# Cybersecurity Professional Career Paper: Ethical Hacker

Student Name: Cerezo, Mason

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Yalpi, Veereswara Lakshmi Diwakar

Date: November 13, 2025

## Introduction

This paper's purpose is to inform readers on how ethical hackers use social science research and principles in their work. Companies and businesses are susceptible to data breaches and cyberattacks daily from hackers and cyber criminals alike. Cybersecurity measures are in place to prevent these attacks from happening; the role of an ethical hacker, also known as a white hat hacker, is crucial to implementing these measures. Ethical hackers use the same techniques as malicious hackers, but with the motive to test the systems defences. Their work involves identifying vulnerabilities to fix them before malicious hackers can exploit these weaknesses. Key concepts learned from class will be discussed as well as how this career interacts with marginalized groups and society as a whole.

## Social Science Principles

Social science principles play a significant role in ethical hacking since cyber threats are driven by human behavior rather than technology alone. Understanding human behavior can help you understand how individuals might act under certain circumstances. For example, social engineering, one of the most common types of hacking used in cyberspace, relies on exploiting a person's weakness or psyche rather than technical vulnerability. Most cyberattacks succeed because of human error, not technical failures (CISA, 2021). By understanding vulnerabilities caused by human behavior, ethical hackers can design better practices and security systems.

Social science research also helps with ethical decision making in cybersecurity. Ethical hackers often face challenges when testing system defenses or handling sensitive data. Principles from sociology and psychology allow them to simulate realistic attacks that make it easier to identify weak points in a system. Additionally, studies in human-computer interaction help ethical hackers develop interfaces and authentication systems that align with user behavior,

reducing accidental vulnerabilities. As such, social science makes cybersecurity not just a technical challenge, but a social one as well.

## Application of Key Concepts

The principle of relativism helps ethical hackers understand how cybersecurity threats are shaped by social systems which in turn create vulnerabilities. They must be objective and use parsimony when making decisions based on evidence presenting simple, clear explanations for how attacks succeeded. Empiricism is a core principle to ethical hackers because penetration tests rely on observable evidence such as logs, system responses, and user behavior rather than assumptions.

Finally, determinism and skepticism guide ethical hackers in understanding why people engage in risky digital behavior and in questioning every system or claim they encounter. Determinism helps them recognize patterns so they can simulate realistic attacks. Skepticism ensures they test systems thoroughly, questioning every assumption and exploring hidden human and technical weaknesses. Together, these principles show that ethical hacking is not only a technical career but also one deeply connected to the scientific study of human behavior and society.

## Marginalization

Cybersecurity analysts must also consider how cyber threats and security measures designed to counteract them affect marginalized groups. According to a report by Pew Research Center (2022), individuals from lower income communities are at higher risk of identity theft and online fraud due to the lack of cybersecurity awareness. Cybersecurity analysts as well as ethical hackers use this type of research to create inclusive strategies and measures to allow individuals from all backgrounds to understand and have access to these resources.

## Career Connection to Society

Ethical hackers must maintain ethical neutrality when conducting research on individuals or analysing human behavior. This is the same with ethical hackers; they must follow strict ethical guidelines as well as rules that are put in place by the companies that hire them in order to prevent causing accidental damage to data systems. With these measures in place, ethical hackers contribute to societal infrastructure by identifying and fixing security vulnerabilities before malicious hackers can exploit them for all systems that hire them.

## Scholarly Journal Articles

**Source 1:**

The CISA report states that the majority of successful cyberattacks begin with social engineering rather than technical exploitation. It explains that attackers rely on psychological manipulation, emotional triggers, and deception to trick individuals to reveal sensitive information. Ethical hackers must understand these human behaviors and why they fall for these types of exploitations.

**Source 2:**

The Pew Research Center supports the social science principles throughout this paper by presenting evidence about how different groups in society perceive cybersecurity risks and experience cybercrime. Individuals with lower income, limited digital literacy, and the elderly are likely to experience identity theft and scams due to the lack of cybersecurity awareness. This article also suggests that people's trust in technology and their confidence in managing digital risks vary significantly depending on socioeconomic status, age, education, and access to resources. This information reinforces the fact that marginalized groups and social principles need to be included in security strategies made by analysts.

**Source 3:**

This source contributes to understanding how cybersecurity careers connect to society by demonstrating that insider threats are deeply rooted in human, psychological, and organizational factors. The National Institute of Standards and Technology (NIST) clearly outlines how emotional stress, job dissatisfaction, and social isolation can influence an individual to engage in cybercrimes. The source shows that cybersecurity analysts must examine internal social systems to protect organizations and other individuals.

## References

CISA. (2021). *Security Tips: Recognizing and Avoiding Email Scams*. Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov

Greitzer, F., & Frincke, D. (2010). *Combining Traditional Cybersecurity Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation*. National Institute of Standards and Technology (NIST). https://www.researchgate.net/publication/227064429_Combining_Traditional_Cyber_Security_Audit_Data_with_Psychosocial_Data_Towards_Predictive_Modeling_for_Insider_Threat_Mitigation

Pew Research Center. (2022). *Americans and Cybersecurity: Attitudes and Experiences*. https://www.pewresearch.org