Cybersecurity Professional Career Paper

Tracy Adomfrimpong

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

November 14,2025

Introduction

One of the most crucial cybersecurity specialists is a Security Operations Center (SOC) Analyst, who oversees keeping an eye on, identifying, and reacting to cyberthreats that affect businesses. SOC Analysts heavily rely on social science concepts, such as behavioral analysis, criminology theories, social patterns, and an awareness of how digital risks affect individuals, marginalized groups, and society, even if the technical aspects of this position are generally recognized. This study looks at how SOC Analysts apply social science ideas in their day-to-day job, how their work affects communities, and how the profession helps safeguard vulnerable groups. This article illustrates the interdisciplinary aspect of the SOC career by connecting classroom topics to practical cybersecurity duties.

Application of Social Science Principles in SOC Work

Even though SOC analysts operate in highly technical settings, many facets of their work are influenced by social science studies and human behavior. People are the source of cyber risks, and analysts can better anticipate and respond to attacks by knowing the motivations, decision-making styles, and social contexts of offenders. For instance, SOC Analysts use Routine Activities Theory to build organizational defenses and identify suspicious activity patterns. It states that cybercrime happens when motivated offenders discover ideal targets who lack qualified supervision (Yar & Steinmetz, 2019).

To spot abnormalities, SOC analysts also need to comprehend user behavior. The social science idea that people follow patterns in communication, login frequency, and gadget usage is the foundation of behavioral analytics technologies. Analysts look into whether the conduct is a

valid aberration or a possible threat when these patterns shift. This confluence of technology, criminology, and psychology highlights the social scientific basis of cybersecurity surveillance.

Daily Routines and Social Science Concepts

Log monitoring, incident triage, escalation protocols, and staff communication are all common components of a SOC workflow. Analysts must use human-centered thinking, conflict resolution, and communication skills in these tasks. For instance, when conducting phishing investigations, SOC Analysts are required to assess the emotional triggers—such as fear, urgency, and deception—that are employed in phishing messages and have their roots in psychological manipulation (Hadnagy, 2021). Additionally, analysts use social science data to inform staff members about social engineering tendencies, highlighting how human behavior—rather than just system flaws—creates points of entry for attackers.

Additionally, the work necessitates cultural sensitivity and knowledge of how various demographic groups use technology. For example, differing communication styles, technical exposures, and cybersecurity literacy levels may exist among multinational staff. In order to guarantee inclusion and understanding among a variety of demographics, SOC analysts must modify incident response tactics.

Interactions With Marginalized Groups and Society

Low-income persons, immigrants, people of color, first-generation students, and elderly adults are among the marginalized groups that are disproportionately affected by cybersecurity threats.

These groups are particularly susceptible to fraud, identity theft, and digital exploitation because they frequently lack access to cybersecurity training, struggle with language challenges, or use antiquated technology (Gangadharan & Niklas, 2019). By creating user-friendly security training, customizing communication techniques, and making sure that organizational rules do not inadvertently disadvantage groups, SOC Analysts play a crucial role in addressing these disparities.

By preventing data breaches, safeguarding personal information, and reacting to threats that could endanger social institutions, SOC analysts contribute to public safety on a societal level. Their efforts assist businesses, governments, schools, and hospitals—all of which have a direct bearing on the welfare of the community. The social importance of the SOC profession keeps rising as cyberattacks increasingly target vital services.

Conclusion

A Security Operations Center (SOC) Analyst's responsibilities go much beyond technological detection and response. Understanding human behavior, criminology ideas, injustices, and society systems is necessary for this career, which is based on social science principles. SOC analysts employ behavioral insights to identify threats, use psychological and communication concepts to inform users, and strive to make cybersecurity procedures inclusive of underrepresented groups. SOC analysts make a substantial contribution to digital equity and public safety by shielding communities and organizations against cyberattacks. The crucial relationship between cybersecurity and the social sciences is highlighted by this multidisciplinary approach

References

Gangadharan, S. P., & Niklas, J. (2019). *Decentering technology in digital inclusion: A study of marginalized communities and cybersecurity risks*. Information, Communication & Society, 22(7), 1–18.

Hadnagy, C. (2021). *Social engineering: The science of human hacking* (3rd ed.). Wiley.

Yar, M., & Steinmetz, K. (2019). *Cybercrime and society* (3rd ed.). SAGE Publications.