Cybersecurity Professional Career Paper: Cybersecurity Anaylst

Student Name: Destin Danquah

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: DIWAKAR YALPI

Date: November 14th, 2025

Introduction

The cybersecurity profession looks at on protecting digital systems, data from unauthorize access, network, misuse, attacks, and disruption. As digital technologies keep going and it expands across industries, cybersecurity has become crucial for maintain privacy, safety, and trust online. Today's world depend heavily on digital banking, online communication, healthcare system, cloud computing, and public infrastructure, meaning a single cyber incident can use widespread consequences. This assignment will thoroughly look at cybersecurity from the perspective of a Cybersecurity Analyst, a career oath responsible for monitoring security systems, detecting threats, and responding to incidents. It will explore how social science principle apply to cybersecurity, how key concepts from this course support professional work, how cybersecurity impacts marginalized groups, and how the field connects to society. The paper will also reference scholarly journal articles to support and expand on key ideas.

Social science principles

Social science research plays a crucial role in cybersecurity because cyber threats are often driven by human motivations rather than just skillful weaknesses. Understanding behaviors like curiosity, revenge, financial gain, activism, or the desire for control helps cybersecurity analysts anticipate various hacking approaches. Ethical considerations are also relevant, as analyst must decide what is reasonable and good conduct when monitoring user behavior or investigating potential threats.

Social science principles are integrated into cybersecurity practices through areas like human and computer interactions, user behavior analysis, and communication strategies. For example, research shows that users often ignore security warnings or reuse easy passwords because they cause something more convenient than caution. Cybersecurity analysts apply these findings when improving system design or recommending new security policies.

Professionals also use social science insights to develop training programs and awareness campaigns. Examples have phishing simulations, interactive workshops, and reminders about passwords. These strategies are created around how people learn and make decisions, helping to reduce risk and prevent security mistakes.

Application of Key Concepts

Several cybersecurity concepts from this course applies directly to the cybersecurity analyst career, including the CIA triad, risk assessment, authentication, and compliance. Analyst are able to use these concepts when they are evaluating threats, identifying vulnerabilities, and protecting systems from attack.

Cybersecurity analysts apply these concepts through real world responsibilities like monitoring alerts, conducting vulnerability scans, analyzing unusual network activity, and documenting incidents. They also help make sure the organization follows the rules, laws and standards like NIST, HIPAA, GDPR, or PCI-DSS, depending on what the industry is. Compliance makes sures that proper security control are in place and that sensitive information is protected at all times.

Specific tools and techniques used in this role have security information and event management systems like splunk or Microsoft sentinels, intrusion detection system, vulnerability scanners such a Nessus, and packet analyzer like Wireshark. These tools help allow analyst to detect a threat, respond to an incident, and continuously strengthen security defense.

Marginalization

Cybersecurity impacts marginalized groups in unique ways. Individuals with little to no digital access or lower level of technology literacy may be more important to scam, cyberbullying, misinformation, or even identity theft. Elderly population, low-income communities, and non-English speakers are often targeted in cyberattacks because they may lack knowledge or resources to protect themselves.

Surveillance technology also raises concerns for marginalized groups. Certain monitoring systems may unintentionally reinforce bias, disproportionately track certain populations, or collect data without consent. Because cybersecurity involves both protection and monitoring, ethical frameworks are needed to ensure fairness and transparency.

The cybersecurity profession is working to address these inequities through different initiatives, free cybersecurity literacy programs, and policies aimed at protecting vulnerable users. Increasing representation in the cybersecurity workforce also helps to make sure that systems and policies reflect a wider range of needs and perspective.

Career Connection to Society

Cybersecurity analyst contributes to the stability and security of society by protecting crucial digital systems. Financial business, transportation networks, healthcare providers, and government agencies all rely on secure systems to move safely. Without cybersecurity professionals, sensitive personal information could be compromised, critical infrastructure could be destroyed.

Public policies and laws also shape cybersecurity practices. Regulations makes sures that organization report unauthorize login, implement security protections, and manage user data responsible. These policies help stop misuse of technology and pushes organizations to prioritize cybersecurity. As threats get technical and better each day, cybersecurity analyst plays a big role in supporting national defense, digital reliability, and public trust.

Scholarly Journal Articles

Source 1: This scholarly article looks at cybersecurity workforce readiness and tells us why cybersecurity analyst needs both strong technical skills and analytical thinking. The sources supports my paper by showing that behavioral awareness and critical reasoning are important for looking for threats and making effective security decisions in real world environments.

Dawson, Jessica, and Robert Thomson. “The Future Cybersecurity Workforce: Going beyond Technical Skills for Successful Cyber Performance.” *Frontiers in Psychology*, vol. 9, no. 9, 12 June 2018, https://doi.org/10.3389/fpsyg.2018.00744.

https://pmc.ncbi.nlm.nih.gov/articles/PMC6005833/

Source 2: The second scholarly source focuses on cybersecurity education and user behavior. It highlights that human error stays one of the biggest causes of cybersecurity issues. This supports the paper use of social science principles by allowing us to visualize why cybersecurity analysts must make and implement training programs that reduce risky behavior and improve user security awareness.

Moustafa, Ahmed A., et al. “The Role of User Behaviour in Improving Cyber Security Management.” *Frontiers in Psychology*, vol. 12, no. 12, 18 June 2021, www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.561011/full, https://doi.org/10.3389/fpsyg.2021.561011.

https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.561011/full

Source 3: This is the third article that looks at cyberthreats targeting critical infrastructures like health care systems, banking, and government networks. This source is lined to the tole of cybersecurity analyst to society by demonstrating how these professionals are able to help stop disruptions, protect public data, and maintain national stability.

Carlo, Antonio, and Kim Obergfaell. “Cyber Attacks on Critical Infrastructures and Satellite Communications.” *International Journal of Critical Infrastructure Protection*, vol. 46, 1 Sept. 2024, pp. 100701–100701, https://doi.org/10.1016/j.ijcip.2024.100701. Accessed 27 Aug. 2024.

https://www.sciencedirect.com/science/article/abs/pii/S1874548224000428?utm_source=chatgpt.com