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. 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.

Bug bounty programs, which make hackers want to identify vulnerabilities are beginning to become very essential in cybersecurity policy. The literature review in the article explains how these programs are starting to become grounded in the principles of economy, which rewards individuals based on the value of reporting the vulnerabilities they spot. The discussion of findings suggests that while bug bounties can be highly effective, they vary in success because of factors like payout amounts and the structure of the program which usually influence the hacker engagement and the report's quality. This approach underscores bug bounties as a flexible, economic tool in cybersecurity policies.