Cybersecurity Career Professional Paper

Dante Collier

Old Dominion University

CYSE201S

Diwakar Yalpi

April 7, 2024

As an undergraduate student at Old Dominion University exploring the intersection of social science and cybersecurity, it is intriguing to observe the use of social scientific principles by cybersecurity awareness and training specialists in their professional endeavors. These specialists possess expertise not just in technology, but also in psychology, sociology, and education. They recognize that human elements are frequently the most vulnerable aspect of cybersecurity. Within the dynamic realm of cybersecurity, experts with expertise in awareness and training assume a pivotal position in imparting knowledge to persons and entities regarding optimal cybersecurity methodologies. This career professional paper examines the integration of social science and cybersecurity from the perspective of a Cybersecurity Awareness and Training Specialist. It highlights the influence of social

science concepts on everyday activities and relationships, with a specific focus on marginalized communities and society as a whole.

Regarding human behavior and cognitive biases, these experts are at the forefront, utilizing psychological knowledge to create training programs that target prevalent human mistakes. For instance, they may concentrate on the "optimism bias," which refers to the tendency of individuals to perceive themselves as less susceptible to cyber attacks compared to others. By emphasizing this tendency during training sessions, experts can foster a more accurate evaluation of individual risk and encourage more attentive actions.

Social engineering is a domain in which the use of social science ideas is of paramount importance. Cybersecurity training frequently incorporates modules that focus on identifying and countering manipulative techniques employed by hackers to steal confidential data. Gaining insight into the psychological foundations of trust and anxiety enables employees to identify instances of manipulation, hence reducing their susceptibility to such approaches.

Inclusivity is also key in cybersecurity training. Specialists use their knowledge of cultural dynamics to create programs that speak to everyone, regardless of their background. This means considering different languages, cultural norms, and even socioeconomic factors to ensure that cybersecurity is accessible to all, including those who might otherwise be marginalized.

Science principles are also applied, with experts utilizing educational psychology to create training that is captivating and unforgettable. To enhance conceptual retention, educators may employ techniques such as spaced repetition, narrative, or interactive simulations. The objective is not solely to impart knowledge to learners, but rather to facilitate their ability to effectively apply acquired knowledge in practical contexts.

Behavioral science provides several strategies, such as gamification and nudging, to effectively maintain employee engagement in cybersecurity policies. Gamification transforms the process of learning into a game, incorporating elements such as points, badges, and leaderboards to enhance enjoyment and foster competition. In contrast, nudging is the utilization of subtle cues to steer employees towards adopting secure habits, while ensuring that they do not experience any sense of coercion.

In conclusion, cybersecurity awareness and training professionals serve as the intermediary connecting the technical domain of cybersecurity with the intricate sphere of human behavior. Through the use of social scientific principles, the designers develop training programs that possess the qualities of being informative, engaging, inclusive, and efficacious in facilitating behavioral change. With the ongoing evolution of cyber dangers, the significance of these professionals will inevitably increase, establishing their interdisciplinary approach as a model for addressing intricate difficulties in the digital era.

References:

SANS Institute. "The SANS Security Awareness Professional (SSAP)." SANS Institute. Accessed June 26, 2023. https://www.sans.org/security-awareness-training/career-development/credential/ .

CyberSecOp. "Cyber Security Awareness & Training - CyberSecOp.com." CyberSecOp. Accessed June 26, 2023. https://cybersecop.com/cybersecurity-awareness-training-services .

National Center for Biotechnology Information (NCBI). (n.d.). Cybersecurity Awareness and Training (CAT) Framework for .... Retrieved from https://www.ncbi.nlm.nih.gov/

National Initiative for Cybersecurity Careers and Studies (NICCS). (n.d.). Certified Cybersecurity Awareness Professional (CCAP) Certification .... Retrieved from https://niccs.cisa.gov/

Information Systems Audit and Control Association (ISACA). (n.d.). Better Cybersecurity Awareness Through Research - ISACA. Retrieved from https://www.isaca.org/

Reddit. (n.d.). Is anyone actually a Security Awareness And Training Specialist? Retrieved from https://www.reddit.com/