"It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security

Julie M. Haney and Wayne G. Lutters, ***University of Maryland, Baltimore County***

https://www.usenix.org/conference/soups2018/presentation/haney-perceptions

This paper is included in the Proceedings of the Fourteenth Symposium on Usable Privacy and Security.

August 12–14, 2018 • Baltimore, MD, USA

ISBN 978-1-939133-10-6

Open access to the Proceedings of the Fourteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

"It's Scary...It's Confusing...It's Dull": How Cybersecurity Advocates Overcome Negative Perceptions of Security

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

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

ABSTRACT

Cyber attacks are on the rise, but individuals and organizations fail to implement basic security practices and technologies. Cybersecurity advocates are security professionals who encourage and facilitate the adoption of these best practices. To be successful, they must motivate their audiences to engage in beneficial security behaviors, often first by overcoming negative perceptions that security is scary, confusing, and dull. However, there has been little prior research to explore how they do so. To address this gap, we conducted an interview study of 28 cybersecurity advocates from industry, higher education, government, and non-profits. Findings reveal that advocates must first establish trust with their audience and address concerns by being honest about risks while striving to be empowering. They address confusion by establishing common ground between security experts and non-experts, educating, providing practical recommendations, and promoting usable security solutions. Finally, to overcome perceptions that security is uninteresting, advocates incentivize behaviors and employ engaging communication techniques via multiple communication channels. This research provides insight into real-world security advocacy techniques in a variety of contexts, permitting an investigation into how advocates leverage general risk communication practices and where they have security-specific innovations. These practices may then inform the design of security interfaces and training. The research also suggests the value of establishing cybersecurity advocacy as a new work role within the security field.

1. INTRODUCTION

> *"From the audience's perspective, security can be characterized by three major factors: one, it's scary; two, it's confusing; three, it's dull" (P08, security consultant).*

On a regular basis, the news is filled with reports of cybersecurity attacks [27, 48, 50], with companies, government agencies, and individuals being exploited at an alarming pace [45, 47]. Despite real and evolving cyber threats, users are falling behind in defending their systems and networks. They often fail to implement and effectively use basic cybersecurity practices and technologies, due in part to negative feelings about security.

Cybersecurity advocates are security professionals who attempt to remedy implementation failures by actively encouraging and facilitating the adoption of security best practices. "Cybersecurity advocate" is an emerging term-of-art among practitioners, with few holding it as their official job title. Indeed, many perform advocacy tasks in parallel with other responsibilities. They promote security to a variety of individuals, including home users, office workers, students, faculty, technical staff, developers, and executives. Examples of cybersecurity advocates include: organizational security awareness professionals; secure development champions; security consultants; and non-profit staff who publish resources to aid others in securing their digital assets. Regardless of the scope, advocacy is instrumental to their professional success. To be effective, these advocates must motivate people to engage in beneficial security behaviors, which often necessitates overcoming negative perceptions.

Prior research studies have investigated user perceptions of security and intentions toward following security practices. This body of work reveals incomplete, inaccurate mental models and a variety of sociotechnical factors that influence people's decisions to implement security solutions (e.g., [15, 19,35,49]). However, no research has been done to explore this problem space from the perspective of those actually doing the influencing, such as cybersecurity advocates.

To address this gap, we interviewed 28 self-identified cybersecurity advocates from industry, higher education, government, and non-profits. This paper presents a subset of findings from this larger study. Here we focus on answering the following research questions: 1) What are the professional characteristics and skills that security advocates employ in their work? and 2) What techniques do security advocates use to encourage security adoption?

The findings reveal ways in which advocates attempt to overcome users' widely-held negative views of security. We found that, as a foundation, advocates must first establish trust with their audience. To overcome perceptions of security being fear-invoking, advocates are honest, yet discerning, about the risks they communicate. They also attempt to empower their audience by engendering a feeling of hope and self-efficacy. Advocates address feelings that security is con-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018.
August 12–14, 2018, Baltimore, MD, USA.

fusing, complex, and difficult by "bridging the gap" between security experts and non-experts. They do this by serving as security educators who promote recommendations that can be realistically accomplished with usable security solutions. Finally, to overcome perceptions that security is irrelevant and boring, advocates create interest by incentivizing and employing engaging rhetorical techniques.

Our research has several contributions. Foremost, it identifies the cybersecurity advocacy role and its evolving definitional boundaries. It also provides insight into real-world security advocacy techniques in a variety of contexts, including how advocates leverage general risk communication practices and where they have security specific innovations. These practices may then inform the design of security interfaces and training resources. Additionally, the research suggests that there is value in establishing cybersecurity advocacy as a new work role within the security field, and provides a foundation for the recommended attributes of those who might perform it.

2. RELATED WORK

In this section, we lay the foundation for our study and its implications by summarizing past research in risk communication and persuasion within the security context.

2.1 Risk Communication

To form a basis for the skills, knowledge, and abilities necessary for cybersecurity advocacy, it is helpful to look at the literature on risk communication. Although much of this work has been conducted outside the cybersecurity context in fields such as health, environmental hazards, disaster planning, and home security, there can be much to learn about strategies to effectively communicate risk.

Kasperson [20] found that risk communicators aim to develop trust, create awareness strategies, facilitate understanding of concepts, employ mediating skills, and motivate people to act. Rowan [38] observed that risk communication can be controversial because it involves threatening and poorly understood concepts that can invoke hostile feelings towards the communicator. Therefore, they must be able to diffuse negative feelings so as not to erode trust, reframe negative messages into positive ones when appropriate, and use negotiation skills. Since a foundational aspect of risk communication is the establishment of trust and credibility, communicators need to exhibit empathy, honesty, openness, listening skills, and commitment [9, 42]. Trustworthy risk communicators serve as the bridge between technical experts and non-experts [14]. This bridging is akin to establishing common ground, which is the mutual knowledge, beliefs, and assumptions that are believed to be essential for successful communication between people [7].

Risk communication is a learned competency that includes a variety of approaches, including: keeping communications simple, but specific and unambiguous; customizing information to target audiences; assisting people in seeing the consequences of their decisions; providing clear and precise directions for action; building self-efficacy; and presenting information in an engaging manner [9, 11, 26, 39].

The risk communication literature begins to form a picture of what is required to be effective. However, little research has been done to investigate whether these characteristics, approaches, and goals are relevant for advocates within the security realm.

2.2 Influencing Security Behavior

Understanding what motivates people to change their behavior and practice good security is essential to evaluating whether advocates' approaches address these motivations.

2.2.1 Perceptions of Security

Before determining the most effective way to persuade people to practice good security, there needs to be an underlying understanding of their perceptions of security. Numerous studies have explored these perceptions, mostly among non-technical users. Huang et al. [16] conducted a survey of over 600 individuals that revealed influential factors, including knowledge, impact, controllability, and awareness of exposure to a threat. Furnell and Thomson [12] and Stanton et al. [44] discussed "security fatigue," a weariness towards security when it becomes too burdensome. From an organizational perspective, Post and Kagan [31] found that employees view stringent security measures as counterproductive since it impedes their ability to be flexible in their day-to-day operations.

A set of researchers explored mental models of security, with some examining the general public's often incomplete and inaccurate mental models and how these perpetuate poor security practices [19, 32, 49]. Other researchers shed light on the differences in mental models of security experts and non-experts [17,30]. Bravo-Lillo et al. [5] and Raja et al. [33] examined mental models while applying risk communication principles to security warnings. Camp [6] discussed how mental models of physical security, medical infections, criminal behavior, economics failure, and warfare might be applied to communicate cybersecurity risk. Zhang-Kennedy et al. [51] extended these models, suggesting that the use of surveillance and medical metaphors within infographics and a comic resulted in better security learning. However, Brase et al. [4] investigated the impact of Camp's suggested models in cybersecurity situations and found that there was little indication that any of these resulted in significantly better outcomes.

2.2.2 Persuasive Techniques

Protection Motivation Theory (PMT) [22, 37] claims that risk behavior is based on a cost-benefit analysis in which a threat appraisal (severity, likelihood, rewards/consequences) is weighed against a coping appraisal (response cost, effectiveness of response, self-efficacy). Sommestad et al. [43] sought to determine whether the PMT held true in the information security domain and found that it did explain security behavior if the threat and coping mechanism were concrete and when the threat was personally relatable.

Several studies applied PMT to explore the effectiveness of fear appeals in changing security behaviors within organizations. Johnston and Warkentin [18] suggested that, because people naively think that bad things will not happen to them, fear appeals should emphasize the likelihood of an occurrence by using concrete examples of negative consequences related to a threat. Herath [15] found that both intrinsic (e.g., perceived effectiveness, contribution to the greater good) and extrinsic (e.g., social pressures, penalties) motivators influenced security behaviors. However, the

severity of penalty approach has a negative impact because penalties are often inconsistently applied or may generate hostilities.

Additional efforts investigated approaches for influencing security behavior change among employees. Albrechtsen and Hovden [1] found that small group workshops were more effective at changing security behaviors than mass communications. Siponen [41] suggested that security awareness programs should include reasons for why people should follow security guidelines and engender feelings of wellbeing, rationality, and logic. Other efforts examined similar techniques from a home user perspective. Rhee et al. [35] discovered that the threat of negative consequences has limited impact on decisions to implement security, whereas users with higher feelings of security self-efficacy were more likely to engage in positive behaviors. In a study on the adoption of security technologies, Shropshire et al. [40] found that negative framing (presenting outcomes in loss terms) is better suited for detection technologies (e.g., virus scanners, firewalls) than for prevention technologies (e.g., password settings, access controls). Redmiles et al. [34] investigated why people choose to accept security advice, discovering that advice sources were evaluated based on perceived trustworthiness, and that fictional narratives with relatable characters may be effective for teaching security concepts.

Although much literature has focused on persuasion in security, little research examined this topic from the viewpoint of those attempting to do the persuading. This paper seeks to understand their expert craft and how they appropriate these techniques and creatively respond to the particular context at hand. Ultimately this reveals the art of effective security advocacy. To best illuminate these practices, we had to deeply engage with expert advocates.

3. METHODOLOGY

Over a nine-month period, we conducted semi-structured interviews of cybersecurity professionals performing advocacy tasks as a major component of their jobs. We chose semi-structured interviews over other methods, such as surveys, because of the richness of data afforded, the latitude to ask follow-up questions to clarify or delve deeper into participant responses, and the ability to encourage participants to add other relevant information not explicitly targeted [8].

Our institutional review board approved the project. Prior to the interviews, participants were informed of the purpose of the study and how their data would be used and protected. Participants then signed a consent-to-participate form, also indicating whether they would allow audio recording of the interview (two declined). All interviews were transcribed from the audio recordings or field notes and stored without personal identifiers. Interviewees were not compensated for their participation.

3.1 Recruitment

Our conceptualization of an advocate originated from field observations on how this group of professionals described themselves. Therefore, we initially recruited from researcher contacts and internet searches those who self-identified as security advocates. We then were open to snowballing recommendations that allowed interviewees to identify others like themselves. Our definitional boundary of the cybersecurity advocate role continued to take shape and guided our subsequent recruitment as the interviews progressed. To ensure that a broad range of security advocacy contexts would be included in the study, we purposefully selected individuals who performed different types of security advocacy, for example, security awareness training, public campaigns, advocacy for a particular community, or security consultation. Additionally, we sampled advocates working in a variety of organizational types, including government, industry, higher education, and non-profits, to account for different viewpoints that may be inherent in each of these sectors. This yielded a collection of information-rich cases [28].

We employed theoretical sampling throughout data collection to guide recruitment [8]. Following this approach, we recruited participants four or five at a time. The next group of potential participants was then purposely chosen to include those who might be able to provide more insight on concepts or areas of interest emerging from the analysis of the preceding set. For example, when several participants raised gender diversity concerns in the security field, we subsequently made an effort to recruit additional female participants to gain their perspectives.

3.2 Data Collection

We conducted 28 semi-structured interviews lasting on average 45 minutes. If logistically feasible, interviews were face-to-face (12 interviews). Otherwise, participants were given the option of a phone (9) or video conference (7) interview.

The first three interviews were pilots to discover potential flow and timing issues. Because there were only minor revisions to the protocol following, data from these interviews are included in the final data set. In line with accepted qualitative research methods, we interviewed until we reached theoretical saturation, the point at which no new themes or ideas emerged from the data [23].

Interview questions addressed several areas: work practices, professional motivations and challenges, characteristics of successful advocacy, and how participants stay up-to-date on security happenings. The interview protocol is included in the appendix. Separate from the interview, participants also completed a short, online demographic survey that collected information about years of experience in the field, current position, sectors in which they had worked, and education. One participant did not complete the survey.

3.3 Analysis

We conducted iterative, inductive coding and analysis on the data. This commonly used qualitative research approach allows for an organic emergence of core concepts, starting with the categorization of the data into initial codes and then progressing to the recognition of relationships among those codes [13]. We began preliminary analysis at the onset of data collection to assess the quality of data and themes arising from the interviews. This allowed for small adjustments in the interview protocol over time as some questions reached saturation or when new themes started to arise as part of theoretical sampling. Throughout this process, we also engaged in axial coding to link related codes together (demonstrated by the subsections in section 5), wrote analytic memos, and identified core concepts. We regularly met to discuss emerging themes and our interpretations.

At the conclusion of data collection, both researchers began

construction of a final codebook. We reviewed five interviews (2,482 lines) individually and performed open coding to label, look for meaning, and begin to categorize the data. We then met multiple times to discuss identified concepts in those interviews. These discussions led to the development of the codebook. The first author then used the codebook to deductively code the remaining interviews.

4. PARTICIPANT DEMOGRAPHICS

We interviewed 10 female and 18 male professionals, clustered in age from 25-34 (3 participants), 35-44 (7), 45-54 (7), and 55+ (10), with one undisclosed. Overall, they were a veteran group, with all but six having more than 10 years experience in the security field, and the rest having at least five years. Table 1 summarizes participant demographics. Some details are generalized to protect confidentiality.

The participants had diverse educational and career backgrounds. Interestingly, 14 participants had at least one degree in non-technical fields as diverse as public policy, communication, history, law, business, English, and graphic design. Participants had worked in a variety of government, private industry, higher education, and non-profit organizations, with most having experience in more than one of these sectors. When asked to describe their target audience, 10 said their audience was mainly external to their organization, three mainly focus within their organization, and 15 said they advocate both externally and internally. Their diverse audiences included the general public, co-workers, professional communities, government organizations, students and faculty, policy makers, corporate boards, developers, and other security professionals. The advocates performed a number of functions, several having more than one. Some were security engineers, led organizational security awareness programs, or served as security consultants. Others were security educators, non-profit organizers, researchers, or secure development experts.

5. FINDINGS

In this paper, we focus on how advocates attempt to overcome negative perceptions that security is scary, confusing, and dull. An overview of our framework is provided in Fig. 1. We first discuss a prerequisite condition for successfully overcoming negative perceptions: the advocate's ability to be viewed as a trustworthy information source. Subsequent sections begin with a description of each underlying negative perception reported in security advocates' audiences. Subsections describe strategies that advocates employ to attempt to overcome the perception. Note that strategies gleaned from the interviews are based on participant *perceptions* of effective advocacy strategies.

Counts of participants who mentioned a concept are provided throughout this section. However, due to the semi-structured format of the interviews, we caution the reader against making quantitative inferences beyond frequency. Counts are reported to add weight to concepts that were repeatedly mentioned throughout the interviews, but the significance of an insight may not be determined solely by the number of participants voicing it.

5.1 Establishing Trust

Before advocates can overcome negative perceptions of security, they must first establish trust, which is a foundational aspect of risk communication. A security engineer who provides consultation to government customers spoke of this trust: *"To me, trust is the most important thing that I have. If they trust that what I'm telling them and what I'm doing is the right thing, then I am much more successful" (P12).* Advocates gain audience trust by relying on organizational reputation, demonstrating technical knowledge, building relationships, and leveraging insider access.

5.1.1 Relying on Organization Reputation

As noted in four interviews, organizational reputation may help to establish credibility, at least initially. One participant suggested that the most effective advocates are sometimes *"people who have the credentials and are associated with organizations that are viewed as having some authority" (P07).* This credentialing can especially be helpful when advocating to the general public, especially online where personal interactions are rare. However, when interacting directly with an audience, organizational reputation only goes so far, and must ultimately be upheld on an individual basis. A government security analyst discussed this external bump versus sustained personal reputation: *"Our agency... carries with it a great deal of credibility... And I think that helps out a lot. But [individuals have] to be able to exhibit and illustrate the qualities that go along with the respect they bring into the door" (P01).*

5.1.2 Demonstrating Technical Knowledge

One way that advocates establish individual credibility is by demonstrating technical knowledge, as suggested as an important characteristic by 19 participants. One participant exclaimed, *"First and foremost, you really do need to understand the technology... This stuff's tricky, and you don't just guess your way out of it" (P08).* Advocates that work with technical staff are particularly held to high standards with respect to technical acumen. A participant with over 30 years in the security field emphasized this: *"This is a business that is very technology oriented, and full of people... who want to one-up you. So if you can't kind of deal with that, it's going to be hard for you to be an effective advocate because people will kind of eat you up" (P04).*

5.1.3 Building Relationships

Whereas technical skill may be an important component in building credibility and trust, our findings support previous risk communication research that emphasizes the importance of exercising interpersonal skills to build relationships and foster trust. A security usability specialist emphasized the value of these non-technical skills: *"If you're a computer scientist, and all you know is the computer science, and you don't have the empathy, you don't have the skills to listen,... you don't have that psychological side, I don't think you can make it work" (P03).*

Relationship building is facilitated by demonstrating empathy (mentioned by four participants) and listening skills (by six). A participant suggested, *"The most important part is to go in and listen... to what their challenges are, what their problems are" (P05).* A technical executive at a higher education institution expressed the importance of empathy:

> *"I think people have to have a high emotional intelligence and especially empathy. Part of being successful in this is being able to have a conversation and put*

Table 1: Participant Demographics

ID	Gen	Role	Sector	Edu	Audience	Audience Description
P01	M	Security analyst	***G***	T,N	B	tech staff, managers
P02	M	Professor	***E***,G,I	T,N	B	general public, students
P03	F	Computer scientist	***G***,I	T	B	tech staff, managers, general public
P04	M	Security evangelist	***N***,G	T	B	tech staff, managers
P05	M	Security researcher	***I***,G	T	B	tech staff, managers
P06	M	Director	***N***,G,E,I	N	B	public policy makers, managers
P07	F	Senior technologist	***G***,***E***,I	T	E	general public, managers
P08	M	Security consultant	***I***	N	E	non-tech professionals, managers
P09	M	Training director	***E***,G	N	E	tech staff
P10	M	Instructor, consultant	***I***,***E***,G	T	E	tech staff, managers
P11	M	Director	***N***,I	N	E	public policy makers, tech staff, managers
P12	M	Security engineer	***I***,***E***,G	T	E	tech staff, managers
P13	M	Security engineer	***I***	U	I	tech staff, managers
P14	M	Security awareness director	***E***,G	N	B	students, faculty, tech staff, managers
P15	F	Director	***N***,***E***,I	N	B	tech staff, managers
P16	M	Computer scientist	***G***,E,I	T,N	I	managers
P17	M	Researcher	***I***	T	E	developers, tech staff
P18	M	CIO	***E***	T	B	students, faculty, tech staff, managers
P19	F	Senior Architect	***I***	T	I	developers
P20	M	Professor	***E***,***G***	T	E	students, tech staff, managers
P21	F	Company co-founder	***I***,G	T	E	end users, tech staff, managers
P22	M	Security researcher	***I***, E	T	B	developers
P23	F	Security consultant	***I***,E	N	B	tech staff, general public
P24	F	Director	***N***	N	E	general public, tech staff, managers
P25	F	Deputy CIO	***G***,I	N	B	end users, tech staff, managers
P26	F	CISO	***G***,I	T	B	end users, tech staff, industry partners
P27	M	Director	***N***,I	N	B	tech staff, managers
P28	F	Security Awareness director	***I***,E	N	B	end users, tech staff, managers

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 to own organization, B=Both internal and external

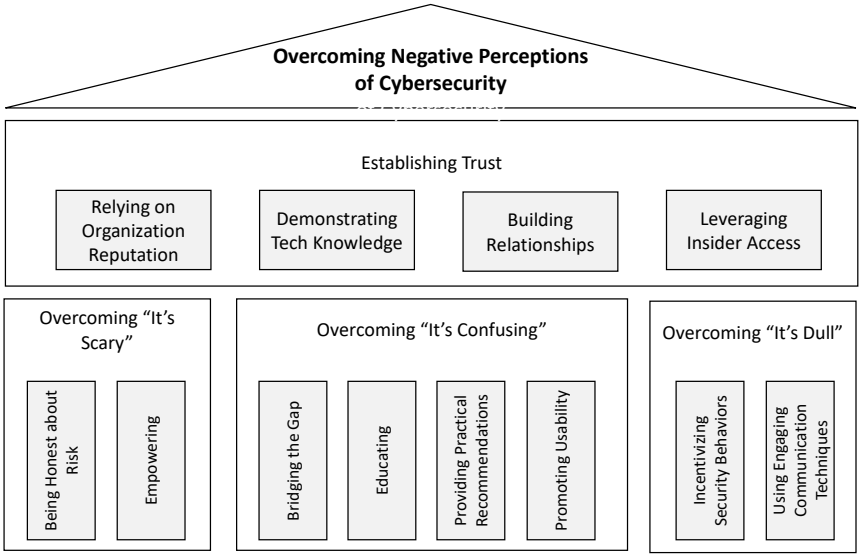

Figure 1: Framework of how cybersecurity advocates overcome negative perceptions of security

yourself in the place of the person that you're working with, and then be able to give effective advice that is not preaching, is trying to be helpful, and is letting them know that they're not stupid because they may not know how to do certain things" (P18).

Humility was mentioned by five participants as another interpersonal skill important for trust-building. Several noted that those advocates who approach a situation with an attitude of *"I'm in charge. I know best. You must listen to me" (P02)* are not generally very effective in enacting security behavior change because they put their audience on the defensive. A deputy CIO with a strong technical background remarked on the importance of not being arrogant because *"You'll never have all the answers" (P25).* A security consultant discussed his personal philosophy of humility: *"Whenever I walk in the room, I assume I'm the stupidest one there, and everything works out great" (P10).*

Trust is also created by being open to multiple viewpoints and building consensus. Consensus was especially important for the participants from non-profit organizations that relied on volunteers to inform their advocacy efforts. A founder of a non-profit group discussed their commitment to consensus building: *"We prioritize and cherish a multi-stakeholder approach. There [are] lots of voices... The goal is to surface beliefs, combine them with other beliefs, come to a set of shared beliefs" (P11).* Another participant described her collaborative role with members of her non-profit organization as *"an uber-facilitator. Our job is to get these people together and make them work for the common good" (P15).*

Interpersonal skills do not only apply to advocates who have in-person interactions with their audience; others must utilize these skills for any security guidance that reaches their audience. For example, P24's non-profit conducts extensive anonymous consumer research prior to publishing security guidance to ensure they address their audience's concerns and use language that will be easily understood. This attention to their audience's needs, in effect, demonstrates listening skills and empathy.

5.1.4 Leveraging Insider Access

Nine participants gained credibility due to their past experience in the professional communities to which they advocated. This experience helped them to be portrayed as "insiders." For example, one participant with a law background began her career in security advocacy when a legal organization recruited her to help with security compliance: *"They needed a translator to translate law to geek... And I learned that I sort of have a unique aptitude in this area where law and information security policy intersect" (P15).* Another participant remarked, *"It's very difficult to integrate yourself into someone else's daily work when you don't know what the daily work is" (P17).*

However, gaining credibility can be challenging when the advocate is perceived as an outsider. To overcome this, six mentioned the value of enlisting the support of opinion leaders and decision-makers within the target community. One participant talked about this value: *"You need to find whoever it is that you think is a change maker and make sure they have that data, that they're excited by that data, and they can use it to their benefit to make a difference" (P03).*

5.2 Overcoming "It's Scary"

The consequences of poor security can be catastrophic personally, organizationally, and societally. All participants had a solid understanding of the current state of security and potential consequences of poor security practices. One participant opined that the internet is *"getting more insecure constantly... The bad guys are getting better" (P06).* Another was concerned with global consequences, saying, *"It is so easy to imagine a really big cyber incident. And the barrier to entry is really, really low" (P16).*

Security risks are real, but several participants believed that, in some cases, these risks are sensationalized. Two participants partially blamed other security professionals, with one advocate noting, *"We're just really a fear-mongering industry" (P21).* Another who came into the security field with a humanities background observed security professionals *"tend to be really negative and really fatalistic. Everything's awful, everything's burning, everything's dead" (P23).*

Three participants also blamed media portrayals of security incidents for creating anxiety, particularly among non-technical audiences. A security consultant reflected that when people see depictions of cyber incidents on television and in the movies, *"the computer looks like some kind of magic box where somebody touches it, and zing! They attacked our network and taken our children, and look, they've wilted our lettuce!" (P08).* Another commented on how media portrayals can build fear around concepts that are unfamiliar: *"People are afraid of what they don't understand or don't want to learn... Their consciousness is kind of framed in this Hollywood... sort of approach where it's this evildoer. And that terrifies people" (P02).*

It is not surprising, then, that some people view cybersecurity as scary. To address this, advocates must strike a careful balance between being candid about security risks while being hopeful and encouraging. The latter are essential for developing a sense of empowerment in the audience.

5.2.1 Being Honest, Yet Discerning, About Risk

To convey a sense of importance and urgency to their audience, our participants said that they must be forthcoming about risks. One remarked, *"You can't appreciate the importance of security without first understanding what's at stake, what's at risk" (P14).* Another recommended, *"In terms of it being scary... take that head on. Here are all the terrible things that can happen" (P08).*

However, six participants noted the importance of being discerning: not "crying wolf" (being an unnecessary alarmist) over every little security issue, lest their audience become overwhelmed, disinterested, or skeptical. One said a mistake in security advocacy is *"being more sensational, and theoretical, and hypothetical than practical and rational... Focusing on the possibility is a very easy way to get known as crying wolf" (P02).*

In some cases, advocates may only want to engage a select group with the authority to address a security issue, especially when dealing with issues that have broader-reaching organizational or national consequences. An advocate who promotes security to industries that build safety-critical products, such as medical devices, commented, *"If I told everybody what I know, they'd freak out. I want to tell a smaller*

list of people I know so that we can quietly fix it" (P11).

5.2.2 Empowering

For many users, an overabundance of fear may result in a feeling of futility regarding their security situation. This can lead to paralysis and inaction. This was echoed by one participant when she opined, *"if you have a little bit of fear, it's actionable. But if you have too much fear, it becomes so overwhelming that you give up on it" (P21).*

Feelings of helplessness can be perpetuated by security professionals who regularly express their belief that users are unable to comprehend and practice good security behaviors (mentioned by six). An advocate who had led her company's security awareness program expressed her frustration with these professionals: *"I feel like there's just a lot of people saying, 'Oh humans are the weakest link. They're always hopeless... They haven't changed their behaviors, so what's the point?"' (P21).* Another commented on the harsh way non-experts are treated by security experts in online forums, remarking, *"smashing them and telling them they're stupid, that's not going to help. Instead, we need to be more encouraging, more open-armed in the industry" (P10).*

To overcome feelings of inadequacy, advocates must empower their audience to take action. Empowerment was a concept mentioned by 16 participants, mostly in the context of non-technical users. A prerequisite seemed to be instilling a sense of hope, as noted by eight advocates. One participant reflected:

> *"You can't last for decades in this cybersecurity business without being one of two personality types: the hopeless cynic or the hopeless optimist... You can make an entire living just pointing out other people's problems or mistakes... But I just don't find that satisfying. I'm much more interested in creating positive change" (P04).*

Advocates then use this hope to foster self-efficacy in their audience. Self-efficacy is a belief in one's own ability to exert control in specific situations or accomplish a task [3]. This is the cornerstone of independence, which was expressed by one advocate when he said, *"we have to be able to get to a point at which they can do a lot of it themselves" (P01).*

The interviews suggested that self-efficacy can be encouraged by providing people with basic, concrete actions that will allow them to be proactive in their security situation. Instead of simply raising an alarm, a security technologist believed, *"it's really important to tell people what they can do so they that don't just go, 'Oh my gosh. The world is a scary place, but there's nothing I can do about it, so I guess I just won't worry about it' " (P07).* Another commented,

> *"I love empowering people and seeing their lightbulbs go off in the moment that they understand why they are a target and what they can do about it. So, it's not a place of fear. You have to start with fear to get them to understand that there's a problem, but then you also give them the tools" (P21).*

Framing messages in a positive light and comparing security measures to more familiar, accessible protective mechanisms can also help to alleviate fear and empower. A security advocate talked about how she chooses to frame her communications during her work with senior citizens:

> *"you slip that message of 'You're going to get attacked and everything's going to get stolen' to 'Well, it's kind of like home improvement when you put a better deadbolt on your door or you decide that you're going to shore up your foundation"' (P23).*

5.3 Overcoming "It's Confusing"

Few non-professionals have the technical know-how to address security issues, so *"security is mysterious to most people" (P07).* A participant underscored the impact of this knowledge deficiency when she commented, *"people don't actually know what the names of the tools they need are. They don't know the proper, technical words that are going to lead them to a solution" (P23).* This lack of understanding leads to the perception that security solutions are confusing and difficult to implement, as noted by 20 participants.

The barrage of security messages and advice people receive at work, from the media, and from friends can create *"a lot of uncertainty of what is the right thing to do" (P04).* One participant commented on this state of being overwhelmed: *"You're getting hit from every single side... We have almost an information overload happening, and it's hard to sort through it" (P08).*

Security can also be seen as a burden, *"just one more thing to remember, one more rule" (P28)* that gets in the way of doing other tasks. A participant observed, *"there's a complete misunderstanding that to be secure takes an immense amount of time. That's a huge obstacle to get over" (P23).*

To overcome the perception that security is confusing, advocates "bridge the gap" between security experts and non-experts, educate people on how to practice good security, provide practical recommendations, and promote usable security solutions.

5.3.1 Bridging the Gap

The process of mediating between technical and non-technical audiences requires establishing common ground, which necessitates advocates to have strong communication and translation skills and an awareness of audience context. A nonprofit director underscored the importance of communicating in a manner that is meaningful to the audience:

> *"you can produce as many policies and processes as you like, if you cannot communicate them to people in a language that they understand, in a language that means they're going to be receptive to your message, then they're worthless" (P27).*

A security consultant described his role as a connector between groups: *"I'm sort of the in-between person, between the business interests of the company and the technical interests because they don't talk to each other very well. I can translate both languages" (P08).*

Bridging the gap was a concept discussed in 22 interviews. Participants described their connective capacity with various terms such as translators, boundary spanners, ambassadors, cross-pollinators, and information carriers.

Translating: Highly technical security experts often unwittingly make security seem more elusive as they rely heavily on disciplinary jargon. One participant remarked, *"There's*

also, I think, a big language issue... it is a highly technical field with a very specialized language" (P04). A lack of understanding of the skill level of their audience also results in confusion, as described by a security awareness educator: *"It's not that people are stupid, it's that we need to communicate in their language" (P09).*

To overcome the language difference, advocates act as "translators," reframing highly technical concepts using terms their audience can understand. Twenty-three participants commented that the underlying communication skills required for translation were important for security advocacy. In fact, despite being a highly technical person, when asked about the characteristics of successful security advocates, a security consultant said, *"communication skills I think are number one" (P10).* While describing the importance of effective communication in his work, a participant asserted, *"Being able to translate complicated things very simply is crucial to... advocating security" (P02).*

Being Context Aware: Context awareness is critical for effective security advocacy, as expressed by 22 participants. As much as possible, they need to be aware of the operational environment of their audience, including technology, roles, social structures, constraints, and goals. One participant commented, *"Understanding your environment, and the different, unique threats and vulnerabilities in your environment is hugely important" (P14).* A non-profit organizer used a metaphor to convey this necessity:

> *"This is more of an ambassador role where you're going to a foreign country. You need to represent your own country, but you have to assimilate to and acclimate to the language and the beliefs and the culture that you are trying to affect" (P11).*

Advocates must also use their knowledge of context to tailor the security message to the skill level and concerns of the audience. When appealing to non-technical audiences, a veteran security evangelist realized, *"You have to change your language, which means in the non-techno speak figure out how to translate what you know into concerns people have about economic and social issues" (P04).* A security engineer who advocates to a wide swath of people within his organization remarked, *"The message, even though it's going to be the same, it's going to be delivered differently depending on the level of person that you're talking to" (P13).*

5.3.2 Educating

A greater understanding of security helps to overcome confusion and leads to empowerment, as discussed earlier. To that end, advocates saw themselves as security educators. Eleven participants had served at one point in a formal educator role, but all discussed the educational component of their jobs. A security awareness director at a large university saw his role as foundational: *"The only way you can fully understand what's at risk and what's at stake is through education and awareness. So, it's the starting point for everyone. I'm ground zero in security" (P14).*

Eleven participants mainly taught non-technical audiences. Their goal was to provide simple, straightforward instruction and help people make informed decisions about their security behaviors: *"I think it's a lot like knowing when you see power lines are down, not to touch the power lines. It's just a basic level of knowledge you need to know for self-preservation purposes" (P15).* For example, P08 created *"security awareness basics"* videos targeted at the general public. For his other audiences of non-technical professionals in the legal, healthcare, and finance industries, he tailored both video and in-person presentations to their specific needs. He commented on the value of his security education courses: *"I'm not going to make you into a security expert in three hours ... But I want you to be able to have a conversation with one where you can be able to follow each other" (P08).*

In contrast, 15 participants primarily taught technical audiences of developers, IT specialists, college students, and other security professionals on issues such as secure products and network security. For example, P22 educated product teams within his organization on secure development practices. Five mentioned that it was important to educate the next generation of security professionals *"so that they don't make or sustain the same mistakes... that got us into the mess that we're in with cybersecurity" (P02).* One participant often does presentations for high school students at cybersecurity summer camps, *"just talking about information security, and just having fun and making them laugh. And talking about how meaningful this is" (P10).*

5.3.3 Providing Practical Recommendations

Our participants agreed that the amount of security information to be aware of can be overwhelming, even for them. To counter this, 16 participants discussed providing practical, prioritized recommendations. Six mentioned condensing security information into more manageable chunks containing the most important security actions to take. P11 mentioned how his advocacy group had developed a set of *"first principles,"* which are foundational security measures that should be in place within an organization before anything else.

While some security guidance is universal, other recommendations are dependent on the audience's environment. Several participants spoke out against "one-size-fits all" solutions, emphasizing the importance of context. A non-profit organization approached this issue by producing general guidance that can be customized and disseminated by others: *"Our goal is to create non-proprietary resources so that our local partners can take those and tailor them for their community... because it could mean different consequences for different people" (P24).* Others felt the responsibility to directly provide tailored security guidance that is based on the actual risk within a given situation. One participant was a proponent of this approach within organizations:

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

To ensure guidance was practical to their audience, an advocate in higher education described her organization's efforts to regularly poll members on their biggest security risks and challenges. These risks then became the cornerstone of their annual "top 10 list" of security recommendations:

> *"You're never going to be able to remediate or mitigate every single information security risk that you have,*

but you should be able to identify the ones that are the most likely and the ones that would be the most devastating to your environment, and take steps to mitigate those" (P15).

5.3.4 Promoting Usability

Security technologies and policies are not generally known for usability, leading to feelings of frustration and confusion [10, 52]. One participant felt that security professionals are *"putting too much pressure on the user, and the user doesn't have the knowledge" (P03).* She also observed that the volume of security-related tasks a user must perform on a daily basis (e.g., multiple logins, security warnings) can be overwhelming when viewed as a whole: *"In isolation, none of these security things are that big of a hardship or have significant usability concerns. The aggregation of them is what causes the usability concerns" (P03).*

To alleviate the complexity and burden of security, nine participants emphasized the need to advocate for systems and policies that are usable, minimize requisite knowledge, and compensate for the inevitability of user error. Three participants conducted usability research to directly influence vendor products as well as organizational and national policies. One of these participants explained her motivation metaphorically: *"Most of us drive a car, but don't know how to fix cars. We shouldn't have to know how to fix cars in order to drive them. And I think that should be true about computers, too" (P07).* Another participant who has been a champion for usable security both internally and externally to his organization, stated that the usable security challenge must address the question of *"How do we build and deploy systems that are easy to use, easy to manage, that result in cost savings?" (P16).*

5.4 Overcoming "It's Dull"

Another negative perception, voiced by 19 participants, is that security is boring, not relevant, not of concern, or not worth the investment. This drives user apathy in adopting good security behaviors.

Security can seem boring to less technical audiences, especially when a technologist fails to frame it in terms the audience can understand. This can be exacerbated by poor communication skills, for example *"presentations where the speaker's doing monotone and talking security. If you really love it, you can get through those, but for normal people, they're torture" (P08).* Additionally, the most common negative exposure users receive is from their annual security awareness training for organizational compliance, described vividly by one participant as *"a layer of Dante's Hell" (P21).* A security engineer who had once been tasked with refreshing an organization's security training noted that the original training *"was boring... there [was] absolutely nothing to get the user to buy into security thinking"* (P12). The training often mandates specific actions that are deemed unwelcome, unnecessary inconveniences. For example, one participant lamented password policies: *"You force them to change their password. We all hate that" (P28).*

Besides disinterest, people may be apathetic towards security because of not appreciating their own personal vulnerability and responsibility. A security awareness director expanded on this: *"if people don't understand why and how this affects them, they're simply not going to comply with whatever initiative it is you're trying to roll out" (P14).* Another participant discussed how security is not something most people take under consideration when acquiring a computing device: *"We don't want secure,... we don't even want to think about it. [We want] pretty, functional, cheap" (P06).* Security is also not a primary function for most: *"I think for end users, it's just nobody wants to spend their time doing security. That's not what they signed up for when they bought a computer" (P07).* Lack of concern may be partially due to a *"belief of it won't happen to me. It's like I'm a great driver, so I can text while driving because it won't ever happen to me, so I don't have to worry about it" (P21).*

From an institutional perspective, organizations may also be apathetic to security because it can be hard to show a clear return on any investment. Security measures are preventive in that they are implemented to lower the likelihood of some unwanted event occurring in the future [36]. Therefore, it is hard to measure prevented events because they typically cannot be observed. A participant discussed this challenge, remarking, *"It's hard to prove that it's working for you. Is it working because you've done such a good job and you've invested in all the right places, or is it working because you're just not the target today?" (P05).* An advocate working at a non-profit observed:

> *"One of the other trends that we see... is that of cyber fatigue in the boardroom: people constantly asking for more resources, yet they can't guarantee any form of security. There's no real return on investment, and it seems to be a black hole that we pour money constantly into" (P27).*

Cybersecurity advocates attempt to overcome boredom and apathy by incentivizing security behaviors and using engaging communication techniques.

5.4.1 Incentivizing Security Behaviors

Successful advocates must be able to persuade their audience to practice good security behaviors by appealing to both intrinsic and extrinsic motivations, as mentioned by 17 participants. A former security awareness director reflected, *"I really want to get people to want to do security instead of having to" (P21).*

Selling Security: Advocates, in effect, must market security in order to motivate people to take appropriate security actions. A participant commented on the importance of marketing skills: *"you have to be able to make a... good case... that's based on good data, that the dollar figures support, and that you can get excited and get them excited about. And if you can't... market that, you can forget it" (P03).* One advocate had an interesting and honest perspective on his use of persuasion:

> *"I am trying to drive them to make themselves more secure by using various argumentative techniques, and, in some way, that's manipulating them. But if you're manipulating somebody for their own good, that's not wrong" (P10).*

As discussed earlier, having context awareness is critical to being able to sell security in a manner that the audience understands and cares about. One advocate observed, *"you need to be able to be flexible in terms of adapting your argu-*

ment to their particular needs" (P06). Another commented: *"It's not a one-size-fits-all approach. You could take a given security concern and have to frame it four or five different ways depending on who you're talking to" (P02).* As an example, one security consultant was having a difficult time convincing an executive to spend resources to implement secure hypertext transfer protocol (HTTPS) for his company's website. However, when the consultant mentioned that Google ranks websites using HTTPS higher in its search results, the executive immediately changed his mind since *"Their biggest business risk was not being on the first page of Google" (P10).*

Ten participants said that they must also be able to communicate the reasons behind their security recommendations in order to convince their audience of potential benefits. An advocate stressed the importance of providing concrete reasoning: *"We gotta stop leading with 'what' and start leading with 'why.' Like why does this matter? If you get someone to care why, they'll seek the what and the how" (P11).* Along this vein, for those advocating within an organizational context, establishing the business drivers for security is essential. A former business executive believed, *"we should be concerned with selling security as mission assurance, revenue assurance, reputation assurance" (P02).*

Interestingly, three participants thought that lessons learned from persuasion within the public health field could inform the security advocacy field. An IT executive commented:

> *"It has struck me that we have not leveraged the hundred plus years of research in public health to really garner how to change people's behavior effectively. How do you teach people to wash their hands? How do you teach people to do the handful of basic things that we know will solve 80% of the problems is the hard part of this" (P18).*

A non-profit security evangelist echoed this thought, saying that public health is *"well-defined, it's a social expectation, and you know that it provides value even though you probably can't quote the actually medical studies... You should just do it. We're not to that stage yet [in security]" (P04).*

Creating Reward (and Consequence) Systems: Advocates encourage a culture that incentivizes security adoption. As mentioned earlier, showing return on investment in security can be a challenge. A non-profit director saw his role of influencing public policy as critical to creating an economic reward structure for organizations to practice good security: *"Most of these people are not doing what they ought to be doing with cybersecurity for economic reasons. And so we need to find ways to make cybersecurity more economically attractive to these people" (P06).*

Several participants saw economic incentives as only part of the solution in that they need to be coupled with appeals to the values of the audience. For example, one participant discussed motivating secure development practices, not by framing them in security terms, but in terms developers care about, such as *"you can avoid unplanned, unscheduled work, you'll be on time, on budget, you'll reclaim 20% boost in developer productivity across the calendar year. You'll get your bonus. You'll crush your competitors" (P11).*

We uncovered a tension regarding the use of negative reinforcement strategies based on audience type. Three participants pushed for more accountability with negative consequences for organizations that experience serious security breaches that result in the loss of sensitive, personal information. However, three others believed that negative incentives were not useful from an end user perspective. A security awareness director at a large university opined that these kinds of incentives are *"completely the wrong way to approach things in security. It's all about education. It's all about driving awareness, raising awareness, and getting people to understand the importance of security through non-punitive measures" (P14).* Another participant felt that simple, positive incentives could be effective, but observed:

> *"security teams generally have a lot of history and best practice in negative behaviors... We have very few examples where, 'Here are the compliance requirements. When you meet or exceed this, we will reward and recognize you as being a champion'... It doesn't have to be monetary, it can be a thank you" (P21).*

5.4.2 Using Engaging Communication Techniques

To overcome feelings that security is boring and irrelevant, advocates attempt to make their communications engaging and relatable while varying communication channels.

Exhibiting Enthusiasm: To overcome disinterest, participants felt that modeling enthusiasm for security to their audience captured their attention and promoted greater engagement. This was not difficult for the participants, considering 18 expressed passion for their role as advocates. The director of a non-profit effused, *"I believe in what we're doing, and I think we're making the world a better place" (P06).* When asked about effective security advocates he had encountered in his career, a security engineer mentioned those for whom *"you can really feel the energy that they believe in it" (P12).* Another participant expressed the importance of having passion for her work when she remarked, *"I can't sell something I don't believe in. I can't sell something I don't like. I mean, I'm not going to sit and lie to you. And so, I am passionate about it" (P03).*

Making Security Relatable: Our findings reveal that advocates also overcome apathy by making security relatable, described by one participant as putting *"the personal use and behavior in it so that people own what you're telling them" (P28).* To do so, they often used rhetorical devices in both written and oral communications to convey meaning and persuade people to take action. Among the rhetorical devices mentioned were anecdotes and narratives (by eight advocates), analogies and metaphors (4), imagery (3), alliteration (2), and pop culture references (2).

Narratives might involve stories about hypothetical, but plausible scenarios, or actual occurrences of security-related incidents. One advocate liked to share stories about her own experiences since she believed, *"Personalizing the message is useful, seeing that this happens to real people" (P07).* Another discussed how he shares stories of things that have happened to others, for example *"a person whose money might have been stolen out of their bank account because of the poor security they did at home, not because of what the bank did, but because of what they did" (P05).* Four advocates mentioned how leveraging narratives of current events can serve as *"an opportunity because [the audience's] aware-*

ness is already heightened" (P24).

Advocates also used analogies and metaphors to relate security to situations and phenomena that are more familiar to their audience. For example, the analogy to public health and basic hygiene (e.g., washing your hands, brushing your teeth) was mentioned several times to explain the concept of cyber hygiene (basic, fundamental security practices). This was described by one participant:

> *"Do you tell someone to exercise and get enough sleep, or do you wait until they are having some serious problems and then you're going to bring them in for surgery? Which route would you rather go? It's not exactly the same, but it's kind of analogous to what's going on there [with security]. And it's getting people to understand, OK, here's your basic network health hygiene" (P08).*

Even though analogies and metaphors can be useful, two participants cautioned that these must be meaningful and tailored to the audience. One participant thought that oversimplifying these *"can be dangerous. You can be too glib, and it's superficial" (P06).* P08 provided a critique of a security training video that depicted someone fishing to explain the concept of phishing. He felt that such a metaphor was *"corn-ball"* (trite and unsophisticated) and would not resonate with his audience of attorneys.

Visual representations were also valuable in making complex topics more relatable and memorable. For example, after the Heartbleed vulnerability [46] was announced, one participant said, *"I was trying to explain that and ended up using a cartoon to explain a very complex topic to people" (P25).* Another revealed, *"When I start talking about two-factor authentication, I like to call it two-raptor authentication. I like dinosaurs. It's more fun when you imagine that they're going to eat someone's face off. People will remember the name of the feature" (P23).*

The participants used a variety of platforms to peak interest and advocate for security. The most mentioned communication channels were: written materials (e.g., books, papers, frameworks, newsletters) (by 18 advocates); small group/individual face-to-face interactions (17); large forum and conference presentations (16); social media (12); and formal classroom training (9). Interestingly, several participants utilized particularly unique communication channels. For example, three had developed games to teach security concepts. One organization sponsored a food truck event for their employees during which people standing in line for their lunch were engaged with security trivia. Another creative idea was putting a security-themed vinyl wrap on a public bus: *"it becomes essentially... a traveling billboard" (P26).*

6. IMPLICATIONS

Although there have been research studies exploring techniques to encourage security best practices and technology adoption, there is much to learn from successful practitioners who are engaged in this activity on a regular basis. We also discuss the potential of cybersecurity advocacy becoming a formally recognized work role in the security field.

6.1 Advancing Risk Communication

6.1.1 Relationship to Non-Security Risk Domains

Our results confirm that cybersecurity advocates exercise many of the same risk communication best practices observed in other fields such as health (e.g., [9]), environmental hazards (e.g., [39]), and home security (e.g., [11]). For example, they expressed common goals, such as building trust, creating awareness strategies, and motivating people to act. To build trust and credibility, they employed a variety of non-technical "soft" skills. In communicating their message, security advocates similarly used engaging techniques, served as a bridge between security experts and non-experts, encouraged audience self-efficacy, and tailored their message to the audience based on context awareness.

Similarities suggest there may be much to learn from risk communication in non-security fields, especially those with longer histories and hard-fought successes. In particular, we see the value of greater investigation into how lessons learned in public health advocacy might be applied to cybersecurity given that this connection was raised repeatedly in our interviews.

Moving beyond these similarities, our findings suggest some unique properties of security risk which may advance the overall discipline. Specifically, we identified how advocacy in the security domain may be more urgent and challenging than in other domains, and may require additional tactics. Foremost, the security field is incredibly dynamic, having to adjust to constantly changing technologies and defend against determined adversaries who can exact significant damage with relatively little cost or sophistication. Second, security applies to everyone and every organization within an interconnected, technology-dependent society. However, most are not equipped to deal with security measures since security consists of abstract concepts not well understood by the typical person, and people are often dependent on security interfaces with poor usability. Motivation to enact security measures may likewise be problematic because consequences of poor behavior are not always immediate or easily observed. The economics and effectiveness of security are hard to measure. To better explore these similarities and differences, we see future research potential in performing in-depth comparisons of security advocacy practices to those in other domains.

6.1.2 Strategies for Communicating Security Risk

As discussed in Related Work, most prior research on persuasive methods in the security context has taken the perspective of the target end users and not those who do the influencing. Our study addressed this gap and does indeed confirm previous findings concerning the value of small group interactions [1], the necessity of framing security communications [40], the use of positive vs. negative incentives [15], and the importance of encouraging security self-efficacy [35]. However, our findings go beyond, for example, by uncovering a set of non-technical advocacy skills and competencies focused on bridging the gap between security experts and non-experts.

The study also questions the universal effectiveness of rhetorical devices like narratives, analogies, and metaphors, within security contexts. For example, even though only four participants explicitly said that they employ metaphors and analogies when communicating with their target audiences,

we observed that many advocates naturally used a variety of these to describe security concepts during our interviews. This was the case even though the interviewer was known to be a security expert, suggesting that their use goes beyond being purely instructive. Additionally, in line with the mixed findings in past studies about the efficacy of metaphors [4], two of our participants cautioned against incorrect use of these for fear that they may oversimplify security concepts and create misunderstandings leading to risky behaviors. Future work is needed to look more deeply into the use of metaphors and the level of detail and relevancy they must provide in order to affect security learning and behavior.

We also see value in applying security advocacy techniques to the design of security interfaces and training resources. To overcome negative perceptions of security, these resources should aim to empower users to take appropriate security actions and create a positive affect towards security. Security resources should create a level of concern without overwhelming or paralyzing by conveying severity and likelihood in clear, understandable terms. Resources must be usable, tailored to the audience, and encourage empowerment by providing concrete, achievable steps in simple language. Additional references to threat information that includes real stories of security incidents can lend greater credibility to risk claims. Training materials should consider the incorporation of storytelling and other creative rhetorical methods (e.g., [21]).

6.2 Emerging Cybersecurity Advocate Role

The majority of the participants in our study demonstrated an innate understanding of human behavior, even though few had formal training in the social sciences or humanities. They regularly employed techniques to combat common behavioral heuristics and biases that could negatively affect security decisions, as suggested by Pfleeger and Caputo [29]. For example, they addressed cognitive load by breaking recommendations down into manageable, prioritized chunks. Storytelling, sharing personal experiences, and referencing recent events helped with availability, which is an evaluation of the likelihood of an event based on recall of similar events happening.

Although the participants seemed to consider these behavioral aspects (even if subconsciously), they suggested that most other security practitioners do not share this basic interpersonal orientation. These professionals often contribute to negative perceptions of security by not taking the human element under consideration when describing, designing, administering, and enforcing security mechanisms. The advocates revealed a desire to move away from common security practitioner perceptions that "users are the enemy" and "users are stupid" to instead take the human element under consideration and regard users and security professionals as capable partners.

In some meaningful ways, the practice of securing a system appears to be different than advocating for securing a system. Yet, there is no professional preparation for the latter. An analogous situation was the foundation of human-factors/usability engineering as a profession distinct from other disciplines such as testing or business analysis. This was rooted in a discovery that human errors in systems were fundamentally different than system errors. As a result, this observation necessitated different approaches. Similarly, we see a new and rapidly growing need for security professionals with a special set of advocacy skills and techniques. Therefore, we propose that there should be continuing education efforts to aid in the progression to cybersecurity advocate from both security and non-security fields.

Currently, most of the emphasis within security professional development curricula [2,24,25] is on gaining technical knowledge. A quick review of cybersecurity work roles in these guidelines reveals that none contain set of skills that resemble the work of an advocate. Therefore, our future work may include developing a framework of cybersecurity advocate knowledge, skills, and abilities, along with an outline of a development program to facilitate advocate professionalization.

6.3 Limitations and Future Work

The study has a few limitations we intend to address in the next phase of the project. This study is a one-sided view through the lens of security advocates themselves. While this is critical for constructing a grounded understanding of their work, it does not provide evidence that any of the techniques they deemed successful were indeed effective with their intended audiences. Second, interviews may suffer from self-report bias in which participants may adjust their answers to appear more acceptable to the researcher, who had been revealed to be a security professional. This was a reasoned tradeoff in the study design meant to assist with recruitment and trust building as the researcher spoke the same technical language as the participants.

To address these potential issues, results can be triangulated with data from planned follow-on studies. We next intend to reverse the polarization of our lens and work with a diversity of organizations to understand their experiences with security advocates.

7. CONCLUSION

Cybersecurity advocates are emerging as a unique role in the ecology of security professionals. They employ a variety of skills and techniques to overcome negative perceptions of security. Our study confirms the applicability of past risk communication literature to the security domain while revealing additional considerations to address differences in cybersecurity. It also proposes the establishment of a new cybersecurity advocate career track to address the urgent need for security adoption.

Acknowledgements

The authors would like to thank the following people for their insightful comments that resulted in improvements to this paper: the anonymous reviewers, Yasemin Acar, Sascha Fahl, Sandra Spickard Prettyman, and Mary Theofanos.

8. REFERENCES

[1] E. Albrechtsen and J. Hovden. Improving information security awareness and behaviour through dialogue, participation and collective reflection: An intervention study. *Computers & Security*, 29(4):432–445, 2010.

[2] Association for Computing Machinery. Toward curricular guidelines for cybersecurity: Report of a workshop on cybersecurity education and training.

https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf, 2013.

[3] A. Bandura. Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 1977.

[4] G. L. Brase, E. Y. Vasserman, and W. Hsu. Do different mental models influence cybersecurity behavior? Evaluations via statistical reasoning performance. *Frontiers in Psychology*, 8, 2017.

[5] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy*, 9(2):18–26, 2011.

[6] L. J. Camp. Mental models of privacy and security. *IEEE Technology and Society Magazine*, 28(3), 2009.

[7] H. H. Clark and S. E. Brennan. Grounding in communication. *Perspectives on Socially Shared Cognition*, 13:127–149, 1991.

[8] J. Corbin and A. L. Strauss. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Sage, Thousand Oaks, CA, 4th edition, 2015.

[9] V. Covello. Risk communication. In H. Waldron and C. Edling, editors, *Occupational Health Practice*, chapter 6. Arnold Publishers, London, 1997.

[10] L. F. Cranor and S. Garfinkel. *Security and usability: designing secure systems that people can use*. O'Reilly Media, Inc., Boston, MA, 2005.

[11] M. Dolata, T. Comes, B. Schenk, and G. Schwabe. Persuasive practices: Learning from home security advisory services. In *International Conference on Persuasive Technology*, pages 176–188, 2016.

[12] S. Furnell and K.-L. Thomson. Recognising and addressing 'security fatigue'. *Computer Fraud & Security*, (11):7–11, 2009.

[13] B. G. Glaser and A. L. Strauss. *The Discovery of Grounded theory: Strategies for Qualitative Research*. Transaction Publishers, 2009.

[14] J. A. Gordon. Meeting the challenge of risk communication. *Public Relations Journal*, 47(1):28, 1991.

[15] T. Herath and H. R. Rao. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2):154–165, 2009.

[16] D.-L. Huang, P.-L. P. Rau, and G. Salvendy. A survey of factors influencing people's perception of information security. In *International Conference on Human-Computer Interaction*, pages 906–915, 2007.

[17] I. Ion, R. Reeder, and S. Consolvo. '... no one can hack my mind': comparing expert and non-expert security practices. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 327–346, 2015.

[18] A. C. Johnston and M. Warkentin. Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, pages 549–566, 2010.

[19] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. 'my data just goes everywhere:' user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*, 2015.

[20] R. E. Kasperson, D. Golding, and S. Tuler. Social distrust as a factor in siting hazardous facilities and communicating risks. *Journal of Social Issues*, 48(4):161–187, 1992.

[21] E. Lastdrager, I. C. Gallardo, P. Hartel, and M. Junger. How effective is anti-phishing training for children? In *Symposium on Usable Privacy and Security (SOUPS)*, 2017.

[22] J. E. Maddux and R. W. Rogers. Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5):469–479, 1983.

[23] S. Merriam and E. Tisdell. *Qualitative Research: A Guide to Design and Implementation*. John Wiley & Sons, San Francisco, CA, 4th edition, 2016.

[24] National Security Agency. National Centers of Academic Excellence in Cyber Defense. https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/, 2018.

[25] W. Newhouse, S. Keith, B. Scribner, and G. Witte. NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf, 2017.

[26] J. R. Nurse, S. Creese, M. Goldsmith, and K. Lamberts. Trustworthy and effective communication of cybersecurity risks: A review. In *Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 60–68, 2011.

[27] Office of the Director of National Intelligence. Assessing Russian activities and intentions in recent US elections. https://www.dni.gov/files/documents/ICA_2017_01.pdf, Jan. 2017.

[28] M. Q. Patton. *Qualitative research and evaluation methods*. Sage, Thousand Oaks, CA, 4th edition, 2015.

[29] S. L. Pfleeger and D. D. Caputo. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4):597–611, 2012.

[30] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & Management*, 51(5):551–567, 2014.

[31] G. V. Post and A. Kagan. Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, 26(3):229–237, 2007.

[32] S. S. Prettyman, S. Furman, M. Theofanos, and B. Stanton. Privacy and security in the brave new world: The use of multiple mental models. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*, pages 260–270, 2015.

[33] F. Raja, K. Hawkey, S. Hsu, K.-L. C. Wang, and K. Beznosov. A brick wall, a locked door, and a bandit: a physical security metaphor for firewall warnings. In *Symposium on Usable Privacy and Security (SOUPS)*, page 1, 2011.

[34] E. M. Redmiles, A. R. Malone, and M. L. Mazurek. I

think they're trying to tell me something: Advice sources and selection for digital security. In *IEEE Symposium on Security and Privacy*, pages 272–288, 2016.

[35] H.-S. Rhee, C. Kim, and Y. U. Ryu. Self-efficacy in information security: It's influence on end users' information security practice behavior. *Computers & Security*, 28(8):816–826, 2009.

[36] E. M. Rogers. *Diffusion of Innovations*. Simon and Schuster, New York, NY, 5th edition, 2003.

[37] R. W. Rogers. Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo and R. E. Petty, editors, *Social psychophysiology: A sourcebook*, pages 153–176. Guilford Press, New York, NY, 1983.

[38] K. E. Rowan. Why rules for risk communication are not enough: A problem solving approach to risk communication. *Risk Analysis*, 14(3):365–374, 1994.

[39] P. M. Sandman. Getting to maybe: Some communications aspects of siting hazardous waste facilities. In T. S. Glickman and M. Gough, editors, *Readings in Risk*. RFF Press, Washington, D.C., 2013.

[40] J. D. Shropshire, M. Warkentin, and A. C. Johnston. Impact of negative message framing on security adoption. *Journal of Computer Information Systems*, 51(1):41–51, 2010.

[41] M. T. Siponen. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1):31–41, 2000.

[42] P. Slovic. Perception of risk. *Science*, 236(4799):280–285, 1987.

[43] T. Sommestad, H. Karlzén, and J. Hallberg. A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, 9(1):26–46, 2015.

[44] B. Stanton, M. F. Theofanos, S. S. Prettyman, and S. Furman. Security fatigue. *IT Professional*, 18(5):26–32, 2016.

[45] Symantec Corporation. 2016 internet security threat report. `https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf`, 2016.

[46] US-CERT. OpenSSL Heartbleed vulnerability (CVE-2014-0160). `https://www.us-cert.gov/ncas/alerts/TA14-098A`, 2014.

[47] Verizon. 2016 data breach investigations report. `http://www.verizonenterprise.com`, 2016.

[48] K. Waddell. Yahoo suffers history's biggest known data breach. *The Atlantic*, Dec. 14, 2016.

[49] R. Wash. Folk models of home computer security. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 11–26, 2010.

[50] J. L. Yang and A. Jayakumar. Target says up to 70 million more customers were hit by December data breach. *Washington Post*, Jan. 10, 2014.

[51] L. Zhang-Kennedy, S. Chiasson, and R. Biddle. Stop clicking on update later: Persuading users they need up-to-date antivirus protection. In *International Conference on Persuasive Technology*, pages 302–322, 2014.

[52] M. E. Zurko and R. T. Simon. User-centered security. In *Proceedings of the 1996 Workshop on New Security Paradigms*, pages 27–33, 1996.

APPENDIX

Interview Questions

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 about your work?
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?