Motivating Cybersecurity Advocates: Implications for Recruitment and Retention

Julie M. Haney
julie.haney@nist.gov
National Institute of Standards and Technology &
University of Maryland, Baltimore County
Gaithersburg, Maryland

Wayne G. Lutters
lutters@umd.edu
University of Maryland
College Park, Maryland

ABSTRACT

Given modern society's dependence on technological infrastructure vulnerable to cyber-attacks, the need to expedite cybersecurity adoption is paramount. Cybersecurity advocates are a subset of security professionals who promote, educate about, and motivate adoption of security best practices and technologies as a major component of their jobs. Successfully recruiting and retaining advocates is of utmost importance. Accomplishing this requires an understanding of advocates' motivations and incentives and how these may differ from other cybersecurity professionals. As the first study of its kind, we interviewed 28 cybersecurity advocates to learn about their work motivations. Findings revealed several drivers for cybersecurity advocacy work, most of which were intrinsic motivators. Motivations included interest in the field, sense of duty, self-efficacy, evidence of impact, comradery, and, to a lesser degree, awards and monetary compensation. We leverage these insights for recommendations on how to frame cybersecurity advocacy as a profession that fuels these motivations and how to maintain this across advocates' careers.

CCS CONCEPTS

• **Social and professional topics** → **Computing occupations**;
• **Security and privacy** → *Social aspects of security and privacy*.

KEYWORDS

Cybersecurity; advocacy; motivations; recruitment; retention

ACM Reference Format:
Julie M. Haney and Wayne G. Lutters. 2019. Motivating Cybersecurity Advocates: Implications for Recruitment and Retention. In *SIGMIS-CPR '19: ACM SIGMIS Computers and Personnel Research, June 20–22, 2019, Nashville, TN*. ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3322385.3322388

1 INTRODUCTION

Even with a rise in the frequency and severity of cyber-attacks, people often fail to adequately implement security best practices and technologies [28]. Given modern society's dependence on technology, the need for implementing effective cybersecurity ("the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation" [21]) is paramount. A critical role in this adoption is the cybersecurity advocate who, recognizing that technology alone cannot solve security problems, is adept at addressing the interpersonal, societal, economic, and organizational factors often impeding adoption.

Cybersecurity advocates are security professionals who promote, educate about, and motivate adoption of security best practices and technologies as a major component of their jobs. In addition to technical knowledge of the security domain, this role requires non-technical competencies, such as interpersonal skills, communication skills, and context awareness [16]. Advocates' audiences are diverse and may include home users, office workers, students, technical staff, developers, and executives. Examples of cybersecurity advocates include security awareness professionals, secure development champions, those who advocate for security frameworks, and security consultants.

Due to the emphasis on technical skills within the cybersecurity field [10] and an estimated worldwide cybersecurity workforce shortfall of three million [17], there may be a dearth of professionals possessing the mix of technical and non-technical skills required for cybersecurity advocacy. Therefore, recruiting new advocates and retaining those already in the role is of utmost importance. Accomplishing this requires an understanding of advocates' motivations and incentives and how these may differ from other cybersecurity professionals.

To address this gap, we conducted interviews of 28 cybersecurity advocates. This paper reports on a subset of results from our first-of-its-kind investigation of cybersecurity advocates' work practices. Our previous papers focused on cybersecurity advocate skills and characteristics [16] and how advocates overcome people's negative perceptions of security [15]. In this paper, we extrapolate implications for recruitment and retention by analyzing answers to the following research questions from the broader study:

- What are the motivations of cybersecurity advocates?
- What is most rewarding about their advocacy jobs?

Our findings revealed a number of drivers for cybersecurity advocacy work, most of which were intrinsic motivators. Motivations included interest in the field, sense of duty, self-efficacy, evidence of impact, comradery, and, to a lesser degree, awards and monetary compensation. In particular, sense of duty and evidence of impact are intrinsically tied to advocates' roles as change agents and educators and their direct interactions with their audiences.

SIGMIS-CPR '19, June 20–22, 2019, Nashville, TN

ACM ISBN 978-1-4503-6088-3/19/06…$15.00
https://doi.org/10.1145/3322385.3322388

We are the first to begin to discover and enumerate motivating factors for cybersecurity professionals who serve as advocates. By understanding these motives, we begin to form a picture of how to attract and retain those who would be successful in the advocate role. To that end, we discuss implications for framing cybersecurity advocacy as a professional role fueled by these motivations and how these incentives may be maintained across advocates' careers.

2 RELATED WORK

We turn to past research on professional work motivation to provide context for our study. Work motivation is "a set of energetic forces that originates both within as well as beyond an individual's being, to initiate work-related behavior, and to determine its form, direction, intensity and duration" [23]. Motivation is often described in terms of being either intrinsic or extrinsic. Intrinsic motivators arise from an individual's feelings about a work activity and are inherent within the work itself [1]. These motivators can include interest, enjoyment, or feelings of accomplishment. Conversely, people are extrinsically motivated when they do the work in order to "obtain some goal that is apart from the work itself" [1]. Within the workplace, extrinsic motivators may include recognitions and monetary compensation.

While intrinsic and extrinsic motivators do interact, psychologists have found that intrinsic motivators most positively impact employee performance, creativity, and job retention [13]. In fact, offering excessive extrinsic rewards for work that is already intrinsically rewarding can be detrimental and lead to a decrease in overall motivation [13].

Work motivations of technology professionals were first explored within information technology (IT) and information systems (IS) fields. Based on Shein's career anchors (factors that give stability and direction to a person's career) [24], Crepeau et al. [9] identified significant IS worker anchors that included identity, service, and variety. Over 10 years later, Sumner and Yager [26] perhaps captured the evolving landscape of IT work, finding that the most compelling anchors for IT workers included organizational stability and variety, while identity, competence, creativity, and autonomy were viewed as less important.

Others explored motivation through lenses other than career anchors. Thatcher et al. [27] revealed that intrinsic motivators positively affected IT workers' job attitudes and suggested that further research is needed to identify nuances in motivation among different job types. Lounsbury et al. [20] found that disposition to teamwork and the motivation to achieve were positively related to both job and career satisfaction. Blum [5] explored gender-specific motivations for entering the computer science field, which is a primary feeder discipline into cybersecurity. He found that for men, computer science was seen as an interesting, fun discipline. Women, however, viewed it more as a means to achieve a socially motivated purpose.

Subsequent studies built upon this work to explore motivators within the much newer cybersecurity field. Chai and Kim [7] and Bashir et al. [4] identified security skill self-efficacy as a strong motivator for attraction to cybersecurity careers. Grounded in a literature survey, Dawson and Thomson [10] suggested that the future cybersecurity workforce should include those with a love of learning, a strong desire to work in teams, and sense of civic duty. Our previous paper on advocate characteristics revealed service orientation and an interest in incorporating diverse disciplines within the work [16].

Others focused on retention. Burrell et al.'s [6] analysis of focus groups of government cybersecurity employees implied that intrinsic motivators are more effective than extrinsic motivators for retention and success in the public sector since government institutions cannot compete with private-sector salaries. An industry survey [18] revealed that over 60% of cybersecurity job seekers desire to work in a job where they are empowered and can protect data and people, while roughly half were motivated by salary.

While this literature provides valuable insight, it is unclear as to whether these same motivations apply to cybersecurity advocates. While their jobs possess similarities to those of other cybersecurity and IT workers, advocates play a unique role. For example, like their counterparts they must possess technical expertise, but their main focus is not on technology administration or oversight. They must be skilled in the art of influence, but are not technical sales representatives or marketers. Our research discovers where advocates' motivations are similar and where they differ from those performing other cybersecurity roles and how these distinctions might influence advocate recruitment and retention techniques.

3 METHODOLOGY

We conducted semi-structured interviews of 28 cybersecurity professionals who performed advocacy tasks as a significant component of their jobs[1]. We followed a research approach inspired by Grounded Theory in which data collection and analysis are conducted concurrently, with analysis influencing decisions on future data collection [8].

The study was approved by our institutional review board with participants providing informed consent and receiving no compensation. To protect confidentiality, data associated with a participant were assigned a code (e.g., P16).

3.1 Recruitment and Participants

We initially recruited from researcher contacts and internet searches those who self-identified as security advocates. We then considered snowball recommendations that allowed interviewees to identify other advocates. Our definitional boundary of the cybersecurity advocate role continued to evolve and guided subsequent recruitment as interviews progressed. To ensure the representation of a broad range of advocacy contexts, we purposefully selected individuals who performed different types of advocacy (e.g., security awareness training, security consultation) who worked in a variety of sectors, and who served different types of audiences. This resulted in a collection of information-rich cases [22].

To guide recruitment, we practiced theoretical sampling throughout data collection [8]. We recruited participants four or five at a time. The subsequent group of potential participants was then selected to include those who might be able to provide additional or different insights on areas of interest surfacing from the analysis of the preceding set. For example, when several participants raised

[1]This section is summarized from the methodology sections of previous papers [15, 16]

gender diversity concerns, we subsequently recruited additional female participants.

Table 1 provides an overview of relevant participant demographics, with some roles generalized to preserve anonymity. Our study sample consisted of 10 female and 18 male professionals with all having at least five years of experience in the cybersecurity field, and 22 having more than 10 years. Fourteen participants had at least one non-technical degree (e.g., philosophy, communications, business, and law), with 11 of those having no formal technical degrees. Participants had worked within diverse sectors throughout their careers, including government, private industry, education, and non-profit organizations, with most having experience in more than one sector. Ten participants advocated security mainly external to their organization, three were focused within their organizations, and 15 advocated both internally and externally.

3.2 Data Collection

Interviews lasted on average 45 minutes and were audio recorded and transcribed. Interview questions addressed work practices, professional motivations, rewards and challenges, characteristics of successful advocates, and advocacy techniques. The interview protocol is included in Appendix A. All but one participant also completed an online demographic survey that included career background information.

The semi-structured nature of the interviews allowed for follow-on questions and the elicitation of rich data. The interview structure was ordered enough to facilitate cross-participant comparison, but open-ended enough to permit participants to raise themes we had not imagined in advance. Interviews were conducted until we reached theoretical saturation, the point at which no new ideas emerged from the data during our concurrent analysis [8]. Since the goal of qualitative research is rich, holistic contextual understanding, and not predictive generalization, the attainment of theoretical saturation indicated that we had reached an appropriate number of interviews [8]. This number also well exceeded the recommended minimum sample size of 12-20 for identifying themes in qualitative interviews [14].

3.3 Analysis

Methods for data coding and analysis were informed by Grounded Theory, which allows for an organic emergence of themes [8]. Each author initially reviewed five interviews and conducted inductive, open coding to label and discover meaning. We later met several times to discuss concepts identified from the interviews and begin to develop a codebook. The first author then used the codebook to recode the initial five interviews to align, and then deductively code the remaining interviews. As analysis progressed and additional concepts emerged, we made adjustments to the codebook. We then evolved our analysis into axial coding (the recognition of relationships among codes), captured emerging ideas within analytic memos, and identified core concepts (selective coding) [8].

4 FINDINGS

In this section we report on motivations for cybersecurity advocates as mentioned by study participants. These motivators contributed to a great passion for advocacy work, as expressed by 15 participants. One participant commented that advocacy *"became kind of calling over the years for me" (P04).* Another, from a non-profit, reflected on her work: *"I love it. It actually has a lot of the different gratifying qualities I enjoy in a job" (P24).*

No appreciable differences were observed among the various demographic groups (e.g., gender, formal education). In this section, we also provide participant counts to reflect frequency of concepts mentioned during the interviews. However, because our analysis was focused on identifying centrality of data codes to concepts, we caution the reader against making inferences beyond frequency.

4.1 Personal Interest

The belief that cybersecurity is a challenging and an *"intellectually exciting" (P16)* field was a motivator for 19 participants. A graphic designer-turned-advocate commented that the security awareness profession is *"like a giant puzzle. And challenges are my thing. I like being able to put effort into something that's creative and interesting and different" (P28).*

Since the cybersecurity field is relatively young and quite dynamic, it offers opportunities for innovation, which appealed to participants. One said, *"I'm attracted to areas where there's new things to do,... where it's not really established, where I get to solve a new problem, and solve a new problem that matters" (P19).* A security awareness program director at a public university commented,

> *"It's ever-evolving... I find it to be a challenge because threats and vulnerabilities in all environments... are always there and they're always becoming more sophisticated... That's what motivates me to stay in" (P14).*

We also identified an interest in interdisciplinary work (7 participants). The nature of advocates' work is multi-faceted in that it must consider challenges *"at the people level, at the business level, the strategic level" (P27).* An advocate with a strong cybersecurity background fell into security awareness when she became exposed to the human aspects of security: *"the power of human motivation fascinates me. And I think if I wasn't doing this, I'd probably be a behavioral psychologist or something" (P21).*

Another participant worked at the intersection of cybersecurity and usability:

> *"I tend to have an interest in things that are interdisciplinary and kind of at the border of different things... So, this combination of the technical and human factors interests me, and I guess I seem to be good at it, so that encourages me to want to do more" (P07).*

4.2 Sense of Duty

Almost all participants (26) exhibited an acute sense of duty and service. For example, a participant who works to influence public policy stated, *"I think we're making the world a better place" (P06).*

At the core of sense of duty was the perception of the importance of advocacy work. Although cybersecurity problems may seem overwhelming, participants thought that potential personal, economic, and national security consequences were too significant for them not to act. As one participant said, the role of cybersecurity is important *"in our future economy and in the management of social*

Table 1: Participant Demographics

ID	Gender	Role	Sector	Education	Audience
P01	M	Security analyst	***G***	T,N	B
P02	M	Professor	***E***,G,I	T,N	B
P03	F	Computer scientist	***G***,I	T	B
P04	M	Security evangelist	***N***,G	T	B
P05	M	Security researcher	***I***,G	T	B
P06	M	Director	***N***,G,E,I	N	B
P07	F	Senior technologist	***G***,***E***,I	T	E
P08	M	Security consultant	***I***	N	E
P09	M	Training director	***E***,G	N	E
P10	M	Instructor, consultant	***I***,***E***,G	T	E
P11	M	Director	***N***,I	N	E
P12	M	Security engineer	***I***,***E***,G	T	E
P13	M	Security engineer	***I***	U	I
P14	M	Security awareness director	***E***,G	N	B
P15	F	Director	***N***,***E***,I	N	B
P16	M	Computer scientist	***G***,E,I	T,N	I
P17	M	Researcher	***I***	T	E
P18	M	CIO	***E***	T	B
P19	F	Senior Architect	***I***	T	I
P20	M	Professor	***E***,***G***	T	E
P21	F	Company co-founder	***I***,G	T	E
P22	M	Security researcher	***I***, E	T	B
P23	F	Security consultant	***I***,E	N	B
P24	F	Director	***N***	N	E
P25	F	Deputy CIO	***G***,I	N	B
P26	F	CISO	***G***,I	T	B
P27	M	Director	***N***,I	N	B
P28	F	Security awareness director	***I***,E	N	B

Sector (***Current***,Past): E=Education, G=Government, I=Industry, N=Non-profit; **Education**: T=Technical degree, N=Non-technical degree, U=unknown/not reported; **Audience**: I=Internal to own organization, E=External to own organization, B=Both internal and external

issues like privacy and the way that we interact as social creatures across society. Cybersecurity is central to all of that" (P04).

Several advocates saw the potential of poor cybersecurity resulting in the loss of lives. One participant warned, *"If we don't get computers right, people are going to starve. And right now, we're not doing a good job" (P16).* Another advocate who leads a non-profit discussed his group's motivation:

> *"We had said we want to save lives through security research. It was really wherever bits and bytes meet flesh. That could be cars, medical devices, industrial control systems. But everyone's so focused on data and the confidentiality of data… We're spending nothing on our life and limb" (P11).*

Precipitated by the importance of the work, participants had a keen desire to help people navigate the dangers and complexities of the cyber world. A usable security champion commented, *"I like making people's lives easier" (P03).* Another participant said *"There's huge difference between my job satisfaction level when I know what I'm doing, day-in and day-out, is out there helping ultimately the citizens and the general population" (P26).*

All participants attempted to address the gap in security knowledge by playing formal or informal educator roles. Fifteen served as educators/mentors to future and current security professionals. A veteran advocate stated:

> *"I'm really conscious of my role as an old guy in this, a pioneer, someone who's got a lot of history. And so there's an excitement to that, to feel that you've seen a lot of things happen, made a lot of mistakes you get to convey to other people… So, feeling responsible. I feel the role there. It feels like I'm supposed to be doing this" (P04).*

Other advocates educated less-technical audiences. For example, one participant extended her advocacy responsibilities outside of work:

> *"I actually spend a significant time of my personal life … educating teachers and working with the old lady gang on my block to get them to understand security so that they're not in a position where they have to deal with some criminal stealing their information or stealing their hard-earned money" (P23).*

Another discussed his upcoming talk to a local community group:

> *"I'm trying to tune the message. What should citizens care about?… They're all great people, but they're not going learn what I've learned. So what is it that I can tell them that will*

help them, to get their attention, to cause them to change behavior?... there's a lot of great technologists in this business, but based on technology, we're not going to change people's behavior – well, only in niches. So, how do we put our work in other people's context" (P04)

4.3 Self-Efficacy

Self-efficacy, a belief in one's own ability to accomplish a task or exert control in specific situations [3], can be an important motivator [4, 7]. A large part of self-efficacy is self-confidence that one has the necessary knowledge and skillsets.

All participants exhibited self-confidence in their abilities to effectively perform advocacy tasks. This confidence was gained through years of experience and continuous learning. An advocate reflected on how his involvement with operational and threat intelligence organizations contributed to his effectiveness: *"Those two perspectives help me bring some unique value to the problem" (P05).*

Other advocates expressed confidence in their non-technical "soft" skills which were often deemed as more important than technical skills in advocacy work. For example, the ability to translate technical topics into layman's terms was noted as an important competency by 24 participants. When giving presentations to non-technical audiences, one participant commented, *"I seem to have the magic power to make these things make sense" (P08).*

4.4 Evidence of Impact

Since the goal of cybersecurity advocacy is behavior change, evidence that an advocate's recommendations have been understood, concurred with, and acted upon served as strong motivators for our participants and contributed to self-efficacy (23 participants). One participant said the most rewarding part of her job was *"seeing the impact, seeing some difference was made ... however minor or modest" (P19).*

We must also note that, although most advocates focused on successes, others were more forthcoming about challenges. When asked about his professional motivation, one participant commented on his frustrations:

"I'd love to say that it's to help people fight the good fight and make the world a better place. And it is certainly part of that, but I have to say, it isn't all that because, if it was, I would be very discouraged... We as an industry [are making the same mistakes] we've been making forever" (P10).

In the following subsections, we describe ways in which advocates realized the impact of their work as categorized by the sources providing evidence of impact.

4.4.1 Organizational Impact. Impacting organizations (mentioned by 10 participants) can be especially challenging since organizational barriers to cybersecurity, such as security culture, can be difficult to change. Therefore, a positive shift in attitude often provided hope of future behavior change. One participant commented:

"The impact isn't always... an easy thing to quantify in this field. So, I think a lot of times it's when the organization starts showing the passion, starts showing and are being responsive to the ideas you're trying to suggest. That can be very rewarding" (P05).

Another advocate, who had spent a substantial amount of his career conducting vulnerability assessments, talked about a feeling of accomplishment coming with

"the knowledge that the people were really onboard and believed what it was they were doing, believed that what we were telling them was important, and had the right guidance and the right authority to be able to move forward with it" (P01).

One participant spoke about how the effectiveness of a security awareness program might be measured by incremental shifts in security culture:

"It goes beyond just behavior, but more on the culture. So when you're talking to people, if they have a positive attitude about cybersecurity, a positive attitude about the cybersecurity team, if they feel like their behaviors have a positive impact, that's the first real big indicator that you've got a long-term win. Now the problem you have is changing culture's a three to ten year process" (P09).

4.4.2 Individual Impact. Eleven participants talked about the satisfaction of educating and making an impact on individuals. One advocate said:

"I always get really excited when I can just tell people have learned something. So when I see that little lightbulb come on... when I get confirmation that something I've said makes a difference, I get really excited" (P23).

A participant noted that, after giving a presentation,

"I definitely like interacting with people and people telling me, 'Wow, I learned something. I can use this. I'm going to change what I do, and this will help me.' I find that rewarding" (P07).

Another commented that he feels energized

"when I'm working with an adult, and they have the 'Eureka!' moment. They're struggling with understanding something, and you kind of sit next to them, and then they get it and you can see it in their eyes. Often a high-five moment happens" (P10).

4.4.3 Policy Influence. Five participants were able to influence broad-reaching cybersecurity policies. One participant who had worked in the government sector talked about how his organization had *"shaped the spending of hundreds of millions of dollars and the behavior of thousands" (P04).* P06's non-profit successfully lobbied for a substantial paradigm shift in cybersecurity public policy within the United States. P11 influenced medical device policy that prevented serious vulnerabilities from claiming lives.

4.4.4 Transfer of Knowledge. A deeply satisfying aspect of the job is the observation of the target audience taking the information they had learned and transferring that to others, as was mentioned by eight participants. A participant told a story about how an elderly neighbor whom she had taught cybersecurity best practices taught her son a lesson:

"Her son was buying a house, and she kept telling him, 'Don't email that stuff. Don't email your personal stuff.' Well, probably

about two weeks into purchasing the home, he realized that his email had been completely compromised…She saved him probably three million dollars because what happened is, in the middle of setting up escrow, someone asked for a bank account number. It wasn't anyone from the real estate firm" (P23).

Three participants discussed their roles in helping good security habits blur across the home/work divide. For example, one participant remarked,

"if you can train them with their home life and help them there, too, they can hopefully bring those behaviors to work and bring that sense of awareness up. So a lot of the organizations share those personal, consumer-focused resources with their employees so they can keep their families safe at home, too" (P24).

A security awareness program director provided another example:

"We had a videotape…One of the presenters…had been kidnapped. She had been social engineered by a man online…And I know some of the people took their laptops home, logged in, and made their kids watch that. So I think that's great, too, when the information that you're giving at work, people are sharing with friends and family, too" (P28).

4.4.5 Metrics. Nine participants viewed metrics as motivating evidence that they were on the right path with their approaches. Metrics mentioned by participants included how many people accessed publications and videos, the number of newsletter subscriptions, attendance of security events, the growth of non-profit membership, and statistics showing improvement in security behaviors. A participant discussed the importance of metrics in showing success of an organization's security awareness program: *"initially you may have to measure success by some specific behaviors such as phishing, exposing of sensitive data, use of ID badges and things like that" (P09).*

Advocates monitored these metrics as one indicator of both the reach of their message and effectiveness of a communication channel. For example, one participant noted that one of her talks had been recorded and posted online and had *"been viewed like two million times…There's a lot of bang for that buck" (P07).* A participant whose organization produced cybersecurity implementation resources said:

"We create specific things, sort of products to give away, ideas and papers. So part of that is it comes with some natural mechanism now to calibrate feedback. How often is it downloaded, how often is it referenced?…So we see lots of interest worldwide. We can count how many tens of thousands of downloads there have been" (P04).

4.4.6 Praise. Praise is an extrinsic motivator that, when sincere, can significantly contribute to intrinsic motivation. Fourteen participants felt valued after receiving positive feedback from their audience. Some feedback was more formal, often obtained through surveys. For example, a non-profit advocate commented:

"We have teams to reach out to adopters of our work, talk to them, ask them questions through surveys, write down use cases if they're willing, that sort of thing …feedback is not an issue. We get a lot of that. I'd say it's overwhelming positive" (P04).

Informal feedback, such as face-to-face comments and email, seemed to be most personally satisfying. A participant who advocates to lawyers talked about one member of his audience saying, *" 'This is amazing! So many lawyers don't understand this.'…it's wonderful to get those sorts of reactions" (P08).* A security awareness director at a university remarked:

"I'll get stuff directly if I run an event of some kind, an awareness event, whether it's a conference or just a small brown bag session. I will receive emails from attendees saying, 'Hey, this was extremely helpful. I was unaware of XYZ component of data privacy. Or HIPAA [Health Insurance Portability and Accountability Act] privacy.' Whatever the topic might be. So the feedback that I receive in many instances is informal feedback" (P14).

4.5 Comradery

When asked about the rewards of their jobs, seven participants discussed their enjoyment working with others in the field. Whereas this motivation is not unique from other professions, it highlights the importance of a sense of belonging and collaboration in the cybersecurity advocate role and runs counter to commonly-held stereotypes of cybersecurity being a solitary profession [25].

A security course instructor and consultant commented, *"most of my very close friends are in this industry. I love to spend time with them thinking good thoughts" (P10).* A security evangelist at a non-profit described the benefits of working with a large group of volunteers to produce security guidance:

"It's a business full of really bright people, lot of diverse, creative, smart people of good will…So I love that part of it, the sort of community, this collaboration…it's something that's personally satisfying" (P04).

The interactions advocates have with others in the field are not just personally satisfying but are a necessary component of the job. Because of the distinctly dynamic nature of the cybersecurity field in which major developments can occur on a daily basis, advocates rely on a symbiotic relationship of receiving and contributing information within their personal networks. For example, an advocate who is active in a security awareness community commented, *"not only am I always giving to the community, I'm listening to the community…So, I always understand the latest and greatest risk from a human side" (P09).*

4.6 Awards and Monetary Compensation

Only five participants mentioned official recognitions or monetary compensation as motivators. One participant, referencing her team's best website award, said, *"I love it when my team is recognized" (P26).* Another was motivated by continued research funding: *"if they didn't like what you were doing, and they didn't think there was value, they wouldn't continue to fund you. And so, our funding's pretty stable" (P03).*

When asked about the rewards of his work, one advocate first mentioned the fun he has educating youth about cybersecurity and

the gratitude of his clients. However, he was then quite frank when he also included financial reward:

> *"As long as you're not cheating people or doing something dishonest, if you're providing real value, the way people indicate that you're providing real value to them is by paying you. So the more that they pay you, the more value you're providing…So I know that might sound crude, and maybe I should be more noble,…but I always realize at the end of the day, I gotta make payroll" (P10).*

5 IMPLICATIONS

Our findings confirm many of the same motivations as IT and cybersecurity professionals identified in the prior literature, such as sense of duty/service, self-efficacy, working with others, and interest, although sometimes to different degrees. We also similarly found an emphasis on intrinsic motivations (e.g., personal interest and sense of duty) inherent in the work of cybersecurity advocacy and its immediate goal of enacting positive behavior change. However, even extrinsic motivators (e.g., praise and compensation) were contributors to intrinsic motivation. For example, we observed that most participants were not ego-driven, so praise was viewed in the context of reinforcing self-efficacy and sense of duty.

Despite the similarities, we also recognize the uniqueness of the cybersecurity advocate role versus traditional IT or cybersecurity professionals, such as analysts, administrators, and system architects. To be effective, advocates must be more socially-oriented and skilled in persuasion and communications then their non-advocate colleagues [16]. They appear to be driven by a sense of duty and evidence of real impact, and often have larger spheres of influence. We therefore see the need for a more nuanced approach to feature advocate motivators in recruitment and retention by 1) advertising cybersecurity as a profession that has the potential to fuel these motivations via an advocacy role, 2) increasing motivations by providing opportunities for traditional cybersecurity professionals to progress into advocate positions, and 3) sustaining motivation for current advocates by documenting impact and providing energizing feedback.

5.1 Recruitment

When marketing cybersecurity positions having advocacy duties, in addition to touting the work as interesting and challenging {supported by section 4.1}, there should be emphasis on the important service to individuals and society {4.2}. For example, when recruiting advocates for jobs in the public sector, salaries can seldom compete with those in private industry, so appealing to motivators like a sense of civic duty and national pride may be especially helpful in attracting qualified individuals [10]. Service orientation of the work may also appeal to currently underrepresented populations in the cybersecurity workforce who may perceive cybersecurity as having no social benefit [25] or women who desire a career with a socially motivated purpose [5].

The opportunity to work collaboratively with talented, diverse people from multiple disciplines should also be highlighted {4.1}. This emphasis may counter a lack of awareness of the breadth of opportunities available in security careers [12] and belief that only those with deep technical skills can be successful [11, 12]. The interdisciplinary framing might help attract individuals from other fields who possess important non-technical skills and unique perspectives and encourage a greater sense of self-efficacy {4.3}. Additionally, an emphasis on the value of diversity may encourage participation of women and minorities who otherwise may be deterred by the stereotype of a white male, hacker-dominated workforce [2, 11].

5.2 Retention

Due to the dynamic nature of cybersecurity, organizational challenges, and human nature, the work of advocates can sometimes be daunting and thankless, requiring perseverance and resilience. In addition, individuals qualified for cybersecurity advocate positions possess a valuable blend of skills [16, 19], so are in danger of being recruited away by others. Therefore, special emphasis should be placed on their retention.

To aid in retention, foster advocate motivation, and encourage progression of current professionals into advocate roles, we propose the following recommendations for employers.

(1) Learn to recognize those who are doing advocacy work within the organization, even if in the background. Offer sincere praise and feedback about their successes (even if minor) and tout their mix of technical and non-technical skill. Provide opportunities to assume more responsibility for security promotion activities. {4.3, 4.4}
(2) Provide ample opportunity for advocates to receive direct feedback from their audience (face-to-face especially) about their efforts. Implement mechanisms to measure effectiveness and value of advocacy approaches. {4.2, 4.4}
(3) Support advocates in trying innovative approaches. {4.1, 4.3}
(4) Encourage advocates to participate in collaborative and information sharing opportunities with others working in related areas. {4.1, 4.5}
(5) Clearly communicate to the workforce that advocates are supported by leadership as important contributors in protecting people, systems, and information. {4.2, 4.3}
(6) Arm advocates with professional development and continuous learning opportunities that can aid them in their jobs. This learning should address the interdisciplinary nature of cybersecurity and include organizational, social, and technical aspects of cybersecurity. {4.1}
(7) Be cautious with offering excessive extrinsic incentives as these may interfere with intrinsic motivation. However, try to promote and pay advocates commensurate with the value they bring to the organization. If that is not possible, provide advocates with clear feedback about the importance and value of their work. {4.2, 4.4, 4.6}

6 LIMITATIONS

Our study is limited in that interviews are commonly subject to self-report and social desirability bias in which participants may adjust their answers to appear more acceptable to the interviewer. These biases may have particularly been a factor when so few participants mentioned monetary compensation as a motivator. In addition, although an interview protocol was used to ensure consistency across several predetermined topics, the semi-structured

interviews allowed for exploration of ideas that may not have been discussed equally in all interviews. Bias and consistency concerns were primarily mitigated by the diversity of our sample and constant comparison method of our analysis.

As the first to look at cybersecurity advocacy, we are discovering variables of interest that can be validated in future studies. For example, follow up efforts are underway to observe cybersecurity advocacy in practice within organizations.

7 CONCLUSION

Cybersecurity advocates serve as important enablers to security adoption. Our study is the first purposeful effort to learn about their work motivations. Most critically, we suggest ways to leverage these motivations in cybersecurity advocate recruitment and retention efforts to better position the cybersecurity workforce to meet the challenges of the future.

DISCLAIMER

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology nor does it imply that the products mentioned are necessarily the best available for the purpose.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their comments that helped improve the quality of this paper.

REFERENCES

[1] Teresa M. Amabile. 1993. Motivational synergy: Toward new conceptualizations of intrinsic and extrinsic motivation in the workplace. *Human Resource Management Review* 3, 3 (1993), 185–201.
[2] Sharmistha Bagchi-Sen, H. Raghav Rao, Shambhu J. Upadhyaya, and Sangmi Chai. 2010. Women in cybersecurity: A study of career advancement. *IT Professional* 1 (Jan. 2010), 24–31.
[3] Albert Bandura. 1977. Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review* 84, 2 (1977).
[4] Masooda Bashir, Colin Wee, Nasir Memon, and Boyi Guo. 2017. Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security* 65 (2017), 153–165.
[5] Lenore Blum. 2001. Women in computer science: the Carnegie Mellon experience. *women@ scs2* 2, 1 (2001).
[6] Darrell Norman Burrell, Maurice Dawson, William Quisenberry, Aikyna Finch, and Angelique Goliday. 2012. An exploration of government talent management strategies for information assurance and cyber-security employees in organizations with public health and safety missions. *Journal of Knowledge & Human Resource Management* 4, 8 (2012).
[7] Sang-Mi Chai and Min-Kyun Kim. 2012. A Road To Retain Cybersecurity Professionals: An Examination of Career Decisions Among Cybersecurity Scholars. *Journal of The Korea Institute of Information Security and Cryptology* 22, 2 (2012), 295–316.
[8] Juliet Corbin and Anselm L. Strauss. 2015. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (4th ed.). Sage, Thousand Oaks, CA.
[9] Raymond G. Crepeau, Connie W. Crook, Martin D. Goslar, and Mark E. McMurtrey. 1992. Career anchors of information systems personnel. *Journal of Management Information Systems* 9, 2 (1992), 145–160.
[10] Jessica Dawson and Robert Thomson. 2018. The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology* 9 (2018).
[11] Katharine D'Hondt. 2016. *Women in Cybersecurity.* Master's thesis. Harvard University, Cambridge, MA.
[12] Matthew D. Gonzalez. 2015. Building a Cybersecurity Pipeline to Attract, Train, and Retain Women. *Business Journal for Entrepreneurs* 3 (Sep. 2015).
[13] Richard A. Griggs. 2010. *Psychology: A concise introduction.* Macmillan.
[14] G. Guest, A. Bunce, and L. Johnson. 2006. How many interviews are enough? An experiment with data saturation and variability. *Field Methods* 18, 1 (2006), 59–82.
[15] Julie M. Haney and Wayne G. Lutters. 2018. "It's Scary…It's Confusing…It's Dull": How cybersecurity advocates overcome negative perceptions of security. In *Proceedings of the Symposium on Usable Privacy and Security.* USENIX, Baltimore, MD, 411–425.
[16] Julie M. Haney and Wayne G. Lutters. 2018. Promoting skill and discipline diversity in cybersecurity advocacy. https://cdn.website-editor.net/22097006d5ba4ddbb1a13216c1bd98ca/files/uploaded/SP-JoC-18-05002.pdf. *Emerging Trends in Cybersecurity: Journal of Cybersecurity - Online* (October 2018).
[17] ISC2. 2018. Cybersecurity professionals focus on developing new skills as workforce gap widens - ISC2 Cybersecurity Workforce Study. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx.
[18] ISC2. 2018. Hiring and Retaining Top Cybersecurity Talent. https://www.isc2.org/-/media/Files/Research/ISC2-Hiring-and-Retaining-Top-Cybersecurity-Talent.ashx.
[19] Ray Lapena. 2017. Survey Says: Soft Skills Highly Valued by Security Team. https://www.tripwire.com/state-of-security/featured/survey-says-soft-skills-highly-valued-security-team/.
[20] John W. Lounsbury, Lauren Moffitt, Lucy W. Gibson, Adam W. Drost, and Mark Stevens. 2007. An investigation of personality traits in relation to job and career satisfaction of information technology professionals. *Journal of Information Technology* 22, 2 (2007), 174–183.
[21] National Initiative for Cybersecurity Careers and Studies. 2019. Glossary. https://niccs.us-cert.gov/about-niccs/glossary.
[22] Michael Q. Patton. 2015. *Qualitative research and evaluation methods* (4th ed.). Sage, Thousand Oaks, CA.
[23] Craig C. Pinder. 2014. *Work motivation in organizational behavior* (2nd ed.). Psychology Press.
[24] Edgar H. Schein. 1978. *Career Dynamics: Matching Individual and Organizational Needs.* Addison-Wesley, Reading, MA.
[25] Rose Shumba, Kirsten Ferguson-Boucher, Elizabeth Sweedyk, Carol Taylor, Guy Franklin, Claude Turner, Corrine Sande, Gbemi Acholonu, Rebecca Bace, and Laura Hall. 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.* ACM, Canterbury, UK, 1–14.
[26] Mary Sumner and Susan Yager. 2004. Career orientation of IT personnel. In *Proceedings of the 2004 SIGMIS Conference on Computer Personnel Research.* ACM, Tucson, AZ, USA, 92–96.
[27] Jason Bennett Thatcher, Yongmei Liu, and Lee P. Stepina. 2002. The role of the work itself: An empirical examination of intrinsic motivation's influence on IT workers attitudes and intentions. In *Proceedings of the 2002 SIGMIS Conference on Computer Personnel Research.* ACM, Kristiansand, Norway, 25–33.
[28] Verizon. 2018. 2018 Data Breach Investigations Report. https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf.

A INTERVIEW PROTOCOL

Items in **bold** are those most relevant to the theme of motivations discussed in this paper.

(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) What do you think is the importance of your role in promoting security?
(5) How is your work is valued by others?
  (a) What kind of feedback do you get?
  (b) Can you talk about any times when you felt that your work wasn't appreciated?
(6) What do you think are qualities or characteristics of people who are successful in promoting security?
(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 promote 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) What are your thoughts about whether or not you are 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 about your work?

(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 individuals and 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) Is there anything else you'd like to add with respect to what we've talked about today?