

The Role of Social Science in Cybersecurity: A Study of Social Engineering Analysts

Student Name: Tenny Boone

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/18/2026

Introduction

Overtime cybersecurity has become an important career profession in the current world as organizations and individuals continue to rely on technology for communication, commerce, and data storage. A social engineering analyst is a specialized cybersecurity professional that focuses on understanding how attackers manipulate human behaviors to gain unauthorized access to people's systems and sensitive information. This career path relies heavily on analyzing the human decision-making process, trust, and social interactions. Cybersecurity plays a key role in the modern world because cyberattacks can mess heavily with financial systems, healthcare infrastructures, and personal privacy. The purpose of this paper is to examine how social science principles are integrated into the role of a social engineering analyst, how key concepts from social science apply to this career, how marginalized groups are affected, and how this profession contributes to society.

Social Science Principles

Social engineering analysts use social science research to understand human behavior when it comes to cybersecurity contexts. Cybercrime is not only a technological issue because it is deeply rooted in human psychology and social interactions. Research shows that individuals are often the weakest link in cybersecurity because they can be easily tricked or manipulated (Back & LaPrade, 2019). Human behavior, trust, and decision-making are important factors when considering what these analysts chose to study. Social science principles such as empiricism, determinism, and objectivity are essential in this field. For example, empirical research is used to study how individuals are responding to phishing attacks and what factors influence how they respond. The Health Belief Model, a social science theory, is used to understand why individuals implement or ignore security measures. This model looks at factors

such as perceived risk, self-efficacy, and perceived benefits of protective actions (Du et al., 2024). Social engineering analysts also apply concepts from human and computer interactions and user behavior analysis to help with design training programs and awareness campaigns to prevent unauthorized access. An example widely used by companies is organizations using simulated phishing emails to study employee responses and improve security awareness based on whether the employees click the links. These implemented practices show how cybersecurity professionals integrate social science insights into beneficial strategies.

Application of Key Concepts

Two important social science concepts that are directly applied in the role of social engineering analysts are behavioral analysis and social influencing norms. Behavioral analysis involves studying how individuals react to the threats and make their decisions. Research indicates that factors like perceived vulnerability and previous experience have a huge influence on whether or not individuals adopt secure behaviors (Du et al., 2024). Social influence and norms means are related to this career because cybercriminals often exploit authority, urgency, and trust to aid in the manipulation of individuals. Understanding these concepts allows for professionals to design a better security protocol for everyone to follow along with better training programs. For example, cybersecurity awareness programs help educate users on recognizing whether or not an email is suspicious and teaches them to avoid scams. Social engineering analysts also use these concepts to assess risks and add security measures. Tools such as phishing simulations, user behavior analytics, and security awareness training show how these concepts are applied in the field. Additionally, these professionals are ensuring compliance with legal and ethical standards by developing these policies that promote responsible technology use and data protection for everyone.

Marginalization

Cybersecurity issues do affect marginalized groups heavily, especially individuals with limited access to technology, lower levels of digital literacy, or less access to cybersecurity education or practices. Research shows that differences in gender and fluency when it comes to technology can alter attitudes toward cybercrime prevention and security behaviors (Ige, 2018). This highlights how social and demographic factors impact people's vulnerability to cyber threats. Vulnerable populations such as children and students are often main targets due to their increased online activity and the way they lack the needed awareness. Social engineering analysts must consider these factors when designing strategies for the best security. Efforts to address these challenges include developing more inclusive training programs, promoting cybersecurity education in schools to make them more accessible for everybody, and increasing diversity within the cybersecurity workforce.

Career Connection to Society

Social engineering analysts help maintain the safety and stability of infrastructures in society. By preventing cyberattacks, they help protect financial systems, healthcare organizations, educational institutions, and government operations. Cybersecurity professionals also contribute to public policies by advising on implemented regulations related to data protection or privacy. The addition of more human focused strategies highlights the importance of combining technology and social science. As cyber threats continue to evolve with time, understanding human behavior remains essential for protecting society. This profession ensures that individuals and organizations can safely use any digital spaces as they wish while still supporting economic stability and public trust.

Scholarly Journal Articles

Du et al. (2024) examines how the Health Belief Model explains individuals' email security behaviors. The study finds that factors such as self-efficacy, perceived vulnerability, and prior experience significantly influence how people respond to phishing attacks. This source is relevant because it shows how social science theories are applied in cybersecurity research. Ige (2018) explores how gender and technological fluency affects attitudes when it comes to cybercrime prevention methods. The study highlights how social and demographic differences influence cybersecurity awareness and behaviors. This supports the discussion of marginalized groups and the importance of more inclusive cybersecurity strategies. Back and LaPrade (2019) emphasize the importance of human factors in cybercrime prevention. The article argues that technology alone is not sufficient enough and that understanding human behavior is needed for effective cybersecurity strategies. This source contributes to understanding how cybersecurity professionals incorporate social sciences into their work.

Conclusion

In conclusion, the role of a social engineering analyst demonstrates the strong connection between cybersecurity and the social sciences. By studying human behavior, decision-making, and social interactions, the professionals in this field develop strategies to prevent any possible cyber threats. Empiricism, behavioral analysis, and theoretical models like the Health Belief Model are essential in understanding and improving cybersecurity practices. Addressing the needs of overlooked groups and promoting more equal access to cybersecurity education are important components of this profession. Overall, social engineering analysts play a vital role in protecting society and ensuring the safe use of technology in a digital world that's growing by the day.

References

- Back, S., & LaPrade, J. (2019). The Future of Cybercrime Prevention Strategies: Human Factors and a holistic approach to Cyber Intelligence. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(2), 1–4.
<https://doi.org/10.52306/2578-3289.1034>
- Du, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: Determinants of Preventative Security behaviors. *Journal of Cybersecurity*, 10(1).
<https://doi.org/10.1093/cybsec/tyae012>
- Ige, O. A. (2024, August 2). *Effects of gender and technological fluency on learners' attitude to cyber crime prevention in urban learning ecologies: Lessons for swedish gymnasiums*. Zenodo. <https://zenodo.org/records/1467888>