**Journal Entry 13**

This article mentions that companies should promote a vulnerability disclosure policy. Vulnerability disclosure is important for bug bounties because companies send out these bounties to find vulnerabilities in their systems. Someone that might be taking on a bug bounty might want to be aware of this policy, since the company would set the rules in what is acceptable under the conditions of the bounty. Bug bounties are a popular way for companies to find vulnerabilities in their system. A lot of systems are complex, meaning the risk of an error increases with complexity. The company might not have time to search for these vulnerabilities, so a third-party could be useful as another set of eyes. Once the bounty hunter finds bugs in the system, they would then claim their monetary reward. This paper explains the importance of bug bounties well and why they would be needed in the technological field. It talks about the benefits of bug bounties and rationalizes the usefulness of these types of programs. For example, this article talks about industry effects. Hackers are more likely to target industries such as finance and health because of their monetary values and importance of data over an industry such as retail. Those that have more valuable data would then be better prepared, making it harder for bug bounty hunters to find bugs in a system.