

A later module addresses cybersecurity policy through a social science framework. At this point, attention can be drawn to one type of policy, known as bug bounty policies. These policies pay individuals for identifying vulnerabilities in a company's cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try explore the cyber infrastructure using their penetration testing skills. The policies relate to economics in that they are based on cost/benefits principles. Read this article <https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=true>Links to an external site. and write a summary reaction to the use of the policies in your journal. Focus primarily on the literature review and the discussion of the findings.

Charles W. Pridgen

July 21, 2024

I believe the policy for companies to pay individuals to identify vulnerabilities in their cyber infrastructure is great. As the researchers mention in their article, the quote from software developer Eric Raymond, "Given enough eyeballs, all bugs are shallow," epitomizes how cybersecurity is best through teams/ groups of people. The more people combing through a company's cyber infrastructure, the more coverage and viewpoints it will be looked at through. It goes without saying as well, since Hackerone is open to the public, the diverse amount of people is guaranteed which enforces different viewpoints and strategies. Almost like a game, the policy enables competition, and creates a race for hackers to find vulnerabilities first. This can drive hackers to push their skills to the limits, increasing the amount of quality cybersecurity researchers overall, through real time experience, while at the same time increasing the cybersecurity posture of the company's cyber infrastructures.

The other aspect of the policy helping small and medium companies is also great. As mentioned in the article, large companies with plenty of money are able to invest a lot in cybersecurity efforts. This results in some of the best talents being unavailable. The bug bounty policy opens it up to every ethical hacker to find their vulnerabilities, allowing diverse groups of people of all ranges of talent, different viewpoints, and skillsets to find the vulnerabilities in their cyber infrastructure. I believe this is a highly valuable policy for small companies to efficiently pinpoint what

cybersecurity measures they need to implement to avoid major data breaches that would cause them to shutdown permanently.

Reference

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *Journal of Cybersecurity*, 7(1), tyab007.