Gabrielle Gaston
CYSE 201

Journal 13

Bug bounty policies, as discussed in the article, are cybersecurity strategies that offer financial incentives to ethical hackers, formally known as white-hat hackers, for identifying and reporting security vulnerabilities within a company’s systems. The passage review emphasizes the increasing adoption of these programs, particularly in the tech industry, due to their cost effectiveness when compared to traditional security audits or hiring internal penetration testers. These programs are grounded in economic principles, especially cost benefit analysis. Rather than waiting for costly breaches or paying high salaries for full time cybersecurity experts, companies can crowdsource vulnerability discovery at a lower price point. The article illustrates that payouts for valid reports are often minimal compared to the potential damage a successful cyberattack could inflict on a company’s finances and reputation. This model not only makes financial sense but also encourages a more dynamic and diverse group of cybersecurity professionals to contribute to the protection of digital infrastructure.

However, the article also cautions that the effectiveness of bug bounty programs is not guaranteed without proper structure and oversight. The findings indicate that successful implementation depends heavily on setting clear rules of engagement, defining the scope of testing, and maintaining open lines of communication between companies and researchers. If poorly managed, these programs can overload cybersecurity teams with wasteful reports, leading to resource strain and reduced efficiency. Furthermore, there's a risk that ambiguous policies may encourage unethical behavior or foster distrust between companies and hackers. Therefore, while bug bounty policies align with market incentives and public interest by promoting collective cybersecurity efforts, they must be strategically designed to ensure quality control and ethical collaboration. This approach may foreshadow a shift in cybersecurity policy. There is potential to create a industry that blends technical innovation with social and economic theory to create more adaptive and resilient defense systems.