Andre Beckwith, Jr.

Dr. Trinity Woodbury

CYSE 201s

04 October 2026

Cybersecurity Analyst: Applying Social Science to Protect Digital Networks

A Cybersecurity Analyst ensures the security of a company's data, systems, and networks from a variety of cyber threats. This is often perceived as a purely technological job involving only code and firewalls. However, there is also a significant social aspect to this role. Cybersecurity is a social problem because all technology is created, employed, and attacked by individuals. A Cybersecurity Analyst who is able to analyze both the culture, society, and behavior of individuals will be better able to design secure systems that will be employed appropriately and also prevent many cyberattacks. This paper will highlight the relationships between social science concepts, concepts learned in class, and the issues that affect members of minority groups and how all of these relate to this role as well as the relationship between this role and society.

Application of Social Science Concepts to the Role

There are several applications of social science concepts to this role. Individuals can be both a threat and a resource. As a threat, individuals can be manipulated by using social engineering techniques, including phone or email phishing to obtain access or passwords. A Cybersecurity Analyst who is able to consider the social influence of stress, trust, authority, and urgency on individuals will be better at both risk assessment and creating defenses against these attacks. As a

resource, individuals are the first line of defense, and so training programs should be created to account for individual behavior and learning rather than just on paper appearance.

Human-centered design is also an important application of social science within this role. Nobles (2018) notes that overcomplicated or slow security controls will be circumvented by individuals creating additional attack vectors. An example of this is in health care, where staff may cover biometric login controls with paper cups to circumvent multiple logins in an emergency situation. A Cybersecurity Analyst should develop security controls that account for individual behaviors as individuals will circumvent security that does not account for their behavior. This demonstrates the relationship between social science and cybersecurity. Even a technically secure system can fail if it does not take into account human behavior.

Class Concepts and Application to the Role

1. Social Engineering - Use of psychological concepts such as fear and trust to anticipate and avoid manipulation that an attacker may employ.
2. Structural Functionalism - A company can be thought of similarly to a social system. Individuals, HR, legal, and IT are all components within the system and must all interact. Security can be thought of as the structure that ensures the smooth running of the system.
3. Subcultures - Cybersecurity can create a subculture of honesty, data protection, and evidence based practices. Hackers create a different subculture based around rule breaking and secrecy. Holt (2020) notes the importance of understanding the hacker subculture in anticipating possible attacks and tracking activity on the dark web.
4. Human-centered design - As noted previously, this is an important concept that security should take into account human behavior in order to be successful in practice.

5. Media Distortion - Media reports on cybersecurity often over exaggerate the threat, creating confusion within the public. A Cybersecurity Analyst can use factual information rather than media hype to assist in management decision-making regarding security controls and investment.

Marginalized People and the Career

There are two ways that this career is connected to marginalized people. The first has to do with inclusion within the field of cybersecurity. A study by Katcher et al. (2024) on cybersecurity professionals found that underrepresented individuals often experience less inclusion and safety within their work environment. This can have an impact on how many people of these groups remain in the field as well as how many will speak up about issues that occur. These factors may have a quiet influence on security within the workplace.

The second connection has to do with marginalized individuals in society who are at a greater risk of becoming the target of cybercrime. Elder individuals, individuals with low levels of technology education, underprivileged individuals, and non-native English speakers are at a greater risk of being deceived by scams as well as lacking the tools for adequate protection, such as current equipment and subscriptions to security services. A Cybersecurity Analyst can use this knowledge to help design education and outreach programs that are effective with these groups rather than assuming all individuals have the same levels of knowledge and access to resources.

Society and the Career (Two-Way Relationship)

This career impacts society but also is impacted by society. On one hand, this career helps secure the institutions that society relies upon on a daily basis including schools, hospitals, and banks. A

security incident can disrupt services, expose sensitive information, and cause a loss of confidence in the use of technology within society. On the other hand, society can also impact this career. Societal fear caused by the media can cause organizations to invest in security. Data privacy legislation can create new regulations that cybersecurity professionals must adhere to. Lastly, the demand for increased security in services and applications are driven by society. This two-way relationship shows that a Cybersecurity Analyst is not only responsible for technology within their career, but also must be aware of the needs, fears, and demands of society.

Conclusion

Within a Cybersecurity Analyst's role, there is more than simply code. Structural functionalism, subcultures, social engineering, human-centered design, and media distortion all play a role within this career on a day-to-day basis. The career is also related to marginalized individuals both within the field of cybersecurity and also within society that can be at a greater risk for cybercrime. Additionally, there exists a two-way relationship between this career and society. Being aware of these social science concepts can help a Cybersecurity Analyst perform their job more effectively and also better protect those who rely on them.

References

1. Holt, T. J. (2020). Computer Hacking and the Hacker Subculture. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 1–20.
2. Katcher, M., et al. (2024). A Survey of Cybersecurity Professionals' Perceptions and Experiences of Safety and Belonging. *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*, 211–228.
3. Nobles, C. (2018). Botching Human Factors in Cybersecurity in Business Organizations. *HOLISTICA - Journal of Business and Public Administration*, 9(3), 71–88.