Student name: Justin Cotman

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor name: Diwakar Yalpi

Date: 4/16/26

BLUF

This article examines cybersecurity bug bounty initiatives. Businesses use ethical hackers to identify vulnerabilities in their systems. The outcomes of the study on incentives are quite apparent. More reports are produced when there are clear guidelines and greater benefits. You observe how structure and money influence behavior.

Relation to Social Science Principles

This subject relates to important concepts in social science. How businesses evaluate reward costs to breach damages is demonstrated by economic concepts. The way incentives influence hacker choices is explained by behavioral psychology. Sociology demonstrates how trust fosters collaboration between hackers and businesses. You observe how incentives and human behavior impact cybersecurity results.

Research questions

Whether bug bounty programs lead to more vulnerability reports is the question posed by the study. Higher rewards, according to the idea, result in increased participation and reports. The program's structure and the size of the rewards are independent variables. The quantity of vulnerabilities that are reported is the dependent variable. Incentives and outcomes are directly correlated.

Types of research methods used

A quantitative research approach is used in the study. Businesses with bug bounty programs provide data to researchers. Before and after the program's launch, they compare the outcomes. Additionally, they contrast several businesses with varying amounts of compensation. You can see how the study's conclusions are supported by the data.

Types of data analysis used

Measurable information from corporate reports is used in the study. The quantity of vulnerabilities reported over time is monitored by researchers. To observe changes following program adoption, they examine trends. They evaluate outcomes from various organizations. You may see how the conclusions are supported by statistical analysis.

Connections to other concepts

This topic relates to important cybersecurity course concepts. Early reporting of vulnerabilities improves cyber hygiene. When businesses address problems before attacks happen, risk management gets better. The involvement of ethical hackers increases the prevention of cybercrime. You observe how human behavior and policies influence cybersecurity results.

Connections to the concerns or contributions of marginalized groups

Programs like bug bounties give those with less formal education access. People from other nations participate and make money. Participation in cybersecurity work has increased as a result. Some groups are constrained by a lack of resources and instruction. You observe access disparity as well as opportunity.

Overall societal contributions of the study

The research demonstrates how incentives enhance cybersecurity results. Vulnerabilities are discovered and added more quickly. Businesses lower reputational and financial risk. Stronger digital systems are advantageous to society. You can see how security is enhanced at scale by structured rewards.

Reference

Finifter, M., Akhawe, D., and Wagner, D. 2013. An empirical study of vulnerability rewards programs. Journal of Cybersecurity.

Article Link: https://academic.oup.com/cybersecurity