy, and cybersecurity. One said, *"They were looking to have a lawyer on staff to help them translate… legal requirements for information technology into a language that… technologists could understand" (P15).* Another, who started out in security by educating other lawyers, commented on the benefit of engaging others with similar backgrounds, *"I know that audience because that's the audience I relate to. As I understand the information, that's how I presented it to them" (P08).*

Four other participants with business-oriented degrees often leveraged their interpersonal skills and understanding of business contexts. When asked how to establish trust and credibility, a participant harkened back to his formal training: *"I think that kind of goes back to being a student of the humanities and knowing... how to deal with people"(P02).* A former management consultant's tendency to pitch cybersecurity as a *"competitive advantage" (P27)* helped convince corporations to implement incentives for rigorous security practices.

5 Implications

5.1 Cybersecurity Advocate Career Track

We observe that advocates in our study tended to be more advanced in their careers, having built on prior real-world experience in both security and non-security fields. Many became advocates by chance, with no pre-meditated intention. Phrases used to describe their progression to advocate included *"fell into it" (P24), "accident" (P08),* and *"a perfect storm of good stuff that fell together" (P14).* Although we recognize that career paths are often influenced by happenstance, we wonder what would happen if there was a defined career track for this role. Would more people aspire to become a cybersecurity advocate instead of leaving it up to chance? To that end, we suggest that there should be a more formalized definition of the advocate role and continuing education efforts to aid in the progression to advocate.

Professional development efforts must also address aspects of the work beyond the already-mentioned skills. Although not explicitly discussed in this paper, there are other facets of advocacy that emerged from our data. One such facet includes intrinsic and extrinsic motivations that attract and retain advocates. For example, many are motivated not just by their desire to serve, but also by the challenge of the field, as one noted: *"I think it's intellectually exciting. Security is like a puzzle... that never goes*

away" (P16). They also desire to see tangible results of their efforts: *"It's one thing to be able to have positive feedback about what people felt we did, but also have knowledge of the fact that what we did really helped... and they were successful at it" (P01)*. Future work may explore how development opportunities and organizations can incentivize professionals to do this type of work.

Advocates also have to be adept at recognizing and navigating myriad challenges. For example, seven advocates discussed how attitudes of other security professionals hinder their security promotion efforts: *"I'm really frustrated with the security field because they keep saying that employees are the weakest link" (P21*). Other participants' efforts were hampered by organizational issues, including one advocate who was frustrated with corporate structures that fail to acknowledge that security is *"cross-cutting" (P06)* among all aspects of the organization.

To address nuances of advocates' work, education efforts might encourage the development of an organizational change agent skill set, as described by Markus and Benjamin (1996). Like advocates, change agents work to facilitate change, build a solid information exchange relationship, and attempt to ensure long-term adoption. These researchers proposed a preparatory course that includes units on approaches, personality characteristics, how to cope with challenges, ethical considerations, and awareness of environmental conditions. Building on this foundation, future work may include modernizing and tailoring this curriculum to the specific needs of cybersecurity advocates.

5.2 Discipline Diversity in Cybersecurity Advocacy

While we sought participant diversity with respect to gender, sector, and audience, we did not purposefully sample along education or career dimensions. Therefore, one of our most surprising observations was the resultant participant diversity with regard to discipline. As described earlier, this diversity appeared to be quite beneficial. We observed that discipline diversity was not a prerequisite for a cybersecurity advocate, but rather a conduit through which individuals became proficient in skills not typically emphasized in the cybersecurity field. Additionally, although security applies to all industries and sectors, contexts vary widely. Advocates working within a particular professional setting may have more intimate knowledge of that environment than an external advocate might. It is then 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, finance, and health.

Based on our findings, we also suggest that the formation of multi-disciplinary security advocacy teams should be encouraged. For example, a non-profit director described his volunteer community:

> *"We happen to have the most diverse participants of any cross-section you might see in cybersecurity... We have psychologists, data scientists, social work background, PR communications experts… And I don't think we succeeded in spite of those, I think we probably have been successful because of those" (P11).*

Therefore, to encourage greater discipline diversity, there appears to be a need for educational opportunities to facilitate the transition from working in non-security professions to cybersecurity advocacy. These may focus more on how to apply non-technical skills in the cybersecurity context as well as provide resources for mastering technical concepts.

5.3 Cybersecurity Advocacy as a People and Service-Oriented Profession

While interpersonal and communication skills are generally noted as useful professional skills, we have also identified service orientation as an attribute not typically emphasized in security professions, but essential for those performing advocacy roles. Given a cybersecurity career is often marketed through a purely technical lens, it may inadvertently dissuade those who seek a career in which they can regularly engage with people, employ a variety of communication techniques, and make a positive, societal impact. Likewise, individuals in non-security fields may not understand how their skills might be valuable, especially in advocacy roles. Therefore, to enhance the future cybersecurity advocacy workforce pipeline, we call on cybersecurity education and recruitment programs to expand the scope of security professions by incorporating and advertising the non-technical skills and service orientation identified in our interviews as relevant attributes of security advocates.

In addition to encouraging discipline diversity, framing cybersecurity advocacy as a people and service-oriented profession may aid in attracting populations currently underrepresented in the security field as a whole. Several studies explored reasons for the underrepresentation of women and minorities within the security field. They found that these populations are often deterred by the perception of security as a "male-dominated, solitary profession with no social benefit" (Shumba et al., 2013) and a lack of understanding of the breadth of opportunities available in security careers (Gonzalez, 2015). Additionally, the portrayal of security advocacy as a service-oriented profession may appeal to values of younger generations. At close to 50% of the U.S. population, Millennials and Generation Z are the largest potential source of new cybersecurity professionals. These generations want to positively impact the world and have a job with meaning and purpose (Myers and Sadaghiani, 2010; Seemiller and Grace, 2016), which are important qualities for cybersecurity advocacy as identified in our study.

6 Limitations and Future Work

Our study is limited in that, like all self-report data, findings reflect the perceptions of participants, which may not represent ground truth. Participants may have exhibited self-report bias in which they adjust their answers to be viewed more favorably by the interviewer. This is primarily mitigated by the diversity of our participants and the constant comparison method of our analysis.

This study represents an initial discovery of the cybersecurity advocate role, with its key characteristics and professional development pathways, that will be confirmed and expanded in future work. This may include formalizing findings to a model to be validated with a broadly-distributed, quantitative survey of those in advocacy roles. Our planned future work also involves examining advocacy from the perspective of the

target audiences, exploring questions such as: which characteristics and techniques of advocates are most important and effective? What most successfully motivated behavior change?

7 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. To support advocates in their work, our study suggests the need for an expansion of current, predominantly technocentric cybersecurity career tracks. This expansion necessitates the consideration of nontechnical competencies and discipline diversity in both professional development and recruitment efforts for cybersecurity advocates.

Our study also offers an opportunity for a repositioning of cybersecurity work (in particular, advocacy) as not solely the primarily technical work of its cryptographic roots, but as a people-oriented, service profession. This recharacterization brings with it profound workforce development implications that could have a transformative impact on the discipline. Given the growing dire conditions due to a workforce shortage and increasingly common and severe attacks, it may be time for a radical rethink about what cybersecurity means and how advocacy roles may contribute in the coming decade.

8 References

Ben-Asher, N. & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior, 48*, 51-61.

Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). Towards understanding IT security professionals and their tools. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (pp. 100-111). ACM.

Corbin, J. & Strauss, A. (2015). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. 4th ed. Thousand Oaks, CA: Sage.

Goodall, J. R., Lutters, W. G., & Komlodi, A. (2009). Supporting Intrusion Detection Work Practice. *Journal of Information Systems Security, 5*(2), 42-73.

Gonzalez, M.D. (2015). Building a cybersecurity pipeline to attract, train, and retain women. *Business Journal for Entrepreneurs, 2015*(3), 24-41.

Haber, E. M. & Kandogan, E. (2007). Security Administrators: A Breed Apart. In *Proceedings of the Workshop on Usable IT Security Management held with the Symposium on Usable Privacy and Security* (pp. 3-6). ACM.

Haney, J. M. & Lutters, W. G. (2018). "It's Scary… It's Confusing… It's Dull": How cybersecurity advocates overcome negative perceptions of security. In *Proceedings of the 14th Symposium on Usable Privacy and Security* (pp. 411-425). USENIX.

Hiscox. (2017). The Hiscox Cyber Readiness Report 2017. Retrieved July 8, 2018, from the Hiscox Inc. web site: http://www.hiscox.com/cyber-readiness-report.pdf

Hogan, J., Hogan, R., & Busch, C.M. (1984). How to measure service orientation. *Journal of Applied Psychology*, *69*(1), 167-173.

Markus, M.L. & Benjamin, R.I. (1996, December). Change agentry - The next IS frontier. *MIS Quarterly*, 385-407.

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.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. Retrieved July 8, 2018, from the National Institute of Standards and Technology publications web site: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Paul, C. L. (2014). Human-Centered Study of a Network Operations Center: Experience Report and Lessons Learned. In *Proceedings of the 2014 ACM Workshop on Security Information Workers* (pp. 39-42). ACM.

Seemiller, C. & Grace, M. (2016). *Generation Z goes to college*. Hoboken, NJ: John Wiley & Sons.

SFIA Foundation. (2018). SFIA 7 - the seventh major version of the Skills Framework for the Information Age. Retrieved July 8, 2018, from the SFIA Foundation web site: https://www.sfia-online.org/en/framework/sfia-7

Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., Sande, C., Acholonu, G., Bace, R., & Hal, L. (2013). Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. In *Proceedings of the ITiCSE Conference on Innovation and Technology in Computer Science Education* (pp. 1-14). ACM.

Appendix A Interview Guide and Demographic Survey

Interview Guide

1. Can you tell me about what you do in your job?
2. How did you come to do this type of work?
3. What motivates you to do this work?
4. Do you think your role as a security advocate is important? Why or why not?
5. Do you think your role is valued by others? Why or why not?
6. What do you think are qualities of a successful security advocate?
7. Have you had experiences with or know of security advocates who you don't think were particularly effective? What was it about them or what did they did or did not do that contributed to their ineffectiveness?
8. Through what means do you advocate for security? For example, conferences, invited talks, blogs, social media, articles, client visits, face-to-face meetings, phone, email. *[If conferences are mentioned, ask which ones.]*
9. Which of those means do you think are the most effective? Why?
10. Do you feel that you're reaching the right population of people and organizations?

    [Follow up questions if the answer is no:]
    a. What is preventing you from reaching the right people?
    b. What do you wish you could do to reach the right population?

11. How do you keep up with the latest in security?
12. What do you find most rewarding, if anything, about your role as a security advocate?
13. What do you find most challenging or frustrating, if anything, about your role as a security advocate?

14. What do you think are the biggest obstacles organizations face with respect to implementing security measures and technologies?

15. What do you see as your role in helping organizations overcome these obstacles?

16. What are other ways these obstacles might be overcome?

17. Is there anything else you'd like to add with respect to security advocacy?

Online Demographic Survey

1. What is your job title or position?

2. How many years of experience do you have in the cyber security field?
   - Less than 5 years
   - 5-10 years
   - More than 10 years
   - Prefer not to answer

3. Which category best describes your ***current*** organization?

   - Consumer services
   - Education
   - Energy
   - Financial
   - Government – Defense
   - Government - Other
   - Healthcare
   - Retail
   - Technology (non-telecommunications)
   - Telecommunications
   - Other. Please describe:
   - Prefer not to answer

4. Which category or categories best describe the organizations you have worked for in the ***past***? Check all that apply.

   □ Consumer services
   □ Education
   □ Energy

- □ Financial
- □ Government – Defense
- □ Government - Other
- □ Healthcare
- □ Retail
- □ Technology (non-telecommunications)
- □ Telecommunications
- □ Other. Please describe:
- □ Prefer not to answer

5. Do you represent or work closely with a specific security vendor?
   - □ No
   - □ Yes, I represent a security vendor
   - □ Yes, I work closely with a security vendor
   - □ Prefer not to answer

6. Who is your target audience with respect to advocating for security practices or technologies? Please do not use specific names of organizations, but do include audience groups/types (for example, technical personnel, management) and sectors or types of organizations (for example, health industry, government).

7. Select the option that best describes your audience.
   - o My audience is mainly within my own organization.
   - o My audience is mainly external to my organization.
   - o My audience is both with and external to my organization.
   - o Prefer not to answer
   - o Other:

8. How would you describe your preferred approach to security advocacy?
   - o I create security technologies or methodologies or coordinate the implementation of these.
   - o I facilitate change by increasing people's/organization's capacity to create the conditions of informed choice, valid information, and personal responsibility
   - o I advocate for the direction of change, try to persuade people about the need for change, and model how to make those changes.
   - o Prefer not to answer

9. What is your gender?
   - o Female
   - o Male

- Other
- Prefer not to answer

10. What is your age range?
    - Under 25
    - 25-34
    - 35-44
    - 45-54
    - 55 and over

11. What is your highest level of education?
    - High school
    - Associate’s degree
    - Bachelor’s degree
    - Master’s degree
    - PhD
    - J.D.
    - Other - Please describe:
    - Prefer not to answer

12. In what area(s) is your formal education (for example computer science, business, mathematics)?

Appendix B Codebook Development

This appendix includes a description of the development of the sub-codebook presented in this paper and the full codebook for the overall study.

We began open coding with each author independently reading a subset of five interview transcripts (2,482 lines). Open coding, also called inductive coding, is an iterative process involving a constant comparison of data pieces to each other to induce a concept/code. With the intent to surface the meaning in each transcript, we marked and annotated to categorize the data. Codes were tentatively assigned to units of meaning within the data which include data snippets (phrases, sentences, paragraphs, or an entire answer to a question) that address a common topic.

After performing open coding independently, we met to discuss 1-2 transcripts at a time. A tentative, preliminary codebook containing identified codes was created after the first coding discussion. As coding progressed, we compared all units that had the same code to ensure suitability of that code and refine codes as necessary.

A near-final codebook was finished after reviewing the initial five interview transcripts. The first author then used the codebook to deductively code the remaining interviews using NVivo qualitative data analysis software. New codes that were identified during coding were added to the codebook, with previously coded interviews then re-examined to account for the additions. This process is inherently iterative. Note that a unit of meaning could be placed into multiple codes. For example, P08 was referencing the short training courses he provides to non-technical audiences when he said, *"I'm not going to make you into a security expert in 3 hours. It's not going to happen. But I want you to be able to have a conversation with one where you can be able to follow each other."* This data fragment was coded as both "Education and awareness" and "Empowerment." The final sub-codebook used for this paper is included in Appendix Table 1.

During this process, we wrote several analytic memos to reflect on interesting ideas that were starting to emerge. For example, one memo written early in the analysis process entitled "Education of Security Advocates" was the first attempt at capturing the technical and non-technical skills and discipline diversity noted in the interviews.

After coding all interview transcripts, we began to identify relationships between the codes. Related codes were then grouped into higher-level categories called axial codes. For example, interpersonal skills, context awareness, communications skills, and hope/optimism were grouped together into the axial code "non-technical competencies." These axial codes formed the basis of the identification of a unifying central concept or theme, in this case, "Skill and discipline diversity."

Appendix Table 1. Codebook. Codes with sub-bullets are more complex and fine-grained. Codes in bold have been solidified and were either used to develop the central theme of this paper or were mentioned at least in part as supporting data. Other codes have not been as deeply analyzed and may be refined in the future as additional themes are explored.

Career demographics
- **Formal education**
- **Career history**
- **Roles and identity**

Technical Knowledge
- **Technical skills**
- **Staying relevant**

Credibility/Reputation
- **Technical (individual)**
- Organizational

Interpersonal skills
- **Empathy**
- **Listening skills**
- **Humility**
- **Teaming**
- **Honesty**
- **Hope/optimism**
- **Understanding people**

Communication/translation skills

Context awareness

Service profession

Passion/enthusiasm

Audience type

Audience Perceptions of Security
- Scary
- Confusing/difficult
- Boring/irrelevant/apathetic

Security field
- **Security professional characteristics**
- **Perceptions of users/audience**
- **Diversity**

Risk-threat
- Actual risk-threat
- Discernment

Communication Methods
- **Channels**
- **Techniques**

Opinion Leaders

Usability

Intrinsic Motivations/Rewards - advocates
- **importance of the work**
- Interest/aptitude
- **Challenge/feeling of accomplishment**
- Enjoying working with others in the field

Extrinsic Motivations/Rewards (success indicators) - advocates
- **Evidence of behavior change (in others)**
- **Evidence of learning (in others)**
- Monetary reward
- Views/downloads

Frustrations

Barriers to good security practices
- Communication/framing
- People – biases, skill level
- Economic
- Organizational
- Policy
- Technology
- **Security field issues**

Solutions to security behavior problems
- Technology/automation
- Incentives/reward structures
- User empowerment/self-efficacy
- **Education and awareness**
- **Persuasion/selling security**
- Policy

Metaphors and analogies