

Shawn Ziegler

CYSE 201S

4/12/25

Course Paper

Cybersecurity Analyst

Introduction

The roles of cybersecurity analysts can vary depending on the industry and the specific company in which they work. However, all cybersecurity analyst positions involve monitoring threats as well as computer systems and networks. A cybersecurity analyst is responsible for ensuring that both hardware and software are up to date. This includes monitoring file access and maintaining firewalls, along with implementing necessary network updates. If a breach occurs, a security analyst will collaborate with their team to assess the impact and risks in order to resolve the issue.

Social Science Principles

The cybersecurity analyst role encompasses various skills that we have discussed in class, including vulnerability assessment, incident response, risk analysis, and risk management. In this career, analysts develop plans and technologies to protect computer files and data from cyber threats and malware (Duvall, n.d.). During our discussions, we explored social engineering techniques that involve manipulation and psychological tactics to persuade individuals to share personal information or perform certain actions. By analyzing communication through social

media and understanding human interactions, specialists can better prepare themselves to combat cyber threats and maintain a secure environment.

Cybersecurity specialists can use motive identification as a valuable tool, applying social science techniques to uncover the root causes of cyber-attacks and identify the attackers' intended targets (Carly, 2020). This information is essential for developing effective defense strategies and managing the consequences of cyber threats. In today's world, where misinformation is prevalent in the field of cybersecurity, incorporating social science research is critical. For example, inaccurate information circulating on social networks can cause significant harm, and differing beliefs and traditions can lead to community divisions. By leveraging social science research, we can mitigate the spread of fake news and promote critical thinking (Duvall, n.d.).

Phishing, a method of social engineering, has significantly increased security vulnerabilities for marginalized groups facing social and economic challenges. Individuals with limited technological awareness are particularly at risk of cyber-attacks, making them more vulnerable (Khando et al., 2021). As we discussed in class, it is essential to invest in training programs rather than solely relying on technology. This approach is more cost-effective, as it equips individuals with the knowledge and skills necessary to combat cyber-attacks. Furthermore, investing in training provides greater versatility compared to technology, which often follows a one-size-fits-all model.

Conclusion

The role of a cybersecurity analyst involves protecting an individual or organization's information by monitoring networks and security systems. It is crucial for analysts to keep firewalls and network systems updated to ensure smooth operations within the company. Being detail-oriented is an essential skill, as it enables analysts to identify minor details that may significantly impact the situation at hand. Moreover, analysts must be capable of thinking ahead

based on existing data and information, allowing them to provide feedback and make effective recommendations for handling various situations. The development of strong analytical and technical skills, and having good communication skills, allows the analyst to resolve a breach or cyberattack as efficiently as possible. As a cybersecurity analyst, it involves handling situations as a team. If one person is not knowledgeable on a certain issue, there are others on the team who will either have the knowledge or provide insight on how to handle the situation at hand.

Sources

Alassad, M., Spann, B., Al-khateeb, S., & Agarwal, N. (1970, January 1). *Using computational social science techniques to identify coordinated cyber threats to Smart City Networks*. SpringerLink. https://link.springer.com/chapter/10.1007/978-3-030-64217-4_35

Carley, K. M. (2020, November 16). *Social Cybersecurity: An emerging science - computational and mathematical organization theory*. SpringerLink. <https://link.springer.com/article/10.1007/s10588-020-09322-9>

Written by Cybersecurity Guide Contributors – Last updated: February 28. (2025, February 28). *Become a security analyst: Skills and steps*. Cybersecurity Guide. <https://cybersecurityguide.org/careers/security-analyst/>