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=trueLinks 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.

After reading this article on bug bounty policies, I have found it very informative. This review provided an in-depth understanding of the development and history of policies on how to identify vulnerabilities in a company's cybersecurity framework. This article also discusses the effectiveness of these policies in increasing cybersecurity and preventing cyber-attacks. Company's such as Facebook and google are major companies that have implemented these policies. This article also highlights the role of cost-benefit analysis towards determining the rewards for ethical hackers. This approach attracts hackers while being cost effective for companies. This article provided evidence that bug bounty policies enhance a company's cybersecurity and recommends that companies should use these policies to reduce cyber-attacks and protect sensitive data within the company.