Jahmire Whitehurst 04/15/2025

Social Principles Relation to an Information Security Awareness Specialist

Introduction and BLUF

The chosen career to be reviewed will be an information security awareness specialist. The chosen career deals with creating learning and awareness programs centered around cybersecurity in an organization. The review will be on social principles, key concepts of the job and how they relate to class, and marginalized groups and society.

Body

There are seven social principles that are followed in the information security awareness specialist career. The first is relativism, the principle that all things are related, meaning that preceding events lead to current events. As an information security awareness specialist (ISAS), awareness programs identify risks to an organization and what can be done to minimize those risks or completely reduce them (Spitzner, 2014). Therefore, if excellent awareness programs are created ,then the chance of risks in the future will be lower and the entire company will benefit. Not only this ,but social awareness has changed from the innovation of technology perpetuating the cycle of new programs. The second principle is parsimony, the principle that all things should be simple and understandable to every person void of their background. As an ISAS, awareness programs are required to be understood by everyone and still convey security policies. The third principle is objectivity, the principle that science exists to advance knowledge. As an ISAS question like what can humans do to prevent their information from being stolen?. These questions are asked to advance knowledge in the subject and present an important research question. The fourth principle is empiricism, the principle that scientists study behavior that is

real and can be experimented on. As an ISAS we should only enact programs that have been proven by experimentation and real evidence. The fifth principle is ethical neutrality, the principle that scientists should only study things using ethical methods. As an ISAS this would mean I should not torture a cybercriminal to understand how to prevent what they do. I should conduct ethical surveys, experiments ,and studies to find evidence. This can mean taking a less than ideal path, but ethical standards have to be held up. The sixth principle is determinism, the principle that current events are determined by preceding events. As an ISAS this raises the question of what can be an interactive way to get employees to review security policies. Meaning that if security policies are interesting then employees will be more likely to read and follow them. The last principle is skepticism, the principle that any claims that are made should be questioned and examined (Yalpi, 2025). As an ISAS this means that if I would like to use a program it must be proven and tested before being implemented.

As an ISAS the career is heavily focused on human behavior, human factors,and social behavior. When a program is created if human factors are not factored into it it could cause a decrease in users that read the program and happiness in an organization. Human behavior is also important because of the cognitive theory that people behave based on their emotions and beliefs (Yalpi,2025). As an ISAS if this is not understood then you will almost certainly fail(Planet 9,2022).

As an ISAS multiple different marginalized groups must be taken into consideration (RIberio,2024). For example, disabled people, LGBQT+ individuals ,and african americans. When it comes to disabled people programs must be accessible by all people no matter their

situation. When it comes to LGBQT+ individuals their pronouns and genders must be taken into consideration. This means using they/them when describing individuals in programs. When referring to considering african americans their beliefs and thoughts must be taken into consideration. For example an African American may not have access to the same technology as another man and the programs should consider that.

As an ISAS there are many dynamic interactions between society and the career that must be taken into consideration. For instance, cyber threats are constantly evolving and becoming stronger than before. Therefore, a society must update their tech and train their employees to prevent these ever increasing threats (Planet 9, 2022). This can also be said for social engineering attacks and phishing attacks that hackers are updating to get more phishing attacks. Finally, ISAS's need to keep in consideration the tendencies of society. For instance, with the eruption of social media and the access to phones people lost interest in things very quickly. Therefore, programs must be made as interactive and interesting as possible to peak interest (Arctic Wolf, 2021)..

Conclusion

Overall, An ISAS is heavily related to social principles and social science research.If an ISAS were not focused on social principles they would not excel in their job position. They should also be focused on marginalized groups and how to accommodate them in any way possible. Finally, there are not many parts of this job that were not described in class.

References

Jobs NYC. (2024, January 27). *Security Awareness Specialist*. New York City. https://cityjobs.nyc.gov/job/security-awareness-specialist-in-manhattan-jid-19917#:~:text

=A%20Security%20Awareness%20Specialist%20develops,how%20to%20defend%20against%20them.

Spitzner, L. (2025, March 13). Job Description for Security Awareness Officer. *Sans*. Retrieved April 15, 2025, from. https://www.sans.org/blog/job-description-for-security-awareness-officer/

Wolf, A. (2021, February 14). 6 Biggest Security-Awareness Program Challenges—And What To Do About Them - RH-ISAC. *RH-ISAC*. Retrieved April 17, 2025, from https://rhisac.org/risk-management/6-biggest-security-awareness-program-challenges-and-what-to-do-about-them/#:~:text=Challenge%20%231:%20Security%20Awareness%20Content,no%20way%20of%20keeping%20up.

Yalpi, D. (2025). *Modules 1-10* [Slide show; Canvas]. ODU, United States of America. Canvas.odu.edu. Retrieved April 17, 2025, from https://rhisac.org/risk-management/6-biggest-security-awareness-program-challenges-and-what-to-do-about-them/#:~:text=Challenge%20%231:%20Security%20Awareness%20Content,no%20way%20of%20keeping%20up.

Planet 9, Inc. (2022, May 4). *Security awareness Training. Important Things to Know - Planet 9 Inc.* Planet 9 Inc. https://planet9security.com/security-awareness-training-important-things-to-know/#:~:text=Fundamental%20Topics%20for%20Security%20Awareness%20Training&text=These%20include%20password%20security%2C%20anti,able%20to%20create%20strong%20passwords.

Riberio, R. F. S. L. C. S. (2024, October 6). *Fostering cybersecurity awareness for effective risk management and creating cyber-resilient environments*. Industrial Cyber. Retrieved April

17, 2025, from https://industrialcyber.co/features/fostering-cybersecurity-awareness-for-effective-risk-management-and-creating-cyber-resilient-environments/#:~:text=Effective%20inclusive%20security%20practices%20are,environments%20in%20today's%20digital%20landscape.