Career Paper: Security Awareness and Cultural Engineer

John F. Ryan

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity as a Social Science

Prof. Trinity Woodbury

October 28, 2024

Career Paper: Security Awareness and Cultural Engineer

There are many careers in cybersecurity outside of technical fields. One such career is that of a security awareness and cultural engineer (Udeh, 2022). Much of an organization's cybersecurity posture is dependent on the culture within. A security awareness and cultural engineer must create and maintain a culture that fosters good cyber hygiene and mitigates risk through the people in the organization instead of through technical means. This is especially important given that people are usually the weakest link in any cyber defense.

Culture can be both internal, or organizational, and external. Internal culture describes common customs and behaviors within the organization. External culture, the broader, more traditional definition of the word, encompasses the sum of an individual's experience prior to joining an organization. This could include the customs and ways of thinking common in a particular geographic area or country, religion, political views, etc. When crafting a positive cybersecurity culture, the cybersecurity professional should factor these external factors in as this increased understanding could help serve the effort to get all members of the organization onboard.

The Role of a Security Awareness and Cultural Engineer

The exact job duties of this career may vary from company to company, but H Layer Credentialing's (n.d.) Security Awareness and Culture Professional (SACP) certification exam content is a good survey of what the role entails. In this exam, candidates are measured on competency in the following domains:

1) Define organization's security awareness strategy
2) Provide security awareness training and education to end users
3) Reinforce security awareness with communications

4) Assess user behavior
5) Define and validate awareness metrics
6) Monitor effectiveness of security awareness program
7) Report status of compliance and outcomes

Within these domains there are specifics that directly map to external culture and social science considerations. Security awareness and culture professionals should "define content based on audience (e.g., social, environmental, regional)," "adapt communication to target audience," "identify potential cultural/organizational misalignment," "select appropriate behavioral interventions based on contextualized factors (e.g., environmental, social factors)," and "compare pre and post behaviors" (H Layer Credentialing, n.d.).

Social Science Principles

Bhattacherjee (2012) defined social science as "the science of people or collections of people, such as groups, firms, societies, or economies, and their individual or collective behaviors" (p. 1). Bhattacherjee (2012) further explained that "the goal of scientific research is to discover laws and postulate theories that can explain natural or social phenomena" (p. 3). Social science is no different than other scientific research. While the nature of studying people often prevents the use of laboratory experiments, social science experiments must also adhere to the same scientific rigor found in the "harder" sciences. Hypotheses should be posed, data should be gathered in an unbiased and representative manner, hypotheses should be tested using accepted statistical methods, and theories should be established based on the acceptance or rejection of these hypotheses.

Security awareness and cultural engineers would not be expected to conduct field research or studies of their own. However, there are two ways in which they should leverage

social science principles. First, they should routinely review existing peer-reviewed studies related to cybersecurity. This will grant a better understanding of human behavior relative to cybersecurity and external cultural influences. Second, they should apply these principles in security awareness program development within their organization. As mentioned above, these professionals are expected to measure awareness before implementing a program, implement the program, and measure awareness after implementation. While this is far from a scientific study, lacking a control group, it does share some features. Awareness metrics must be defined (akin to crafting a study and posing hypotheses), measurements must be taken and quantified before and after program application (just as data is gathered in a study before and after some treatment), and the efficacy of the program must be determined based on the pre- and post-program data (just as hypotheses would be accepted or rejected). The closer a security awareness and cultural professional adheres to social science principles, the better their security awareness programs will mitigate risk, and the more likely future iterations will improve on missteps of programs implemented before, just as studies build on those before them to increase the sum of knowledge in a field.

Relation to Cybersecurity as a Social Science

As noted in *Cybersecurity as a Social Science*, diversity in cybersecurity has benefits, including differences in mindset producing better decision making and diverse teams being more innovative and productive. Security awareness and cultural engineers would benefit from the added perspective if they themselves were from an underrepresented group. Even if this is not the case, they should always consider the varied backgrounds (external culture) of the members of the organization and leverage this for the organization's benefit.

Another topic discussed, human systems integration, is relevant to the development of any security awareness program and culture. Often security awareness programs will use learning management systems or gamification to educate on cybersecurity. It is imperative that these be tailored to native human inclinations. For example, if annual refresher training is not engaging to the students, it will not be effective.

Research showing that peer networks contribute to cyber behavior was covered as well. The relevance here for the security awareness and cultural professional is that peers can influence one another in both positive and negative ways. For instance, if a department in a company has shown disregard for cyber best practices, turning a portion of its members around through targeted training can encourage the remainder to come along. The inverse is also true. If a particular department is meeting expectations, a subset of members could cause the remainder of the group to backslide. Peer networks can create culture in even small groups, which could bleed into the larger organizational culture.

Finally, cybersecurity culture in organizations was examined directly. It is the security awareness and cultural engineer who would be tasked with creating a culture that empowers people, projects meaning, establishes partnerships, and provides training. As mentioned above, groups could be targeted, but so could individuals and, most importantly, leadership. Leadership must be involved in any cultural shift as this is where a lot of culture stems from. Leadership buy-in and involvement must be secured if effective change is to be made, and the security awareness and culture professional must find a way to secure it.

Marginalized Groups

Marginalized groups within an organization should be considered when developing any security awareness program. Wongkrachang (2023) noted how programs designed “by and for

people from dominant racial and gender groups" may fail the relatability test for minority populations within the organization (p. 38). If members of an organization cannot relate to training or an attempted culture shift, both will be less effective.

Trust is essential for any awareness program or culture change, and due to historical reasons minority populations may have a lower level of trust in institutions (Wongkrachang, 2023, p. 43). This can lead to a lack of engagement from minorities and puts them at a higher risk of cyberattacks and makes their inclusion in culture change more difficult (Wongkrachang, 2023, p. 44). Building foundational trust across all groups is an important element of the cybersecurity professional's job.

Immigrant communities, often underserved in society, may also lack adequate preparation for good cyber practices in an organization. Al-Shehri & Clarke (2009) illustrated just how divergent cybersecurity knowledge and hygiene is across different countries. Members of an organization from cultures where cybersecurity is undervalued, or cyber knowledge is lacking, may struggle to meet organizational standards. If language barriers are present, this represents an even greater challenge.

Conclusion and Connection to Society

The security awareness and cultural engineer should have two goals, each apparent in the title of the job. First, they are responsible for developing a cybersecurity awareness program. This is necessary but not sufficient for a strong cybersecurity posture. Stahl (2006) explained the need for the second half of the title well: "although an awareness training program can impart information security knowledge, it rarely has significant impact on people's feelings about their responsibility for securing information or their deeper security instincts" (p. 294). Culture must be targeted, "creating spaces in which information learning can take place" (Stahl, 2006, p. 294).

What does a well-built culture look like? Uchendu et al. (2021) conducted a study of studies, reviewing 58 research articles to reveal common guidance for the creation of a strong security culture. In order of times appearing in the research, the following were given as key factors regarded as important for building and maintaining a cyber security culture: management support, security policy, security awareness, security training, change management, compliance, knowledge, accountability and responsibility, security risk, commitment, communications, user management, motivation, trust, national culture, ethical conduct, and regulations (p. 9). These factors, aggregated from peer-reviewed sources, provide a roadmap for setting culture.

The latest social science studies can and should form the backbone of a security awareness and cultural engineer's success. This success will measurably reduce risk for the organization due to its effective security program and strong culture of cyber awareness. Yet the benefits also extend outside of the organization. The organization will be a better partner for other organizations, customers, clients, etc. as it will be less vulnerable to cyber incidents or breaches that can have external impacts. Further, every member of the organization can take an improved cyber culture to their private lives and to future organizations. Just as external culture affects organizational culture, organizational culture can feedback into external culture. Each member of the organization can become an advocate for solid cybersecurity practices, a net gain for the whole of society.

References

Al-Shehri, Y., & Clarke, N. L. (2009). Information security awareness and culture. *Advances in Networks, Computing and Communications, 6*, 12-22.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices* (2nd ed.). University of South Florida. https://digitalcommons.usf.edu/oa_textbooks/3

H Layer Credentialing. (n.d.). *About the exam*. https://www.thehlayer.com/about-exam

Stahl, S. (2006). Beyond information security awareness training: It is time to change the culture. In H. F. Tipton & M. Krause (Eds.), *Information security management handbook* (pp. 285-294). Auerbach Publications.

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*. https://doi.org/10.1016/j.cose.2021.102387

Udeh, C. (2022, May 17). *10 Non-technical cybersecurity roles*. Hacktales. https://hacktales.com.ng/2022/05/17/non-technical-cybersecurity-roles

Wongkrachang, S. (2023). Cybersecurity awareness and training programs for racial and sexual minority populations: An examination of effectiveness and best practices. *Contemporary Issues in Behavioral and Social Sciences, 7*(1), 35-53.