Cybersecurity Professional Career Paper: Cybersecurity System Engineer

Student Name: Adrian Valencia

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: 13 November 2025

Introduction

This paper will discuss the career of a cybersecurity system engineer which is work that revolves around protection of digital infrastructures through designing, implementing, and maintaining systems within companies or organizations. Workers in system engineering tend to have and manage technical skills but should have a strong sense in social dynamics in order to understand human behavior and ethics behind the function of their job. Furthermore, sense of the social science principles like the understanding behind hacking, group behavior, and cultural diversity are important role in a career of system engineering. Essentially, their goal is to use their creative skills to help develop a strong security through understanding social cues in marginalized populations.

Social Science Principles

More specifically, cybersecurity system engineers are the designers of system architecture that control the defense within technology system in devices. They help ensure that organizations are compliant with the policies that they provide. Their range can revolve from working with networks, systems, access control, and vulnerabilities within a company. Throughout this process, they must have a strong understanding about the concepts of social science. By analyzing the behavior and social aspects of attackers or common global issues, system engineers can user their skills to predict possible future issues and must communicate the possibilities effectively within the staff. From the National Institute of Standards and Technology (NIST, 2024), 80% of breaches involve human error meaning that more insight should be overlooked with regards for social and behavioral aspects.

Application of Social Science

Behind it all, human behavior and motivation are both used when a engineer is designing a secure system. This is imperative to the job as it evaluates and anticipates flaws within humans that is often missed or neglected. An example of this can be systems that contain a two-factor authentication system or training from attack like vishing, phishing, and others that use psychological support help create user error.

Additionally, with most jobs come the ethical reasoning and decision making skills required for the job. It is important that the system engineers design systems to have a balance of privacy while maintaining a strong required system security (ISC). All workers must adhere to a code of conduct that follow a rule of ethical standard requirement not pry into an harm the users of the system. It is imperative that cybersecurity system engineers designs system to protect data without exploiting ethical standards.

Marginalized Groups

By protecting systems al around, cybersecurity naturally protect marginalized groups like low-income areas and other groups like racial minorities. They do so by making systems easy to use for all people, ensuring that it is inclusive to everyone by providing easy access and interfaces to the systems. Giroud (2025), show the importance of an equitable framework by gaining the trust of others and reducing isolation of certain groups.

Conclusion

In essence, a cybersecurity system engineer requires technical expertise with a strong understanding of social science principles that connect the two together. Through understanding changing behavior, ethics, and communication skills, a system engineer must create systems that

adapt to the constant changing style. They must adapt to human needs and marginalized groups while working with others in both technical and social settings. As technology grows, the creativeness and skills of the engineer must adhere to the world today.

References

Cybersecurity framework. NIST. (2025, October 1). https://www.nist.gov/cyberframework

Giroud, K. (2025, April 14). *European cybersecurity journal, "toward inclusive and equitable cybersecurity governance."* Common Good Cyber. https://commongoodcyber.org/library/european-cybersecurity-journal-toward-inclusive-and-equitable-cybersecurity-governance/

ISC2 code of Ethics. Cybersecurity Certifications and Continuing Education. (n.d.). https://www.isc2.org/ethics