Cybersecurity Career

Juan David Restrepo Gomez

CYSE201S

Matthew Umphlet

01 Aug 2024

Cybersecurity Analyst

Cybersecurity analysts are the first line of defense in a company's security system due to the multiple roles task that this role has to perform. Like monitoring the network, respond to cyber threads, making sure that classified information stays safe. The connection between cybersecurity and social science is much observed frequently due to most of threads are made by human behavior, social trends, difference of culture. This paper explores how this career needs social science research and principles, with the attention on marginalized groups and society in general.

In the principles of social science in cybersecurity analysts can found the human behavior and social engineering, by understanding how humans behave anticipation can be performed allowing analyst to counteract social engineering attacks. As we learned in class, social engineering is employed by the manipulating individuals, with the outcome of people reveling personal information. With the help of social psychology, analyst can build effective security measurements like training that address the cognitive biases and social triggers exploited by attackers. For example, conducting research on the psychology of influence can help recognized methods of phishing attacks, such as urgency, and reciprocity. Analyst can develop plans to

show awareness to the personal to recognize and resist these social engineering attacks (Cialdini, 2007). Another principle of social science in cybersecurity analyst to consider is sociocultural awareness and diversity, as the world is more connected than ever, the difference of communication and culture norms play a big role in today's society, developing inclusiveness and good security practices is fundamental specially when addressing the security needs of marginalized groups, who may face unique threats and vulnerabilities. For instance, analyzing the digital behaviors of different demographic groups can reveal specific security challenges they may face (Solove, 2008). Like being more susceptible to certain types of cyber threats due to economic disadvantages or lack of access to cybersecurity education. Finally, ethical principles and legal frameworks are the base of a cybersecurity analyst. Social science research on ethics provides deep understanding into moral reasoning and ethical decisions-making. Analyst must take complex choices between privacy rights and security needs. For example, The General Data Protection Regulation (GDPR) in the European Union emphasizes the ethical handling of personal data. Cybersecurity analysts must ensure compliance with such regulations while maintaining robust security measures, while making informed decisions that respect individual rights and societal values (Nissenbaum, 2010).

The material from the class in relation with cybersecurity analyst allows us to apply the usage of risk Assessment and management, utilizing risk assessment identifying, analyzing risks to the organization. Social science principles allows the understanding the behaviors and habits of the employees associated with the risk to the company (Pfleeger et al., 2012). Also, applying incident response and crisis management improves the coordination and communication between stakeholders, with social science research on group dynamics and crisis management informs

how analyst and collaborate during cybersecurity incidents (Trompeter & Scholtz, 2020). Lastly, with the help of educational psychology and learning theories, analysts can benefit by providing training that engages all employees to reinforce good security habits, and address common misconceptions.

The impact on marginalized groups and society relates to this career due to the great responsibility to protect not only their companies but also the whole society and marginalized groups, these groups often face disproportionate risks in the digital landscape, making it essential for analysts to consider their unique needs. For example, research shows that marginalized communities are more likely to be targets of cyber harassment, identity theft, and fraud. By applying social science research, analysts can develop targeted interventions to safeguard these vulnerable populations (Solove, 2008).

Conclusion

In today's society, social science research and principles are paramount to cybersecurity analysts to understand and mitigate cyber threads. By incorporating insights from social psychology, cultural studies, ethics, and legal frameworks, analysts can develop comprehensive security strategies that address the human and societal aspects of cybersecurity. These approach, not only benefits the security measurements executed but it leads to a safer digital world and more equitable for everyone, including marginalized groups.

References

-*Cialdini, R. B. (2007). Influence: The Psychology of Persuasion. Harper Business.*

-Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books.

-Solove, D. J. (2008). Understanding Privacy. Harvard University Press.

-Trompeter, B., & Scholtz, T. (2020). Cybersecurity and its ten domains. Wiley.

-Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2012). Security in computing (5th ed.). Prentice Hall.