Mohammad Sulaiman

Professor Teresa Duvall

CYSE 201S

04/09/2024

Journal Entry 13: Bug Bounty Policies

Reading through the journal article on vulnerability disclosure policies (VDPs) and bug bounty programs was truly enlightening. The extensive literature review provided me with a comprehensive understanding of the theoretical underpinnings and previous empirical studies in this domain. I found the methodology employed, particularly the utilization of Hacker One's extensive database and advanced regression techniques, to be exceptionally robust, demonstrating a rigorous approach to analyzing the factors influencing bug bounty program success.

The findings discussed in the article were particularly intriguing to me. Discovering insights about hacker price elasticity and its implications for bug bounty programs was eye-opening. I was fascinated by the revelation that company size and profile do not significantly impact the number of vulnerability reports received, highlighting the accessibility of bug bounty programs for companies of all sizes. Additionally, the identification of industry-specific trends, such as the lower number of reports in the finance, retail, and healthcare sectors, sparked my interest and prompted further questions.

The acknowledgment of limitations and the discussion of implications for future research were crucial aspects of the article. Recognizing the complexities and potential biases in the analysis underscored the necessity for continued exploration in this field. Overall, this article has deepened my understanding of vulnerability disclosure policies and bug bounty programs, and I

am eager to see how future research builds upon these insights to further enhance cybersecurity practices.

In summary, this journal article offers valuable insights into vulnerability disclosure policies (VDPs) and bug bounty programs. Through a thorough literature review and analysis of findings, it provides a deeper understanding of the theoretical foundations and practical implications of these cybersecurity initiatives. Key findings include insights into hacker price elasticity, the impact of company size and industry profile on vulnerability reports, and industry-specific trends. Acknowledging limitations and discussing implications for future research, the article contributes to both academic understanding and practical cybersecurity strategies.