Journal Prompt 2 from Module 11

Ray Montes Jr

2 August 2025

The article talks about how companies are using bug bounty programs to help find weaknesses in their cybersecurity systems. These programs pay ethical hackers or “white hat” hackers, to find problems before real cyber attackers can. In the literature review, the authors explain that this idea comes from the fact that companies can’t always find every flaw on their own. They also say that working with hackers that used to be seen as threats can actually be beneficial if it is done in a safe and controlled way. Some companies have rules, contracts, or reward systems that try to keep the process fair and legal. In the discussion, the article explains that the programs don’t always work the same. The way companies set up the rules truly matters. For example, hackers are more likely to report what they find when they feel safe and respected. If the company threatens legal action or doesn’t pay fairly, hackers might not help at all. The article also points out that most of the hackers doing the work are not from inside the company, but rather outsiders who do it for money, experience or curiosity. This means companies need to think about trust and communication. Overall, I think bug bounty policies are a smart way to use the skills of people outside the company. It is kind of like paying someone to break into your house, just to see if your locks are good. If they find a weak spot, you can fix it before a real criminal shows up. It is risk, but it makes sense when done right.

References

Sridhar, K., & Ng, M. (2021, March 12). *Hacking for good: Leveraging hackerone data to develop an economic model of Bug Bounties | Journal of Cybersecurity | Oxford academic*. Journal of Cybersecurity. https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453