Cybersecurity Advocates: Force Multipliers in Security Behavior Change

Julie Haney, NIST
Wayne Lutters, University of Maryland
Jody Jacobs, NIST

Despite an abundance of widely-available cybersecurity technologies and guidance, individuals and organizations continue to fall prey to digital attacks at an alarming pace, sometimes with devastating consequences. Security is often viewed as inconvenient, irrelevant, costly, or even mysterious, resulting in a lack of security adoption and failure of people to fundamentally change their security behaviors. Practitioners and researchers have put significant effort into developing security training products to remedy these issues. However, these attempts are often overly-focused on compliance and may fall short in providing the deeper, continuous engagement needed to make security an intrinsically-motivated habit.

There is a need for professionals who are adept at motivating individuals and organizations to adopt sustainable, positive security behaviors. Those taking on this role require a unique combination of technical and interpersonal skills along with an understanding of how to address the interrelatedness of underlying sociotechnical factors – human, organizational, social, economic, and technical factors – that impact security adoption. We call the professionals who perform these functions *cybersecurity advocates*.

Finding and developing these advocates is not easy, especially since this role has not yet been popularized. Based on insights gained from our research, we describe the qualities of successful advocates. Our findings have practical implications for expanding the cybersecurity workforce by recruiting and developing professionals who can be effective in advocate or other people-oriented security roles.

Qualities of Successful Cybersecurity Advocates

As scholars interested in sociotechnical cybersecurity, we embarked on a multi-year effort (2017-2021) to discover who cybersecurity advocates are, what they do, and what skills they employ in their work. We first conducted in-depth interviews with 28 self-identified cybersecurity advocates, with diverse backgrounds and job functions across a range of industry sectors. To understand how their practices play out in routine efforts to affect behavior change, we then completed a one-year, longitudinal case study of a three-person team of security awareness professionals (a type of advocate) in a U.S. government agency. We observed the team's annual training compliance calendar and activities in between, while focusing on how they plan for change and measure success. We broadened that understanding with focus groups of an additional 29 government security awareness professionals.

We found that cybersecurity advocates work in a variety of sectors with diverse audiences. Some perform advocacy work as their principal job and hold obvious titles, such as security awareness professional or security evangelist. However, many take on an advocacy role in a part-time capacity to enable success in their primary role, for example, a security consultant whose primary responsibility is to convince a client to adopt a particular security mitigation. Beyond identifying advocates' job responsibilities, from a workforce education and development perspective, we began to build a comprehensive picture of the professional qualities and skills of successful advocates.

Sufficient Technical Knowledge and Skills

To be successful in a techno-centric field, cybersecurity advocates should possess knowledge and skills related to information technology (IT), security technologies, and security threats. After all, advocates must be able to accurately interpret and present information to others, which requires a strong understanding of how certain actions lead to positive or negative security outcomes. Advocates who have worked in the IT or security fields gain much of their competence via on-the-job experience but must continue keeping updated on the latest in security threats and solutions. However, advocates coming into the security field from non-computing disciplines may gain knowledge through short-cut proxies (e.g., training courses, certifications) for years of experience. This was perhaps best exemplified by one study participant, a lawyer who became a security trainer for other attorneys. Although lacking a security background, he engaged in significant self-study and earned security certifications because he believed "You really do need to understand the technology…This stuff's tricky, and you don't just guess your way out of it."

Interestingly, we observed conflicting opinions about the depth of technical knowledge needed for the role. Some with IT-focused backgrounds tended to put more emphasis on strong technical competency. However, others viewed security knowledge and skills as something that, while necessary to a certain degree, could be picked up without formal education. From this discourse, we surmise the level of technical knowledge and skill required for security advocacy is often dependent on the context, including domain and level of audience technical expertise. For example, a secure development champion would need to be well-versed in software development practices in order to effectively converse with and persuade other developers. Conversely, as one study participants aptly said, security awareness professionals who are primarily communicating basic security concepts to their workforce "don't have to be hardcore techie." Therefore, we identify an overall need for advocates to have *enough* technical knowledge to establish credibility and trust with their intended audience.

Non-technical Skills

While technical skills may be an obvious assumption for those working in cybersecurity, there is much more required for a successful advocate. Our research participants touted non-technical skills as being just as, if not more, important as technical skills. Instead of the common mindset that less technology-savvy users are "the weakest link," a human-centered focus can facilitate a shift towards user empowerment. Unfortunately, many in our studies noted the lack of these skills within the cybersecurity community. For example, an advocate with decades of experience in the security field believed "We're terrible at empathy…We're terrible at soft skills. We're very mono-cultured and bring technical solutions."

Interpersonal Skills. To engender trust, build relationships, and facilitate behavior change, advocates must employ strong interpersonal skills, including listening skills, patience, and collaboration. A university Chief Information Officer commented about two other critical interpersonal skills, emotional intelligence and empathy: "Part of being successful in this is being able to have a conversation and put yourself in the place of the person that you're working with and then to be able to give effective advice,… letting them know that they’re not stupid because they may not know how to do certain things.” Interpersonal skills help establish positive relationships with stakeholders, making it more likely that they will listen to and act on security advice.

Context Awareness. Being keenly aware of the context of their audiences – including skill levels, values, and challenges – is another essential competency. To change people’s behaviors and instill a sense of personal responsibility, advocates must acknowledge that security is not one-size-fits-all and tailor tactics and messages based on audience context. Once the context is understood, advocates can employ creativity and adapt to their audience’s preferences, learning styles, and constraints. As an example, one security awareness team found that phishing email reminders were typically not read by employees due to email overload, so the team devised an alternative solution – placing small reminder postcards with a piece of candy on each employee’s desk.

Communication Skills. Context awareness goes hand-in-hand with strong communication skills and the ability to appropriately frame security messages. When working with less-technical individuals, advocates need to translate highly technical information into plain language. For example, a security awareness professional commented, “I think you need someone who is able to converse with network engineers, incident response teams. And when those people start talking about…encryption or cloud infrastructure,… they're able to take that information and restate it in a way that users will understand.” To communicate to diverse audiences in an engaging manner, advocates may become adept at using analogies, metaphors, storytelling, imagery, humor, and pop culture references. Conversely, ineffective translation can hamper success of a security program. This shortcoming was highlighted by an advocate working with large corporations: “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.”

Service Orientation

In our studies, we uncovered a strong desire to be of service to others. This service orientation was rooted in a deep passion for the importance of the work and wanting to help individuals, organizations, and society protect themselves from security threats.

Many advocates gravitate towards helping professions, expressing their motivations in terms such as “I am the type of person that likes to help other people.” They especially may be energized by assisting less-technical individuals navigate the complexities of cybersecurity. For example, the security awareness program lead of a government organization commented that his efforts “will make a difference not only for the agency and its mission but the people here as well… so they can just be aware of what’s going on and what they can do to make their life easier and protect themselves.”

Others saw far-reaching impacts of their work. For example, a usable security and privacy advocate said, “I primarily do it to fix society… If we don’t get computers right, people are going to starve.” A government security analyst, who promotes the adoption of security mitigations, saw his work as service to his nation: “It gives me a great deal of pride to be able to…help as many people as possible.” An advocate working with medical device manufacturers expressed his motivation as wanting “to save lives through security research.”

Discipline Diversity

Our participants had diverse educational backgrounds (Table 1). Only seven had a cybersecurity degree, while 25 had at least one formal degree in another computing or technology field (e.g., computer science, engineering, mathematics, IT, or information systems). Interestingly, many advocates did not come from these fields. Of the 60 cybersecurity advocates participating in our studies, 34 had at least one degree in a non-computing discipline such as business, psychology, law, English, communications, and education, with 11 of those having no technical degrees. Several came directly into security advocacy positions after years of working in non-IT positions.

Degree Field	# Participants
Cybersecurity/Information Assurance	7
Tech field (excluding cybersecurity)	25
Non-tech field	34
Unknown	7

Table 1: Participant degree fields. Note that many participants had more than one degree.

Non-technical skillsets, honed during prior careers or educational experiences outside of cybersecurity, were seen as advantageous in performing security advocacy. One participant's organization had surveyed security awareness professionals working in higher education and found that they are "not necessarily IT professionals by trade. They are communication professionals, or marketing professionals, or teachers. And they just come to this area, and they flourish because they have a unique set of skills." A non-profit director felt that advocacy skillsets are in short supply among security professionals in the corporate world, so the security community should "try to encourage people from outside of that security space to come into it. And they can pick up the technical skills very quickly… It's much more… how you can position security within the business context and ensure that you're delivering value."

Finding a single individual who possesses the right mix of technical and non-technical skills for advocacy work can, admittedly, be challenging. We observed that some organizations did not rely on just one person, but rather took a multi-disciplinary approach. For example, a security awareness director commented on the diverse backgrounds of her team: "I have people who can design, are very artful, creative people. I have people who can run a learning management system… I have good project managers. I have cybersecurity professionals."

Bolstering the Cybersecurity Workforce

During our investigation of cybersecurity advocates, we uncovered implications for workforce education, recruitment, and professional development. We suggest ways in which the security community might ensure there are enough people equipped to take on the cybersecurity advocacy role. We also describe how our advocate-focused discoveries may inform efforts towards building a more diverse and capable cybersecurity workforce.

Progressing the Cybersecurity Advocate Role

Advocates can be cultivated either from the existing security ranks or from outside the field. For those already practicing within the field, the advocate role may be a natural pivot. For example, mid-career progression often means transitioning to responsibilities more focused on leadership and influence. There may also be an advantage to having already security-literate people perform advocacy work, as they have less of a learning curve and may command more respect from colleagues. However, as demonstrated by our research, those from other disciplines may possess non-technical strengths that could also lead to success in an advocate role.

Regardless of prior career path, there is a need for a more formal definition of the advocate work role. This should include the tasks they perform and the knowledge and skills they must possess. A standardized cybersecurity advocate work role – akin to other roles in the National Initiative for Cybersecurity Education (NICE) Framework[1] – can also aid organizations in identifying, hiring, and developing qualified cybersecurity advocates.

The current NICE Framework includes a few work roles that map to advocacy work. One example is the Cyber Instructional Curriculum Developer, which is similar in function to a security awareness professional. SANS proposed a related work role, 'Security Awareness and Communications Manager,'[2] that places more emphasis on the non-technical skills that we identified in our studies. However, both the NICE and SANS awareness roles are focused on the delivery of educational materials and cannot be generalized to other types of security advocacy that may require a different and deeper level of engagement. Furthermore, our research shows that many perform advocacy work on a part-time basis as a secondary role, so may need to maintain high levels of technical skill/knowledge commensurate with their primary role (e.g., in the case of secure software development champions or security consultants). Therefore, we see the value of formally defining a generalized cybersecurity advocate work role that could be coupled with other roles as appropriate.

Once a work role is defined, professional development training courses and materials can be designed. A program of study for advocates may include the concepts and topics proposed in Table 2.

Concept	Example topics
Cybersecurity advocacy essentials	role/purpose of advocates, types of advocates, advocacy techniques, building discipline-diverse advocacy teams
Cybersecurity foundations	security principles, technologies, threats, and mitigations
Non-technical skills	interpersonal skills, understanding context, and communication skills as related to advocacy
Human-centered cybersecurity	behavioral theories, social considerations, usable security concepts
Organizational factors	cybersecurity economics, governance, and overcoming organizational barriers

Table 2: Example training program for cybersecurity advocates

Developing Non-technical Competencies Early

Non-technical skills are essential for cybersecurity advocates in their quest to catalyze behavior change within their target audiences. Obviously, not all security professionals have the need or aptitude to become an advocate. However, our research may have implications beyond advocate work, as it corroborates others who highlight that non-technical skills are becoming increasingly necessary for cybersecurity professionals in general. [3] An understanding of sociotechnical factors can be an advantage for any security professional, since most perform work that impacts people in some way. Furthermore, security professionals may occasionally (and perhaps, unexpectedly) find themselves having to perform advocate functions to be more impactful in their jobs.

For those already in the workforce, employers could encourage their security staff to pursue professional training that focuses on development of non-technical skills and fosters a greater understanding of sociotechnical factors, similar to the program in Table 2. Perhaps even more beneficial, though, is allowing up-and-coming advocates opportunities to gain hands-on advocacy experience and receive feedback from their audience.

Despite the recognized need for non-technical proficiencies, these skills are currently underrepresented in formal cybersecurity and computer science curriculum (e.g., the Centers of Academic Excellence-Cyber Defense Education[4]). This issue may be remedied in part by providing opportunities for developing non-technical skills within existing courses. As an exemplar, the cybersecurity program at University of Maryland, Baltimore County includes opportunities to practice non-technical skills in its courses because, as their graduate program director stated, "Just being a cybersecurity geek is not good enough. You also have to be knowledgeable and competent and have soft skills that allow you to be a team player... You need to write well and think critically. All of these skills are important to be a truly well-rounded and effective cybersecurity practitioner."[5]

In addition to incorporating non-technical skills in existing courses, institutions could offer more courses dedicated to the sociotechnical aspects of security. As an example, the University of Maryland College Park's undergraduate cybersecurity minor offers electives focused on topics such as: cyber communications; leadership, inclusion, and diversity; and the technical, policy, and social aspects of cybersecurity risk management.[6] Furthermore, the university's Information Science major offers a specialization focusing on human-centered cybersecurity.[7]

Expanding the Pipeline

Much effort has been invested to expand the current pipeline – including a focus on workforce diversity – to reduce the burgeoning shortfall of cybersecurity professionals, with mixed results. While we offer no silver bullet for this challenge, our research on advocates identifies potential opportunities to market cybersecurity careers a bit differently towards increasing both demographic and discipline diversity within the field.

Foremost, our research suggests that there may be a benefit in framing cybersecurity not just as a technology-focused field, but also as one in which those with strong interpersonal and communication skills can thrive. The awareness of cybersecurity jobs that are more people-oriented may aid in attracting currently underrepresented populations, such as women and certain minorities, as well as those with non-traditional backgrounds. These populations are often deterred by the perception of the security field as a male-dominated, hacker-focused culture without social benefit, the lack of understanding of the breadth of security careers, and the belief that only those with highly technical skills can succeed.[8,9]

Reframing cybersecurity as an important, service-oriented profession may additionally appeal to those drawn to helping professions. Anticipated outcomes that may be gleaned from a job description, such as 'I will optimize this cryptographic algorithm' or 'I will create this security application,' may not be as attractive for some compared to service-related impacts such as 'I will empower people to defend themselves from security threats' or 'I will contribute to national security.' The portrayal as a service profession may especially be well-aligned with the values of women as well as those of young people in 'Generation Z' soon to enter the workforce as they are, in part, characterized by their social mindedness and desire to positively impact the world.[10]

We also see value in the security community being open to bringing in people with non-traditional educational backgrounds and skills. These individuals may be able to gain sufficient knowledge of the technical aspects of security while contributing valuable perspectives. As it may be difficult to find people who have the right mix of technical and non-technical skills required for certain work roles, multi-disciplinary teams could be constructed to perform not only advocacy functions, but also to engage in comprehensive efforts to overcome a multitude of other security challenges.

Conclusion

Given the recent uptick in pandemic-induced cyber attack activity and the blurred line between home and work contexts due to an increasingly remote workforce, achieving sustained security behavior change is essential. Long-lasting change is ultimately predicated on appealing to intrinsic motivations for cyber hygiene to become a habit. Technical solutions alone will not solve the cybersecurity crisis. Cybersecurity advocates, with their unique mix of technical, interpersonal, and communication skills, can be a force multiplier in this effort, if we can find enough of them fast. Understanding the qualities of these advocates may also have implications for recruiting and retaining a more diverse workforce ready to tackle the sociotechnical problems in security and work towards more holistic security solutions.

Disclaimer

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

References

1. R. Petersen et al., "NIST Special Publication 800-181 Revision 1 – Workforce Framework for Cybersecurity (NICE Framework)," 2020, Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

2. SANS, “NIST NICE Work Role Description for Security Awareness and Communications Manager,” 2019, Retrieved from https://www.sans.org/security-awareness-training/blog/nist-nice-work-role-description-security-awareness-and-communications-manager

3. J. Dawson and R. Thomson, “The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance,” *Frontiers in Psychology*, vol. 9, 2018, pp. 744, https://doi.org/10.3389/fpsyg.2018.00744

4. National Security Agency, “National Centers of Academic Excellence in Cybersecurity,” 2021, Retrieved from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

5. R. Forno, “Extending Beyond with Cybersecurity,” 2020, Retrieved from https://gritinaction.umbc.edu/extending-beyond-with-cybersecurity/

6. “Advanced Cybersecurity Experience for Students,” 2021, Retrieved from https://aces.umd.edu/

7. “Curriculum & Cognate Areas - Bachelor of Science in Information Science at College Park (InfoSci),” 2021, Retrieved from https://ischool.umd.edu/academics/bachelor-of-science-in-information-science-college-park/curriculum

8. R. Shumba, et al., “Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation,” in *ITiCSE Conference on Innovation and Technology in Computer Science Education*, 2013, pp. 1-14.

9. M.D. Gonzalez, “Building a Cybersecurity Pipeline to Attract, Train, and Retain Women,” *Business Journal for Entrepreneurs*, vol. 3, 2018.

10. C. Seemiller and M. Grace, *Generation Z Goes to College*. Hoboken, NJ: John Wiley & Sons, 2016.