Cybersecurity Professional Career Paper: Cybersecurity Analyst

Student Name: Chase McKnight

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 04/14/2026

Introduction

I am most interested in the career of a cybersecurity analyst. These professionals help protect systems, networks, and data from cyber attacks. As more of our lives move online, cybersecurity has become even more important. Businesses, governments, and individuals all depend on secure systems to function safely and efficiently. In this paper, I will explain how social science relates to the work of a cybersecurity analyst, how these ideas are used in real life, and how this career affects the world, especially for marginalized groups.

Social Science Principles

Cybersecurity is not only about technology. It also relies on understanding how people think and act. Social science research helps analysts figure out why people commit cybercrimes and how users behave online. For example, hackers often use social engineering, which means tricking people instead of breaking into systems directly.

Analysts use ideas from psychology and sociology to look at patterns in how people behave, like why someone might click on a phishing link or use a weak password more than once. These understandings help them design better training and security systems. By knowing people's actions, cybersecurity professionals can lower risks and make security stronger.

Application of Key Concepts

Some key ideas from class connect directly to cybersecurity jobs. One is the routine activities theory, which says crime happens when a motivated offender finds a suitable target and there is no one to stop them. Analysts act as guardians by watching over systems and stopping attacks.

Another idea is social learning theory, which means people learn by watching others. At work, if some employees ignore security rules, others might do the same. Analysts try to build a culture of security by promoting safe habits.

Analysts use these ideas every day when they look for risks, watch over systems, and respond to threats. They also use tools for example firewalls, security detection systems, and security awareness programs to put these concepts in practice.

Marginalization

Cybersecurity has a big impact on marginalized groups. For example, older adults or people in low-income communities might not have as much access to technology education, which makes them more likely to fall for scams or cyberattacks. Attackers regularly target these groups because they think they are easier to trick.

Cybersecurity professionals need to think about these problems and aim for protection that includes everyone. This means making security tools easy to use, helping people learn more about technology, and making sure everyone is protected online. Bringing more diversity to the cybersecurity field also helps find better solutions to these problems.

Career Connection to Society

Analysts help protect critical systems such as banks, hospitals, and government networks. Without their work, these systems could be attacked more easily, which could cause problems like losing money or having personal data stolen. They also have a role in cybersecurity. Regulations help ensure that organizations follow proper security practices and secure user data. Cybersecurity professionals work within these rules to maintain safety and faith in digital systems. Their work helps keep society stable and secure in an ever more digital world.

Scholarly Journal Articles

Source 1:
Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress*.
This source explains how cybercrime works and how theories like routine activities theory apply to online crime. It supports the idea that cybersecurity analysts act as guardians to prevent attacks.

Source 2:
Verizon. (2023). *Data Breach Investigations Report*.
This report provides real-world data on cyberattacks, showing how human error, like clicking phishing links, plays a major role. It supports the discussion of social science principles and user behavior.

Source 3:
National Institute of Standards and Technology (NIST). (2020). *Cybersecurity Framework*.
This source explains how organizations manage cybersecurity risks and protect systems. It helps connect the career to society and shows how professionals apply key concepts in real-world situations.

.