Tgen Hampsher

CYSE 201S

4/14/2025

Professor Yalpi

**Ethical hacking and Using Social Sciences to Combat Cyber Attacks**

**BLUF:** Ethical hackers are an essential defense against cyber attacks through using the social sciences to predict the moves of malicious attackers.

## Introduction

In our current world where both human and technological vulnerabilities are found within critical networks, being maliciously hacked is not a matter of if but when. As a result, many organizations both private, public, and government look to ethical hackers to detect these vulnerabilities and assist in patching them before a threat agent can do the same. According to IBM, Ethical Hacking is using "**hacking techniques**" by "**friendly parties"** in attempt to "understand and fix security vulnerabilities in a network or computer system" (IBM, 2023). Essentially, ethical or "white hat" hackers have the same skills and strength of malicious or "black hat" hackers, however they only use these skills to help improve security rather than damage it.

## Social Science Principles

One of the social science principles that heavily correlate with ethical hacking is determinism. Determinism is the social science principle that everything that happens is determined by a previous event in a continuous cause-and-effect relationship (Bhandari, 2023). Ethical hackers understand this cause-and-effect relationship well, as they understand that no cyber-attack can succeed by random luck, therefore there is always a cause for every attack and its effects. Understanding this, ethical hackers are careful with their decisions as every decision they make on the network will have some form of a consequence, whether it's good, bad, or neutral.

Additionally, skepticism is another fundamental social science principles woven into ethical hacking. Skepticism is the principle that everything researchers do must be

second guessed and criticized to further strengthen the validity of conclusions made from research (Bhandari, 2023). For ethical hackers, they must go beyond second guessing, sometimes rescanning network infrastructures five or six times before deciding to run exploitation tests. Furthermore, after recommending fixes and/or implanting fixes to a network, they must do the same checks many times again to ensure they have fixed all the vulnerabilities they possibly can that they detected. Therefore, ethical hackers arguably must be one of the most skeptical based people in the world.

Furthermore, the principle of parsimony is another essential aspect of ethical hacking. Parsimony is the idea that researchers should strive to provide explanations that are as simple and easy to understand as possible (Bhandari, 2023). For ethical hackers, a key point to their work is after discovering vulnerabilities within organizational networks, they must effectively communicate to business leaders, many with little cyber knowledge, on what these vulnerabilities are and how they should be fixed. However, if ethical hackers cannot make their explanations simple for the organization, the message will not be clear and overall, it will be less beneficial to the organization as they might still be unsure of how to better protect the network.

## Applied Concepts

Many applied concepts from CYSE 201S are found in ethical hacking. One application is social engineering. IBM finds that social engineering is the use of psychological manipulation to produce a desired outcome by the manipulator (IBM, 2022). In cybersecurity, social engineering attacks are designed to exploit the natural human

vulnerabilities found in employees to enter and harm networks, rather than focusing on technological vulnerabilities. Ethical hackers must understand how social engineering attacks work and may even use them themselves when conducting penetration tests, as this will dramatically help them understand the mindset and strategies of malicious hackers.

Another important concept of social sciences in ethical hacking is the idea of having great diversity in the workforce (Chamlou, 2022). Specifically, a diverse team of ethical hackers coming from different cultures, locations, and beliefs will likely be more effective in detecting and solving vulnerabilities compared to a team of people that are very like-minded, because the second group will be less likely to challenge each other's ideas and create out of the box solutions when needed.

Furthermore, human-centered cybersecurity is a concept that ethical hackers understand very well. This cybersecurity model is essentially designed to focus the security of the network on preventing human errors more than focusing on technological vulnerabilities. Ethical hackers understand that most attacks succeed from human errors. Therefore, most of their simulation testing on networks usually looks to target individuals rather than the systems themselves.

Lastly, another concept applicable to ethical hackers is the social behavior of being a systematic thinker. For cybersecurity, this means professionals must be able to understand how a variety of systems may be impacted by a single change. Systematic thinking is crucial for ethical hackers because they have to understand an entire network

before they decide to implement penetration tests and patches for vulnerabilities they discover.

## Marginalized Groups and Challenges

Many marginalized groups interact with ethical hackers differently. For example, smaller businesses with smaller revenue can not afford to obtain ethical hacking services as well as larger corporations (A&M, 2024). Not being able to afford the same services can lead to smaller organizations being less protected then larger corporations, which means these companies will be attacked more and suffer more losses. For ethical hackers, they must decide between chasing profit and only working for larger corporations that pay more, or trying to reach fewer profiting corporations and take a smaller payout.

Additionally, ethical hackers must account for people with a variety of physical and mental disabilities, as the patches ethical hackers may suggest may not be user friendly to all people. For example, certain authentication methods like biometrics may be difficult for people with physical disabilities, which means suggesting that change to a network may not be helpful. For ethical hackers, the challenge then arises of how they should balance ensuring protection of systems without compromising the usability of the systems they are trying to protect.

Furthermore, other minorities like ethnic and racial minorities may be more prone to phishing attacks and cyber discrimination. This may lead to these minorities being the biggest target of attacks within a network for a variety of reasons. Therefore, ethical hackers must detect these minorities when they are able to in any company, as well as biases that

may be present within their security systems, and design solutions that address these biases adequately.

## Career Connection to Society

Ethical hackers is a considerably controversial job for a majority of society. Some feel that ethical hacking is an essential tool in combatting malicious hacking and is ultimately worth the reward despite the risk and uncertainties that come from purposely allowing someone entry into a critical network. On the other hand, some believe that hacking is bad no matter what the intent, and ethical hackers are more concerned with the financial reward or reputational reward rather than genuine good for society. Nonetheless, ethical hackers give insight into where vulnerabilities exist before they can be exploited maliciously, so they continue to help in protecting society from cyber-attacks.

## Conclusion

Ethical hackers are arguably one of the most important pieces to defend against the worst cyber-attacks, because these professionals all have the same skills as malicious hackers. They differentiate themselves from criminals because rather than harming networks where they find vulnerabilities, they help the individual or organization patch these vulnerabilities to bolster their security. As cybercrime continues to increase, more ethical hacking will help prevent attacks before they can ever occur.

## References


A&M. (2024, September 30). *Cybersecurity Budgets: Spend More or Spend Better?* Alvarez & Marsal | Management Consulting | Professional Services. https://www.alvarezandmarsal.com/insights/cybersecurity-budgets-spend-more-or-spend-better

Bhandari, M. P. (2023). The Fundamental Principles of Social Sciences. *Business Ethics and Leadership*, *7*(2), 73–86. https://doi.org/10.21272/bel.7(2).73-86.2023

Chamlou, N. (2022, February 28). *Why Diversity in Cybersecurity Matters | CyberDegrees.org*. Www.cyberdegrees.org. https://www.cyberdegrees.org/resources/diversity-in-cybersecurity/

DAU. (2022). *Human Systems Integration | www.dau.edu*. Dau.edu. https://www.dau.edu/acquipedia-article/human-systems-integration

IBM. (2022, June 14). *Social Engineering*. Ibm.com. https://www.ibm.com/think/topics/social-engineering

IBM. (2023, October 20). *Ethical Hacking*. Ibm.com. https://www.ibm.com/think/topics/ethical-hacking