John Monrouzeau
11/13/2025
CYSE 201S

Economic and Social Implications of Bug Bounty Programs

Introduction

The article I have picked talks about how huge changes, like sudden increase in cyber threats, can affect bug bounty programs and the behaviors of those who participate. Making a basis using real world data, Zrahia talks about how market incentives determine the status of current cybersecurity performances. Combining psychology, economics, and social science principles, such as the ones studied in class, we can begin to explain how hackers respond to all of these market changes in the digital world.

The relationship between the article and social principles

The big reasoning as to why I chose this article was due to its strong connection to the social science principles, as I had mentioned earlier, like motivation and human behaviors. Many theories came to my mind during my first reading of this article, like rational choice theory and systems theory. Rational choice, because people willingly choose whether they participate in bug bounty programs or not; and systems theory, displaying how businesses and individual hackers participate through the cyber space and its "ecosystem."

Research question, Hypothesis, and independent/dependent variables

The basis of this article, and the set research question I will put into place, is: How does an external market or policies being put into place affect the quality AND quantity of vulnerabilities being reported on bug-bounty programs. My hypothesis is that when increased external factors, like big cyber threats, occur, there will be drastic change in the amount of people who participate in bug-bounty programs. The independent variable would be the external

factors, like policy changes or big cyber events. The dependent variable would be the amount and the quality behind the actual reports made on these bug-bounty platforms.

Research and data analysis

Zrahia uses a quantitative approach to economic modeling, based on the analysis of secondary data from a large bug-bounty platform. She assesses the activity before and after certain external shocks. Using regression models and comparative statistics, she comes to the conclusion of the regular connections between disruptions in this market and researcher behavior. The data are based on thousands of submitted vulnerabilities under various programs. The author looks at changes in submission rate, average reward, and participation of researchers to determine a conclusion. The author applied statistical inference and time-series regression to analyze how these eventful “shocks” affect program dynamics and the reward distribution, thus giving insight into short-run and long-run behavioral effects.

Connection to class

Concepts that we have learned from class, like risk management, economic motives, and cyber policy designs, very clearly tie into this article and the study. The study itself also references the social science ideas about collective behavior and trust systems from within the cyber space, where the bond between organizations and the individuals who hunt down bugs creates a stronger cyber space for everyone.

Groups and Social Concerns

Indirectly, the subject is about the digital divide in the context of unequal access to cybersecurity participation across marginalized groups. Bug bounty platforms favor those with more advanced skills or technology, which blocks underrepresented groups from participating in

the cybersecurity workforce. Helping to rebalance this so that bug bounty ecosystems are more representative around the world could make it more inclusive.

Societal contributions and Impact

This study informs us on how open cybersecurity systems adapt and change to shocks in the cyber space, like spikes in cybercrime or policy changes. It also talks about how important the relationship between businesses and individuals who report bugs, or public and private entities, when it comes down to protecting infrastructure in the companies themselves. This research helps policy makers establish better and more rewarding bug-bounty programs that will benefit everyone in the cybersecurity space, without depending entirely on traditional and expensive methods of defense.

Conclusion

Zrahia's research shows us how social science and economics connect with cybersecurity in terms of their rules and policies. Bug bounty programs are heavily dependent on the public and their motivations to even report bugs to the platform, it is not only about the technology. Its good to understand peoples' incentives, and how other factors outside of the cyber space can make an impact on participation, which will lead to more resilient and cost effective cybersecurity systems.

References

Zrahia, A. (2024). *A simple economics of an external shock to a bug-bounty platform. Journal of Cybersecurity, 10*(1), tyae006.

https://academic.oup.com/cybersecurity/article/10/1/tyae006/7667075