**Week 12 – Journal Entry 13**

**Sheldon Horrell**

**CYSE-201S**

**4/6/25**

Bug Bounty Policies

After reading this journal article it helps explain how bug bounty programs are becoming a key tool in fighting cybercrime, especially in a shortage cybersecurity professionals. It highlights how many companies still lack clear policies for disclosing vulnerabilities, leaving them open to attacks and more.

The study shows how bug bounty programs work well even for smaller companies. It also highlights that hackers are only slightly motivated by money, meaning they may do it for reasons other than financial motivation, like building a hacker reputation. This means companies don’t always have to pay high rewards for results. The research in this study also found that the size or brand doesn’t significantly affect reporting of vulnerabilities. Industries like finance and healthcare see fewer reports, possibly due to higher risks or tighter security measures from laws like HIPAA.

The article makes it clear that while bug bounty programs aren’t perfect, they offer a promising way for companies to improve cybersecurity without needing larger financial resources. It also points out that programs tend to slow down as they age unless they keep expanding their scope. These is useful for businesses and policymakers looking to increase and strengthen digital security.

**Reference**

Kiran Sridhar, Ming Ng, Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties, Journal of Cybersecurity, Volume 7, Issue 1, 2021, tyab007, <https://doi.org/10.1093/cybsec/tyab007>