Cybersecurity Professional Career Paper: Vulnerability Testing

Student Name: Alissia Metcalfe

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Professor Yalpi

Date: April 16, 2026

Introduction

A Vulnerability Analyst identifies security weaknesses in networks and systems within an organization. Things like conducting penetration testing to find potential areas of weaknesses before malicious hackers. Then giving written solutions to patch the system/ networks vulnerabilities. In today's modern world, with rapidly growing technology such as AI. It is important that cybersecurity is kept up to date to mitigate the ever-growing threat of cybercriminals. In this paper I will cover how a Vulnerability Analyst career connects to the principles of psychology, sociology, and behavioral economics.

Social science principles

Vulnerability Analyst study psychology to understand why cyber criminals target specific networks/ systems. Using psychodynamic theories to understand cyber offenders and better understand their behavioral patterns. Gaining a better understanding of their cognitive thinking and aligning behavioral traits. These social science principles are heavily integrated into the practice of cybersecurity to address the "human factor" point. More than half of data breaches are not due to technical failures, but the weakest link the human. To understand the technical side is important but only half the battle, being able to identify and predict human behaviors is the main component. Professional in this field use social science insights to develop company cybersecurity use-regulations and protocols, having an understanding on how people react to rules, helping vulnerability analysts construct protocols employees are more likely to adhere to rather than ignore or deviate. "By understanding human cognitive limitations, security practices are being redesigned to be less complex." Having short and to the point lessons and even cyber awareness quarterly certifications can help reduce employee stress due to work overload on top of cybersecurity training and fatigue. Strongly correlating to the social science principle of relativism "behavior depends on context", employees are more likely to skip cybersecurity training due to work overload and stress which leads to their victimization to cyber-crimes.

Bypassing security prompts and software updates is what leads to security breaches but understanding the behavior of employees and cognitive thinking process makes for better actionable security protocols. Pop ups that are more than reminders to update software, things like “just-in-time” lessons when users are about to make a risky decision like clicking on links inside of phishing emails and a pop up appears on their screen to make the user question their decision again.

Application of Key Concepts

A key concept taught in class that corelate to this career is the three dark triad traits, machiavellianism, narcissism and psychopathy. Vulnerability testers like ethical hackers adopt these dark triad traits to adopt the mindset of a cyber attacker. Using these traits to mimic their malicious behaviors and manipulate humans through social engineering. Drawing connections to malicious behavioral-patterns and creating a system that can identify this malicious behavior such as phishing emails within the company and sending an automatic notification to the cybersecurity department, also known as “real-time” detection. Another concept is social engineering attacks. Vulnerability Testers can also use social engineering attacks on a company to test the human factors. How employees react to these social engineering attacks and if they respond correctly or incorrectly. This gives the cybersecurity department direct results of the cyber awareness trainings being conducted throughout the company and if they are effective or ineffective on the employees. How cybersecurity departments policies can use results to enhance user policies in the company/ organization to prevent employees falling victim to social engineering attacks and protect the company from legal lawsuits. For example, employee’s accidentality giving cyber criminals access to the organizations private network and data. Which can lead to the company being sued in class action lawsuits resulting in major financial losses due to the payout.

Marginalization

Vulnerability Testers also focus on the marginalized groups who are targeted due to having less access to digital resources, low-income, lack of digital literacy all leading them to their victimization. How these groups are more susceptible to social engineering attacks like phishing, vishing and SMS phishing. As well as software and network attacks because of the inability to afford software/ network anti-malware security or because the systems they own are old and out to date not compatible with updated security software programs. “In 2020 Innovations for Poverty Actions launched a four-year initiative to help protect digital finances users by investigating effective channels for building consumer protection in DFS.” Article Cyber Resilience by Aubra Anthony. Professions in the field are actively finding ways to focus on marginalized groups being targeted and better laws that can be set into place to help protect them from cyber crimes.

Career connection to society

Vulnerability Tester along with ethical hackers and penetration testers play a major role in protecting financial institutions, hospitals, businesses, organizations and armed forces. Constantly testing systems for possible weaknesses before cyber attackers get to them and abuse/ exploit their systems. Actively patching security weaknesses and finding ways to secure systems and networks and protect companies from facing legal lawsuits. Stopping hackers and protecting systems.

Scholarly Journal Articles

- Source 1: Cyber Resilience Must Focus On Marginalized Individuals, Not Just Institutions Aubra Anthony (April 2026) https://carnegieendowment.org/research/2023/03/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions

This source helped me develop and understanding of how marginalized groups contributed to their victimization and what the field of cybersecurity was doing to solve this.

- Source 2: Back, S., & LaPrade, J. (2019). The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence. International Journal of Cybersecurity Intelligence & Cybercrime,2(2), 1-4. https://www.doi.org/10.52306/02020119KDHZ8339

  This article provided information on the human factors contribution to cybersecurity which helped me form my argument that humans are the weakest link in an organization.

- Source 3: https://niccs.cisa.gov/tools/cyber-career-pathways-tool?selected-role=PD-WRL-007&quiet=1

  The NICCS career framework helped me establish the career timeline as well as titles within this job. Drawing connections to different roles and how they contribute to the entirety of Vulnerability Testing.