The Role of Social Science in Cybersecurity Analysis

Khamari Phillips

Old Dominion University

CYSE201S Cybersecurity and Social Sciences

Professor Yalpi

November 14, 2025

The Role of Social Science in Cybersecurity Analysis

Introduction

As entities and governments increasingly depend on technology, cybersecurity has become an area of concern. A cybersecurity career is aimed at securing digital systems, networks, and data against threats like hacking, malware, and unauthorized entry. Cybersecurity analysts observe the systems, detect vulnerabilities, and manage the incidents. This paper delves into how social science principles influence analyst work, how vital concepts are applied, and how the profession contributes to society, supported by scholarly sources.

Social Science Principles

The study of social science is necessary to comprehend the human behaviors that define the risks to cybersecurity. Analysts use sociological and psychological knowledge in the explanation of why people commit cybercrimes. Some of the possible motives include financial gain, curiosity, revenge, and ideology. According to Khadka and Ullah (2025), patterns of human decision-making, emotional provocation, and the workplace culture play a significant role in shaping vulnerability. Social science principles also influence cybersecurity patterns related to user behavior and human-computer interaction. According to Tsauri (2025), authority cues and the pressure of a situation are some of the most frequent elements utilised by attackers. This observation explains why user awareness and communication strategy are also critical aspects of cybersecurity.

Application of Key Concepts

Risk assessment, ethics, compliance, and organizational behavior are some of the crucial concepts used by cybersecurity analysts. Analysts undertake risk assessments through the

evaluation of technical weaknesses and human factors that intensify exposure to threats. When dealing with delicate information, ethical issues play a pivotal role in that the monitoring and security processes should not infringe on user privacy and the law. Such concepts as social responsibility and critical thinking help an analyst to assess threats, make decisions, and act in response to incidents. All these concepts are applied in the form of cybersecurity measures and techniques including threat modeling, vulnerability evaluation, and behavioral analytics devices. Behavioral analytics helps to detect any unusual user behavior and make sure that the rules of data protection are adhered to through compliance structures.

Marginalization

Discriminated persons and populations face distinct cybersecurity issues. They experience such problems due to the failure to obtain secure technology, reduce digital literacy, and increase vulnerability to fall victims of scams. It also carries with it more dangers of monitoring on certain communities. Osman et al. (2023) also note that poor exposure, the absence of mentorship, and insufficient training are some of the factors of underrepresentation. The cybersecurity professionals respond to these issues by providing literacy programs, diversity, and implementing policies in an equitable manner.

Career Connection to Society

Experts in cybersecurity support such sensitive sectors as the medical sector, financial sector, transport, and the government. Their services provide security on sensitive information, they eradicate organizational downtime and their digital infrastructure is reliable. The responsibilities of the analysts and compliance of the organization are founded on the provisions of the corresponding data protection legislation and national strategies on cybersecurity. By

enhancing digital resilience, analysts contribute towards making societies stable and winning the trust of the people.

Conclusion

Cybersecurity is a profession, which is closely related to the principles of social science. These are some of the principles, which are critical in the explanation of human behavior and a threat when using digital tools. The interdisciplinary ideas allow the analyst to analyze the threats, improve security systems, and guarantee the observance of the ethical and legal requirements. The issue of marginalization is also related to cybersecurity where in this regard, there is a necessity to foster fair digital security and diversity in the field. Cybersecurity analysts are the key to the successful and stable digital society as they not only protect the vital infrastructures but also help in the implementation of the popular policy.

References

Khadka, K., & Ullah, A. B. (2025). *Human factors in cybersecurity: An interdisciplinary review and framework proposal*. *International Journal of Information Security, 24*, Article 119. https://doi.org/10.1007/s10207-025-01032-0

Osman, M. C., Namukasa, M., Ficke, C., Piasecki, I., O'Connor, T. J., & Carroll, M. (2023). *Understanding how to diversify the cybersecurity workforce: A qualitative analysis*. *Journal of Cybersecurity Education, Research and Practice, 2023*(2), Article 4. https://files.eric.ed.gov/fulltext/EJ1415204.pdf

Tsauri, M. S. (2025). *Human vulnerabilities to social engineering attacks: A systematic literature review for building a human firewall*. *Journal of Applied Informatics and Computing, 9*(4), 1127–1136. https://jurnal.polibatam.ac.id/index.php/JAIC/article/view/9585