Cybersecurity Professional Career Paper: Security Analyst

Student Name: Stephen Price

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Sciences

Instructor Name: Professor Diwakar Yalpi

Date: November 16, 2025

Introduction

A security analyst is someone who protects a company's computer networks, systems, and data from cyber-attacks by monitoring suspicious activity, detecting vulnerabilities, and responding to incidents by implementing security policies or security measures that can help minimize the likelihood of a company being at risk. Security analysts have become a vital component in the modern world because they serve as the first line of defense in protecting companies from data breaches that can result in financial loss and damage their reputation. This paper will cover the role security analysts play in cybersecurity and how it integrates social science principles, key social science concepts, marginalization, and how it contributes to our society.

Social Science Principles

Social science research in psychology and sociology is important for understanding why people engage in cyber-attacks. It's also important in understanding the motivations of why cybercriminals engage in cyber attacks for financial gain, thrill seeking, and hacktivism. These motivations can help security analysts predict attack vectors and resource allocation. Social science principles are integrated into cybersecurity practices like Human Computer Interaction (HCI) and User Behavior Analysis (UBA). Security analysts use HCI principles to design security systems that are simple and recognize that complexity can be the enemy of security. UBA allows security analysts to detect anomalies that signal compromised accounts or insider threats. Security analysts also use social science principles to develop strategies for cybersecurity awareness and education by designing phishing simulations and training programs. For example, security analysts have training activities that make the person engage more so that they gain understanding organizational culture on cybersecurity behaviors.

Application of Key Concepts

The key concepts that I learned in class relate to how security analysts use a structural functionalism approach and Maslow's hierarchy of needs. Structural functionalism is applied to security analysts as a system for a company where every component has a role to play to protect from cyber-attack. If one component gets at risk it disrupts the system which won't ensure confidentiality, integrity, and availability (CIA Triad). Structural functionalism is also used by security analysts to implement security measures to help the company have a strong security posture and to maintain stability. Security analysts can also apply Maslow's Hierarchy of Needs to look at insider risks. An employee whose needs are not met can motivate them to engage in cybercrime and put the company at risk.

Marginalization

Cybersecurity can affect marginalized groups like low-income populations or disabled people with issues like unequal access to technology, increased targets, and surveillance. People with low income most of the time use old technology due to not having enough money to upgrade which can make them more vulnerable to data breaches due to lack of updates and compatibility issues. Also, people who have visual or cognitive disabilities may have trouble with complex CAPTCHA or implementing two-factor authentication which can make them more likely to be at risk of a data breach. Security analysts are addressing these challenges by creating a protocol for disabled people that promote multi factor authentication that can accommodate different physical and technical capabilities.

Career Connection to Society

Security analysts are the frontline defense for critical infrastructure which where the systems are so important in our society that if it's affected it would affect national security, economic stability, and public health. Security analysts protect financial systems like banks from ransomware and fraud to ensure safe transactions and consumer trust. They also protect healthcare systems like hospitals by protecting patient's health records from data breaches that could shut down patient care. This would violate the CIA triad's Confidentiality and Availability which would put patient data at risk of being exposed. Security Analysts are heavily influenced by public policy and have major societal implications. Policies like European Union's GDPR or the US CCPA mandate data handling and data breach procedures. Security analysts must interpret these laws and translate them into technical security controls and make sure they align with the organization's procedures. If security analysts fail to comply with this it can result in them getting fines, but these policies reinforce citizen rights to digital privacy and control over their own data which Security Analysts must protect the social contract of digital trust.

References

Mitropoulos, S. I., Kumar, D., & Pang, K. (2023). Teaching Social Science Aspects of Information Security. Journal of Cybersecurity Education, Research and Practice, 2023(1).

Renaud, K., & Smith, J. (2022). Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. Frontiers in Computer Science, 4.

Roberts, R. E., & Smith, J. R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Frontiers in Psychology, 9.