Cybersecurity Analyst - Career Paper

Amari Fisher

CYSE 201S

11/24/2024

Introduction

In today's world, cybersecurity is a crucial element toward ensuring digital security remains in top shape. Without cybersecurity, information is ripe for the taking and criminals would use that information to do things like ransomware, steal identities, and much more. There are many roles within the cybersecurity workspace, but today I will specifically be talking about the role of a Cybersecurity Analyst. Cybersecurity Analysts are responsible for detecting and managing cyberattacks to sensitive information and systems. Although their work heavily involves the technical aspect of cybersecurity, the often overlooked social aspect of cybersecurity is also a key part to succeeding in this job. This paper intends to explore how Cybersecurity

Analysts rely on social science principles to help analyze and mitigate threats. It will include the concepts of social engineering, social theories, economic theories, cultural awareness, and showcase how this career relates to society in general.

Significance of Social Science

Social science is a key part of cybersecurity as a whole, and in particular cybersecurity analysts leverage their social science knowledge to help identify which groups would be more inclined to attack other groups, and the reason for particular attacks. Common social science principles like social engineering, social theories, and economic theories are used to explain why a cybercriminal/organization would do something or not. Social engineering refers to the principle of being able to use skills like charisma, and certain tactics to make someone trust and believe in what you are saying. Did you know that "84% of cyber-attacks are conducted by social engineers with high success rate" (Salahdine, 2019) Social engineering is one of the biggest ways cyberattacks occur, by human error and a too trusting staff. However, cybersecurity analysts can also leverage social engineering by pretending to be peers or people participating in a hacking group chats. They do this through "honeypots" which are "A sacrificial computer system that's intended to attract cyberattacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets"(usa.kaspersky.com) and are used by cybersecurity analysts to lure people into trying to access or manipulate a website, in fact, sometimes cybersecurity analysts keep seized websites running to ensure as much information of the offenders as possible is retrieved. Social theories are a collection of theories used to identify why people might do something, but they can also be applied to cybersecurity because

cybercriminals often fall under these categories of social theory. One particular way they leverage social science is through motive identification like discussed in Module 10. Additionally other principles like behavioral analysis are used by cybersecurity analysts to detect suspicious activities or behavior committed by people. Economic theories are often theories applied to businesses and organizations that demonstrate how organizations work to ensure the greatest amount of money is made, the main economic theory that is used by organizations that rely on cybersecurity is the Costs/Benefits theory which weigh benefits and costs meaning that security may be leveraged against the potential cost of applying the correct security principles. “In fact, many of the problems plaguing cybersecurity are economic in nature, and modest interventions..”(Moore, 2010)

Sociology/Marginalized Groups and Cultural Awareness

Cybersecurity Analysts must also identify how cyber threats often attack marginalized communities because these groups often lack the resources and education to deal with certain attacks, making them more vulnerable to things like phishing attacks and malware. Analysts often use sociology research to identify possible vulnerabilities and push for security measures against them, In fact, women and minorities are also more likely to be targeted for cyberattacks because of the often inexperience when dealing with such attacks and potential vulnerability (insuregood.org) As the world becomes more globalized, Cybersecurity Analysts have to navigate cultural differences when implementing security measures. Social science principles allow analysts to create policies that adhere to many different cultures, additionally, ethical decision making is a must in social science because it is crucial to balance security and people’s

rights. Cybersecurity Analysts often have to keep in mind the ethics of something like data collection or monitoring when creating policies to ensure both security and ethical agreements are followed.

Societal Impact/Challenges

As mentioned above, cyberattacks often target marginalized or vulnerable groups which lead Cybersecurity Analysts to often face the challenge of combating these cyber attacks that disproportionately affect these groups. Analysts typically advocate for policies that ensure everyone has access to the knowledge and tools necessary to ensure their own digital safety. Moreover, the societal impact of a Cybersecurity Analyst isn't just through preventing data breaches and other attacks. By creating trust in digital systems, Analysts contribute to the broader security of the entire nation and lead toward building a more safe and more secure digital society. This showcases the importance of social science in cybersecurity and society as a whole.

Conclusion

In conclusion, the role of a Cybersecurity Analyst demonstrates the importance of both the technical and social aspects of cybersecurity. By applying principles of psychology(theories), sociology, and ethics. Analysts address the human aspects of cybersecurity, and their work doesn't only protect individual systems but contributes to the overall security and safety of the world as a whole. As cyberthreats continue to evolve and bypass new security measures, the

combination of social science and cybersecurity will remain essential toward finding solutions to those new threats, showcasing the importance of an interdisciplinary approach to cybersecurity.

References

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and mathematical organization theory*, *26*(4), 365-381.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future internet*, *11*(4), 89.

insurgegood.org. (N.D) Cyber Attacks – Women and Minorities are Top Targets. https://insuregood.org/cyber-attacks-women-and-minorities-are-top-targets/

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3-4), 103-117.