Cybersecurity Professional Career Paper: Social Sciences in Cybersecurity Instruction

Student Name: Macon Tankard

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/16/2025

Introduction

The field of cybersecurity contains a vast number of careers that involve developing and maintaining systems, incident response and remediation, employee awareness training, and researching new and emerging cybersecurity threats. Cybersecurity Instruction plays a crucial role in preparing both cybersecurity and non-cybersecurity personnel to address significant cyber threats. This position heavily involves working with other cybersecurity experts, employees, and executives to ensure their system usage is secure and in line with organizational guidelines. Human error has become the leading cause of cybersecurity breaches, making this role a necessity (NICE Framework, 2025).

Cybersecurity Instruction is by no means an entry-level job. Professionals pursuing this career require strong fundamentals in cybersecurity, communication skills, and experience in the field of cybersecurity. Although a background in social sciences is not required for this role, it is strongly encouraged. Having this background allows instructors to apply psychological concepts to their teaching, resulting in a better understanding of the employees they teach and providing them with the knowledge they need to adapt their training programs to their employees' needs (NICE Framework, 2025).

Marginalization

Group training programs are effective in educating many employees simultaneously; however, those less proficient with technology may struggle and feel excluded. Instructors must pay close attention to employees who may be struggling to understand the program's content and assist whenever needed. An additional challenge is maintaining the engagement of employees who may see this training as boring or complex. By providing clear and reasonable explanations and conducting life-like simulations, employees become more likely to stay engaged and

complete their training. An inclusive design of a cybersecurity awareness program will allow marginalized groups, who may be less proficient with technology, to remain engaged and confident throughout their training (Ghosh, A., Sudip Diyasi, & Dey, D., 2023).

Social Science Concepts and Application

Utilizing psychological concepts in employee training can be crucial in the early detection and prevention of security breaches. Specifically, cognitive theory can be applied in training to identify how employees may respond to cyber threats. To apply this theory in practice, virtual environments can be utilized to empirically measure how different individuals respond to cyber threats. Additionally, individuals with traits linked with higher susceptibility to cybercrime, such as impulsiveness, low self-control, agreeableness, neuroticism, and openness, can be recorded. Using this data, instructors can identify employees who are at risk of becoming victims of cybercrime and prepare them accordingly. Lastly, detailed training programs should be created while maintaining parsimony, ensuring employees, who may be less familiar with technology, understand the content (Pappas, S., 2019).

Societal Benefits

Cybersecurity training programs not only protect the organization from cyber threats, but can also protect individuals associated with the organization. Healthcare and banking organizations, for example, are prime targets for cybercriminals, as they protect databases containing sensitive customer data. Attackers may attempt to breach the database using simple methods such as phishing, impersonation, and social engineering, putting millions of customers at risk of data theft. Cybersecurity awareness programs will prepare employees to deal with these attempts by teaching them how to identify and respond to attacks (University, C., 2023).

Conclusion

By applying social science principles to a cybersecurity environment, the security of a system can be enhanced, allowing employees to use organization devices safely. By applying social science principles to training programs for employees, cybersecurity instructors can gain a thorough understanding of the habits and weaknesses of employees they teach, allowing training programs to be tailored to their specific needs. In conclusion, by applying social science principles when educating employees, human factors-related breaches can be reduced, and an organization's digital landscape becomes secure.

References

Cybersecurity Instruction [NICE Framework Work Role]. (2025). National Initiative for Cybersecurity Careers and Studies. https://niccs.cisa.gov/tools/nice-framework/work-role/cybersecurity-instruction

Ghosh, A., Sudip Diyasi, & Dey, D. (2023). Cybersecurity Literacy Programs for Marginalized Communities: Bridging the Gap in Digital Security. *Zenodo*. https://doi.org/10.5281/zenodo.14740269

Pappas, S. (2019, February). The Psychology of Cyberthreats. *Https://Www.apa.org*. https://www.apa.org/monitor/2019/02/cyberthreats

University, C. (2023). *The Growing Importance of a Career in Cyber Security | CCU Online*. Ccu.edu. https://www.ccu.edu/blogs/cags/category/business/the-growing-importance-of-a-career-in-cyber-security/