Career Paper:

The Social Science Behind Ethical Hacking

Katherine Chang

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

December 3rd, 2023

Introduction

Ethical hacking, also known as penetration testers or white-hat hackers, is career that requires the use of many social science principles in their job to better understand the human behavior behind a cybercriminal, the motivations behind cyber-attacks, and the vulnerabilities of a system that can be exploited. Social science plays a very important role in the ethical hacking by assisting professionals with assessments and mitigating security risks associated with the human factors that take place within a cybercrime, or potential cybercrime.

A major concept from social science that ethical hackers use is human factors analysis. The Human Factors community is the ideal group of experts to assess the role human cognition, technology, and organizational restraints play within a cyber environment (Knott et al., 2013). When addressing an attack or cybercrime, the initial response is to understand what human characteristics does the cyber criminal carry that may contribute to the crime they committed which also helps to understand the motivation as well.

By using human factors analysis, experts gather information using social psychology, analysis of cognitive bias, decision-making skills, and behavioral patterns to understand how individuals would respond to potential security threats and attacks. One research method that I believe ethical hackers use when determining how human behavior can contribute to certain cyber activities would be inductive research. Inductive research involves utilizing general principles, in this case, psychological, from specific observations against cyber-attacks, and using this information to analyze real-world situations of security breaches and vulnerabilities (Kumar & Carley, 2016).

Ethical hacking closely relates to the marginalized group of neurodivergent individuals. Neurodivergent people often face challenges of when thinking, communicating, and analyzing certain interactions, people, processes in their everyday life, and their conditions can vary from Autism-Spectrum Disorder (ASD), Attention-Deficit/Hyperactivity Disorder (ADD/ADHD), Dyslexia, or Dyspraxia (Weber et al., 2022). In coincidence, ethical hackers have to understand the same type of conditions of neurodivergent individuals as these are the same psychological facts they consider when analyzing cybercrimes. Ethical hacking shares the similar process of diversity when thinking as neurodivergent individuals. Some challenges they may face include having difficulties in traditional communication, social interactions, and navigating change. Neurodivergent individuals may have communication styles that differ from neurotypical norms. This can sometimes lead to challenges in team collaboration, as effective communication is crucial in ethical hacking projects. In terms of social interaction, Neurodivergent individuals may find certain social situations challenging, impacting their ability to build professional relationships and communicate findings effectively. The fast-paced and dynamic nature of the cybersecurity field may pose challenges for neurodivergent individuals who thrive in more predictable and stable environments. Adapting to constant change can be stressful which can also be applied to the ethical hacking as new information about a potential attack can change instantly.

Ethical hacking relates to society in way of analyzing behavior and creating predictions, but the difference is that it is digital base. Everyday, as humans, we assess people by the actions, facial expressions, speech, choice of an outfit, career, and many other factors. After gathering that information, we use that to understand and classify someone else on the type of person they are by using our personal judgement and experience to guess the type of person someone is and how they’ll be in specific situations. With almost every activity being digital in today’s modern world, ethical hacking can be justified as the digital version of human judgement.

**References**

Knott, B. A., Mancuso, V. F., Bennett, K., Finomore, V., McNeese, M., McKneely, J. A., & Beecher, M. (2013). Human factors in cyber warfare. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *57*(1), 399–403. <https://doi.org/10.1177/1541931213571086>

Kumar, S., &amp; Carley, K. M. (2016). Approaches to understanding the motivations behind cyber attacks. 2016 IEEE Conference on Intelligence and Security Informatics (ISI). <https://doi.org/10.1109/isi.2016.7745496>

Weber, C., Krieger, B., Häne, E., Yarker, J., &amp; McDowall, A. (2022). Physical workplace adjustments to support Neurodivergent Workers: A systematic review. Applied Psychology. <https://doi.org/10.1111/apps.12431>

`