

Module 11 Journal Entry #2

Kayle Glaize

School of Cybersecurity

CYSE 201S Section 34568

Professor Matthew Umphlet

July 26th 2026

This article examines the concept of bug bounty boards as a cybersecurity policy, which are programs that allow ethical hackers to search companies for security vulnerabilities in exchange for a reward, in order to help identify whether or not these programs are effective. The author goes on to mention that the frequency of cyberattacks is increasing, as well as the cost to combat them. Combine this with the lack of available skilled professionals, and fighting off cyberattacks becomes very challenging. As a way to draw in support, companies have started to implement bug bounty board programs, offering monetary rewards for ethical hackers willing to put their skills to the test by searching these organizations' systems for vulnerabilities.

The author makes a point to mention that while previous studies conducted on the effectiveness of bug bounty board programs have generally found that they could lead to improvements in cybersecurity, there was a lack of large-scale evidence to explain why certain programs seemed to perform better than others. Many researchers agreed that most ethical hackers were motivated by money, but also stated that things like reputation, opportunities to improve their skills, and taking on a challenge also played a role in attracting participants.

In order to hopefully answer some of these questions, researchers worked with one of the larger bug bounty platforms, HackerOne, to identify the factors that contributed to the number of valid vulnerabilities reported. The study found that while money did play a factor in the number of vulnerabilities reported, it was much less of a motivator than previously believed. The participants seemed to be greatly motivated by things like recognition, personal interest, and the chance to take on a challenge.

The study also found that the size of the company didn't have much of an effect on the number of reported vulnerabilities, but the industry they were in did. Companies in industries like finance,

retail, and healthcare received fewer vulnerability reports, which may suggest that they uphold stronger security practices or that those industries are targeted more frequently, making vulnerabilities more valuable to hackers and therefore less likely to be reported.

The authors end the article by pointing out that bug bounty boards are a cost-effective cybersecurity strategy because an organization only has to pay individuals for each reported vulnerability. They go on to say that human behavior is just as much of a factor in this approach as it is in traditional cybersecurity practices and technology because ethical hackers seem to be less motivated by monetary gain and are instead interested in taking on challenges, improving or gaining a reputation, or honing their skills. They end with a note that while this research is promising, there is still a need for further investigation to truly understand all of the motivations at play.