Tracey Bernasco
10/4/26
CYSE 201S
Dr. Trinity Woodbury

Cybersecurity Career Paper

One career that holds a connection to social sciences is penetration tester also known as pentesting. Penetration testers is a career that focuses on how to test computer systems and networks for weaknesses with organizations consent. Their goal is to find vulnerabilities before a real attack does. While technical knowledge is important in this career, there is also a need to understand human behavior because people can be vulnerable as well. Pentesting depends on social science research and principles because cybersecurity is not only about technology, but it also involves how people think and behave. Professionals of this career use these concepts to evaluate employees and understand the patterns of cyber offending and how criminals may take advantage of human behavior.

One social science concept that connects to penetration testing is social influence. People can be influenced by authority, trust, or pressure from others. For example, an employee may be more likely to give information to someone who claims to be their manager. Penetration testers can use authorized social engineering tests to see how employees respond to these situations. NIST explains that security testing can include social

engineering because organizations need to understand how their employees respond to realistic attacks. Organizations can expect simulated phishing emails to see how employees respond. Another important concept is cognitive bias. People often make quick decisions without considering all the information available to them. Research on phishing has shown that human behavior and cognitive vulnerabilities are key factors in understanding why people respond to deceptive messages. Social learning theory is about people learning behaviors by observing others. This concept applies to this as part of pentesting is auditing and finding weaknesses in organizations. An example of one is employees see other coworkers ignoring security policies. They may believe that these policies are something that do not need to be taken seriously which can lead to failure to follow security procedures. The fourth concept is cyber offending, which is connected to penetration testing as it focuses on why people omit crimes using technology. The United Nations Office on Drugs and Crime explains that criminological, psychological, sociological, and economic theories can help explain cybercrime. One theory that can be applied to cyber offending is Routine Activity Theory, which states that crime is more likely when a motivated offender, a suitable target, and a lack of capable guardianship come together. In cybersecurity, a motivated cybercriminal may target a company that has valuable information while weak security controls make the organization an easier target. Penetration testers use this type of thinking to identify weaknesses before actual offenders can exploit them.

This shows the interdependence between social science and cybersecurity because understanding criminal behavior can help cybersecurity professionals predict threats and decide how organizations should protect themselves.

Pentesting also has to deal with marginalized and underrepresented groups because cybersecurity does not affect everyone in the same way. People and businesses can have less access to technology, accessibility, or education. One such challenge would be language barriers. Employees who are not fluent in the language used in an organization may have difficulty understanding security policies and recognizing phishing attempts. The second is accessibility, People with disabilities may encounter fault websites or training programs that were not designed to fit their needs. The third challenge is digital literacy and unequal access to technology. Individuals who have fewer opportunities to use computers can be more vulnerable to fraud and social engineering. Research also shows that differences in people's education and experiences can affect how they understand cybersecurity information. These challenges are important for penetration testers because testing human behavior without considering people's diverse backgrounds could produce unfair results.

Pentesting has a broader impact on society because they help protect organizations and the people that depend on those services. Their work can also help prevent disruptions to important services such as hospitals, schools, banks, and government agencies. This benefits society because

stronger cybersecurity can increase people's trust in technology and online services. Penetration testers also influence organizations to improve their security practices and take human behavior into consideration instead of relying only on technical defenses. Overall, their work helps create a safer digital environment while reducing the potential social and financial harm caused by cybercrime.

References

National Institute of Justice. (2009, October 13). *Why crimes occur in hot spots*. U.S. Department of Justice. https://nij.ojp.gov/topics/articles/why-crimes-occur-hot-spots

Neil, L., Healy, C., & Haney, J. (2025). “A five-year-old could understand it” versus “This is way too confusing”: Exploring non-expert understandings and perceptions of cybersecurity definitions. *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3706598.3713820

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment* (NIST Special Publication 800-115). National Institute of Standards and Technology https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf