Week 11 Journal Entry 13

A later module addresses cybersecurity policy through a social science framework. At this point, attention can be drawn to one type of policy, known as bug bounty policies. These policies pay individuals for identifying vulnerabilities in a company's cyber infrastructure. To identify the vulnerabilities, ethical hackers are invited to try explore the cyber infrastructure using their penetration testing skills. The policies relate to economics in that they are based on cost/benefits principles. Read this article https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=trueLinks to an external site. and write a summary reaction to the use of the policies in your journal. Focus primarily on the literature review and the discussion of the findings.

It is important to have mechanisms in place to reward both individuals and groups to come forward with vulnerabilities so that systems can be patched. The federal government recognizes this, Rod Rosenstein recognized this, and most, if not all federal agencies have a vulnerability disclosure policy in place now to encourage such reporting. However, many third-party businesses and entities do not.

While in theory an entity's cybersecurity professionals should be finding vulnerabilities, right now there is a shortage of 4 million employees to fill these roles. Bug bounty programs make up for this by giving hackers an incentive to report the vulnerability, rather than to make use of it in a malicious way to make money or illicitly retain some form of gain in other ways. By having vulnerability disclosure policies in place, those that report such vulnerabilities can be rewarded for helping to patch a security failure while not having to fear retribution for digging around in those computer systems in a manner that may otherwise be considered unauthorized.

For bug bounty programs to be effective in encouraging disclosures, there must be a decent financial incentive for those reporting. This is shown in how some industries receive more reports than others. What is surprising is how healthcare companies and entities do not receive a lot of disclosures. Such disclosures should be well-rewarded, and for the one disclosing those vulnerabilities, a sense of pride can be present in knowing that someone's life may have been saved, especially if it involved a vulnerability that could have negatively impacted hospital equipment.

Over time, as the reports detailing the disclosures and data gained from them, the success of these programs has been made evident. These programs have proven themselves

effective, and in turn, have saved the government and private companies millions of dollars that would have been otherwise lost due to cyberattacks or data breaches.