

Cybersecurity Professional Career Paper

Shelton Jones

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

April 16th, 2026

Introduction

Cybersecurity is a rapidly growing field that protects digital systems, networks, and sensitive data from cyber threats. While many people think cybersecurity is purely technical, human behavior plays a major role in security vulnerabilities. One specific career that highlights this connection is a Security Awareness and Human Behavior Analyst, a professional who studies how people interact with technology and why they fall victim to cyberattacks such as phishing. The purpose of this paper is to examine how professionals in this role rely on social science research and principles to understand human behavior, reduce cyber risks, and improve organizational security.

Social Science Principals

Security Awareness Analysts heavily rely on social science disciplines such as psychology, sociology, and behavioral science. Cyberattacks like phishing are not just technical exploits, they are psychological attacks that manipulate human thinking and decision making. Research shows that social engineering attacks exploit cognitive biases, emotions, and trust to deceive individuals into giving up sensitive information. For example, principles from cognitive psychology help analysts understand why individuals click on malicious links. Factors such as urgency, fear, and authority influence decision making. Additionally, sociology helps explain how group behavior, workplace culture, and social norms impact security practices. According to the research, phishing success depends on both individual traits and organizational environments, demonstrating the importance of social science in cybersecurity.

Application of Key Concepts

Security Awareness Analysts apply key social science concepts such as behavior change theory, risk perception, and decision making models. One widely used concept is the Health Belief Model, which explains how individuals assess threats and decide whether to take protective action. Studies show that people are more likely to follow cybersecurity practices when they perceive a high risk and believe their actions can prevent harm. In practice, professionals use this knowledge to design training programs that influence behavior rather than just provide information. For example, instead of simply warning users about phishing, analysts create simulated phishing campaigns to study employee responses. Data from these simulations help identify patterns such as which groups are more vulnerable and why. Research involving over 8000 employees found that factors like age, education, and job role significantly influence phishing susceptibility and reporting behavior. These insights allow organizations to implement targeted interventions, such as customized training or awareness campaigns, improving overall effectiveness.

Marginalization

Cybersecurity also intersects with issues of marginalization. Certain groups may be more vulnerable to cyber threats due to limited access to technology, lower digital literacy, or lack of cybersecurity education. This creates unequal levels of protection in society. Security Awareness Analysts must consider these disparities when designing training programs. For example, individuals with less experience using technology may require more accessible and simplified security education. Additionally, attackers often target vulnerable populations using tailored scams, making it essential for professionals to understand social inequalities. Efforts to address these challenges include inclusive training programs, public awareness campaigns, and initiatives

aimed at improving diversity within the cybersecurity workforce. By applying social science principles, professionals can promote equitable digital protection for all users.

Career Connection to Society

The role of a Security Awareness analyst is critical to society because human error remains one of the leading causes of cyber incidents. Even the most advanced security systems can fail if individuals make poor decisions. Research from government initiatives highlights that understanding user behavior is essential for improving threat detection and prevention strategies. These professionals contribute to the safety of key societal infrastructures such as financial systems, healthcare networks, and government operations. They also influence public policy by supporting cybersecurity awareness initiatives and promoting regulations that encourage safer online behavior. This career bridges the gap between technology and human behavior, ensuring that cybersecurity solutions address both technical and social dimensions of risk.

Conclusion

The role of a Security Awareness and Human Behavior Analyst demonstrates the critical importance of social science in cybersecurity. By applying principles from psychology, sociology, and behavioral science, professionals can better understand why people fall victim to cyber threats and develop strategies to prevent them. From analyzing phishing behavior to addressing societal inequalities, social science research plays a vital role in strengthening cyber security practices. As cyber threats continue to evolve, integrating human focused approaches will remain essential for protecting individuals and organizations in the digital age.

Scholarly Journal Articles

- Source 1: Human Factors in Cybersecurity (Google Scholar)

Chignell, M. H., Chung, M. H., Yang, Y., Cento, G., & Raman, A. (2021). *Human factors in interactive machine learning: A cybersecurity case study*. Proceedings of the Human Factors and Ergonomics Society Annual Meeting.

This source explains how cybersecurity professionals rely on human decision-making, behavior, and interaction with technology when detecting threats. The study highlights that cybersecurity is not only about software and tools, but also about how analysts interpret alerts, make judgments, and respond under pressure. This is highly relevant to your paper because it shows that professionals in cybersecurity depend on social science concepts such as human behavior, cognition, and decision-making to protect systems effectively.

- Source 2: Security Beliefs and Human Behavior (Google Scholar)

Wash, R., & Rader, E. (2015). *Too much knowledge? Security beliefs and protective behaviors among United States internet users*. Symposium on Usable Privacy and Security.

This article focuses on how people's beliefs, knowledge, and behaviors affect cybersecurity practices. It supports your analysis of social science principles, especially psychology and sociology, by showing how users' attitudes influence whether they follow safe online behaviors like strong passwords or avoiding phishing scams. This can also connect to marginalized groups because differences in digital literacy, education

access, and socioeconomic status may affect cybersecurity awareness and vulnerability to attacks.

- Source 3: Diversity and Society in Cybersecurity (Google Scholar)

Zhang, Q., Mohammed, A. Z., Wan, Z., Cho, J. H., & Moore, T. J. (2021).

Diversity-by-design for dependable and secure cyber-physical systems: A survey. IEEE Transactions on Network and Service Management.

This source contributes to understanding how cybersecurity careers connect to society by discussing the importance of diverse perspectives in designing secure systems. It shows that cybersecurity professionals work in ways that affect public safety, infrastructure, and social systems such as healthcare, transportation, and government networks. The article supports key social science concepts like diversity, collaboration, and social responsibility in professional settings.

References

- Montanez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks.
- MDPI. (2024). Phishing and the human factor: Insights from a bibliometric analysis
- National Institute of Standards and Technology (NIST). Human centered cybersecurity research
- Computer Standards & Interfaces. (2025). Human factors in phishing: Understanding susceptibility and resilience.
- DU, J., Kalafut, A., & Schymik, G. (2024). The health belief model and phishing: Determinants of preventive security behaviors. *Journal of Cybersecurity*.