Joshua Punch

4/15/2026

Cybersecurity Career Paper: Security Analyst Introduction

Cybersecurity analysts play a very important role in the protection of organizations and businesses, as well as the public, against threats in the cyber realm. Many people often think of this career as a technical job that includes coding as well as monitoring systems. However, there is a very large connection between it to social science. Cybersecurity typically will require a considerable amount of knowledge in both computers and human behavior. Cyber analysts often are needed to understand how people will think and act, resulting in how they make decisions and errors online. This paper will demonstrate which social science concepts apply to the day to day life of what a cyber analyst will do while at work.

Role of a Cybersecurity Analyst

A cyber analyst typically is going to be responsible for data being safe from attacks, as well as other computer systems. The day to day work for an analyst is going to include monitoring network systems to detect any suspicious activity that is happening. They also will respond to security issues so that they can prevent future attacks. Online training for these analysts is also an important part of their work load.

Technical work requires a good amount of people skills so that you can understand others. Humans by nature make errors, which typically can result in multiple security problems. These occur when humans make mistakes instead of the systems having issues. Analysts tend to study user behavior patterns so that they can identify why people do things such as click on unsafe links, as well as use passwords that are not secure.

Application of Social Science Principles

Social science provides methods of research that help cyber experts understand human behavior, which represents methods of social science. Phishing attacks, as well as most other cyber attacks, require the attackers to deceive users instead of people hacking directly into the systems. Attacks typically will create emergency situations as well as claim false identities to obtain information not known to the public. This requires the analysts to know about all of these strategies because they need to be able to learn how to prevent them.

People tend to view the field of cyber security differently than one another. Some groups will believe that they will never fall victim to different types of cyber attacks as they do not view protection as an essential. These analysts will come up with different security methods in which different groups of people can use without a high understanding.

Interaction with Marginalized Groups

Cybersecurity analysts evaluate professional activities and how they affect the population. Certain groups of people are more susceptible to cyber attacks. Older people are the main group, as well as people who have limited tech experience. Low-income families are another group that falls victim at a higher rate, as they are unable to obtain solutions as well as safety training.

These systems should become easier to access for people according to the requirements that they need. The implementation of easy to use systems requires instructions which will help people through the process of becoming better protected. Without these, certain populations will face higher rates of cyber crimes.

The technology field suffers from bias issues which create obstacles for marginalized groups. When systems fail to accommodate users from underrepresented groups into their design

the technology creates barriers which prevent these users from accessing necessary resources. Cybersecurity professionals must understand this issue while they create systems which serve diverse user groups through extra design efforts.

Impact on Society

Cybersecurity analysts protect essential systems which secure bank operations and hospital functions and government networks against cyber threats. The infrastructure that protects essential systems requires their services because they work to safeguard these facilities from potential cyber threats.

Cyber analysts protect important systems which are used to help operations as well as government networks against malicious cyber attacks. The infrastructure that protects these systems will require services of these analysts as they protect these facilities

Another important part of their job is communication. Analysts need to provide a clear explanation of the current situation to users who do not understand technical information. The task becomes challenging during emergencies because of its unexpected behavior. Social science provides essential communication skills which become vital when social workers interact with others.

Conclusion

Cybersecurity analysts perform many different types of work that have to do with technology. The job they have depends heavily on understanding human behavior, which directly links to social science. This field of work heavily relies on behavior of humans as well as social engineering. Another important aspect is risk perception. This field requires these analyst to understand how much what they do impacts multiple different groups of people, including the

higher risk people. These professionals combine technical skills as well as the expertise in social science so that they can succeed at what they do.

Works cited:

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

National Institute of Standards and Technology. (2023). *Cybersecurity framework*.