Journal Entry 11-2

Name Brandon Tenn

Date 7/20/2024

Companies hiring ethical hackers are a good way for them to know about hidden vulnerabilities in their systems, although many companies are skeptical about the concept of having nonaffiliated work on their network. As the threat of cyber-attacks causing major financial impacts raises, companies need to review and learn new things about cybersecurity policies and their own systems weaknesses. This is where the use of bug bounty programs come into play. There are two main reasons for this, practical and theoretical. Theoretical is referring to the fact that there are more people other than the employees of the organization looking for holes in cybersecurity. Every cybersecurity professional and ethical hacker has something that they specialize in, as well as different skill sets and methods that they implement in their search. This aids in the detection of exploits that normally would have gone undiscovered. This is just like a saying that I heard a lot as a kid: “Two heads are better than one.” Whereas, practical revolves arounds the known shortage of IT and cybersecurity professionals in the workforce now. Which is estimated to be in the millions and will continue to be a problem as technology becomes more advance in the future. So, being able to outsource expert talent with bug bounty programs will help everyone from giant corporations to small business owners to be better protected from cyberattacks. As it stands right now, focusing more on bug bounty programs may very well be the best way to increase the level of cybersecurity across a variety of environments and businesses.

**References**

Sridhar, & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. *Journal of Cybersecurity (Oxford)*, *7*(1). https://doi.org/10.1093/cybsec/tyab007