Cybersecurity Professional Career Paper: Penetration Testing

Chandler Aiden West

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

11/14/2025

Introduction

Cybersecurity is all about protecting data and systems online. As people rely more on technology for everyday tasks, protecting this information has become extremely important. Penetration testers, often called “ethical hackers,” help organizations stay safe by finding weaknesses in systems before real attackers do. This paper explains how their work is closely connected to the social sciences. It also explores how this career impacts society and uses research to guide safer digital practices.

Social science principles

Although penetration testing sounds very technical, it often depends on understanding people. Social science research helps explain why individuals might break into systems. It could be for money, curiosity, or their own beliefs. It also helps professionals understand why people make mistakes online, like clicking on phishing links or using bad passwords. These human behaviors are a major cause of cybersecurity problems. Penetration testers must pay attention not only to computer systems but also to how people think and respond. For example, when testing an organization, a penetration tester might send a phishing email to see whether employees fall for a scam. This is called social engineering, and it is based on understanding trust, communication, and human habits. It is important to know how people interact with technology because it helps testers design better training programs, clearer warnings, and safer systems.

Application of Key Concepts

Some ideas from the social sciences directly shape the work of penetration testers. Concepts such as risk perception, decision-making, and organizational teams help testers understand how a workplace handles safety. For example, if employees believe that security slows down their work, they may ignore important rules, such as using an easy password to type.

This in turn makes the organization more vulnerable. Penetration testers use these insights when they examine both technical issues and the behavior of the people who use those systems. They also need to follow laws and regulations that protect sensitive information, especially in sensitive areas like healthcare or finance. This means they must understand not just technology but also cybersecurity policies and ethics. Professionals in this field use many tools to test whether an organization is protected. Some examples include simulated attacks, fake phishing messages, and exercises where a team pretends to be real hackers. These tools show how people react in real situations and help organizations strengthen their defenses.

Marginalization

Cybersecurity problems don't affect everyone equally. People who have less experience with technology are often more vulnerable to scams and identity theft. Low-income communities may also lack access to strong security tools, putting them at greater risk. In some cases, marginalized groups have more surveillance or have their data collected without clear knowledge. Penetration testers and cybersecurity professionals are increasingly aware of these inequalities. Many organizations now support efforts to diversify the cybersecurity workforce and ensure that cybersecurity is fair and accessible. By understanding the challenges different groups face, professionals can design safer systems that protect all individuals.

Career Connection to Society

Penetration testers help keep society running safely by protecting important systems like hospitals, banks, transportation networks, and government services. Their work prevents data breaches, service interruptions, and financial loss. Cyberattacks could cause major harm to communities and even national security without them. Public policies also guide how cybersecurity works. Laws requiring companies to report data breaches or take minimum

security measures are designed to protect the public. Penetration testers play a role in making sure organizations follow these policies and maintain safe environments for everyone who depends on them.

Scholarly Journal Articles

Source 1: Parsons et al. (2017).

This article reviews research showing that people play a huge role in cybersecurity, not just computers/technology. It talks about the idea that understanding human behavior is essential for penetration testers.

Source 2: Hadnagy & Fincher (2015).

This source explains how social engineering works and why psychological factors influence whether people fall for scams. It helps explain how penetration testers use the social sciences when reviewing organizations.

Source 3: Tanczer et al. (2018).

This article examines how cybersecurity impacts marginalized communities. It adds depth to the discussion on inequality and shows why digital protection must be fair and accessible to all people.

Conclusion

Penetration testers do more than running technical tests. They rely on the social sciences to understand human behavior, organizational culture, and societal issues. Their work protects essential services and supports public safety, showing that cybersecurity is not only a technical field but also a human-centered one.

References (APA Format)

Hadnagy, C., & Fincher, M. (2015). *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails* https://www.oreilly.com/library/view/phishing-dark-waters/9781118958483/

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014) Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Carr, Madeline & Lesniewska, Feja & Brass, Irina & Tanczer, L. (2018). Governance and Policy Cooperation on the Cyber Security of the Internet of Things. https://www.researchgate.net/publication/332379987_Governance_and_Policy_Cooperation_on_the_Cyber_Security_of_the_Internet_of_Things