

Cybersecurity Professional Career Paper: Penetration Tester

Student Name: Zack Fok

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 4/14/2026

Introduction

The cybersecurity industry refers to the protection of computers, networks, and data from attacks via the Internet or other digital means. The expansion of the use of digital technology and our reliance on it will ultimately change the virtual landscape to a point where those who work in cyber security are critical to keeping our privacy, our financial security and our countries safe. We see that the use of ransomware and phishing attacks and the consequences of such attacks speak to the need for individuals with the skills to identify and address vulnerabilities in our systems. This paper will address the social science principles associated with cybersecurity; the real-world implications of the key concepts associated with cybersecurity; the impact of cybersecurity on marginalized groups; and how a career in cybersecurity, most specifically penetration testing, positively impacts society. All ideas presented will be supported by scholarly research.

Social science principles

Cybersecurity relies heavily on social science; many cyberattacks exploit human behavior. For example, cyber security experts are trained to think like hackers to anticipate how people could exploit systems. This is the same logic behind penetration testing; security professionals must understand both human behavior and the behavior of those who would seek to attack. Another factor is that security decisions are not based solely on technology, but also on interpersonal and human judgment. By showing that security is shaped by the needs of the stakeholders and involves negotiation and risk assessment; it shows that both psychology and sociology influence the practice of cybersecurity. Furthermore, research showing how members of the public react to cyber threats illustrates how awareness can create fear and ultimately impact the behavior of individuals. For example, while exposure to a cyberattack may create fear

in the public at first, continued exposure may lead to a reduced emotional response through desensitization over time. This demonstrates how human perception can alter an individual's behavior and ultimately lead to a difference in cyber security outcomes. For penetration testers, these insights are important in creating realistic attack simulation exercises and improving security awareness training by factoring in the human element. By being able to showcase what the vulnerability is to the stockholders or owners of the company, they can help alleviate some of that company's fear of being targeted through open vulnerabilities.

Application of Key Concepts

Risk assessment, ethical responsibilities, and decision making are three key elements of successful employment in the field of Cybersecurity, and especially in penetration testing. In one of the articles, Cybersecurity professionals evaluate risk based on two criteria: the nature of the potential attack, and the expected probability of the risk occurring. In penetration testing, or even in ethical hacking, this risk-based evaluation provides a framework for deciding how to exploit and report vulnerabilities. Research shows that Cybersecurity compromises between cost, usability, and protection, meaning that organizations need to weigh these competing factors when establishing their security controls. This shows us that security may not be as absolute as we would like to believe but rather is based on individual circumstances and priorities. The article also discusses the importance of legal and ethical principles as "good faith" security research must be done without causing harm to any individuals and used strictly for the purpose of improving system security. This directly affects penetration testing, as ethical hackers must follow an established set of ethical guidelines when testing for vulnerabilities; if they go beyond the scope of what they're supposed to, they can get into legal trouble and be classified as a black hat hacker. All these principles can be applied through various tools that Cybersecurity

professionals use to identify and remediate risk, including vulnerability scanning tools, penetration testing framework tools, and security audit tools. Some notable tools include Kali Linux, John the Ripper, and NMAP.

Marginalization

Marginalized communities could be disproportionately impacted by cybersecurity issues, due to differing levels of access, education and resources, which can make them more vulnerable to attacks by means of phishing or other types of scams if they have less digital literacy. Research has shown that cyber threat events can impact the public's perception and emotional response; potentially creating increased levels of fear and anxiety about themselves or their country. In a penetration testing view, if companies don't find someone to properly expose their vulnerabilities so that they may fix them; it can lead to a data breach. This would not only ruin the company's reputation but diminish trust in the public view. The effects may well be amplified in communities already facing social and/or economic disadvantages. Furthermore, existing laws and protections regarding cybersecurity do not necessarily protect all researchers or individuals in their work. The article tells us that even in the case where ethical security researchers use social engineering techniques to aid cybersecurity solutions, they will often find themselves exposed to legal risks via the DMCA or CFAA. This creates an obstacle that will likely discourage individuals from participating within cybersecurity, contributing to underrepresentation. Many groups and organizations are working to overcome these obstacles through diversity initiatives and developing more inclusive policies within their organizations.

Career Connection to Society

Cybersecurity experts are critical for safeguarding society's key systems in the health care, financial, and government sectors of our economy. Through penetration testing, you are able to

strengthen that further by showing companies exactly what they're missing. A strong cybersecurity posture is a prerequisite to prevent those systems being compromised through interruption, sabotage, and theft. There are many repercussions associated with cyber intrusions or attacks such as devastating damage to key infrastructure, theft of sensitive information , disruption of essential services . These illustrate the need for professionals who defend against & respond too such attacks. Security researchers as playing a critical role in discovering vulnerabilities that need to be fixed and making systems more secure by providing solutions to improve system security. Furthermore, they have established a firm case for expanding legal protections around security research work. Penetration testing provides organizations with the ability to identify vulnerabilities before they are exploited by malicious actors and therefore assist organizations in strengthening their overall security posture, in complying with applicable laws and furthermore, in maintaining public trust. In conclusion, not only are Cybersecurity experts are an invaluable resource to maintain a stable & safe digitized world, but penetration testers are apart of a key foundation in keeping other's data and company's businesses safe.

Scholarly Journal Articles

Source 1:

This article focuses on the legal challenges faced by cybersecurity researchers. It explains that even ethical hacking can carry legal risks under laws like the DMCA, though exemptions exist for "good-faith security research" . This is highly relevant to penetration testing, where professionals must operate within strict legal boundaries.

Source 2:

This study examines how cybersecurity professionals think and work in practice. It highlights the importance of risk assessment, stakeholder communication, and thinking like an attacker . This directly supports the application of social science principles and key concepts in cybersecurity careers.

Source 3:

This research explores how the public responds to cyber threats, showing that awareness can

increase concern but may also lead to desensitization over time . This supports the importance of understanding human behavior in cybersecurity and its societal impact.

Reference

Rampášek, M., Andraško, J., Sokol, P., & Hamulak, O. (2026). Hunting for vulnerabilities: call for European protection of security researchers. *Journal of Cybersecurity*, 12(1). <https://doi.org/10.1093/cybsec/tyag002>

Weir, C., Rashid, A., & Noble, J. (2020). Challenging software developers: dialectic as a foundation for security assurance techniques. *Journal of Cybersecurity*, 6(1). <https://doi.org/10.1093/cybsec/tyaa007>

Maréchal, L., Mermoud, A., Percia David, D., & Humbert, M. (2025). Are cybersecurity firms different? Intra-sector and cross-industry comparisons of financial performance. *Journal of Cybersecurity*, 11(1). <https://doi.org/10.1093/cybsec/tyaf032>