Prompt: Bug Bounty Policies

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. There 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 penetrations testing skills. The policies related to economics in that they are based on cost/benefit principles. Read this: 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.

There is a lot of money being poured into cybersecurity and professional basis. Bub bounties help companies have multiple eyes on possible problems making it a possibly better option for those who cannot afford to spend millions of dollars on a cybersecurity team. Bug bounties also help people who are getting interested in cybersecurity get money and those who prefer to freelance. This can cause ethical concerns as those who find bugs might not report them right away leading to the credentials of the company being left on the black market. This is quite a new field where the market not fully set, and the previous research pool is great enough to decide which would be best. This study does show that if there are bug bounties for new hackers the best reward would be acknowledgment of their skills. The ones that have been acknowledged for their skills then move on to wanting monetary rewards. This is the same for bug bounty websites that start out private but once gaining positive feedback they move to a more public space. That would be for more deals and allowing others more opportunities also creating more competition for the hacker market. The bug bounties might take away from funding for research and finding new ways to exploit and protect a system.