Social Science Principles in the Career of a Cybersecurity Specialist

Iedoubina Marc

Old Dominion University

CYSE – 201S

Professor Teresa Duvall

04/13/2024

Social Science Principles in the Career of a Cybersecurity Specialist

In cyber security, experts protect digital property by keeping it safe from different hazards, including computer attacks, misinformation, and leaking of information. The abilities of their roles range from risk assessment and incident response to security measure implementation. Nevertheless, the proficiency of cybersecurity experts would depend not only on technical ability but also on a good grasp of social science theory. Cybersecurity experts effectively use social science principles to reduce cyber threats, safeguard society, and uplift the needy population.

Social Cybersecurity Principles

One main concept in cybersecurity, particularly for social media, is to detect and deal with social engineering operations (Duvall, n.d.). The social engineering technique includes inducing people to disclose their secret information or perform specific tasks by applying psychological manipulation. Therefore, cybersecurity practitioners should study how people usually behave psychologically to expose phishing (Social engineering) and fight it (Carley, 2020). For example, by scrutinizing social media communication objectives and human behavior, specialists can prepare to counter cyberspace threats, continuing to keep entities and people safe.

Additionally, social cyber-forensics, as well as motive identification, would be helpful for cybersecurity specialists in undertaking thorough research of the case (Carly, 2020). The experts can adopt computational social science techniques to get to the root of cyber-attacks, determine the attackers' aims, and foresee the spread of influence campaigns. This information is critical for developing robust defense methods and the optimal measures to manage the outcome of cyber threats (Alassad et al., 2021). In addition, information campaign effectiveness and diffusion patterns analysis help specialists evaluate the social impact of cybersecurity measures and low socioeconomic population groups.

Consequences of Fake News and Disinformation

When dealing with cyber threats, cybersecurity specialists must not only tackle the spread of fake news and disinformation (Duvall, n.d.). Such inaccurate information posted on social networks can do real damage, from molding political beliefs to dividing communities. What should be of utmost concern is that some groups can be campaign targets with false stories and harmful misinformation. Hence, social science research should be used to devise techniques for curbing fake news and teaching people alertness, critical thinking, and media literacy.

Social Engineering and Marginalized Groups

Social engineering methods like phishing and pretexting have raised security challenges for marginalized groups that are already fighting social and economic miseries (Duvall, n.d.). Cyber attackers frequently take advantage of vulnerabilities that result from poor awareness or ignorance of technologies. Such groups, in turn, are easily exposed to malicious actions (Khando et al., 2021). As one of the significant challenges, cyber security experts must work with social scientists to create cyber security education programs that adopt inclusion and are designed for the needs of the marginalized. Such specialists are to ensure digital resilience and equip individuals with the appropriate knowledge and skills for counteracting undesirable social engineering tactics.

Conclusion

Cyber security specialists do not only involve the technical field but also cover a wide range of social science perspectives. Through social cybersecurity insights, professionals can work in a preventive manner to avoid cyber threats, secure marginalized groups, and protect peoples’ values. Collaboration between cybersecurity practitioners and social scientists is requisite to develop robust strategies that merge the multiple dimensions of technology usage, human behavior, and socio-cultural dynamics.

References

Alassad, M., Spann, B., Samer Al-khateeb, & Agarwal, N. (2021). Using Computational Social Science Techniques to Identify Coordinated Cyber Threats to Smart City Networks. Sustainable Civil Infrastructures (Online), 316–326. https://doi.org/10.1007/978-3-030-64217-4_35

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

Duvall, T. (n.d.). CYSE 201S (Module 10) Social Cybersecurity.

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employee's information security awareness in private and public organisations: a systematic literature review. *Computers & Security*, *106*(1), 102267. ScienceDirect. https://doi.org/10.1016/j.cose.2021.102267