

Hacking for Good

Abdias Noel

July 27, 2026

Traditionally organizations either spend money to acquire good talents and security appliances or risk the cost associated with breaches when they occur. A third option called exists called “bug bounty” where the companies crowdsource additional skills to uncover vulnerabilities in their systems . In this article, the authors examine data from Hacker One from 2014–2020, to determine what affects the number of valid bug reports companies receive.

Some of the key findings were:

A company’s revenue and brand popularity had no economically meaningful effect on how many valid reports it received. This suggests small and large companies can equally benefit from a bug bounty program.

Finance, retail, and healthcare companies tended to receive fewer valid reports than companies in other sectors, although some of those findings were not statistically strong it may suggest that companies in these sectors proactively invest in the security of their systems.

Older programs received fewer valid reports over time because the easiest vulnerabilities are likely found first. Considering the scope of engagement allowed, this is to be expected. Expanding the program’s scope to allow researchers to test more assets may help offset this decline.

The researchers could explain only part of the variation in reports, meaning other factors, especially program scope and vulnerability severity—still matter and need more study.

Overall, the article argues that bug bounty programs are a useful crowdsourced cybersecurity tool. They give organizations access to a broad pool of ethical hackers, help uncover weaknesses internal teams may miss, and can be especially valuable for smaller businesses that cannot afford large in-house security teams.

The main conclusion is that bug bounties can benefit companies of all sizes, not only large or famous organizations. The findings also show that hackers are not motivated only by money because raising rewards produces only a small increase in valid reports. Other incentives of interests were reputation, learning, career opportunities, and altruistic motives.

Sources

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of bug bounties. *Journal of Cybersecurity*, 7(1), Article tyab007. <https://doi.org/10.1093/cybsec/tyab007>