Kaemon Powell

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Science

Professor Yalpi

4/14/2026

Cyber Security Analysts: A Deep Dive

Cybersecurity analysts play a major role in protecting organizations from cyber threats by monitoring systems, identifying vulnerabilities, and responding to different attacks. In today's digital world, their work is a lot more important than ever because nearly every part of society depends on technology. The purpose of this paper is to explain how cybersecurity analysts rely on social science principles in their daily work.

Social Science Principles

Cybersecurity analysts rely on social science research to understand and respond to each human behavior in the digital environment. One key is empiricism, this is where, as discussed in class, analysts use real-world data like user behavior patterns to make informed decisions about security threats instead of assuming. Another is parsimony, which includes choosing the simplest explanation for a security issue like assuming error with user threats before more complex causes. Objectivity is very important as well. Analysts have to evaluate threats without bias when investigating different incidents. Additionally, determinism suggests that human behavior has causes. This allows analysts to predict and prevent attacks. The principle of theoretical perspective helps analysts interpret cyber threats through a number of frameworks like psychology

or economics. Ethical neutrality is also used as an analyst because they analyse hacker behavior without judgement personally. Instead, they have to focus on understanding the motives. Finally, replication makes sure that security findings ans solution are and can be tested and repeated to confirm effectiveness. As a collective, these principles guide cybersecurity analysts in making evidence-based decisions.

Application of Key Concepts

Several class concepts are directly used by cybersecurity analysts. Social engineering is a major threat and analysts work to find it and prevent it by informing their clients or users. Risk management helps analysts decide which type of vulnerabilities are the most important to fix. Human factors in cybersecurity show that most users often make mistakes, so analysts create awareness programs to reduce those errors. Cybersecurity policy and compliance guide how organizations follow the laws and security standards. These concepts are used daily when analysts monitor their systems and improve security practices.

Marginalization

Cybersecurity analysts also consider how their work may affect marginalized groups. One issue is limited access to technology and education. This can make some groups vulnerable to cyber threats. Another challenge is that marginalized populations are most of the time targeted more frequently in scams and fraud. There are also some concerns about privacy and surveillance, where certain communities may face monitoring more often. Cybersecurity professionals address these issues by promoting digital literacy and supporting diversity in the field so different perspectives are included.

Career Connection to Society

Cybersecurity analysts play a major role in protecting society by securing certain systems like banks, hospitals, and government networks. Their work helps prevent data breaches and disruptions to daily life. At the same time, society influences this career by its need for stronger cybersecurity practices and systems. Laws and policies also shape how analysts do their jobs. This shows a strong connection between cybersecurity and society where each affects the other.

Scholarly Journal Articles

Source 1:

Hadlington (2017) shows that human behavior is a major cause of cybersecurity breaches, supporting the importance of social science principles.

Source 2:

Workman (2008) explains how social engineering attacks rely on psychological manipulation, connecting directly to human behavior and trust.

Source 3:

Assante and Tobey (2011) highlight the importance of workforce diversity in improving cybersecurity outcomes and addressing broader societal concerns.

Conclusion

In conclusion, cybersecurity analysts depend on social science principles heavily to perform their jobs effectively. The seven principles play a major role in how analysts approach security challenges. Key concepts like social engineering and risk

management are shown daily. They show that cybersecurity is not just technical but also social. The career also has implications for marginalized groups and society as a whole. Overall, cybersecurity analysts are essential for maintaining safety and trust in the digital world.

References

Hadlington, L. (2017). Human factors in cybersecurity. *Heliyon, 3*(7).

Workman, M. (2008). Social engineering threats. *Journal of the American Society for Information Science and Technology, 59*(4).

Assante, M. J., & Tobey, D. H. (2011). Cybersecurity workforce development. *IEEE Security & Privacy, 9*(1).