Career Paper: Cybersecurity Analyst

Student Name: Liangshun Cheng

School of CyberSecurity, Old Dominion University

CYSE 201S: Cyber Security and the Social Sciences

Instructor: Diwakar Yalpi

Date:4/4/26

Introduction

There are many careers in cyber security a person can go into. Each and everyone of them works in some way to help keep our cyberspace safe from malicious actors that want to take our money and or data. Some act as bad actors in order to test security, and some are in fact threats sponsored by states. This paper will cover one of those careers, specifically the career of a Cyber Security Analyst. This position has appeared in many places where technology is used, and is on the front line when a cyber threat occurs. They monitor network traffic for suspicious actions, respond to incidents, fix found vulnerabilities, and much more. This paper will cover how a Cyber Security Analyst will use the social sciences to aid them in their work. What kind of methodologies can be applied while working in their field? Finally, we will discuss how a Cyber Security Analyst works in social systems, and how they and society work with marginalized groups.

Application of Social Sciences

Now, the first thing we need to discuss is how social sciences can be applied to the Cyber Security Analyst career field. Psychology, which is the study of the human mind and behavior. Sociology, which is the study of human societies and the structures behind them, and many other fields of social science play a key role in their careers. Due to the advancements in security technology in recent years, it has become rarer for threat actors to use technology to break into systems. Instead, many look to the human side of things for vulnerabilities. Attacks like this are often called social engineering attacks, an attack that takes advantage of people in order to get access to a computer system. Cyber Security Analysts often are the first to respond to these types of attacks and even take measures to prevent further attacks by teaching security to their peers within the workforce. Social Sciences also help Cyber Security Analysts understand the

motivation behind an attack, and by extension, help them develop strategies to counter such attacks in the future. Human and sociological behaviors are also necessary to develop a defence strategy that is easy to fit in, especially since the cultures of different places are different and would need different strategies to be effective.

Methodology

Secondly, we need to discuss a few of the methods these professionals use in their work. There are many tactics and methodologies we learned in CS201S that a Cyber Security Analyst would use; they also apply certain cybersecurity principles when forming methods to counter threats. One of these methods would include conducting experiments within cyberspace. For example, conducting Social engineering attacks on their own workplace to gather data to teach coworkers, or pen testing their own systems to find vulnerabilities to fix. As mentioned before, this role is often also responsible for developing and promoting workplace practices that take cyber security into account, building a better human firewall, and preventing social engineering attacks.

Societal Role and Marginalized Groups

Finally, we need to look at how this career plays a role in our societies and how marginalized groups can be affected. Due to how technology has evolved, it is now playing a vital role in many of our society's structures. Things like financial institutions, medical facilities, and government bodies all use cyberspace in one way or another for all sorts of purposes. With cyberspace now being so closely tied to these systems, Cyber Security Analysts are a core part of protecting those spaces from bad actors. Through their work, they help develop and train others to protect the systems they use from attack. They are also the first to respond to an attack often

times. Now, the effect of marginalized groups also plays a role in their work. This is mostly because marginalized groups are often more susceptible to cyber attacks. This is due to a mix of factors, including communication issues, lack of or limited access to resources, and discrimination getting in the way. As such, when a cybersecurity analyst works with these groups, the understanding that slightly different societies will mean slightly different norms. Analysts should work to understand these norms on a social and psychological level so that communication of a message isn't lost in translation and so that cybersecurity strategies take into account the social norms of the people they are made to protect.

Conclusion

In conclusion, the role of the Cybersecurity Analyst is a large one that will continue to grow as technology and society also grow. Their work, although technical, also applies social factors in order to protect cyberspace and those who use it. As more threats come to cyberspace as it grows, Analysts will need to understand both the technological side in order to prevent system vulnerabilities, but they will also need to understand social sciences to prevent attacks through things like social engineering.

Works Sited

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). *Hacker types, motivations and strategies: A comprehensive framework*. Computers in Human Behavior Reports, 5, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Coursera. (2026). *What does a cybersecurity analyst do? 2026 job guide*. Retrieved April 9, 2026, from https://www.coursera.org/articles/cybersecurity-analyst-job-guide

Wongkrachang, S. . (2023). Cybersecurity Awareness and Training Programs for Racial and Sexual Minority Populations: An Examination of Effectiveness and Best Practices. *Contemporary Issues in Behavioral and Social Sciences*, *7*(1), 35–53. Retrieved from https://researchberg.com/index.php/CIBSS/article/view/112