In this journal I will write a summary reaction to the use of policies based on Hacking for good focusing primarily on the literature review and the discussion of the findings. The authors of the article research the overall concept of bug bounties as well as the economics incentivizing freelance security researchers to engage with corporate entities and find weaknesses in their IT systems. Outside of monetary incentives bug hunting is popular among security researchers for several reasons. First, it presents a challenge. uncovering vulnerabilities and exposing vectors of attack can provide an exciting challenge for bug hunters. Second, is the opportunity for professional development and education that bug hunting provides. Participation in bug bounty programs give hackers and security researchers alike hands-on experience identifying attack vectors and remediation of vulnerabilities to include defensive strategies. This practical experience often translates into better cybersecurity jobs prospects. Aside from individual motivations to participate in bug hunting programs, the paper puts forth two factors that that drive organizations to use freelance security researchers and hackers to find bugs. One is a worldwide shortage of four million cybersecurity professionals. This gap in the number of cyber professionals translates into small and medium organizations finding it difficult to recruit and retain qualified personnel those positions. Second, is that the bug bounty system enables organizations of any size the ability to discover and remediate vulnerabilities that would otherwise be overlooked given the number of freelance bug hunters that can contribute versus the limited number of qualified professionals within the organization. So, given the incentives both organizational and individual, what were the paper's findings?

First, are that bug bounties are cost effective. With limited budgets to pay security researchers, bug bounties maintain a high benefit versus cost ratio when organizations consider the best financial return for strategies and solutions that enhance their security posture. Second, as previously intimated when discussing individual motivations is that hackers are largely motivated by experience and reputation gain over financial considerations. This means that less experienced hackers and security researchers are likely reject lower bug bounties overall. Second, that an organizations total revenue and brand does not statistically affect the number of valid security vulnerability reports it receives. This means that the size of the organization did not significantly affect the overall number of bug reports Although the paper did find that financial and retail industries did receive between 2.34 and 1.42 fewer report that other categories. Third that an increase in companies using bug bounty programs did not decrease the number of valid vulnerability reports received by organizations already participating in those programs. Finally, the article did reveal that bug bounty programs do receive fewer valid reports as they age, due to bugs becoming harder to find in a particular program or set of IT systems. Overall, bug programs have a positive affect both for individuals seeking to gain practical experience and organizations seeking to leverage a cost-effective mechanism that strengthens their cybersecurity posture.