Cybersecurity Professional Career Paper: Breakdown of an Information Security Analyst

Student Name: Jared Peel

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Yalpi

Date: 4/15/2026

Introduction

An Information Security Analyst protects computer networks, data, and systems from cyberattacks and unauthorized acess for companies and organizations. They also hold responsibility for the monitoring of encryption software, firewall installations, holding testting for vulnerabilities to limit the threats, security breaches, and policy development to mitigate risks. Threats in the cybersecurity industry are growing and evolving, and these analysts are critical to the cyber world by protecting what is necessary. This paper will focus on the social science aspect of this career, and how it relates to cybersecurity and each other, making sure there is relevance.

Social Science Principles

Relating to an information security analyst, social science research is basically an extension to understanding human behavior online, which happens to be very important in this field. Criminology and psychology research display several mindsets and reasons why hackers do the things they do and what drives them, such as circumstances, recognition, curiosity and much more. Vulnerabilities such as trust issues and exploits are also identified by social science. The point being understanding human behavior has the same importance as understanding systems. Social science is integrated into the field very efficiently. The psychological effect is already there without the practice of it intentionally, such as requiring strong passwords and managing them correctly. Analysts identify study patterns in how ussers acess data, respond to emails, and log in to see if the account has been compromised (unauthorized access). Tools must be user friendly and are designed to be so users can work to the best of their ability without frustration. Some education and awareness displayed in the field are training to counter and respond to attack correctly. Targeted education is even used if a certain group has a higher risk of encountering a vulnerability, making sure they are prepared to deal with the threat.

Application of Key Concepts

Some key concepts from class are human factors and causes of human behavior. Analysts do not always follow instructions to the core, and some errors can come from this, an example being designed authentication for a user but instead of single, they use multi-factor and mess up the authentication. There are many human factors that take place in analysts, such as their capabilities, limitations, and behavior that are used to provide security that can come in many forms based off position, circumstance, and ability. Tools and techniques that are used are penetration testing which simulate attacks to test weaknesses in the system which go back to the human who designed it. Behavior analytics to identify weird movements. Splunk is a great tool which has proved efficient.

Marginalization

In cybersecurity, marginalized groups are impacted more because of the larger number of inequalities that exist in the industry. Communities that have low-income individuals or rural environemnts lack access to reliable technology, which makes them more vulnerable and a decent target to cyber threats. Groups who also lack education and resources do not have the awareness of safe practices online. Information security analysts must identify and address the differences when doing their job. Certain populations cannot have their privacy invaded or be discriminated against unfairly. It is very important for risk assessment to be considered across all demographics has different groups face different risks. Inequality reduction and protection improvement are being worked constantly in cybersecurity fields. Efforts such as bringing diversity into the field to gain different perspectives are being done. The importance of equal security policies is focused on, and accessible tools are spreading so even limited skilled users can achieve the same goals all cybersecurity individuals have. “Organizations have developed

various initiatives and programs to address these issues and promote diversity within the field of cybersecurity. One such initiative is the Cybersecurity Education Diversity Initiative (CEDI), created by the Center for Academic Excellence (CAE)" (Bowcut 2).

Career Connection to Society

Cybersecurity professionals contribute to societal infrastructure stability in several ways. Banks have their online transactions and systems protected from cyber-attacks, and fraud is prevented. Patient data is secure, and medical records are protected from breaches.

Articles

In this source https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-1, I was able to gather defintions about an analyst and the benefits the job has.

This article https://identitymanagementinstitute.org/psychology-of-cybersecurity-and-human-behavior/ , assisted me in identifying differences in the field and the incorporations of social science in cybersecurity, mainly focusing on human behavior.

This article https://cybersecurityguide.org/resources/diversity-equity-inclusion/ , also helped me with finding diversity in the field, but really emphasized issues within the industry and why society does not practice cybersecurity to the highest degree.