The article presents a case for the use of bug bounty programs as a strategic approach to strengthening cybersecurity across organizations. The literature review offers two main justifications: the global shortage of cybersecurity professionals, particularly affecting small and medium-sized enterprises (SMEs), and the theoretical benefit of crowdsourcing cybersecurity through Linus’s Law—more eyes lead to more bug discoveries. What stood out to me in the literature was how bug bounty programs are not just about money; they’re about access to a flexible and diverse group of researchers. It’s a modern solution to a pressing tech industry problem and fits well into the broader gig economy narrative.

The discussion of the findings drove home the idea that bug bounties can work for companies beyond just tech giants like Google. The fact that brand profile and company revenue had statistically significant but economically *insignificant* impacts on the number of valid reports means that even less-known companies can benefit just as much.

Another point I found interesting was the discussion on industry effects. It makes sense that finance and healthcare companies receive fewer reports because of the higher black-market value of vulnerabilities in those sectors, which may dissuade ethical hackers from reporting them.

Finally, the observation that programs receive fewer reports over time was a good reminder that companies can’t just launch a bug bounty program and forget about it. They need to continuously adapt. Overall, the article was insightful and made a strong case for the scalability and practicality of bug bounty programs in a world where traditional cybersecurity hiring isn’t always feasible.