Cybersecurity Professional Career Paper: Cybersecurity Analyst

Charlotte Lacy

Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 12, 2025

Introduction

Cybersecurity has become essential as digital threats grow across all areas of society. While often viewed as a purely technical field, cybersecurity work deeply relies on understanding human behavior, social structures, and criminological patterns. Cybersecurity analysts depend heavily on social science research, including psychology, sociology, and criminology, to understand threats, guide decision making, interact with diverse users, and protect marginalized groups, making social science principles central to their daily work.

A cybersecurity analyst monitors networks, analyzes threats, prevents attacks, and educates users on safe practices. Daily tasks include reviewing security logs, investigating suspicious activity, responding to alerts, updating security policies, and training employees. These responsibilities require understanding not just systems, but the people who use and abuse them. Since attacks often succeed due to human behavior, the analyst must constantly apply social science knowledge to interpret motives, predict user actions, and design better protections.

Application and Use of Social Sciences

There are different social science principles that could be applied to this career. One of these principles is psychological. Cybersecurity analysts study user behavior to identify vulnerabilities such as cognitive biases, stress, and decision fatigue that make people susceptible to phishing or scams. Analysts use psychological insights to create more effective security awareness programs, such as explaining phishing cues, using behavioral nudges. Understanding attacker psychology, motives, risk tolerance, and social manipulation strategies, helps analysts anticipate tactics. Researchers argue that social engineering attacks work because they exploit

human cognitive shortcuts and biases (Montañez et al., 2020). As an example, analysts use research on attention and memory to simplify security instructions so users actually follow them.

Another application is with sociological principles. Analysts examine organizational culture to understand why employees follow or ignore policies. Social norms affect password strength, information sharing, and reporting suspicious emails. Team dynamics also influence how quickly security incidents are reported or escalated.The field of social cybersecurity emphasises the importance of social and organisational networks in shaping cyber threats and responses (Carley, 2020). As an example, if a workplace culture discourages asking questions, employees may hide mistakes, analysts must adjust training to create a supportive reporting environment.

One last application to the social sciences is with criminological principles. Cybersecurity analysts rely on theories like Rational Choice Theory, which explains how attackers weigh benefits of an attack against the risks. Routine Activities Theory is applied by reducing opportunities for crime: controlling access, monitoring critical systems, and hardening vulnerable assets. Analysts study social strain and economic factors that push individuals toward cybercrime, helping them understand evolving threat landscapes. As an example, analysts track patterns in cybercrime behavior to predict when certain attacks, like fraud scams, will spike.

Cybersecurity analysts use social science research in their daily routines. Analysts apply research on phishing behavior, fraud psychology, and user risk perception to improve defenses. They use surveys, log analysis, and user behavior data to understand patterns of mistakes or risky decisions. According to the National Academies, integrating behavioural science into cyber defence enables more accurate prediction of manipulative threats and design of effective interventions (National Academies of Sciences, Engineering, and Medicine, 2019). Social

science frameworks help analysts design communication strategies for policy rollouts, training sessions, or incident announcements. For example, using social learning theory, analysts develop training programs where employees learn safe habits by observing coworkers' correct actions.

Interaction with Society and Marginalized Groups

The way that cybersecurity analysts interact with society and marginalized groups can differ such as the social impact of cyber work. Analysts protect critical systems in healthcare, finance, education, and government, directly impacting the public's safety. Security decisions affect millions of people, especially those who rely on essential service. Marginalized groups often face digital inequities such as low digital literacy, limited access to training, or greater exposure to online fraud. Analysts must design inclusive training materials accessible to people with disabilities, low reading levels, or limited English proficiency. Analysts also work to reduce bias in monitoring systems or automated alerts, ensuring minority groups are not unfairly targeted by technology. For example, providing security guidance tailored to elders or to communities who may use shared devices or outdated technology.

Conclusion

Overall, cybersecurity analysts rely on core social science principles every day to understand attackers, predict user behavior, and design effective defenses. The integration of psychology, sociology, and criminology allows analysts to create stronger protections and build safer digital environments. Because their work impacts society at large, including marginalized groups, cybersecurity analysts must continue applying social science research to create ethical, inclusive, and effective security practices.

References

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

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. *Frontiers in Psychology*, *11*(1). https://doi.org/10.3389/fpsyg.2020.01755

National Academies of Sciences, Engineering, and Medicine. (2019). *A decadal survey of the social and behavioral sciences: A research agenda for advancing intelligence analysis.* The National Academies Press. https://doi.org/10.17226/25335