Cyber Security Professional Career Paper: SOC Analyst

Dorian Jones

School of Cyber Security, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 4/8/2026

Introduction

Cybersecurity has become one of the most critical fields in the modern digital world as organizations increasingly rely on interconnected systems to operate. A Security Operations Center (SOC) Analyst is a cybersecurity professional responsible for monitoring networks, analyzing threats, and responding to security incidents in real time. SOC analysts serve as the frontline defenders against cyberattacks, ensuring that sensitive data and infrastructure remain secure.

Cybersecurity is increasingly important as attacks become more frequent and impactful, impacting individuals, businesses, and governments. The purpose of this paper is to examine how SOC analysts rely on social science research and principles in their daily work. It will explore how human behavior influences cybersecurity, how key concepts from class apply to this role, how marginalized groups are affected, and how SOC analysts contribute to society.

Social Science Principles

SOC analysts rely heavily on social science research to understand human behavior, which plays a central role in cybersecurity threats. Many cyberattacks, such as phishing and social engineering, exploit human psychology rather than technical vulnerabilities. Understanding motivations behind cybercrime, such as financial gain, political influence, or personal grievances, helps analysts predict and respond to threats more effectively.

Social science principles such as human-computer interaction and behavioral analysis are integrated into cybersecurity practices. For example, SOC analysts study how users interact with systems to identify abnormal behaviors that may indicate a breach. If a user suddenly accesses large amounts of sensitive data at unusual times, this behavioral anomaly may trigger an alert.

Additionally, SOC analysts use social science insights to develop cybersecurity awareness programs. By understanding how people perceive risk and respond to training, analysts can design more effective education campaigns to reduce human error. For instance, phishing simulations and training programs are often based on psychological research to improve employee awareness and response to threats.

Application of Key Concepts

Several key concepts from class are directly applied in the role of a SOC analyst, including risk assessment, human factors, deterrence theory, and routine activity theory. Risk assessment is essential for identifying vulnerabilities and prioritizing threats based on likelihood and impact. SOC analysts use this concept daily when analyzing alerts and determining which incidents require immediate attention.

Human factors play a critical role in cybersecurity, as human error is one of the leading causes of breaches. SOC analysts must account for how users behave, including weak password practices or susceptibility to phishing attacks. Deterrence theory is also relevant, as organizations implement monitoring systems and policies to discourage malicious behavior by increasing the likelihood of detection and consequences.

Routine activity theory explains that cybercrime occurs when a motivated offender, a suitable target, and a lack of capable guardianship are present. SOC analysts act as the "capable guardians" by continuously monitoring systems and responding to threats. Tools such as Security Information and Event Management (SIEM) systems, intrusion detection systems, and endpoint monitoring platforms demonstrate how these concepts are applied in practice to detect and mitigate risks.

Marginalization

Cybersecurity disproportionately affects marginalized groups, who may have limited access to resources, education, or secure technologies. These groups are often more vulnerable to cyberattacks such as identity theft, financial fraud, and misinformation campaigns. SOC analysts must be aware of these disparities when analyzing threats and developing defensive strategies.

Additionally, marginalized communities may face increased surveillance or misuse of data, raising ethical concerns within cybersecurity practices. SOC analysts must balance security with privacy, ensuring that monitoring systems do not unfairly target or impact specific populations.

The cybersecurity profession has made efforts to address these challenges by promoting diversity and inclusion within the field. Increasing representation of underrepresented groups helps bring different perspectives to cybersecurity problems and improves the development of equitable security solutions. Furthermore, public awareness campaigns and accessible training programs aim to provide better protection for vulnerable populations.

Career Connection to Society

SOC analysts play a vital role in maintaining the safety and stability of societal infrastructures. They protect critical systems such as financial institutions, healthcare networks, and government databases from cyber threats. A successful cyberattack on these systems could disrupt essential services, cause financial loss, and compromise sensitive information.

Public policies related to cybersecurity, such as data protection regulations and breach notification laws, directly impact the work of SOC analysts. These professionals must ensure

that organizations comply with legal standards while maintaining strong security practices. Their work also contributes to national security, as cyber threats can originate from state-sponsored actors or organized crime groups.

The relationship between cybersecurity and society is dynamic, as advancements in technology create new vulnerabilities while also offering new defensive tools. SOC analysts must continuously adapt to this evolving landscape to protect both organizations and the public.

Reference

Verizon. (2023). *Data Breach Investigations Report*.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7). https://doi.org/10.1016/j.heliyon.2017.e00346

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. *Polity Press*.