Cybersecurity Analyst: Understanding the Human Side of Cybersecurity

Student Name: Alexander Walker

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/2025

Introduction

People typically say that cybersecurity analysts are technical professionals who keep networks safe and address cyber threats. But this job is as much about working with people as it is about working with technology. Cyberattacks are effective due to human decision-making, susceptibility to deception, and predictable behavior. According to Dawson and Thomson (2018) "Cybersecurity professionals must understand not only the technical aspects of their field but also possess an in-depth knowledge of human interactions". A lot of what cybersecurity analysts do is based on social scientific research, notably in the fields of psychology, sociology, criminology, and ethics. This research discusses the reliance of analysts on social science principles in their everyday practices, the direct relevance of major ideas from social science to their professional duties, and the profession's engagement with both disadvantaged communities and society at large.

Social science principles

Experts in cybersecurity often examine human behavior, which is a significant aspect of social science. The majority of cyber incidents occur when users click on phishing links, use weak passwords, fall for scams, or disregard policy requirements. Analysts depend on a grasp of people's decision-making processes, risk perceptions, interpersonal trust, and motivations for avoiding these issues. Relativism and other social science concepts assist analysts keep in mind that different people have different perspectives on technology and risks, so what seems "obviously suspicious" to one individual may appear normal to another. Because people's online decisions are influenced by their surroundings, stress levels, and prior experiences rather than merely chance, determinism also plays a part.

Psychological triggers such as fear, haste, curiosity, or authority are used by cybercriminals to achieve their goals. Analysts must understand how persuasion works and why some social methods regularly deceive individuals in order to combat these assaults with technology alone. In order to determine what really works and what doesn't, analysts depend on real-world facts, such as incident reports, phishing tests, and user behavior patterns. This is where empiricism comes in. They utilize these data to determine who is most likely to be attacked, how attackers craft their communications, and what training techniques will really alter people's reactions. Whether they are looking into occurrences, determining why a user made a mistake, or creating new security recommendations, analysts often use social science concepts.

Application of Key Concepts

Cognitive Biases and Human Behavior

People often use cognitive biases, which are shortcuts in thinking, that attackers use to their advantage. To understand how social engineering communications are made, analysts need to know about biases including "authority bias," "scarcity," "overconfidence," and "social proof." When analysts construct phishing simulations or training material, they actively target these behavioral characteristics to educate consumers how to spot deception. According to Mark (2023) “The success rate of phishing attacks on unsuspecting individuals is attributed to a person’s failure to be vigilant and mindful of socially engineered threats when interacting in online social networks.”

Ethics and Responsibility

Ethical ideals are vital in this vocation. Analysts analyze sensitive data, do monitoring, and occasionally examine employee activities. They must consider privacy, justice, and the acceptable limitations of monitoring. Ethical decision-making guarantees that security measures do not injure people or break trust within the company.

Risk and Decision-Making

Another essential topic from class is that individuals do not perceive danger rationally. Employees may dismiss warnings, misjudge hazards, or prefer convenience above security. Analysts must consequently build methods that account for normal human characteristics. This involves streamlining processes, eliminating friction, and establishing regulations that match with real-world user behavior rather than ideal conduct.

Deterrence

The notion of deterrence—changing behavior by escalating consequences—shows up in cybersecurity regulations, access restrictions, and monitoring techniques. When logs, audits, or alarms generate a feeling that damaging behaviors will be noticed, users and insiders are less inclined to participate in hazardous or malicious conduct. Analysts assist develop these deterrence-based approaches.

Marginalization

Cybersecurity professionals need to be aware of how various marginalized groups are affected by cyber dangers. Due to social, economic, or language limitations, certain communities are more vulnerable to frauds, identity theft, and online abuse.

- Elderly persons, who are regularly targeted by financial frauds.
- People with inadequate computer literacy who may not grasp technical warnings or security measures.
- Immigrant populations, who are exposed to bogus “visa support” schemes or impersonation frauds.
- Low-income people, who may depend on outmoded equipment or public Wi-Fi, increasing the danger of breaches.

To prevent growing digital disparities, analysts must be patient, inclusive in their communication, and sensitive to cultural differences. They must make sure that instructions for training, alerts, or security procedures are understandable, accessible, and considerate of various backgrounds and skill levels. Comprehending marginalization is crucial for ensuring equitable protection and preventing inadvertent prejudice in cybersecurity measures.

Career Connection to Society

Hospitals, banks, schools, public transit, and other digital infrastructure that our society relies on daily are all protected by cybersecurity analysts. According to Maglaras, Janicke, and Ferrag (2022), critical infrastructures are “vital resources for the public safety, economic well-being and national security,” which makes the analyst’s role essential to keeping daily life running smoothly. Cyberattacks that target any of these sectors have the potential to disrupt medical equipment, reveal personal data, or undermine public confidence in large organizations. As a result, analysts are crucial to maintaining stability in daily life and ensuring that people feel comfortable using technology.

The decisions analysts make also influence how secure the internet environment seems. Their work has an impact on people's level of comfort utilizing online services and exchanging information, as well as their level of trust in technology. By ensuring that companies respect privacy and safeguard user data, analysts contribute to the development of moral and responsible digital environments. Therefore, despite the job's seeming technical nature, it also entails a significant social obligation.

Conclusion

Cybersecurity analysts handle complicated human behavior, ethical issues, and social effects in addition to managing technology. In order to comprehend user behavior, stop attacks, and advance digital safety for all communities, their work primarily borrows on social science fields including psychology, sociology, and ethics. The analyst's position becomes more crucial as the digital world becomes more linked, not just as a technical specialist but also as a bridge between people and technology.

Scholarly Journal Articles

Source 1: Dawson and Thomson (2018), *"The Future Cybersecurity Workforce: Going beyond Technical Skills for Successful Cyber Performance"*

This article emphasizes that cybersecurity professionals must understand both technical systems and human behavior. It argues that strong social science knowledge—particularly in psychology, communication, and ethics—is crucial for success. This supports the paper's argument that analysts regularly rely on social science concepts like decision-making, trust, and risk perception in their daily work.

Source 2: Mark (2021), *"An Analysis of Factors Influencing Phishing Threat Avoidance Behavior: A Quantitative Study"*

Mark's research investigates why individuals fail to avoid phishing threats, linking this behavior to social engineering tactics and personal vigilance. His findings support the paper's discussion of cognitive biases such as authority bias and overconfidence, showing how analysts use these insights to create more effective user training and simulations.

Source 3: Maglaras, Janicke, and Ferrag (2022), *"Cybersecurity of Critical Infrastructures: Challenges and Solutions"*

This article examines how cybersecurity analysts help protect critical infrastructure, such as healthcare and transportation systems, which are essential to public safety and national security. It reinforces the idea that analysts play a key societal role and highlights the broader impact of their work beyond just technology—contributing to public trust and stability.

References:

Mark, Marvin S. "An Analysis of Factors Influencing Phishing Threat Avoidance Behavior: A Quantitative Study." Order No. 28320611 Capella University, 2021. United States -- Minnesota: *ProQuest.* Web. 13 Nov. 2025.

Maglaras, Leandros, et al. “Cybersecurity of Critical Infrastructures: Challenges and Solutions.” *Sensors*, vol. 22, no. 14, 7 July 2022, p. 5105, https://doi.org/10.3390/s22145105.

Dawson, Jessica, and Robert Thomson. “The Future Cybersecurity Workforce: Going beyond Technical Skills for Successful Cyber Performance.” *Frontiers in Psychology*, U.S. National Library of Medicine, 12 June 2018, pmc.ncbi.nlm.nih.gov/articles/PMC6005833/.