Quinn Doak

Professor Yalpi

CYSE201S

4/14/2025

Understanding the Social Science of a Security Analyst

Security Analysts play a crucial role in protecting organizations from threats, but their job also involves understanding social behavior, risk perception, and societal impacts. In this paper, I'll be looking at how social concepts can shape the everyday responsibilities of a security analyst, as well as looking at how their work has an overall effect on society.

The Role of Social Science in Cybersecurity Analysis

Security Analysts monitor networks, investigate suspicious activity, and respond to cyber incidents. While all of these might seem technical, there's aspects that heavily relate to the social sciences. For example, psychology helps analysts predict how users might fall for phishing attacks, or how attackers utilize social engineering in order to carry out their attacks. Analysts might also recognize patterns within cybercrime, such as how fraudsters exploit vulnerable groups of people or how different groups of people might fall victim more than others, such as elderly people.

Analysts also draw from criminology, using behavioral profiling to try and detect threats in order to prevent attacks. Many security decisions aren't just based on how systems fail, but also how people fail; whether that's clicking malicious links, reusing passwords, or avoiding security protocols out of convenience. Understanding the psychological profiles and behaviors of cybercriminals is essential for threat detection and prevention. Bada and Nurse (2023) highlight that a deep comprehension of attackers' motivations and tactics can significantly enhance the

development of proactive cybersecurity measures. This human factor is a central part of a security analyst's job, and without knowledge from the social sciences, their ability to interpret risk would be incomplete (Wang, 2021).

Supporting Marginalized Groups

Security analysts need to consider how their work can affect marginalized groups. For example, phishing and fraud attacks often target older adults, immigrants, or low-income individuals who may not have as much education on how to protect themselves online. Analysts may not have a direct role in how these groups and how they interact with technology but recognizing that the bias is there can help dictate when to block scams, or what kind of alerts are prioritized. Another issue is within detection tools themselves, and how at times they can over-monitor certain groups of people.

Dynamic Interaction with Society

Public opinion, media coverage, and legal frameworks all influence how organizations might prioritize their security. For example, after a high-profile data breach, companies will often invest more money into monitoring and response tools, which can affect the workload of an analyst. At the same time, analysts shape how society responds to new threats by creating policies, reports, and risk assessments that inform law enforcement, law makers, and the public. This job also could raise some ethical concerns. Should analysts monitor communications between employees in order to prevent insider threats? How much surveillance is acceptable in the name of security? These are more than just technical questions, they require looking through a social science lens in order to balance security, privacy, and trust (Burton et al., 2020).

Conclusion

The role of a security analyst shows that cybersecurity is as much about understanding people as it is understanding machines and systems. Social science principals help analysts make informed, and ethical decisions. Their work has a wide impact on both marginalized communities and society as a whole. Analysts must be trained not just in code and tools, but also in empathy, psychology, and decision-making skills.

Works Cited

Bada, M., and Jason R. C. Nurse. *Exploring Cybercriminal Activities, Behaviors and Profiles*. 2023. *arXiv*, https://arxiv.org/abs/2308.15948.

Burton, Barbara, Martin Eling, and Alexander Richter. "The Social Side of Cybersecurity: Behavioral Factors and Risk Perception." *Journal of Cybersecurity*, vol. 6, no. 1, 2020, pp. 1–10, https://doi.org/10.1093/cybsec/tyaa005.

Wang, Dong. "Cognitive Biases and Decision-Making in Cybersecurity Incident Response." *IEEE Access*, vol. 9, 2021, pp. 17763–17776, https://doi.org/10.1109/ACCESS.2021.3053172.