Brayden Thompson

Journal #12

In this article, they are explaining a experiment using the Bug Bounty strategy. The Bug Bounty strategy essentially means companies pay people, usually hackers, to exploit bugs and any vulnerabilities that can be found. This way the company can be prepared when these attacks actually come, and it gives a viewpoint from an actual hacker who has experience. The article explains why their experiment is accurate and in their conclusion they stated they found many plaguing sources in the companies cybersecurity field and helped identify strategies to prevent this from happening. Things they studied and concluded were things like for the first time in academic literature, they calculated the elasticity of hacker supply; hackers were found price insensitive. They also concluded some companies have more holes and bugs than others, depending on each company. Another thing they noticed is the Bug Bounty programs were receiving less valid results as time went by. They explain how hacker supply still was not studied completely; it is difficult to round out a justified answer for it. Overall, I think the Big Bounty strategy is a great and efficient tool to help companies dissolve of their vulnerabilities in the workplace. This can help them be ready for future invasions and help the company understand how to prevent attacks the way a hacker would.