

Isaiah Browne
CYSE 201S
12/13/2024

Journal Entry 13

A number of significant contributions, particularly concerning bug bounty programs, are made to the expanding corpus of literature on cybersecurity policy in this article. It questions some prevalent assumptions about what drives the success of these efforts and highlights the potential benefits of these programs for enterprises of all sizes and sectors. The results that hackers are not very price sensitive and that bug reports are unaffected by company size are interesting since they show that bug bounty programs might be useful for smaller companies who don't have the money to build strong internal security teams.

The report does, however, note that additional empirical research is required to fully comprehend the underlying dynamics. Concerning the social and economic aspects that impact hacker involvement and the lasting effects of bug bounties on cybersecurity results, there are numerous unanswered questions. While its conclusions add to the continuing discussion on the optimal form and optimization of cybersecurity rules in today's linked world, the article lays a firm groundwork for future research in this area.

As more and more businesses start using bug bounties, it seems like a great way to boost cybersecurity. According to the literature, in order to improve existing policies and make them even more effective, we need a deeper understanding of the reasons that have contributed to their success as well as the larger social and economic dynamics that are at work.