“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
Baltimore, MD 21250, USA
jhaney1@umbc.edu

Wayne G. Lutters
University of Maryland, Baltimore County
Baltimore, MD 21250, USA
lutters@umbc.edu

Abstract
Cyber attacks are on the rise, but many people fail to implement basic cybersecurity practices and technologies due in part to negative perceptions of security. Our study explores the techniques cybersecurity advocates use to overcome these perceptions. Preliminary findings reveal that advocates attempt to empower their audience, employ context awareness to put security in understandable terms, and practice engaging communication techniques to make security more interesting.

Author Keywords
Cybersecurity; security professionals; security attitudes

ACM Classification Keywords
H.5.3. Group and Organization Interfaces: Computer-supported cooperative work

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).

Overcoming "It's Scary."

"In terms of it being scary…take that head on. 'Here are all the terrible things that can happen. Here's what you can do to defend yourself.' And then you move into…reassuring. 'OK, here are a few things that can genuinely help you.'" (P08)

"I think 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)

"[A mistake in security advocacy is] being more sensational, and theoretical, and hypothetical than practical and rational…Yes, these are concerns, but let's talk not about possibility, but probability. Focusing on the possibility is a very easy way to get known as crying wolf." (P02)

"One of the things I read and believe to be true… is the saying…'Walk in smiling.'" (P01)

On a regular basis, the news is filled with reports of cybersecurity attacks [11][21][23], with companies, government agencies, and individuals being exploited at an alarming pace [19][20]. Despite real and evolving cyber threats, users are falling behind in defending their systems and networks [3]. They often fail to implement and effectively use basic cybersecurity practices and technologies, due in part to negative feelings about security, including frustration and futility [4].

Cybersecurity advocates are security professionals who actively promote and encourage the adoption of security best practices. To be successful, they must overcome negative perceptions of security. However, little research has been done to understand the techniques they use to do so. To address this gap, we interviewed cybersecurity advocates from private industry, academia, government, and non-profits. Our preliminary findings reveal ways in which advocates attempt to overcome widely-held views that security is scary, confusing, and dull.

Related Work

Numerous studies have explored user perceptions of security. Several studies examined people's often incomplete and inaccurate mental models of security and how these models perpetuate poor security practices [13][10][22]. Furnell and Thomson [5] and Stanton et al. [18] discussed "security fatigue," a weariness towards security when it becomes too difficult or burdensome. One project compared informal sources of security information and how each of these provides incomplete views [14]. Other researchers have shed light on the marked differences in security behaviors between security experts and non-experts [8] [12].

Other efforts investigated persuasive and educational techniques and approaches for influencing security behavior change. Several studies focused on security awareness and enforcement strategies within organizations [1][7][16][17] or for home users [9][15].

Methods

We conducted 19 semi-structured interviews, lasting on average 45 minutes, as part of an in-progress study. Using researcher contacts, internet searches, and snowballing, we recruited participants based on their roles as cybersecurity advocates. Interview questions addressed several areas: work practices, professional motivations and challenges, characteristics of successful advocates, and communication approaches. Participants also completed a short, online demographic survey that collected information about their professional backgrounds. Interviews were audio recorded and transcribed. We then performed iterative, inductive analysis on the data to identify core concepts [6]. Representative quotations from the resulting conceptual categories are provided in the sidebars.

Findings

We focus on our preliminary findings of how advocates attempt to overcome negative perceptions of security.

It's Scary

The consequences of poor security can be catastrophic on personal, organizational, national, and global levels. One participant noted that the internet is *"getting more insecure constantly, technologically less secure. The bad guys are getting better"* (P06). It's not surprising, then, that many people view cybersecurity with fear. To address this perception, cybersecurity advocates must

Overcoming "It's Confusing."

"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. Or you're toast." (P11)

"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)

"Being articulate, understanding your environment, and the different, unique threats and vulnerabilities in your environment is hugely important." (P14)

"[Less technical audiences are] 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?" (P04)

strike a careful balance between being candid about security risks while being optimistic and encouraging.

To convey a sense of importance and urgency to their audience, our participants said that they must be forthcoming about threats and potential consequences. One participant remarked, *"You can't appreciate the importance of security without first understanding what's at stake, what's at risk"* (P14). However, our 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. In some cases, advocates may only want to engage a select group with the power to address a security issue: *"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).

For most individuals, feeling helpless to improve their security situation contributes to the fear. Therefore, advocates attempt to empower their audience to protect themselves. Education and awareness are first steps in illuminating the importance of security and providing basic, concrete actions they can take. In addition, advocates elicit confidence by providing evidence that proposed solutions and best practices are sound, for example, by including compelling metrics or showing that recommendations were built with community consensus. Our participants also emphasized that having a positive, optimistic, and service-oriented attitude helps to reassure and alleviate feelings of fear.

It's Confusing

Few people have the technical expertise to understand the underlying security issues and how to remedy these. One participant noted, *"security is mysterious to most people"* (P07). Highly technical people often only serve to make this understanding more elusive: *"They understand technology and problems so well, they have this assumption other people must understand it also… and as a result, they communicate in rather confusing terms"* (P09). Advocates attempt to overcome the perception that security is confusing by being context aware, educating, and translating as needed.

Context awareness is critical. As much as possible, good security advocates need to be aware of the environment of their audience, including the technology, people, social and cultural structures, constraints, and goals. Several participants noted that empathy towards their audience is an important skill.

Our participants exercised this context awareness in their roles as educators. Just as education can empower individuals to overcome fear, it provides a *"basic level of knowledge you need to know for self-preservation purposes"* (P15) and helps people make informed decisions about their security behaviors.

Advocates must also act as "translators," putting highly technical information into terms their audience can understand. When communicating to organizations, advocates *"need to translate technical findings into the need for business action"* (P10).

Our participants unanimously agreed that the amount of security information to be aware of can be overwhelming, even for them. To counter this, several

Overcoming "It's Dull."

"If you don't like what you're doing…you can't sell it. 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)

"The people that I think are successful in really promoting security are the ones that can explain the problem to you, they can put it in your terms, but you can really feel the energy that they believe in it." (P12)

"Personalizing the message is useful, seeing that this happens to real people." (P07)

"You have to do things that are understandable, that are quick-hit, that are unique enough that people want to play and participate and learn and not just delete it." (P02)

"I think it really helps if you can give an entertaining speech." (P06)

participants created recommendations that condense security information into more manageable chunks - "top 5" or "top 10" lists of security actions to take.

Lastly, several of our participants emphasized the need to advocate for security technologies that are usable and minimize required knowledge. One participant explained this 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).

It's Dull

Security can be boring to less technical audiences, especially when a technologist fails to frame security in terms her audience can understand. Additionally, people may have a hard time understanding how security relates to their own daily lives. Feelings of fear and futility, as described earlier, may further contribute to apathy. Cybersecurity advocates try to overcome these negative perceptions by outwardly exhibiting enthusiasm and using engaging communication techniques.

Our participants were passionate about their role as advocates. They felt that openly conveying their passion captures attention and promotes greater engagement. Security professionals who give presentations in a monotone, lackluster fashion risk losing their audience even if the material is valuable. Therefore, our participants employed a variety of communication techniques via different media (e.g. videos, blogs, training courses, presentations) to peak interest and encourage learning. Participants engaged in storytelling to make security more memorable and relatable. They also often used analogies, metaphors, pop culture references, and imagery. For example, the analogy to public health and basic hygiene (washing your hands, brushing your teeth) was mentioned several times to explain the concept of cyber hygiene (basic, fundamental security practices).

Discussion and Future Work

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. The approaches used by our participants warrant further investigation to determine their effectiveness in overcoming negative security perceptions and encouraging behavior change. For example, our interview participants used a variety of metaphors and analogies, not just to explain how they talk to their audiences, but even to describe their advocacy experiences during the interviews to the first author who has a background in cybersecurity. Future work is warranted to look more deeply into these metaphors as suggested by Camp who theorized how mental models of physical security, medical infections, criminal behavior, economics failure, and warfare might be applied to communicate cybersecurity risk [2]. Additionally, we believe there should be more research into storytelling within the cybersecurity context and how advocates can be truthful about risk while encouraging optimism and confidence. Finally, the lessons on context awareness and effective communication methods can serve as a bellwether for the skills cybersecurity professionals must develop to accelerate security behavior change and thwart cyber attacks. To date, most of the emphasis within security professional curricula has been on technical skills, but possessing these other "soft skills" may be as or more important.

References

1. Eirik Albrechtsen and Jan Hovden. "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study." Computers & Security 29, no. 4 (2010): 432-445.
2. L. Jean Camp. "Mental models of privacy and security." *IEEE Technology and society magazine* 28, no. 3 (2009).
3. Larry Clinton. 2014. *Cyber-Risk Oversight*. Director's Handbook Series. National Association of Corporate Directors.
4. Pual Dourish, Rebecca E. Grinter, Jessica Delgado De La Flor, and Melissa Joseph. "Security in the wild: user strategies for managing security as an everyday, practical problem." Personal and Ubiquitous Computing 8, no. 6 (2004): 391-401.
5. Steven Furnell and Kerry-Lynn Thomson. "Recognising and addressing 'security fatigue'." Computer Fraud & Security 2009, no. 11 (2009): 7-11.
6. Barney G. Glaser and Anselm L. Strauss. 2009. The Discovery of Grounded Theory: Strategies for Qualitative Research. Transaction Publishers.
7. Tejaswini Herath and H. Raghav Rao. "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness." Decision Support Systems 47, no. 2 (2009): 154-165.
8. Iulia Ion, Rob Reeder, and Sunny Consolvo. 2015. "... no one can hack my mind": comparing expert and non-expert security practices. In Proc. of the Symposium on Usable Privacy and Security (SOUPS '15), 327-346.
9. Elmarie Kritzinger and Sebastiaan H. von Solms. "Cyber security for home users: A new way of protection through awareness enforcement." Computers & Security 29, no. 8 (2010): 840-847.
10. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara 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.
11. Office of the Director of National Intelligence. Assessing Russian Activities and Intentions in Recent US Elections. Jan 6, 2017. https://www.dni.gov/files/documents/ICA_2017_01.pdf
12. Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, and Ross T. Hightower. 2014. Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information & management* 51,5 (July 2014), 551-567.
13. Sandra Spickard Prettyman, Susanne Furman, Mary Theofanos, and Brian 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, pp. 260-270. Springer International Publishing, 2015.
14. Emilee Rader and Rick Wash. "Identifying patterns in informal sources of security information." Journal of Cybersecurity 1, no. 1 (2015): 121-144.
15. Hyeun-Suk Rhee, Cheongtag Kim, and Young U. Ryu. "Self-efficacy in information security: Its influence on end users' information security practice behavior." Computers & Security 28, no. 8 (2009): 816-826.
16. Ruey Shiang Shaw, Charlie C. Chen, Albert L. Harris, and Hui-Jou Huang. "The impact of information richness on information security awareness training effectiveness." Computers & Education 52, no. 1 (2009): 92-100.
17. Mikko T. Siponen. "A conceptual foundation for organizational information security

awareness." Information Management & Computer Security 8, no. 1 (2000): 31-41.

18. Brian Stanton, Mary F. Theofanos, Sandra Spickard Prettyman, and Susanne Furman. "Security Fatigue." IT Professional 18, no. 5 (2016): 26-32.
19. Symantec. 2016. 2016 Internet Security Threat Report. Symantec Corporation, Mountain View, CA. Retrieved December 18, 2016 from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
20. Verizon. 2016. *2016 Data Breach Investigations Report*. Retrieved December 18, 2016 from http://www.verizonenterprise.com
21. Kaveh Waddell. Yahoo Suffers History's Biggest Known Data Breach. Dec. 14, 2016. The Atlantic. https://www.theatlantic.com/technology/archive/2016/12/hackers-steal-data-from-more-than-a-billion-yahoo-accounts/510716/Retrieved May 12, 2017.
22. Rick Wash. 2010. Folk models of home computer security. In *Proc. of the Sixth Symposium on Usable Privacy and Security* (SOUPS '10), 11-26.
23. Jia Lynn Yang and Amrita Jayakumar. Jan. 10, 2014. Target says up to 70 million more customers were hit by December data breach. Washington Post. https://www.washingtonpost.com/business/economy/target-says-70-million-customers-were-hit-by-dec-data-breach-more-than-first-reported/2014/01/10/0ada1026-79fe-11e3-8963-b4b654bcc9b2_story.html?utm_term=.505f66664110. Retrieved May 12, 2017.