Cybersecurity Professional Career Paper: Cybersecurity Analyst

Student Name: Gavin Bacaoan

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: 16 April 2026

Introduction

A cybersecurity analyst plays a critical role in protecting organizations from digital threats by monitoring networks, identifying vulnerabilities, responding to incidents, and helping prevent data breaches. Today's modern world, cybersecurity is essential because business, governments, healthcare systems, and financial institutions all depend on secure digital systems to function safely and effectively. As cyberattacks continue to grow in frequency and complexity, cybersecurity analysts are increasingly important defending sensitive information, maintaining public trust, and supporting national and economic security. I would be interesting being a cyber analyst working for the bank. If their bank accounts are glitching and going wrong I would have to analyze of whats going on of that glitch and come up with a solution. From the social science view point, people are attracted to cybersecurity analyst roles because they protect individuals and organizations from harm. These jobs help to maintain trust in digital systems that society depends on such as banking, healthcare, and education.

Social science principles

Relativism means a cybersecurity analyst must understand that people behave differently depending on social, cultural, and organizational context. For example, what seems like risky behavior in one workplace may be normal in another, so analysts must consider the environment when evaluating user actions.

Objectivity means cybersecurity analysts must rely on facts, evidence, and data rather than personal opinions. When investigating a phishing attack, insider threat, or breach, they use logs, alerts, and forensic evidence to make unbiased decisions.

Parsimony: Analysts often begin with the simplest explanation for a security issue before assuming something more complex. For example, unusual account activity may first be explained by user error or a misconfiguration before concluding it is a sophisticated attack.

Empiricism means cybersecurity analysts depend on measurable and observable evidence such as network traffic, system logs, incident reports, and vulnerability scans. Their work is based on real data rather than guesses.

Ethical Neutrality means analysts must examine cybersecurity incidents professionally and fairly without letting personal judgments interfere. They focus on what happened, how it happened, and how to respond, even when a case involves unethical or harmful behavior.

Determinism means this principle appears in cybersecurity because certain factors can influence predictable outcomes. Weak passwords, lack of employee training, and poor security culture often lead to greater risk of breaches or phishing success.

Skepticism means cybersecurity analysts must question what they see and avoid accepting things at face value. Suspicious emails, login attempts, system changes, or unusual behavior all require careful verification before conclusions are made.

Application of Key Concepts

In cybersecurity analyst career, several key course concepts are applied directly to everyday job responsibilities. One concept is human factors, because employee behavior and social engineering can create security risks. Another is risk perception,which helps analysts understand how users and orgranizations respond to threats. A third concepts is privacy versus security, since analysts must protect systems while respecting legal privacy concerns. Victimization is also important because analysts examine how people and organizations become targets of cybercrime. Finally, compliance and governance matter because analyst help organizations follow standards such as HIPAA, PCI-DSS, and NIST. Professionals apply these concepts through risk assessments, access controls, incident response, and security awareness training. They also use tools such as SIEM systems, vulnerability scanners, phishing simulations, and audit logs to support security and compliance.

Marginalization

Cybersecurity is closely related to marginalized groups because digital risks do not affect everyone equally. Low-income communities may have less access to secure technology, updated software, and cybersecurity education, which increases vulnerability to cybercrime. Marginalized groups may also face greater targeting through scams, identity theft, harassment,

and online abuse. Another challenge is surveillance, since increased monitoring tools can create privacy concerns for communities that already experience discrimination. Cybersecurity professionals help address these issues by promoting digital literacy, supporting inclusive security practices, and encouraging more diversity in the cybersecurity field.

Scholarly Journal Articles

Khadka, K., & Ullah, A. B. (2025) examines that cybersecurity is strongly influenced by human behavior, decision-making, and orgnizational culture, not just technology. It is relevant to paper because it shows why cybersecurity analysts must understand user behavior, human factors, and social science research when protecting organizations.

Renuad, K., & Coles-Kemp, L. (2022) explains that cybersecurity must also be accessible and inclusive. It shows that not all users have the same level of access, ability, or protection, which connects to concerns about inequality, usability, and fair digital protection. This supports marginalized group of explaining the cybersecurity analyst.

Carley, K. M. (2020) highlights that cybersecurity affects public behavior, institutions, and trust in digital systems. It helps explain why cybersecurity analysts contribute to safety of social infrastructure and why their work matters beyond just technical systems. It contributes to understanding how cybersecurity careers connect to society.

Conclusion

The cybersecurity analyst profession is an important career that combines technical knowledge with an understanding of human behavior and social issues. Cybersecurity analysts

help protect organizations, critical infrastructure, and sensitive information form growing digital threats. Their work is connected to social science principles, key course concepts, marginalized groups, and the overall safety of society. By using both technical tools and social science insights, cybersecurity analysts play a major role in reducing risk, improving security awareness, and supporting the stability of the modern digital world.

Reference

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

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

Renaud, K., & Coles-Kemp, L. (2022). Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. *SN Computer Science*, *3*(5). https://doi.org/10.1007/s42979-022-01239-1