James Applegate

4/2/24

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> 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.

The article discusses the evolving landscape of bug bounty policies in cybersecurity, highlighting the shift in attitudes among companies towards vulnerability disclosure policies (VDPs) and bug bounty programs. It notes that while many firms initially lacked VDPs, there's now a growing recognition of their importance, as evidenced by government mandates and industry recommendations.

Key points from the article include:

**Importance of VDPs:** Companies are realizing the need for VDPs to encourage ethical hackers to report vulnerabilities without fear of legal repercussions. This has led to increased participation in bug bounty programs.

**Government Advocacy:** Government agencies like the US Department of Homeland Security are not just mandating VDPs but actively advocating for bug bounty programs. This signals a broader acceptance of these initiatives as integral parts of cybersecurity strategies.

**Economic Incentives:** Bug bounty programs are not just about ethical hacking, they are also seen through the lens of economic principles. Companies are offering monetary rewards based on performance, creating a win-win situation that incentivizes hackers to find vulnerabilities and companies to strengthen their security. The article mentions HackerOne's milestone of $100 million in bug bounty payments, a testament to the economic viability of these programs.

**Challenges and Opportunities:** The article acknowledges the need for more empirical research on bug bounty programs, particularly regarding their impact on companies' cybersecurity posture, hacker behavior, and industry-specific vulnerabilities.

**Industry Variances:** It highlights industry differences in bug bounty participation and the challenges companies in finance, retail, and healthcare face in receiving bug reports compared to other industries, possibly due to the nature of vulnerabilities and market demands.

**Future Directions:** The article calls for more research into the effects of new compensation structures in bug bounty programs and the potential impact of competition on hacker participation.

Overall, the article emphasizes the growing importance of bug bounty programs in enhancing cybersecurity resilience and addressing industry-specific challenges, as well as the need for further empirical studies to understand their full impact and potential.