Article #2: The Economics and Behavior of Bug Bounty Programs

Kaemon Powell

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Yalpi

4/13/2026

Introduction/BLUF

This article examines how bug bounty programs can function as a cybersecurity strategy by using financial incentives to encourage ethical hackers to identify the vulnerabilities. The bottom line is that these programs are very effective because they combine economic motivation with human behavior, allowing organizations to improve security in a cost-effective way.

Relation/Connection to Social Science Principles

This article connects to many social science principles. First, economic behavior and incentives are central as hackers are always motivated by the rewards. Second, interaction and networks play a role because bug bounty platforms rely on big communities of researchers. Third, human behavior and decision-making are important because participation depends on the rewards and risk. Lastly, institutional trust is relevant because organizations have to build credibility for hackers to engage truthfully.

Research Question/Hypothesis/Independent/Dependent Variables

How do incentives and organizational factors affect participation and effectiveness in bug bounty programs?

Hypothesis:

Higher rewards and company reputation will influence participation and the number of vulnerabilities shown.

Independent Variable:

Reward size, company reputation, and program structure

Dependent Variable:

Number of vulnerabilities reported and level of hacker participation.

Types of Research Methods Used

The study uses quantitative research methods, analyzing the data from bug bounty platforms. It analyzes patterns across a number of programs, focusing on measurable outcomes like participation rates and vulnerability submissions.

Connections to Other Course Concepts

This article connects to a lot of class concepts, including social engineering, risk management, and human factors in cybersecurity. It restates the idea that people are, most of the time, the most important part of security systems. It also connects to cost-benefit analysis, showing how organizations choose bug bounty programs as a less expensive alternative to hiring full-time experts.

Connections to the Concerns or Contributions of Marginalized Groups

Bug bounty programs create opportunities for individuals from marginalized groups by allowing global participation without requiring formal employment. However, there are concerns about

unequal access to resources, such as education or technology, which may limit the people's participation. Additionally, lower payouts or lack of recognition may disproportionately affect less experienced hackers.

CONCLUSION

In conclusion, this study displays that bug bounty programs are a valuable tool for improving cybersecurity and reducing costs. They encourage collaboration between organizations and independent researchers, which highly increases the chances of identifying vulnerabilities. The study also highlights how economic incentives can shape human behavior in cybersecurity. Overall, it contributes to society by promoting secure systems and demonstrating how social science principles improve technological solutions.

Reference

Zhao, L., & Eling, M. (2021). Bug bounty programs: Evidence on the economics of cybersecurity. *Journal of Cybersecurity*.

Article Link: https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453