The Work of Cybersecurity Advocates

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

CHI'17 Extended Abstracts, May 06-11, 2017, Denver, CO, USA
ACM 978-1-4503-4656-6/17/05.
http://dx.doi.org/10.1145/3027063.3053134

Abstract

Cyber attacks are on the rise, endangering our sensitive information at an alarming rate. Cybersecurity advocates attempt to counter this wave of attacks by promoting security best practices. Their impact on organizational uptake varies and there is little research to understand this. Our study explores the motivations, characteristics, and practices of cybersecurity advocates. Eight preliminary interviews reveal that successful advocates must not only possess technical skills, but also a strong orientation toward service, people, context, and communication. Implications may include training and tools that better support security advocacy efforts.

Author Keywords

Security professionals; cybersecurity

ACM Classification Keywords

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

Introduction

Cyber attacks are on the rise and companies, government agencies, and individuals are being exploited at an alarming pace [24][27]. A 2016 survey conducted by a major telecommunications provider found that over 60% of the businesses surveyed had an information technology security breach in 2015, with 42% of those reporting that the breach resulted in significant negative impact [2]. Despite real and evolving cyber threats, organizations and individuals are falling behind in defending their systems and networks [7]. They often fail to implement and effectively use basic cybersecurity practices and technologies [8], leading to questions about why security seems to be so difficult.

General technology adoption models [17][26], such as Diffusion of Innovations Theory [20], reveal a variety of factors that influence whether or not a technology will be accepted within an organization as well as the significant roles individuals play in the adoption decision process. These roles include *change agents*, who work to convince their intended audience that there is a need for change, build a solid information exchange relationship, aid in the deployment of the technology, and attempt to ensure long-term adoption of the technology [20]. In the cybersecurity world, these change agents go by many titles, including security consultants, security evangelists, and information security professionals. In essence, these "cybersecurity advocates" are individuals who encourage positive change by promoting and providing guidance on security best practices and technologies.

Given modern society's dependence on technology, cybersecurity is a critical area for which to advocate. Advocates play a different, but complementary role than that of other security professionals (e.g., security administrators) as they are less concerned with day-to-day operations and more focused on influencing behavior changes. To date, there has been little research to understand the effectiveness and success factors of advocates, specifically within the cybersecurity context. To begin to address this gap, our study explores the motivations, characteristics, and practices of cybersecurity advocates, how effective they are at reaching and influencing organizations to adopt security technologies, and how their efforts may differ from those of advocates in other technology areas. This understanding will ultimately help inform the design of more effective security advocacy tools and techniques.

As an initial effort in a longer term study, we conducted in-depth interviews with eight cybersecurity advocates representing private industry, academia, government, and non-profit security advocacy groups. Our preliminary results suggest that successful cybersecurity advocates must not only possess technical skills, but also a strong orientation toward service which includes emphases on people, context, and communication. In addition, we found the cybersecurity field has its own unique challenges that influence the motivations and approaches of advocates.

Related Work

Security Technology Adoption

A small body of literature focuses on technology adoption within the cybersecurity space. One research team compared and synthesized security technology adoption models from the literature [17]. Others proposed new models based on adoption studies in a particular sector, for example, a theory-based security technology adoption model in banking organizations [25], or for a specific type of security technology, such as public key infrastructure [6] or secure development tools [31][32].

	Gender	Years Security Experience	Current Position	Current Professional Sector(s)	Past Professional Sector(s)
P01	M	10+	Cybersecurity Expert	Government	Government
P02	M	10+	Professor	Education/Academia, Government	Private industry
P03	F	10+	Computer Scientist	Government	Government
P04	M	10+	Security Evangelist	Cybersecurity Non-profit	Government
P05	M	10+	Cybersecurity Researcher	Private industry	Government
P06	M	10+	President	Cybersecurity Non-profit	Government, Education/Academia, Private Industry
P07	F	10+	Technical Executive, Professor	Education/Academia, Government	Private industry
P08	M	5-10	Attorney, Security Consultant	Private Industry, Legal	Private Industry, Legal

Table 1: Participant demographics

There are also lessons from related fields that may be applied within the cybersecurity context, for example, motivators for physical, home security adoption [28]. In the Information Systems (IS) field, there have been multiple research efforts focused on understanding the impact, roles, and adaptability of change agents who play an important role in information technology adoption [15][16][30].

Security Professionals

Limited research has been dedicated to the study of security professionals. Efforts have aimed to define needed security professional skills [22][23] and to understand personality characteristics of those drawn to cybersecurity competitions [3]. Two significant field studies, the HOT Admin project [4][11] and IBM's system administrator study [10], sought to illuminate the characteristics and challenges of security administrators in order to inform the design of more effective tools. However, we have yet to find literature that specifically explores the work practices of security professionals whose primary task is the promotion of security practices, a gap our study hopes to address.

Methods

We conducted eight semi-structured interviews that were between 35 and 80 minutes in length. Interview questions addressed several areas: work practices, professional motivations and challenges, characteristics of successful cybersecurity advocates, and communication approaches. Participants also completed a short, online demographic survey that collected information on gender, years of experience in the field, position, and sectors in which they have worked.

Technical knowledge:
"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)

Importance of the work:
"[The Internet] is getting more insecure constantly, technologically less secure. The bad guys are getting better…so the threat is really scary." (P06)

"It's important because of the implications of not doing it… the significance and the potential of loss of dollars, of information, of man hours, of intellectual property, sensitive information." (P01)

Passion for the work:
"It's personally satisfying…it became kind of a calling over the years for me." (P04)

Using researcher contacts, internet searches, and snowballing, we recruited a purposeful sample of participants based on their roles as cybersecurity advocates. See Table 1 for key participant and transcribed. We then performed iterative, inductive analysis on the data to identify core concepts [9].

Findings

We focus on a portion of our initial findings that suggest that not just technical competencies, but also a service orientation, are integral to the success of cybersecurity advocates. Additionally, there are unique characteristics of the cybersecurity field that may make advocacy more challenging. Successful advocates must be able recognize and address these.

Technical Knowledge is Not Enough

Information technology changes at a rapid rate, with security technology and practices evolving even faster to keep pace with changing threats. Not surprisingly, cybersecurity is most often viewed through a technical lens, with good technology seen as a solution to security problems. Our participants acknowledged that effective cybersecurity advocates must possess strong technical knowledge in order to gain trust and credibility with their target audiences. Several participants also specifically commented that they felt the responsibility to provide accurate, sensible technical information since, even though technology is becoming more ubiquitous, *"security [is] pretty mysterious to most people"* (P07). However, those trained only in traditional computing disciplines may not have all the skills to be an effective advocate. The interviews clearly revealed that addressing social and organizational factors may be more imperative than the technical solutions alone. One participant remarked, "*technology may not be the answer"* (P03).

Service Orientation

Participants expressed passion for their work and demonstrated a strong orientation towards service by helping others to protect themselves and their information— working towards the *"greater good"* (P04). Although the security problem may seem intractable in the midst of dynamic and often sophisticated threats, participants reflected that the job has too much importance, and that the economic, physical, and national security consequences may be too dire for them *not* to do something.

Participants saw the existence of a gap in security knowledge among individuals and organizations and were doing their best to try to fill that gap by serving in the roles of educator, consultant, and information mediator (a collector and carrier of information). To have the most impact, they attempted to address security problems at a larger scale, for example via mass market media and public policy. They maintained hope that they could make some traction towards solving security problems.

In addition to the importance of the work, evidence of success also kept advocates motivated. The ways in which our participants viewed success in this space points heavily to a service orientation: an overall feeling of having added value and been of assistance, a contribution resulting in organization or individual security independence, successful security implementation (and therefore greater protection), and indicators of learning and engagement among their target audience. However, quantitative metrics of

Service profession:
"I think we're making the world a better place." (P06)

"[I]t also gives me a great deal of pride to be able to do this kind of work and to be able to help as many people as possible...I think it's a very, very honorable profession." (P01)

"[I]t's…wanting to do something that is useful and will help people." (P07)

People orientation:
"You develop that rapport with them [your customers] so that they not only listen, but they trust you, and they understand." (P01)

"The most important thing is to go in and listen, listen to what their challenges are, what their problems are, rather than going in feeling like you have all the answers, because there's no one solution in this space." (P05)

security success can be difficult to obtain. One participant remarked, *"It's hard to prove that [security is] 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)

Hogan, et al. [12] define service orientation as the willingness to treat customers with courtesy, consideration, and tact; perceptiveness to customer needs; and the ability to communicate accurately and pleasantly. Although prior service orientation research has been mostly conducted in a customer service business context, we believe it has implications for cybersecurity advocacy as advocates' audiences can ultimately be viewed as "customers" of security information and guidance.

People Orientation

By definition, service orientation requires an alignment towards people: an understanding of human behaviors, biases, and limitations. It also necessitates "people skills," for example, the ability to build relationships. This idea of being people-oriented was repeatedly referred to in our interviews. When asked about the qualities or characteristics that make security advocates successful, several participants noted the ability to build relationships with others by gaining trust and demonstrating credibility. Most participants commented that good advocates often display a positive and genuine disposition in their interactions with others, truly try to understand their audience's needs, and realize that they must listen to, consider, and respect the concerns and viewpoints of others.

Another recurring topic was that security advocacy is not and cannot be an individual effort due to the diversity and interconnectedness of technologies and networks. Our participants especially recognized the importance of cultivating partnerships. In a complex, dynamic field, they themselves do not have all the answers, so they often must rely on collective expertise, common security goals, and the *"good will"* (P04) of others.

Context Awareness

In addition to a willingness to listen to people, being perceptive to customer needs requires context awareness. One participant said quite simply, *"context is king"* (P02). Multiple participants commented that there is no one-size-fits-all approach to cybersecurity, so a good advocate needs to be aware of the environment, including the technology, people, social and cultural structures, constraints, goals, and tasks. This can be challenging especially when the advocate is external to the organization and may have limited access to the customer. Several participants talked about the value of enlisting the support of champions and well-respected individuals within the target community to assist in understanding the environment. Nevertheless, without being context-aware, an advocate has little hope of success.

Participants said that successful cybersecurity advocates are adaptable in response to the situation. They also must understand and communicate the "why" behind security recommendations within a larger context. An important aspect of this is a recognition and understanding of the barriers customers face when trying to make decisions about and implement security practices. These barriers may stem from any number of

Context awareness:
"[An aspect of being successful is] understanding the context and the purpose of the organization…and the network that they were trying to help protect." (P01)

Communication skills:
"Being able to translate complicated things very simply is crucial to… advocating security." (P02)

"You have to know how to market." (P03)

"You have to make this confusing stuff sound like plain English." (P08)

economic, social, political, or structural issues. For example, in cybersecurity, as opposed to other technology areas, the economic value can be difficult to calculate. One participant noted, *"it's hard to show return on investment to things you've prevented."* (P06) However, especially within a business context, emphasizing the economic impacts of poor security is critical. Advocates tried to devise ways to overcome these barriers while remaining orientated towards the best interests of the organization.

Communication Skills

Communication skills were also viewed as critical to the success of cybersecurity advocates. They frame their communications to resonate and motivate their audiences, sometimes using metaphors to explain technical concepts to less-technical audiences. As several participants remarked, they are, in essence, marketing and selling security. They use a variety of communication approaches tailored to their audience, for example, newspaper or television interviews, presentations, or blogs. Several participants noted the importance of practicing discernment when choosing what to communicate, not "crying wolf" (being an unnecessary alarmist) over every little security issue, lest their audience become overwhelmed, disinterested, or skeptical.

Discussion and Conclusions

Our interviews suggest that, when compared to other technology adoption domains, cybersecurity has some critical differences that make advocacy both more urgent and challenging. Foremost, cybersecurity applies to everyone and every organization within a technology dependent and interconnected society. Security technology and behaviors must rapidly change to counter active and sophisticated threats. The consequences of not having good security can be catastrophic on personal, organizational, and national levels. These compelling reasons, however, are not always enough to persuade people to practice better security. This is because security is not well-understood by non-experts, the economics are hard to demonstrate, and effectiveness is difficult to measure.

In addition, communication approaches that influence the adoption of security protections and policies may be different to some extent than those of other technologies as suggested in [1][5][13]. Advocates must also address communication divides with non-expert users who have dissimilar mental models of security than experts [13][19][29]. By better understanding cybersecurity advocates' communication approaches, we may be able to identify more suitable communication techniques within this domain.

To date, cybersecurity adoption research has primarily been conducted within the IS domain. However, little has been done to explore security advocates within the computer-supported cooperative work (CSCW) area. Security can certainly be viewed as cooperative work, the "designation of multiple persons working together to produce a product or service" [21], as security is accomplished only through a dynamic community of security professionals and advocates, organizations, and users. We can then ask, how can computer technologies be designed to better support security advocates in this cooperative work? Therefore, we argue for the need for a greater synthesis of IS, CSCW, HCI, and traditional information security research to address cybersecurity advocacy issues, and plan to design our future research efforts towards this goal.

References

1. Lynda Andrews and Maree V. Boyle. 2008. Consumers' accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal* 11,1 (2008), 59-75.
2. AT&T. 2016. *The CEO's guide to cyberbreach response: What to do before, during, and after a cyberbreach*. AT&T Cybersecurity Insights, Volume 3. Retrieved December 18, 2016 from https://www.business.att.com/ cybersecurity/docs/cyberbreachresponse.pdf
3. Masooda Bashir, April Lambert, Jian Ming Colin Wee, and Boyi Guo. 2015. An examination of the vocational and psychological characteristics of cybersecurity competition participants. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education* (3GSE '15).
4. David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. 2007. Towards understanding IT security professionals and their tools. In *Proc. of the 3rd Symposium on Usable Privacy and Security* (SOUPS '07), 100-111.
5. Burcu Bulgurcu, Hadan Cavusoglu, Izak Benbasat. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* 34, 3 (September 2010), 523-548.
6. Elias G. Carayannis and Eric Turner. 2006. Innovation diffusion and technology acceptance: the case of PKI technology. *Technovation* 26 (2006), 847-855.
7. Larry Clinton. 2014. *Cyber-Risk Oversight*. Director's Handbook Series. National Association of Corporate Directors.
8. Commission on Enhancing National Cybersecurity. 2016. *Report on Securing and Growing the Digital Economy*. Retrieved January 10 from https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf
9. Barney G. Glaser and Anselm L. Strauss. 2009. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Transaction Publishers.
10. Eben Haber and Eser Kandogan. 2007. Security administrators: a breed apart. In *Workshop on Usable IT Security Management* (USM'07) held with the *ACM Symposium on Usable Privacy and Security (SOUPS '07)*.
11. Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, Konstantin Beznosov. 2008. Human, organizational, and technological factors of IT Security. In *CHI'08 Ext. Abstracts on Human Factors in Computing Systems*, 3639-3644.
12. Joyce Hogan, Robert Hogan, & Catherine M. Busch. 1984. How to measure service orientation. *Journal of Applied Psychology* 69, 1 (February 1984), 167.
13. 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.
14. Allen C. Johnston and Merrill Warkentin. 2010. Fear appeals and information security behaviors: an empirical study. *MIS Quarterly* 34, 3 (September 2010), 549-566.
15. M. Lynne Markus and Robert I. Benjamin. 1996. Change agentry – the next IS frontier. *MIS Quarterly* 20, 4 (December 1996), 385-407.
16. M. Lynne Markus and Robert I. Benjamin. 1997. The magic bullet theory in IT-enabled transformation. *MIT Sloan Management Review* 38,2 (Winter 1997), 56-68.
17. Azah A. Norman and Norizan M. Yasin. 2013. Information systems security management (ISSM) success factor: retrospection from the scholars.

African Journal of Business Management 7, 27 (July 2013), 2646-2656.

18. Tiago Oliveira and Maria F. Martins. 2011. Literature review of information technology adoption models at firm level. *Electronic Journal of Information Systems Evaluation* 14, 1 (2011), 110-121.
19. 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.
20. Everett M. Rogers. 2003. *Diffusion of Innovations* (5th ed.). Simon and Schuster, New York, NY.
21. Kjeld Schmidt and Liam Bannon. 1992. Taking CSCW seriously: supporting articulation work. In *Cooperative Work and Coordinative Practices*, 45-71.
22. Dan Shoemaker, Anne Kohnke, and Ken Sigler. 2016. *A Guide to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (2.0, Vol. 3). CRC Press.
23. Edward Sobiesk, Jean Blair, Gregory Conti, Michael Lanham, and Howard Taylor. 2015. Cyber education: a multi-level, multi-discipline approach. In *Proc. of the ACM 16th Annual Conference on Information Technology Education*, 43-47.
24. 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
25. Eric C. Turner. 2009. *A mixed methods study of information security technology adoption in banking organizations*. Ph.D. Dissertation. George Washington University, Washington, D.C.
26. Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, Fred D. Davis. 2016. User acceptance of information technology: toward a unified view. *MIS Quarterly* 27, 3 (September 2003), 425-478.
27. Verizon. 2016. *2016 Data Breach Investigations Report*. Retrieved December 18, 2016 from http://www.verizonenterprise.com
28. Carolos J. Vilalta. 2012. Fear of crime and home security systems. *Police Practice and Research* 13,1 (2012), 4-14.
29. Rick Wash. 2010. Folk models of home computer security. In *Proc. of the Sixth Symposium on Usable Privacy and Security* (SOUPS ’10), 11-26.
30. Elaine R. Winston. 1999. IS consultants and the change agent role. In *Proc. of ACM SIGCPR Comp. Personnel* 20, 4: 55-74.
31. Jim Witschey, Shundan Xiao, Emerson Murphy-Hill 2014. Technical and personal factors influencing developers’ adoption of security tools. In *Proc. of the 2014 ACM Workshop on Security Information Workers* (SIW ’14), 23–26.
32. Shundan Xiao, Jim Witschey, Emerson Murphy-Hill (2014). Social influences on secure development tool adoption. In *Proc. of the 17th ACM Conference on Computer-supported Cooperative Work & Social Computing* (CSCW ’14), 1095–1106.