Cybersecurity Professional Career Paper: Cybersecurity Analyst

Student Name: Caleb Baines

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 4/15/26

Introduction

Cybersecurity analysts are information technology professionals responsible for protecting computer systems, networks, and sensitive data from cyber threats such as hacking, phishing, and malware attacks. As the modern day drives more demand and dependency on digital technology, the need for cybersecurity also grows along with it. The professional career chosen for this paper: Cybersecurity Analyst will be gone over and how social sciences, key concepts learned in class, and societal contexts are applied to this field.

Social science principles

Social science plays a critical role in cybersecurity because many threats exploit human behavior rather than purely technical weaknesses. Analysts must identify and understand why many people fall for many cybercrimes, scams, and social engineering. In the context of social sciences, concepts like social engineering rely on techniques like authority or urgency to trick people into revealing sensitive information. Another example of social science that isn't as dangerous, but rather helpful are Human-computer interactions (HCIs). HCI can help analysts create security systems that are user-friendly and help make people more likely to follow protocols; If a system is too complex, could create vulnerabilities.

Application of Key Concepts

Several key concepts are applied directly to cybersecurity careers. Risk assessment, in this case, involves the analysis of both technical threats and human factors. Cybersecurity analysts evaluate how likely users are to engage in risky behaviors and design controls around these behaviors to minimize those risks. They also use behavior analytics to detect unusual patterns in user activity and identify potential insider threats.

Marginalization

Discrimination can often be prevalent in workspaces that often affect a lot of marginalized groups in the cybersecurity space, through policies and systems like increased surveillance or data misuse aimed directly toward marginalized individuals. Professional cybersecurity analysts must be aware of these discrepancies and work to create diverse and inclusive security measures that ensure that marginalized communities aren't facing discrimination from these policies.

Career Connection to Society

Public policies related to cybersecurity, such as data protection regulations and national security strategies, shape how professionals perform their roles. Cybersecurity analysts must keep up to date about these policies and ensure that their organizations comply with legal requirements. This kind of work ethic not only protects individual organizations but also helps contribute to national and global security.

Conclusion

Cybersecurity analysts rely heavily on social science principles to effectively protect systems and data. Understanding human behavior, social sciences, different populations, and work ethic being essential for addressing modern cyber threats. Furthermore, as cyber threats continue to evolve, the integration of social science research and keeping up with the modern day are impactful in shaping a secure digital future.

Scholarly Journal Articles

Source 1: Verizon. (2023). Data Breach Investigations Report. This report provides up-to-date insights into cyberattack trends, including the role of human error and social engineering in breaches. It is relevant because it demonstrates how understanding human behavior is critical in developing effective cybersecurity strategies.

Source 2: Bada, M., Sasse, A. M., & Nurse, J. R. C. (2020). “Cyber Security Awareness Campaigns: Why do they fail to change behavior?” This updated research emphasizes the importance of behavior-focused cybersecurity training and highlights the limitations of traditional awareness programs. It supports the discussion of social science principles and user behavior in cybersecurity.

Source 3: West, S. M., Whittaker, M., & Crawford, K. (2021). “Discriminating Systems: Gender, Race, and Power in AI.” This article examines how technological systems can reinforce inequalities and disproportionately affect marginalized groups. It contributes to understanding the societal implications of cybersecurity and the importance of equitable digital protection.