Ryan Jackson
11/22/23
CYSE 425W

Policy Analysis Paper 4

The topic of Ethical Hacking comes with plenty of policies and strategies. There is always a goal of addressing security concerns. There are plenty of social factors that contribute to the development of policies and strategies. As time goes on, technology advances and there is an increase in cyber attacks. Malicious intent creates a cause for the mitigation of vulnerabilities. Society relies more on technology, and the risks of cyber-attacks have risen. Dependency on technology then led to the presence of hacking and ethical hacking. Malicious hackers are also evolving with technology by developing new advanced software and tools. There was then an emergence of data protection laws and industry regulations. Laws and regulations have been crucial in the making of ethical hacking policies.

Along with technological growth, public awareness of the topic has also grown. Public awareness of attacks will contribute to more and more companies improving cybersecurity. Instances such as data leaks have as a result increased the demand for ethical hacking to have proactive security measures. Ethical hacking policies themselves contribute to improved cybersecurity by identifying and mentioning vulnerabilities, hopefully prior to exploitation. As stated previously, it is "important to note that teaching hacking creates two separate risks. There is a risk to society if a student misuses the skills they are taught." (Pike, 2013, p.68). The growing interest in ethical hacking education has coincided with concerns over the ethicality of teaching students how to hack. There has also been talk around the topic of whether it is ethical for students to learn about hacking. "The foremost justification for ethical hacking

education is that it is the only feasible approach that prepares future cybersecurity professionals." (Al-Tareq, 2023, p.7).

In terms of influence, ethical hacking practices can lead to the building of trust and reputation of a company, network, etc. Customers, clients, and stakeholders look to have or establish trust and look for a positive and stable company reputation. Interaction between an ethical hacker and an organization needs to maintain a level of trust. Ethical hackers could undergo questionable means and tactics. Their actions might result in a question of their professional ethics. It could be argued that ethical hackers partake in questionable activities, however, if they are ethical, the rationale would likely be justified in some way, shape, or form. But the keyword of that statement is "If." "At what point may this justified ethical behavior become blurred and the practices of the ethical hacker become unethical?" (Georg, 2018, p.8). Customers, clients, and stakeholders may prioritize data/network protection over everything and this could serve as a selling point and competitive advantage in the marketplace.

Cultural and Subcultural Influences include hacker culture itself. Hacker culture is fueled by curiosity and any other societal disadvantage one may believe that they have. This culture has influenced the development of ethical hacking. Ethical hacking must consist of individuals who understand the culture and tactics of hacking in order to stay a step ahead. This goes hand in hand with the culture that companies and organizations should and have fostered. This consists of the way companies handle network security and the usage of ethical hacking. As a result, this will influence how a society as a whole looks at hacking and ethical hacking.

Ryan Jackson
11/22/23
CYSE 425W

In conclusion, ethical hacking policies and strategies have emerged in response to the evolving threat landscape. Malicious hackers will evolve along with the landscape. As mentioned, there are plenty of factors that contribute to the development of the field of ethical hacking. The social effects of these policies include improved security, enhanced trust, etc. Trust in the field is typically implied, however, if mishandled could lead to drastic consequences.

Ryan Jackson
11/22/23
CYSE 425W

References

Al-Tawil, T (2023). Ethical implications for teaching students to hack to combat cybercrime and money laundering. *Journal of Money Laundering Control., Ahead-of-print*(Ahead-of-print), Journal of money laundering control. , Vol.ahead-of-print(ahead-of-print).

Georg, T (2018). Issues of Implied Trust in Ethical Hacking. ORBIT Journal, 2 (1) 10.29297/orbit.v2i1.77

Pike, R. E. (2013). The “Ethics” of Teaching Ethical Hacking. *Journal of International Technology & Information Management*, *22*(4), 67–75. https://doi-org.proxy.lib.odu.edu/10.58729/1941-6679.1021