Cybersecurity advocates: discovering the characteristics and skills of an emergent role

Julie M. Haney
Information Technology Laboratory, National Institute of Standards and Technology, University of Maryland, Gaithersburg, Maryland, USA, and

Wayne G. Lutters
College of Information Studies, University of Maryland, College Park, Maryland, USA

Received 6 August 2020
Revised 28 September 2020
Accepted 5 December 2020

Abstract

Purpose – Cybersecurity advocates safeguard their organizations by promoting security best practices. This paper aims to describe the skills and characteristics of successful advocates.

Design/methodology/approach – This study involved 28 in-depth interviews of cybersecurity advocates.

Findings – Effective advocates possess not only technical acumen but also interpersonal skills, communication skills context awareness and a customer service orientation.

Practical implications – Non-technical skills are deemphasized in cybersecurity training, limiting career progression into the cybersecurity advocate role for existing security professionals and those from other disciplines. This paper suggests improvements for professional development that encourage greater security workforce diversity.

Originality/value – To the best of the authors' knowledge, this study is the first to define and enumerate competencies for the role of cybersecurity advocate.

Keywords Professionals, Core competences, Education, Cybersecurity, Advocacy

Paper type Research paper

1. Introduction

The effects of cyber attacks can be devastating on personal, organizational, national and global levels, costing the global economy over US$ 6tn by 2021 (Cybersecurity Ventures, 2020). However, while security best practices are widely known, people routinely fail to protect their digital assets. A concerted effort is needed to change this status quo. In this paper, we describe *cybersecurity advocates,* who serve as catalysts for cybersecurity adoption.

Cybersecurity advocates 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 executives, office workers, technical staff and home users. Examples of advocates include: security awareness professionals working within organizations; security researchers who promote the use of security technologies; non-profit security advocacy staff

The authors would like to thank the study participants for generously offering their time and insights. The authors would also like to thank the anonymous reviewers whose comments helped improve and clarify this manuscript.

Information & Computer Security
Vol. 29 No. 3, 2021
pp. 485-499

2056-4961
DOI 10.1108/ICS-08-2020-0131

who develop security campaigns and publish guidance; and consultants who work to convince their clients to implement security measures.

Training curricula (NSA – National Security Agency and Department of Homeland Security, 2020) and work role frameworks (Petersen *et al.*, 2020) reveal that cybersecurity education is predominantly viewed through a technical lens, with little focus on non-technical competencies, such as communication and relationship management. These skills are critical to the advocacy role, which has a behavior change focus and impact. A complicating factor is that, while some advocates have conventional computing education, others come into the profession from non-technical disciplines. Currently, there are few resources for becoming effective cybersecurity advocates and no defined career track. This gap is likely due to there being little understanding of the actual work practices and characteristics that lead to successful advocacy.

In this first-of-its-kind investigation of cybersecurity advocates, we build upon our prior findings on advocates' techniques (Haney and Lutters, 2018) and professional motivations (Haney and Lutters, 2019) to address the central question: What are the professional characteristics and skills that cybersecurity advocates employ in their work? By examining these traits, we discovered evidence of discipline diversity beyond the technical competencies usually emphasized in preparatory and continuing education programs.

Our research has several novel contributions. The identification of the cybersecurity advocate role is our main contribution. We define and enumerate competencies for the role that can be used to augment current professional development resources. Additionally, we highlight the benefits of discipline diversity within the advocate community. Our work also uniquely identifies service orientation as a core aspect of cybersecurity advocacy. Accordingly, we see yet unrealized potential to frame this role as a people-oriented service profession, perhaps attracting a more diverse demographic who may not otherwise consider cybersecurity as a career choice.

2. Related work

2.1 Theoretical foundations

The concept of cybersecurity advocacy is informed by "change agents" in Diffusion of Innovations (DOI) Theory and risk communicators. These are literatures not previously applied to the cybersecurity domain in this capacity.

2.1.1 Change agents. The goal of security advocacy is positive behavior change and adoption of beneficial practices or tools. DOI Theory is useful in understanding this goal as it reveals factors that influence the acceptance of "an idea, practice, or object perceived as new by an individual or other unit of adoption" (Rogers, 2003). Here, change agents actively influence clients' adoption decisions. They have several responsibilities, including demonstrating a need for and intent to change, establishing an information exchange relationship, diagnosing problems, stabilizing adoption and fostering client independence. Change agents' success is positively correlated with their ability to develop credibility and a trusted working relationship with their clients (Rogers, 2003).

2.1.2 Risk communicators. Cybersecurity advocates motivate individuals to practice good security habits in large part by conveying and convincing them of cyber risks. While DOI Theory provides insight into how change agents influence adoption decisions, risk is not a central focus. The literature on risk communicators was a useful addition to our initial conceptualization of security advocates.

Kasperson *et al.* (1992) defined five risk communicator goals that hold across multiple domains (e.g. health, environmental hazards): diagnosing and creating trust; creating awareness strategies; understanding why concepts are hard to grasp and finding ways to

overcome this; developing mediating skills; and motivating the public to act. A foundational aspect of risk communication is establishing trust and credibility, so communicators must strive to exhibit interpersonal skills (e.g. empathy, honesty, openness, listening skills) and practice two-way communication with risk message recipients (Covello, 1997; Slovic, 1987). Effective communicators must ultimately serve as the bridge between experts and non-experts (Gordon, 1991). In addition to interpersonal skills, risk communication was observed to be a learned competency that includes: providing engaging and unambiguous communications; customizing information to target audiences; and assisting people in seeing the consequences of their decisions (Covello, 1997; Nurse *et al.*, 2011).

2.2 Security professionals

Cybersecurity advocates are a particular form of security professional. Before security roles can be compared, a baseline understanding of the discipline and its career preparation is required. Various efforts have sought to develop frameworks of necessary competencies for security professionals. The National Initiative for Cybersecurity Education (NICE) Framework published by the U.S. National Institute of Standards and Technology outlines the knowledge, skills and competencies for cybersecurity work roles (Petersen *et al.*, 2020). The SFIA (2018) expands these for more general information technology (IT) roles. In an effort to improve the pipeline of future security professionals, the Joint Task Force on Cybersecurity Education (2017) and other US Government agencies (NSA – National Security Agency and Department of Homeland Security, 2020) proposed curricular guidelines for cybersecurity degree programs. While comprehensive with respect to technical competencies, many of these resources under-emphasize non-technical skills.

Prior research, for example Botta *et al.* (2007) and Haber and Kandogan (2007), sought to understand the work practices of conventional security professionals who perform tasks such as: designing, administering or testing security-related infrastructure; creating security policies and procedures; assessing security vulnerabilities within systems and monitoring, detecting and responding to security events. While technical and analytic skills were often identified, communication and collaboration skills were also deemed important. Other researchers discussed skill deficiencies within the security workforce. Dawson and Thomson (2018) acknowledged that current cybersecurity curricula are largely technology based; however, to address the organizational and social aspects of cybersecurity, the future cybersecurity workforce will need to be proficient in communication, collaboration and social skills. In an industry survey, respondents identified "ability to understand the business" and communication as the top two most significant gaps they see among cybersecurity professionals (ISACA, 2016). To address this, some have advocated for more professional diversity by including non-technical skills in cybersecurity education programs and by building multi-disciplinary teams (Arbuckle, 2018; Hoffman *et al.*, 2012; Lawrence-Fowler, 2013).

2.3 Differentiating the advocate role

Our investigation was an iterative process of uncovering the cybersecurity advocate role. We first identified it as an emerging job function naturally occurring "in the wild." Our conceptualization then evolved to viewing cybersecurity advocates as an instantiation of the more generic roles of change agents and risk communicators found in the literature. We then looked to the security community to discover how this was becoming visible in the profession and how it differed from other security work roles.

As both change agents and risk communicators, advocates appear to have a unique orientation. Instead of a primarily technology-based mission, they are focused on educating,

engaging and empowering individuals to change their security attitudes and behaviors. This requires baseline technical competence, but so much more. While soft skills may be valuable for all security professionals, they appear to be essential for advocates.

We explored the evolving job titles and work descriptions of potential advocates within the security community. By conducting internet searches, completing candidate interviews and leveraging the first author's own related work experience, we confirmed that "cybersecurity advocate" was an emerging term-of-art among practitioners. We found several instances of security practitioners identifying as security advocates or evangelists (Arnou, 2020; Zorz, 2016). In many cases, advocates juggled multiple responsibilities, starting their advocacy by taking on informal roles in a part-time capacity. For example, a consultant may have a primary responsibility of security engineering but may also need to practice advocacy to persuade clients to remedy security deficiencies.

3. Methodology

To understand characteristics and skills of advocates, we conducted semi-structured interviews with these professionals. The study was approved by our institutional review board with informed consent but no compensation for participants.

3.1 Participant recruitment and demographics

Using researcher contacts and internet searches, we recruited individuals who performed cybersecurity advocacy as a significant component of their jobs. Since our investigation was an iterative process of discovery of the cybersecurity advocate role, we employed theoretical sampling throughout data collection (Corbin and Strauss, 2015). We recruited 4–5 participants at a time, with the initial two sets consisting of those who publicly self-identified as working primarily in advocacy. Subsequent sets of participants were purposely selected to include those who might be able provide additional insight on areas of interest that emerged from analysis of preceding interviews. For example, when several participants mentioned security awareness training as a form of advocacy, we subsequently made an effort to recruit security awareness professionals.

Our sampling strategy was aimed at ensuring suitability and maximizing diversity, while allowing interviewees to identify others performing advocacy roles. To account for the potential of different viewpoints and techniques, we sampled advocates with varying backgrounds and roles, working in a variety of sectors, performing advocacy roles on a part-time basis without an obvious title, and who served different audiences.

Table 1 summarizes participant information collected with a demographic survey, 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 technical 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 sector. When asked to describe their target audience, 10 said their audience was mainly external to their organization, 3 focused within their organization and 15 said both external and internal.

3.2 Data collection and analysis

We crafted a study in which data collection and analysis were tightly coupled and occurred in parallel, with analysis of data informing subsequent data collection decisions. As this is the first study to examine cybersecurity advocates, we used an inductive (bottom-up)

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	Non-profit 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	Non-profit 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	Non-profit 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	Non-profit 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	Non-profit director	***N***, I	N	B	tech, mgr
P28	Security awareness	***I***, E	N	B	end, tech, mgr

Notes: 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/external. **Audience Description**: dev=developers, end=organizational end users, fac=faculty, gen=general public, industry=industry partners, mgr=managers, non-tech=non-technical professionals, policy=public policy makers, stud=students, tech=technical staff

Table 1. Participant demographics

approach. Interview questions (Figure 1) were designed to uncover the definitional boundaries of advocates by examining work practices, professional motivations, challenges, perceived characteristics of successful advocates, and techniques. In this paper, we report on a subset of data focused on characteristics and skills.

Interviews lasted on average 45 min and were conducted face-to-face when possible (12 interviews) or via phone (9) or video conference (7). 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 (Corbin and Strauss, 2015). 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. 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 rich data. Our semi-structured interview approach was ordered enough for cross-

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 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 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.
    a. Which of those means do you think are the most effective? Why?
9. Do you feel that you're reaching the right population of people and organizations?
    a. What is preventing you from reaching the right people?
    b. What do you wish you could do to reach the right population?
10. How do you keep up with the latest in security?
11. What do you find most rewarding, if anything, about your role as a security advocate?
12. What do you find most challenging or frustrating, if anything, about your role as a security advocate?
13. What do you think are the biggest obstacles organizations face with respect to implementing security measures and technologies?
14. What do you see as your role in helping organizations overcome these obstacles?
15. What are other ways these obstacles might be overcome?
16. Is there anything else you'd like to add?

Figure 1.
Interview questions

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 independently reviewed five interviews and performed inductive, open coding to label units of data and look for meaning. We then met to discuss 1–2 transcripts at a time. A preliminary codebook containing identified codes was created after the first coding discussion. As coding progressed, we compared units with the same code to ensure code suitability and refine codes as necessary. A near-final codebook was finished after reviewing the initial five transcripts. The first author then used the codebook to deductively code the remaining interviews, adding new codes when appropriate. Previously coded interviews were then re-examined to account for code additions. During analysis, we wrote analytic memos to reflect on interesting, emerging ideas. After coding all interview transcripts, we identified relationships between codes and grouped them into higher-level categories (axial codes). Axial codes formed the basis for the unifying central concept "skill and discipline diversity." Figure 2 shows the coding progression (as outlined in Section 4).

3.3 Limitations

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 social desirability bias in which they adjust their answers to be more favorable to the interviewer, who was an experienced security professional. Limitations were primarily mitigated by the diversity of our participants and the constant comparison method of our analysis.

4. Understanding attributes of cybersecurity advocates

In this section, we describe professional attributes and competencies of advocates as identified in the interviews. We define the term "competency" as "an observable group of

related Knowledge and Skills" (Petersen *et al.*, 2020). We address these competencies at a high level only since the focus of our study was to uncover general characteristics, not create an exhaustive list of specific knowledge and skills like those in the NICE Framework.

We provide counts of the number of participants mentioning certain concepts to illustrate weight or unique cases, not as an attempt to reduce our qualitative data to quantitative measures.

4.1 Technical knowledge

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 audience. A security analyst noted, "if you don't know what you're doing, that's going to become apparent very quickly" (P01).

Staying up-to-date on constantly changing technology and security risks is not a trivial task, requiring significant and sustained effort, as a security consultant observed: "It's a way of life" (P10). Participants revealed a number of ways they try to keep abreast of the latest security happenings, including reading online information, joining security information sharing communities and attending security conferences. They also extensively draw on their professional network to keep updated on security risks and technologies.

4.2 Non-technical competencies

Technical proficiency is indeed important, but those trained only in computing may not have fully developed all 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 prowess 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 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).

4.2.1 Interpersonal skills. All participants noted that advocacy work requires an orientation towards people, 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" (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).

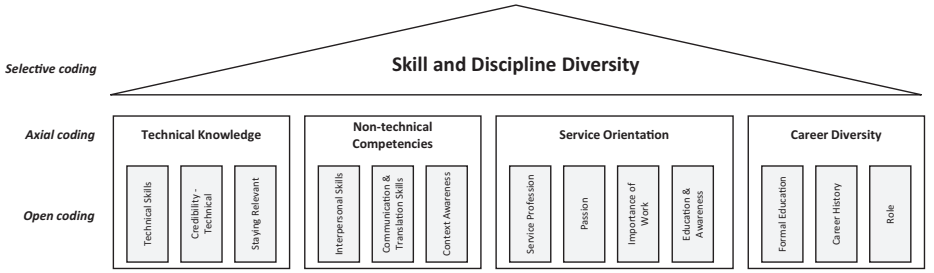

Figure 2.
Code relationships

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), humility (5) and empathy (4). 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).

4.2.2 Context awareness. In addition to technical and interpersonal skills, 22 participants revealed that cybersecurity advocates must be context aware, recognizing that unique audiences have different strengths, values and challenges. This awareness 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 [. . .] 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. 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).

4.2.3 Communication skills. Twenty-three participants mentioned the importance of effective communication skills. To be able to "sell" security, a good advocate should be context aware and tailor her communications for specific audiences, often serving as a translator between technical experts 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) (books, newsletters, papers, 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.

4.3 Service orientation

While technical and soft skills may be expected competencies of cybersecurity advocates, an unexpected finding was participants' strong sense of service in helping others to protect themselves and their information. Hogan *et al.* (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 and a sense of duty. Even though security problems may seem intractable, participants reflected that their job is too important to falter. A participant who worked with US 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 that they tried to remedy through education. Observing the impact of their efforts (e.g. behavior and attitude changes, security adoption or influences on policy) was especially gratifying. 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. A security engineer and part-time college instructor 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).

4.4 Discipline diversity

Our findings reveal that many participants brought to their advocacy work skills honed by formal education or prior careers outside of cybersecurity. This "discipline diversity" – the incorporation of individuals with non-technical professional training/experience into the cybersecurity advocate capacity – was viewed by participants as beneficial.

Fourteen participants had at least one non-technical degree, with eight having worked previously in non-technical positions. 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).

Discipline diversity was not just based on formal education. There were indeed several participants who had non-IT degrees but had worked almost exclusively in security roles prior to becoming advocates (P09, P11, P25). However, there were also participants who became security advocates immediately after having only worked in non-IT positions with no previous security experience (P06, P08, P15, P24, P27, P28).

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:

> 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).

P28, 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.

Three participants who had worked as lawyers became advocates because of their ability to understand the relationship between law, policy and cybersecurity. One said she was hired because her organization was:

> looking to have a lawyer on staff to help them translate [. . .] legal requirements for information technology into a language that [. . .] technologists could understand (P15).

P08, 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.

Four other participants with prior business-oriented experience leveraged their understanding of those contexts. When asked how he establishes trust and credibility, P02 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." A former management consultant's tendency to pitch cybersecurity as a "competitive advantage" (P27) helped convince corporations to implement incentives for rigorous security practices.

Participants also discussed the advantages of building multi-disciplinary advocacy teams. The CISO for a local government reflected on the complementary skill sets on her team:

> We have some technical folks [. . .] But we also have a lot of people with creative flair. And when you meld them all together, that's when we've gotten the best results (P26).

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 [public relations] communications experts [. . .] And I don't think we succeeded in spite of those, I think we probably have been successful because of those (P11).

These findings stress the benefit of teams representing a full range of advocacy skills, especially when individuals may not have all the competencies that are needed.

5. Implications

5.1 Reframing cybersecurity advocacy as a diverse, service-oriented profession

To enhance the future cybersecurity advocacy workforce pipeline, we see the potential benefit of cybersecurity education and recruitment programs expanding the scope of security professions by incorporating and advertising non-technical skills and service orientation as relevant attributes of security advocates. This reframing portrays cybersecurity as an exciting, interesting domain, for not just its technical challenges but also the complex, socio-technical aspects of the field. Based on our findings, we recommend the following.

5.1.1 Encourage the development of cybersecurity advocates from diverse disciplines. Individuals in non-security fields may not understand how valuable their skills might be for advocacy roles. While we maximized participant diversity with respect to gender, sector and audience, we did not purposely sample along education or career dimensions. Therefore, one of our most surprising findings was the resultant participant diversity regarding discipline. 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 sectors, contexts vary widely. Advocates working within a particular professional setting may have more intimate knowledge of that environment than an external advocate might. To increase the reach and effectiveness of security advocacy, encourage the development of cybersecurity advocates who are trusted insiders within diverse fields. The formation of multi-disciplinary security advocacy teams should also be encouraged since not everyone can be expected to possess all needed competencies.

5.1.2 Frame cybersecurity as a service-oriented profession. Given a cybersecurity career is often marketed through a predominantly technical lens, it may inadvertently dissuade those who seek a career in which they can regularly engage with people to make a positive, societal impact. While interpersonal and communication skills are generally noted as useful professional skills, we also identified service orientation as an attribute not typically

emphasized in security professions, but essential for advocacy roles. This orientation may aid in attracting currently underrepresented populations in security. For example, women and certain minorities are often deterred by the perception of security as a "solitary profession with no social benefit" (Shumba *et al.*, 2013) and lack of understanding of the breadth of opportunities available in security careers (Gonzalez, 2015). Additionally, the portrayal of advocacy as service-oriented may appeal to values of younger generations as the source of new cybersecurity professionals. These generations recognize social implications of technology, want to positively impact the world and desire a job with purpose (Myers and Sadaghiani, 2010; Seemiller and Grace, 2016), which are important qualities for cybersecurity advocacy as identified in our study.

5.2 Cybersecurity advocate career track

The 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 "accident" (P08) and "a perfect storm of good stuff that fell together" (P14). Although we recognize that career paths are often influenced by unanticipated opportunities, if there was a defined career track for this role, more people might purposefully aspire to become a cybersecurity advocate.

Our findings also suggest that the work of cybersecurity advocates has similarities to, but does not fall cleanly within, the boundaries of the security work roles identified in prior research. Furthermore, curricula (NSA – National Security Agency and Department of Homeland Security, 2020) and frameworks (Petersen *et al.*, 2020) emphasize technical knowledge without considering the full set of skills that resemble the work of an advocate.

Advocate skills may, in part, align with those of risk communicators in other domains. For example, like other risk communicators, advocates have similar goals of motivating people to act (Kasperson *et al.*, 1992), must be able to establish trust by demonstrating both technical expertise and non-technical skills and should understand their recipients' context. However, risk communication within the cybersecurity domain may have nuances that require communicators to operate differently, for example: cybersecurity being a dynamic field; relative lack of security knowledge by the public; difficult-to-measure economics of security; and less-tangible consequences (Haney and Lutters, 2018). In addition, unlike related risk communication domains, such as personal health, for which benefits are usually more individualistic, cybersecurity may be considered a common good that "nobody owns but everybody is involved in" (de Bruijn and Janssen, 2017). This is an area for which advocates' service orientation and their ability to communicate that to others may be particularly valuable.

We recommend the following for creating an advocate career track.

5.2.1 Define the cybersecurity advocate role. A more formalized definition of the cybersecurity advocate work role should enumerate knowledge, skills and abilities, all of which have been uncovered in our research. We note that the cybersecurity advocacy role is based on an orientation towards engagement/empowering, not on position/title or where an individual sits within the organization. For some professionals, the advocacy role may be in addition to other primary security roles (e.g. penetration tester), while others have full-time advocacy jobs (e.g. security evangelist). Also, when appropriate, advocacy competencies can be incorporated into other work roles that require them. For example, a recent proposal from the SANS Institute to establish a formal NICE framework work role for a "security awareness and communication officer" (SANS, 2019) (a type of cybersecurity advocate) includes a variety of non-technical

skills similar to those identified in our research, including communication, partnering and understanding human behavior.

5.2.2 Develop continuing education efforts for advocates. Continuing education efforts can aid in the progression to cybersecurity advocate from both security and non-security fields. Taking into account the high burnout rate among security professionals (Oltsik, 2017) and current, non-obvious career paths, these efforts may be a way to re-energize security professionals, provide an opportunity for a different career trajectory and reflect professionals' own natural evolution of competencies and interests. Developing advocates from the existing IT/security ranks within an organization may also be more advantageous depending on economic and market factors. When recruiting those from fields outside of IT, focus on facilitating the transition from working in non-security professions to cybersecurity advocacy. Include guidance on how to apply non-technical skills in the cybersecurity context and provide resources for mastering technical concepts.

Also provide guidance on how to be successful within an organizational context by encouraging the development of an organizational change agent skill set, as described by Markus and Benjamin (1996). Units could include approaches, personality characteristics, how to cope with challenges, ethical considerations and awareness of environmental conditions.

6. Conclusion

Cybersecurity advocates serve as essential 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 whether from within the current ranks of security professionals or from outside the field. 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 non-technical competencies and discipline diversity in both professional development and recruitment efforts for cybersecurity advocates.

Our study also suggests repositioning of cybersecurity work as not solely the predominantly technical work of its cryptographic roots, but as a people-oriented, service profession. This recharacterization suggests 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 decades ahead.

References

Arbuckle, A. (2018), "The solution to the cybersecurity talent gap is inclusion", available at: www.securityweek.com/solution-cybersecurity-talent-gap-inclusion (accessed 30 June 2020).

Arnou, S. (2020), "The security advocate", available at: www.thesecurityadvocate.com/ (accessed 15 September 2020).

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

Corbin, J. and Strauss, A. (2015), *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, 4th ed., Sage, Thousand Oaks, CA.

Covello, V.T. (1997), "Risk communication", in Waldron, H.A. and Edling, C. (Eds), *Occupational Health Practice*, 4th ed., Hodder Arnold.

Cybersecurity Ventures (2020), "The 2020 official annual cybercrime report", available at: www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (accessed 30 June 2020).

Dawson, J. and Thomson, R. (2018), "The future cybersecurity workforce: going beyond technical skills for successful cyber performance", *Frontiers in Psychology*, Vol. 9, p. 744.

de Bruijn, H. and Janssen, M. (2017), "Building cybersecurity awareness: the need for evidence-based framing strategies", *Government Information Quarterly*, Vol. 34 No. 1, pp. 1-7.

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

Gordon, J.A. (1991), "Meeting the challenge of risk communication", *Public Relations Journal*, Vol. 47 No. 1, p. 28.

Haber, E.M. and Kandogan, E. (2007), "Security administrators: a breed Apart", *Workshop on Usable IT Security Management*, ACM, Pittsburgh, PA, pp. 3-6.

Haney, J.M. and Lutters, W.G. (2018), "It's scary [. . .] it's confusing [. . .] it's dull: how cybersecurity advocates overcome negative perceptions of security", *Proceeding of the 14th Symposium on Usable Privacy and Security*, USENIX, Baltimore, MD, pp. 411-425.

Haney, J.M. and Lutters, W.G. (2019), "Motivating cybersecurity advocates: implications for recruitment and retention", *Proceedings of the Computers and People Research Conference*, ACM, *Nashville, TN*, pp. 109-117.

Hoffman, L., Burley, D. and Toregas, C. (2012), "Holistically building the cybersecurity workforce", *IEEE Security and Privacy Magazine*, Vol. 10 No. 2, pp. 33-39.

Hogan, J., Hogan, R. and Busch, C.M. (1984), "How to measure service orientation", *Journal of Applied Psychology*, Vol. 69 No. 1, pp. 167-173.

ISACA (2016), "State of cybersecurity implications for 2016", available at: www.isaca.org/cyber/Documents/state-of-cybersecurity_res_eng_0316.pdf (accessed 30 June 2020).

Joint Task Force on Cybersecurity Education (2017), "Curriculum guidelines for post-secondary degree programs in cybersecurity", available at: https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf (accessed 5 August 2020).

Kasperson, R.E., Golding, D. and Tuler, S. (1992), "Social distrust as a factor in siting hazardous facilities and communicating risks", *Journal of Social Issues*, Vol. 48 No. 4, pp. 161-187.

Lawrence-Fowler, W.A. (2013), "Multi-disciplinary approach to cyber security education", *Proceedings of the International Conference on Security and Management, Las Vegas, NV*, p. 1.

Markus, M.L. and Benjamin, R.I. (1996), "Change agentry – the next is frontier", *MIS Quarterly*, Vol. 20 No. 4, pp. 385-407.

Myers, K.K. and Sadaghiani, K. (2010), "Millennials in the workplace: a communication perspective on millennials' organizational relationships and performance", *Journal of Business and Psychology*, Vol. 25 No. 2, pp. 225-238.

NSA – National Security Agency and Department of Homeland Security (2020), "National centers of academic excellence in cyber defense", available at: www.iad.gov/NIETP/documents/Requirements/CAE-CD_Program_Guidance_2020.pdf (accessed 30 June 2020).

Nurse, J.R.C., Creese, S., Goldsmith, M., and Lamberts, K. (2011), "Trustworthy and effective communication of cybersecurity risks: a review", *1st Workshop on Socio-Technical Aspects in Security and Trust*, IEEE, Milan, pp. 60-68.

Oltsik, J. (2017), "The life and times of cybersecurity professionals", available at: www.issa.org/wp-content/uploads/2017/11/2017-ESG-ISSA-full-report.pdf (accessed 13 July 2020).

Petersen, R., Santos, D., Wetzel, K., Smith, M. and Witte, G. (2020), "NIST special publication 800-181 revision 1: workforce framework for cybersecurity (NICE framework)", available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf (accessed 5 December 2020).

SANS (2019), "NIST NICE work role description for security awareness and communications manager", available at: www.sans.org/security-awareness-training/blog/nist-nice-work-role-description-security-awareness-and-communications-manager (accessed 30 June 2020).

Seemiller, C. and Grace, M. (2016), *Generation Z Goes to College*, John Wiley and Sons, Hoboken, NJ.

SFIA (2018), "SFIA 7 - the seventh major version of the skills framework for the information age", available at: www.sfia-online.org/en/framework/sfia-7 (accessed 30 June 2020).

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

Slovic, P. (1987), "Perception of risk", *Science*, Vol. 236 No. 4799, pp. 280-285.

Zorz, M. (2016), "What a security evangelist does, and why you need one", available at: www.helpnetsecurity.com/2016/05/03/security-evangelist/ (accessed 15 September 2020).

About the authors

Dr Julie M. Haney is Computer Scientist and lead for the Usable Cybersecurity program in the Visualization and Usability Group at the National Institute of Standards and Technology (NIST). She conducts research about human aspects of cybersecurity, including the usability and adoption of security solutions and people's perceptions of privacy and security. Previously she spent over 20 years working in the Department of Defense as a security professional and technical leader primarily in the cyber defense mission. She has a PhD and M.S. in Human-Centered Computing from University of Maryland, Baltimore County, an M.S. in Computer Science from University of Maryland and B.S. in Computer Science from Loyola University Maryland. Julie M. Haney is the corresponding author and can be contacted at: julie.haney@nist.gov

Dr Wayne G. Lutters is Associate Professor in the College of Information Studies at the University of Maryland. Dr Lutters' research interests are at the nexus of computer-supported cooperative work (CSCW), social computing and social informatics. He specializes in field studies of IT-mediated work, from a socio-technical perspective, to better inform the design and evaluation of collaborative systems. Recent projects have focused on the human-side of information infrastructure. He has served as a Program Director for Human-Centered Computing at the National Science Foundation. He earned M.S. and PhD in Information and Computer Science from the University of California, Irvine.