JOURNAL ENTRY 13

The bug bounties market is a lucrative business not just in monetary terms but in areas such as reputation building, experience gaining and publicity for hackers. This paper gives a clear understanding of the bug bounty market, its impact, and pattern. It can be considered true that the more lines of code, the more bugs a program will have, and so companies that use more third-party software is more vulnerable to bugs. The paper points out that mainly small companies run this risk, as most big companies develop their software in-house. It is in the opinion of the paper that it is cheaper to get bug bounties than hiring software developers, but this estimate does not cover a few factors such as subscription fees, vulnerability effects, etc. However, with an 8% margin in testing the effectiveness of the processes and a positive Wald test, there is the understanding that the research and industry is growing, with more room for growth and improvement. The regression correlates with over 90% unknowing factors, indicating that there is more to be learned in this field. Public bug bunting serves as good practice for new hackers, while private hunts rely on experienced veterans, which influences the rate of elasticity and inelasticity of pricing. As before, the hackers' focus is not mainly monetary. For young, up-and-coming hackers, reputation, publicity, and experience are the main focus (this is good news for small companies with limited financial budgets), while veterans still aim for more publicity, interest and a challenge is also a factor. This is why there is the thought that small companies with limited resources stand the risk of not getting Bounties.

REFERENCE

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab007