Cybersecurity Professional Career Paper: Cybersecurity Analyst

Student Name: Albreana Butler

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/14/2026

Introduction

Cybersecurity Analysts have a responsibility to protect systems and users' data from cyber threats and prevent those with unauthorized access from accessing systems and critical data within those systems. In today's society, technology has become a thing that we depend on more and more, and cybersecurity has become an essential part in protecting critical infrastructure such as healthcare systems, financial services, and communication between networks. The main objective of this paper is to provide information on how social science research and course concepts apply to the cybersecurity analyst career. Specifically, it focuses on how human behavior, offender psychology, and cybersecurity awareness are learned through research and applied in real-life situations through cybersecurity work.

Social Science Principles

In cybersecurity, social science principles can be used to help describe human behavior behind cybercrime and user error. One main idea supported in the article Human Factors in Cybersecurity is that while cybercrime is often viewed as a predominantly technical field, even human interactions, decision-making processes, and organizational culture significantly influence digital security systems' effectiveness and resilience (Khadka & Ullah, 2025). Determinism is a principle supported throughout the research, demonstrating how behavior is influenced by environments, education, and social factors. The article The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention also explains that cybersecurity behavior is influenced by an individual's level of awareness and learning of cybersecurity risks. Empiricism is another principle that contributes to how cybersecurity researchers study behavior

by using real-life data and analysis. The article Human Factors in cybersecurity emphasizes that cybersecurity must be studied through human behavior patterns and data-driven approaches. The principle of relativism is also seen in cybercriminal behavior in the article Ransomware crime through the lens of neutralisation theory, This article explains that offenders justify their actions through techniques such as denying responsibility or reducing harm. Additionally, Ethical Neutrality is essential in cybersecurity research practice and is seen in this article, as it shows the importance of analysing offender behavior objectively to understand why cybercrime occurs. Finally, skepticism and objectivism are represented in cybersecurity analysis practices discussed in Human Factors in Cybersecurity, which emphasizes evidence-based analysis of human behavior and system data.

Application of Key Concepts

Cybersecurity Analyst can be applied not only to social science principles but also to course concepts to better understand both attackers and users in digital environments. The neutralisation theory connects to the article Ransomware crime through the lens of neutralisation theory. The authors state that cybercriminals use justification techniques such as denying responsibility or reducing harm (Connolly, Borrion, & Arief). This resonates with the course concept of the psychological role of the offender, which explains the thought process of a cybercriminal before, during, and after committing a cybercrime. Understanding their thinking patterns helps cybersecurity analysts predict an attacker's behavior and improve security strategies.

The next important concept that can be applied is reinforcement sensitivity. It explains how behavior is driven by rewards and consequences. This connects to findings in the article,

The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention, showing that cybersecurity behavior improves when individuals have more awareness and knowledge. In cybersecurity practice, analysts use this concept by establishing training programs that reinforce positive behaviors, such as phishing attempts and following security policies. This course also explains how cybersecurity training must be continuous and based on human psychology.

Lee and Chua support this idea in the article, The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention, showing that being aware of cybersecurity impacts behavior and decision making (Lee & Chua, 2023).

This means training is a continuous process, not just a one-time thing, and it must adapt to new things. The last important concept is cyber professional education requirements, including formal education, certifications, practical experience, continuous learning, and soft skills. This is supported by the article Human Factors in Cybersecurity, which explains that cybersecurity requires both technical knowledge and understanding of human behavior (Khadka & Ullah, 2025). Analysts must possess technical skills along with communication, problem-solving, and critical thinking.

Conclusion

In conclusion, Cybersecurity analysts depend on social science principles and research to better understand both attackers and users. The 3 articles mentioned show that cybercrime is influenced by psychological justification, human behavior, and environmental factors. Course concepts such as neutralization theory, reinforcement sensitivity, and offender psychology help explain the behavior of cybercriminals. By using these ideas, cybersecurity professionals

strengthened training, improved security systems, and better protected organizations from cyber threats.

Resources

Claire Seungeun Lee, & Yi Ting Chua. (2023). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9). https://doi.org/10.1177/00111287231180093

Connolly, L. Y., Borrion, H., & Arief, B. (2025). Ransomware crime through the lens of neutralisation theory. *European Journal of Criminology*. https://doi.org/10.1177/14773708251320464

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. *International Journal of Information Security*, *24*(3). https://doi.org/10.1007/s10207-025-01032-0