A later module addresses cybersecurity policy through a social science framework. At this point, attention can be drawn to one type of policy, known as bug bounty policies. These policies pay individuals for identifying vulnerabilities in a company's cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try explore the cyber infrastructure using their penetration testing skills. The policies relate to economics in that they are based on cost/benefits principles. Read this article https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=true Links to an external site.
and write a summary reaction to the use of the policies in your journal. Focus primarily on the literature review and the discussion of the findings.

Response -

After reviewing the article, there are policies that are tied to economics as connected to the structures of social science principles. The concept of the use of the bug bounty policy theory may be initially viewed as inapplicable yet can be pertinent to the theory itself. Then, after further research and examination, the bug bounty policy connects to cybersecurity theory as experts have an advantage over nefarious hackers and their associated trending practices. This policy of "bug bounties" outlines the practice of the employment of freelance hackers (hackers without nefarious intentions) in an attempt to locate flaws and weak points in the data structure chain, as well as outright bugs (a software error). Then, the freelance hackers can notify the IT group so they can fix these problems before a nefarious hacker exploits these weaknesses for their own personal gain.

There are networks which could look enticing to these freelance hackers. Some examples of such networks are Bugcrowed and HackerOne. These services are extremely useful to IT teams as these companies are willing to pay well for the work being completed. For instance, in May 2020, the HackerOne network had generated over $100 million dollars in payments as a result of the utilizing bug bounties. The logic behind bug bounties is simple, whereby someone is hired that has experience in the field of computer science, more specifically someone who has the knowledge of hacking principle themselves. Then, the company can allow them access to the code that is supposed to be checked for flaws, and since these people have the same experience as nefarious hackers. The freelance hacker should be able to notify the company of possible areas of compromises in their code. In practice, this system could be very successful in promoting strong cybersecurity protections in concept, as it not only is checked by industry standards, but it is also checked by individuals with similar

experiences to those who are attempting to do harm to the individual through comprising their data subset and thus their own life securities.