Demontae Watson

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Matthew Umphlet

April 7, 2024

Abstract

Professionals in the cybersecurity field face a complex and fast-evolving landscape of challenges. In addition to technical expertise, an understanding of the complexity of human behavior, organizational dynamics, and societal context is essential. This paper examines how cybersecurity professionals, more specifically, cybersecurity consultants use social science research and principles to improve their effectiveness in understanding marginalized groups and the interactions between society and cybersecurity. By drawing on social science insights, cybersecurity consultants can gain a deeper understanding of the social and psychological factors that influence cybersecurity practices, enabling them to better protect organizations from cyber-attacks and uphold human rights.

It is no secret that social science principles play a significant role in Cybersecurity. Cybersecurity is dependent on human actions as social norms, attitudes, and decision-making impact security practices and procedures. It also includes various aspects such as human behavior, decision-making processes, public policy, and much more that impacts cybersecurity. By exploring the social science principles into cybersecurity, professionals can gain a deeper understanding of the human elements involved in cyber threats and defenses, which in return, would decrease risks and protect sensitive information. Psychology is a big step towards understanding human behavior and how individuals interact with technology, their susceptibility to social engineering tactics, and their cognitive biases which can provide valuable insights for designing security measures that align with human cognition and behavior. A 2015 research found that, "social psychology offers a complementary view, with a rich body of work documenting how an individual's attitudes and behaviors are strongly affected by others" (Hong et al.) Social engineering attacks, for example, use psychological flaws in people to trick them into disclosing private information or taking actions that jeopardize security. Examples of these attacks include phishing and pretexting. By drawing on principles from psychology and even sociology, and behavioral economics, cybersecurity professionals can develop things like targeted awareness campaigns, user training programs, and use interface designs that account for how human factors which would stop or at least reduce the likelihood of social engineering attacks.

Now, let's get more specific and explain why Cybersecurity consultants is the career I'm choosing to explore how professionals require and depend on social science research and social science principles. Professionals with expertise in protecting digital assets and defending enterprises against cyberattacks are known as cybersecurity consultants. They are in charge of

evaluating the security protocols currently in place within an organization and spotting any potential weak points. In doing so, they require a diverse set of skills and qualifications to effectively fulfill their responsibilities including using social science research and social science principles. This is particularly important when talking about marginalized groups such as women, people of color, and other underrepresented individuals in the field. “Minorities remain significantly underrepresented, which means that women and people of color need more initiatives for inclusion in the equation” (Burrell & Nobles, 2018). Groups that are underrepresented may feel like they do not fit in the industry which can lead to self-doubt and reduce their career aspirations.

These underrepresented groups may experience cultural biases and systemic racism in the form of microaggressions or exclusion which negatively affects them and lowers the collaboration cybersecurity consultants require. This could be mitigated by addressing these microaggressions and promoting allyship to build rapport between these marginalized groups to gain trust and be as effective as possible. Paira et al. (2023),

> by weaving inclusivity into the fabric of our cybersecurity strategies, we are not only fortifying our defenses against cyber threats but also fostering a digital world that reflects the diversity, respect, and equality we aspire to uphold.

This highlights the importance that the rapport built between marginalized groups and the cybersecurity field brings other positives like common human rights and not just “making the job easier”.

In summary, the role of social science concepts and principles are important to cybersecurity, and more specifically for cybersecurity consultants especially when it comes to

comprehending how people or groups behave and make decisions that affect security procedures. These principles also focus on the challenges faced by underrepresented groups in the field which diminishes hope and reason for these groups to pursue a career in cybersecurity. In addition to strengthening defenses against cyberattacks, inclusivity and diversity represents the values of equality and respect that are crucial in both real-world and digital contexts.

Works Cited

Burrell, D. N., & Nobles, C. (2018). Recommendations to develop and hire more highly qualified women and minorities cybersecurity professionals. In *International Conference on Cyber Warfare and Security* (pp. 75-81). Academic Conferences International Limited.

Hong, J., Das, S., Kim, T. H. J., & Dabbish, L. (2015). Social cybersecurity: Applying social psychology to cybersecurity. *Human Computer Interaction Institute, Carnegie Mellon University*.

PAIRA, D. ENSURING INCLUSIVITY IN CYBERSECURITY: A HUMAN RIGHTS-BASED APPROACH. *CYBER CRIME &*, 95.