Cybersecurity Analyst

Stuart N. Howard

Old Dominion University

9 April 2023

Cybersecurity Analyst

As technology advances, the need for Cyber Security Analysts becomes more and more critical. Cyber Security Analysts protect computer systems and networks against cyber-attacks, breaches, and other security threats. While technical skills and knowledge are crucial for this career, social science research and principles are also essential. There are several critical social science principles that Cyber Security Analysts apply to their careers, like Criminal Justice, Psychology, and Sociology.

Cybersecurity Analysts have multiple responsibilities in their career, such as monitoring system networks, preventing cyberattacks, communicating security plans, responding to cyberattacks, and researching new strategies (Reid, 2022). The Criminal justice social science principles aid in that job. Cyber, Internet, or Computer crimes have become a part of criminological vocabulary (Payne & Hadzhidimova, 2018). Analysts must know the overlapping aspects of criminal justice and cyber security. “Better understanding of the connections between criminal justice and cyber security will help to strengthen our efforts to promote safer computing in all its forms (Payne & Hadzhidimova, 2018).” Applying principles of the criminal justice system can help law enforcement better understand the motivations behind cybercrime and victimization, develop effective strategies for prevention and intervention, develop research, and understand cyber law (Payne & Hadzhidimova, 2018). Criminal justice social science principles can aid in understanding the psychological factors of criminal behavior.

The psychological factor is vital in determining the cause of a crime. It gives insight into understanding why a crime is being committed. Some crimes are committed because that is what the criminal wants to do. However, the psychological factors give you more insight into why it was committed, like revenge, anger, or boredom. There are some theories that analysts should consider in understanding the reason behind crime, like the Neutralization theory, where individuals know right from wrong and rationalize their behavior before committing a crime, which is claimed by law-abiding citizens and those who commit crimes or break the rules (Siponen & Vance, 2010). Additionally, knowing that cybercriminals associate Sykes and Matza’s five types of neutralization to cybercrimes, Denial of injury, Denial of the victim, Denial of responsibility, Appeal to higher loyalty, and Condemnation of condemners (Payne & Hadzhidimova, 2018) (Siponen & Vance, 2010). Also, the Differential association theory is that individuals learn criminal behaviors through social and relationship interactions, including those formed online. These are a few theories associated with the social science principles that will help cyber security analysts in their careers.

The Sociology social science principles that Cyber Security analysts can apply to assist analysts in their careers as they study the social life and behavior of a cybercriminal. The human factor is a significant component to consider regarding cybersecurity and should not be overlooked. It is projected that over half of all information systems security violations are indirectly or directly caused by employees' poor security compliance (Siponen & Vance, 2010). With more devices connected to the web (some with complex security), criminals have resulted in social engineering like fishing, scams, and malware (keyloggers) to gain access to information systems. The Sociology principles help an analyst understand that not all cybercrimes are committed by criminals. Some are committed by people who use the justification “Mistake of Law” where they did not realize it was illegal, like bullying and trolling, using unofficial streaming services, faking your identity and online copying audio from YouTube. Analysts can use Sociology principles and other tasks to determine more effective security measures (Reid, 2022). The Deterrence Theory, according to Siponen & Vance, Straub and Nance (1990), suggested that the detection and punishment of violators minimize computer abuse (2010) as they analyze data and determine effective security measures, the analyst could directly or indirectly contribute to cyber law and policy by communicating and coordinating with law enforcement agencies.

There are challenges Cyber Security Analysts must also navigate the dynamic interactions between society and their work. Society's views of security and privacy can affect Cyber Security Analysts' approaches to protecting systems and networks. For example, if society values privacy over security, Cyber Security Analysts may need to find ways to balance these priorities. Additionally, they must be aware of their work's ethical and legal implications. They must have Ethical neutrality to adhere to ethical standards, be able to report illegal activities and ensure that their actions are legal and ethical.

Cyber Security Analysts require and depend on social science principles. Key concepts such as Criminal Justice, Psychology, and Sociology are essential to the work of Cyber Security Analysts. The ability to incorporate and understand Neutralization theory, differential association theory, and the Human factor is some social science principles and theories that will help them navigate the interactions between society and their work. It is essential for Cyber Security Analysts to understand these complexities and to be able to apply social science research and principles to their work in order to protect systems and networks effectively.

References

Payne, B. K., & Hadzhidimova, L. (2018). Cyber Security and Criminal Justice Programs in the United States: Exploring the Intersections . *International Journal of Criminal Justice Sciences* .

Reid, A. (2022, September 12). *Computer Science.org*. Retrieved from Day in the Life of an Information Security Analyst: https://www.computerscience.org/cybersecurity/careers/information-security-analyst/day-in-the-life/

Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, 487-502.