Brendan Marcelo
CYSE201S
Journal Entry 13

This article was very insightful on the use of bug bounties and their importance in the realm of software engineering and cybersecurity. The classical economic theory is based on the ideals of supply and demand and belief that the government should not interfere in economy. This relates to cybersecurity specifically in this matter due to the "bugs" or "bounties" found provide companies to utilize hackers or freelanced cybersecurity professionals to enhance their system infrastructure without having the government intervene. Also, the Keynesian theory applies by allowing these companies funding or economic incentives by utilizing freelanced hackers or companies like Hacker One to detect and prevent vulnerabilities within their infrastructure. Companies reward these freelanced hackers or companies like Hacker One to find bugs in their IT system code base. Companies use the Linus Law to determine the use of bug bounties. This law is a principle in software development that states that when a large number of people review code, they can quickly identify and fix bugs and vulnerabilities. I find it very interesting as most of these free-lance hackers work part time and 27% of them are full time students. The average reward per bounty according to the article is $800. This showcases the amount of revenue that comes with being skilled in software engineering and cybersecurity. According to the article as of 2020, Hacker One has received $100 million in bug bounty payments. The areas of healthcare, retail, and finance have fewer reports of bugs and utilization of bug bounties; therefore, their systems are considerably more secure than others. This particular finding was surprising to me due to the amount of personal information these areas contain. The study shows that big companies such as JP morgan spend $600 million on cybersecurity, which raises awareness on the significance of cybersecurity to strengthen the integrity and confidentiality of companies IT systems. Furthermore, the study also shows that 60% of small business shut down within 6 months of suffering security breaches. Cybersecurity and economics intertwine with each other to provide a financially sustainable career and is a major sector of safeguarding private information.