Cybersecurity Career Professional Paper: Cybersecurity Analyst

Logan Gutierrez

Old Dominion University

CYSE 201s: Cybersecurity and the Social Sciences

November 15th, 2025

Professor Diwakar Yalpi

Introduction

A cybersecurity analyst is one of the most important and popular jobs in the cybersecurity field. They protect online information from threats, watch for incidents, and respond to them. An analyst role is very technical, but it also relies on social science principles to protect information. By understanding behavior, culture, social norms, and communication, it will help analysts build defenses against threats. This paper will talk about how cybersecurity analysts combine social sciences into their daily routines, how key concepts apply in the job, how marginalized populations are affected, and how it connects to society.

Social Science Principles

Professionals in this career have to rely on social sciences to understand motivations, behavior, and how we interact with technology. For example, cybersecurity analysts duties include monitoring network traffic, responding to threats, making practices, and examining incidents (Coursera). This means that the role involves not just technical tools, but understanding human behavior. Responding to what people do and how they make errors are all things cybersecurity analysts must handle.

Social science principles help cybersecurity analysts understand the way people interact with technology, make decisions, and cause incidents. Concepts from psychology and sociology can be used to examine how employees and people think about cybersecurity and what motivates their behavior (Carpenter, 2022). These factors allow for cybersecurity analysts to design systems and policies that take into account human behavior. This allows for more effective and safe security practices. For example, social sciences can tell us that attention can decline when something is repetitive, causing people to skip security steps. A cybersecurity analyst can use that to make training modules that are less repetitive and more entertaining.

Application of Key Concepts

Key concepts from class such as human factors, social engineering, ethics, risk perception, and even communication are all important to the work of a cybersecurity analyst. These concepts will help analysts to prevent future attacks and develop security measures.

Cybersecurity analysts use human factors when they study why users click on phishing emails or reuse the same passwords. They use these studies to make interfaces that work with human behavior, not against it. They also use social engineering principles to understand how attacks manipulate people, which shapes how analysts make training programs (Coursera). Analysts use social science concepts to find risks within organizations. This can be lack of awareness or poor reporting habits. These studies guide how they make security protocols and make sure policies remain up to date. Analysts can use these concepts through phishing simulations, which help them detect threats and respond to them.

Marginalization

Cybersecurity can affect marginalized groups in many different ways. Cyber attacks and scams usually impact communities of color, low income families, older adults, and even immigrants (Tisdale, 2024). These groups may have fewer resources to recover from loss and could have less access to protection (Tisdale, 2024). For example, an attack on public assistance systems like EBT cards, can hurt low income individuals the most (Tisdale, 2024). The role of a cybersecurity analyst is to find these risks and then respond to them. This could mean changing protection measures for marginalized groups in order to keep them safe.

Career Connection to Society

Cybersecurity is an important factor for the safety and stability of today's world. Digital infrastructures support almost every aspect of society, that being energy, water, transportation,

education, and so on (Maigret, 2023). With that, weak cybersecurity threatens public safety, national security, and businesses (Maigret, 2023). A cybersecurity analyst helps by protecting systems and making sure society can rely on them. Public policy is important to analysts as it shapes what they do and how they help with society.

Conclusion

In conclusion, a cybersecurity analyst are able to create stronger safety measures by combining technical skills and the social sciences. This is done by understanding behavior, culture, social norms, and communication. Analysts make sure that the digital environment remains secure and reliable for everyone, protecting organizations and society.

References

What does a cybersecurity analyst do? 2026 job guide. Coursera. (2028, October). https://www.coursera.org/articles/cybersecurity-analyst-job-guide

Carpenter, P. (2022, June 24). *Cybersecurity: What can we learn from the social sciences?*. Forbes. https://www.forbes.com/councils/forbesbusinesscouncil/2022/06/24/cybersecurity-what-can-we-learn-from-the-social-sciences/

Tisdale, N. (2024, February 12). *The hidden injustice of cyberattacks*. Wired. https://www.wired.com/story/cybersecurity-marginalized-communities-problem/

Maigret, B. (2023, July 28). *Cybersecurity: A necessity for the sustainability of society*. Fortinet Blog. https://www.fortinet.com/blog/business-and-technology/cybersecurity-necessity-for-sustainability-of-society