The Role of Social Science in the Career of a Security Awareness Training Specialist

Hussein Al Saffar

CYSE201S

Matthew Umphlet

Old Dominion University

July 26, 2025

The Role of Social Science in the Career of a Security Awareness Training Specialist

The Role of Social Science in the Career of a Security Awareness Training Specialist

In the field of cybersecurity, not all threats are purely technical. Human error, manipulation, and misunderstandings are among the leading causes of security breaches. This reality has led to the growth of a vital cybersecurity career: the **Security Awareness Training Specialist**. These professionals are responsible for educating employees and users on how to recognize and respond to potential cyber threats. While this role involves some technical understanding, it primarily depends on **social science research and principles**—particularly those from psychology, sociology, and communication studies—to be effective.

Social Science in Everyday Practice

Security Awareness Training Specialists rely on **behavioral psychology** to understand how individuals perceive risk, respond to threats, and form habits. For example, principles like **operant conditioning** and **habit formation** are used to reinforce positive cybersecurity behavior, such as regularly updating passwords or identifying phishing emails. By offering rewards (recognition, small incentives) for completing security modules or responding correctly to simulated phishing attacks, specialists can encourage behavior change over time.

The Role of Social Science in the Career of a Security Awareness Training Specialist

Another important social science concept used is **social norms theory**, which suggests people are influenced by their perceptions of what others around them are doing. Training programs often use this principle by showing that most employees are completing their training or following best practices, creating peer pressure that leads to better compliance.

Communication and Message Framing

The way cybersecurity messages are communicated significantly impacts their effectiveness. Social science research in **communication theory** helps specialists tailor their language and deliver to different audiences. For instance, fear-based messages (e.g., "Hackers are coming for your data!") may work in some situations but can cause anxiety or avoidance in others. Studies have shown that **gain-framed messaging**—emphasizing the benefits of secure behavior rather than the consequences of insecurity—often produces better results, especially in non-technical populations.

Security Awareness Training Specialists also use **audience segmentation**, a concept from marketing and sociology, to adapt their programs for diverse groups based on age, role, education, or digital fluency. This is particularly relevant when training **marginalized groups**, such as lower-income employees or individuals with limited access to digital literacy resources. Understanding these group-specific needs and barriers is essential to making training inclusive and effective.

Supporting Marginalized Groups and Society

Security Awareness Training Specialists have a direct impact on **digital equity and inclusivity**. In many cases, marginalized populations are more vulnerable to cybercrime due to

systemic gaps in access to education, technology, and institutional support. For example, individuals from lower socioeconomic backgrounds may not receive the same level of digital literacy training as those in higher-income roles, making them more susceptible to phishing and identity theft.

By applying **sociological and psychological insights**, specialists can develop culturally competent and accessible training materials. They can also help organizations understand how biases and assumptions might exclude or disadvantage certain groups, leading to a more ethical and socially aware cybersecurity culture.

Additionally, awareness professionals play a key role in protecting society at large by promoting cyber hygiene across communities. In today's interconnected world, one compromised user can endanger an entire network. Therefore, educating individuals—regardless of background—on how to protect themselves online helps build a stronger, safer digital society.

Conclusion

The career of a Security Awareness Training Specialist is a prime example of how cybersecurity is not just a technical field but also a deeply **social one**. These professionals use principles from psychology, sociology, and communication studies to shape behavior, foster awareness, and bridge gaps in understanding. Their work is especially important in addressing the needs of marginalized groups and ensuring that security training is not only effective but also equitable. As cyber threats evolve, so too must our grounded not only in technology, but in the social sciences that help us understand and protect the people behind the screens.

The Role of Social Science in the Career of a Security Awareness Training Specialist

References

1. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security.*
2. Anderson, R., Barton, C., Böhme, R., et al. (2013). Measuring the cost of cybercrime. *Springer.*
3. ENISA (European Union Agency for Cybersecurity). (2022). Cybersecurity culture in organizations – Building a strong cybersecurity culture.