Cybersecurity Career Professional Paper

Kevin A. Loarca

Old Dominion University

CYSE 201S: Cybersecurity as a Social Science

Professor Woodbury

April 26, 2026

Cybersecurity Career Professional Paper

The role of a Security Operations Center (SOC) analyst is said to provide a central role in an organization's cybersecurity strategy (Kukkonen, 2024). The key mission of this career is to analyze threat intelligence and contextualize real-time incidents. It also provides a robust defense against advanced and evolving cyber threats (Kukkonen, 2024). This type of cyber-career has complexities and connections with social science principles that are important to understand. Specifically, these principles will aid professionals in the field to efficiently spread security practices and understand criminal behavior. The principle, parsimony, explains that experts need to keep their levels of explanation as simple as possible (Duvall, 2024a). The importance of this principle to the career can be used by professionals to explain their security protocols to inexperienced individuals. For example, experts who are tasked to present how an intrusion happened would need to keep the information digestible. They could do this by visually showing the audience key moments to look out for that cause a breach. The other principle, empiricism, focuses on behavior that is real to the senses (Duvall, 2024a). Empiricism can be useful for a SOC analyst to recognize cyber-criminal behavior and their tactics. An example of this could be the communication of malicious coding on an online forum. Individuals could then interact with the coding to be used to hack into an organization's systems. In this example, the senses of sight and hearing are used to demonstrate how malicious behavior is carried out across platforms, which influence the actions of the criminal.

Key Concepts

Other social science concepts that can be accurately applied to a SOC analyst. These four concepts consist of: the risk triangle, human firewall, cyber victimization, and honeypots. The risk triangle, CIA triad, addresses how information security is handled (Duvall, 2024b). It is composed of confidentiality, integrity, and availability. Confidentiality addresses how information is restricted to those who need access. Integrity assures that information is accurate and reliable. Availability would guarantee access to information by authorized persons when necessary (Duvall, 2024b). This first concept is important for a SOC analyst as it would provide them with a structured framework to go by when determining how confidential information should be handled. The next two concepts are connected with one another. Having a "human firewall" focuses on awareness, vigilance, and behavioral training as a necessity (Tsauri, 2025, p. 1). SOC analysts can use this concept to understand how a deceptive social engineering attack becomes successful. This becomes accurate if, for example, they conduct investigations and find that someone has become a victim of those attacks. To make the connection, some factors can increase the risk of cyber victimization. This is because individuals are not presented with sufficient information to make the best decisions in privacy-sensitive situations (Duvall, 2024c). Recognizing this issue could aid a SOC analyst in understanding that others may not understand the security implications and could educate them. The last concept that can apply to a SOC analyst is the use of honeypots. A honeypot is a purposely designed vulnerable computer system or network that attracts cyber attackers (SOCRadar, 2024). It mimics the behavior of a real system but has no valuable information. The information gathered from the attacks can be used to improve threat detection and bolster defenses against real threat actors (SOCRadar, 2024). There are advantages to this, including studying the hacks in real-time and altering interventions

in the environment to see how the intruder responds (Duvall, 2024d). Some disadvantages can include difficulty studying the motive of the trespasser and whether it's an automated attack (Duvall, 2024d). SOC analysts can use this technology to learn how a hacker can exploit vulnerabilities to infiltrate systems.

Marginalized Groups and Societal Connections

A discussion needs to be addressed to determine how the career can have societal impacts. There is an estimated shortage of approximately 3.4 million skilled workers in cybersecurity (Veiga, n.d., p. 6). Challenges will be present if this issue is not resolved. A shortage in these fields can result in insufficient time for risk assessment and management, oversights, patching of critical systems being slower, limited time and resources for training, and misconfigured systems (Veiga, n.d., p. 6). A potential solution to the issue can be resolved if marginalized groups are given the opportunity. To be specific with the gender disparity, women only represent 25% of the cybersecurity profession worldwide (Veiga, n.d., p. 2). This diversity can provide a range of skills required to grow business opportunities in digital technologies and provide solutions to secure it in the digital space (Veiga, n.d., p. 2). The relationship is present between this, as adding a diverse group to the career could resolve those issues if present. Additionally, there are complexities of dynamic interactions between society and a SOC analyst. Society heavily depends on this career to safeguard digital infrastructures. For example, in a hospital setting, it generally holds a lot of patient data in its network, and someone needs to be able to monitor and protect the data. As a SOC analyst, their contribution will be able to protect the data of society that relies on hospitals to be functional to provide public health services.

Conclusion

To conclude, Security Operations Center analysts rely on social science to improve society as a whole. Some principles make it easier for an analyst to educate others and recognize cybercriminal patterns. The concepts mentioned also apply to the career as they need to understand how they can protect themselves digitally, while also acknowledging the risks if others are not careful online. There are also the societal impacts connected to the career. There are negatives, such as a lack of diversity in the field of cybersecurity, that can lead to challenges. There are also dynamic interactions with society and the career, which rely on one another to function safely.

References

Duvall, T. (2024). CYSE201S (Module 2a). Principle of Social Sciences and Cybersecurity.

Duvall, T. (2024). CYSE201S (Module 6b). Psychology Research, Human Factors, and Cybersecurity.

Duvall, T. (2024). CYSE201S (Module 5c). Applying Psychological Principles of Cyber Offending, Victimization, and Professionals.

Duvall, T. (2024). CYSE201S (Module 3d). Strategies to Study Cybersecurity through an Interdisciplinary Social Sciences Lens.

Kukkonen, M. (2024). Competency Requirements for Tier-1 SOC Analyst. Laurea. https://www.theseus.fi/bitstream/handle/10024/875604/Kukkonen_Markus.pdf?sequence=2

SOCRadar. (2024, October 1). The Role of Honeypots in Cybersecurity. https://socradar.io/blog/the-role-of-honeypots-in-cybersecurity/

Tsauri, M. (2025, August). Human Vulnerabilities to Social Engineering Attacks: A Systematic Literature Review for Building a Human Firewall. ResearchGate. https://www.researchgate.net/publication/395230446_Human_Vulnerabilities_to_Social_Engineering_Attacks_A_Systematic_Literature_Review_for_Building_a_Human_Firewall

Veiga, A. (n.d.). Addressing Gender Diversity in the Cybersecurity Profession to Enhance Business Value. https://www.researchgate.net/profile/Adele-Veiga/publication/388574884_Addressing_Gender_Diversity_in_the_Cybersecurity_Prof

ession_to_Enhance_Business_Value/links/67f908e6ded433155727d922/Addressing-Gender-Diversity-in-the-Cybersecurity-Profession-to-Enhance-Business-Value.pdf