Name: Justin Cotman

School of cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor name:

Date: 4/17/26

BLUF

To prevent cyber dangers, you rely on insights into human behavior. A cybersecurity analyst investigates human behavior and identifies threats in day-to-day activities. In 2023, cybercrime resulted in damages of more than $8 trillion worldwide. The majority of breaches are the result of poor judgment or human mistake. How you avoid these mistakes is determined by social science.

Introduction

An organization's networks, systems, and data are safeguarded by a cybersecurity analyst. You keep an eye on things and react to dangers as they arise. Because consumers disregard warnings or believe phony alerts, many attacks are successful. To lower risk, you concentrate on both behavior and technology. This essay describes how you use social science, important ideas, and social consciousness in your job.

Social Science Principles

To learn how attacks are successful, you examine behavior. Phishing emails deceive people by using authority and urgency. According to reports, human activity is involved in more than 80% of breaches. Employees are taught to take their time and confirm requests before acting. Additionally, you create mechanisms that minimize confusion and avoid errors.

Application of Key Concepts

Risk assessment is used to measure impact and identify hazards. You research social engineering techniques and teach people how to spot fraud. Spending on security tools is guided by cost-benefit analysis. Prevention saves money because the average cost of a data breach is 4.45 million dollars. To protect data, you also uphold legal requirements and enforce policies.

Marginalization

You safeguard users who are more vulnerable in online environments. Certain communities do not have access to cybersecurity tools and knowledge. Scammers target low-income users and senior folks. Communities that experience increased surveillance are likewise impacted by privacy risks. To close these gaps, you establish fair security procedures and basic training.

Career Connection to Society

You safeguard everyday life-supporting institutions like banking and healthcare. A single cyberattack damages people and interferes with services. Attacks using ransomware have caused hospitals to close and services to be delayed. You abide by regulations that govern organizational behavior and safeguard data. Your efforts increase people's confidence in the digital systems they utilize on a daily basis.

Conclusion

Social science is essential for understanding behavior and lowering risk. You include important ideas like risk assessment and social engineering into your everyday work. You provide protection and training to help vulnerable populations overcome their obstacles. You uphold the structures that society relies on for security and stability. Human behavior and safe technologies are connected by your work.

References

Anderson, R., & Moore, T. (2006). The economics of information security. Science, 314(5799), 610 to 613. https://doi.org/10.1126/science.1130992

Hadnagy, C. (2018). Social engineering: The science of human hacking. John Wiley & Sons.

Herley, C. (2009). So long, and no thanks for the externalities. Proceedings of the 2009 Workshop on New Security Paradigms, 133 to 144. https://dl.acm.org/doi/10.1145/1719030.1719050