

**Cybersecurity Professional Career Paper: Cybersecurity Analyst's Relationship to Social
Sciences**

Student Name: Thomas Gable

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/2025

Introduction

A Cybersecurity Analyst is responsible for managing and securing a company's digital environment. This can include tasks such as monitoring technology, installing security appliances, responding to incidents, educating employees, and managing risk (Staff, 2025). This is all in an effort to protect the confidentiality, integrity, and availability of computerized data. Cybersecurity is important in contemporary society because technology is continuously integrating with everyday tasks, increasing the attack surface for malicious actors. This means that companies need to harden their technology and workforce to avoid victimization, which is the goal of this field. Most people view cybersecurity as primarily a technical field, overlooking the administrative, governance, and human aspects. This paper will look to bridge that gap, delving into the relationship between the social sciences and a cybersecurity analyst. Furthermore, it will address how cybersecurity affects marginalized groups and plays a role in society.

Social Science Principles

Social science research helps reveal the cognitive and environmental factors that influence cyber attackers, victims, and professionals, showing why they take certain actions and how behaviours influence security results. This can help cybersecurity analysts optimize mitigation efforts and defenses, such as user training and policies to account for human behavioral tendencies. For example, understanding the common psychological manipulation tactics that are used in phishing attacks can help guide user training programs. It enables professionals to emphasize to employees what a malicious email might contain, such as the imitation of authoritative figures or the use of urgency to push an action. This can be taught alongside traditional phishing indicators, such as fake URLs and misspellings, to create a more holistic detection approach. Moreover, understanding behavioral patterns and human-computer interaction can help developers enhance security interfaces, such as a SIEM dashboard, which analysts use daily, making them more effective and user-friendly. Overall, pairing social science

insights with technical strategies creates a more complete and effective approach to cybersecurity.

Application of Key Concepts

One responsibility of a cyber analyst is to conduct risk assessments that evaluate the current security posture. This includes taking an inventory of all assets, identifying associated threats and vulnerabilities, assessing their likelihood and importance, and deciding on further actions (Mukhopadhyay et al., 2019). It's imperative to use the cost-benefit analysis in determining which controls to implement, if any, so the company isn't spending more than it would lose. NIST frameworks and compliance requirements guide assessments, while vulnerability scanners and risk registers detect and organize findings. Furthermore, implementing human-centered cybersecurity practices should be a priority for any cyber analyst. This means providing comprehensive, interactive training to employees, creating accessible, incentive-based reporting systems, and strictly enforcing security policies. This should be in an effort to foster a strong cybersecurity culture, where every employee takes cybersecurity seriously, understanding its impact, to protect themselves and the organization.

Marginalization

Companies with lower budgets are often not capable of acquiring cybersecurity teams or modern controls that adequately protect their digital systems, due to high costs. This leaves them vulnerable to malicious actors, especially lower-skill ones, who are looking to take advantage of easy vulnerabilities. There are many cybersecurity non-profits that are comprised of current and aspiring professionals, who are looking to help these businesses out, such as the Commonwealth Cyber Initiative Coastal Virginia (COVA CCI, n.d.). Moreover, malicious actors target lower-class individuals who don't have access to the latest technology that is properly secured and updated. It's important that those who are cyber-literate, such as professionals, push best practices via social media or community events to protect these individuals as best as possible. Lastly, the cybersecurity field as a whole is dominated by males, leaving out the

potential for diverse and innovative perspectives. Specialized scholarships and women-only cybersecurity groups can help diversify the field, creating an incentive for more women's involvement. Overall, it's pertinent that any cyber professional get involved in their communities, helping marginalized groups feel safe and included.

Career Connection to Society

A world where everything is becoming integrated with technology has given malicious actors a path to commit crimes and create havoc anonymously through the internet, using technical abilities and avoiding physical confrontation. For example, critical infrastructure now uses interconnected networks to monitor and control its systems, leaving them vulnerable to attacks from opposing countries. Online banking is on the rise, delivering hackers a low-risk opportunity for monetary gain. Social media is becoming the primary source of all news, creating a clear attack vector for hacktivists. This is why cybersecurity professionals are highly coveted, and the field is rapidly growing. They secure critical infrastructure networks, protect individuals from financial fraud, and prevent social media misinformation, creating strong and stable societal systems. Their actions are guided by regulations, laws, and requirements, such as HIPAA and NIST. However, without professionals, policies would mean nothing, making cybersecurity a requirement for society's digital safety and stability.

Conclusion

Every aspiring professional should understand the importance of social science insights in cybersecurity. Many hone specifically in on their technician skills, focusing on only a fraction of the field. Humans are widely referred as the weakest link in cybersecurity, so knowing how they are influenced better optimizes mitigation efforts. Moreover, cyber specialists hold a responsibility to positively influence the digitally illiterate around them in this increasingly hostile environment. This applies to both individuals and businesses, as attacks are becoming ever so prevalent with the emergence of advanced technology. It should be our goal to make the virtual space as secure as possible to create a stable, thriving society.

References

1. COVA CCI. (n.d.). Coastal Virginia Center for Cyber Innovation.
<https://covacci.org/>
 - a. This website gave me an overview of one cybersecurity initiative that is connected with ODU to help small businesses with digital security.
2. Mukhopadhyay, A., Chatterjee, S., Bagchi, K.K. et al. Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Inf Syst Front* 21, 997–1018 (2019).
<https://doi.org/10.1007/s10796-017-9808-5>
 - a. This gave me an explanation of a risk assessment and how the cost-benefit analysis is used with it.
3. Staff, C. (2025, October 28). *What does a cybersecurity analyst do? 2026 job Guide*. Coursera.
<https://www.coursera.org/articles/cybersecurity-analyst-job-guide>
 - a. This gave me a description of a cybersecurity analyst, stating their job duties and responsibilities.