Andrew Plum

Mr. Alves-Foss

Cyb 110

10/13/21

Ch. 7 Homework

1) It is important to identify critical information because by identifying the critical information you can better determine which assets are most important to protect. By knowing which assets are most important to protect, you can better defend your assets in order of importance. For example, it is very critical that the government protects the nuclear launch codes from falling into the wrong hands because they are a very important asset, and they should guard it appropriately. Identifying critical information will also help you to implement appropriate defense mechanisms for the asset being guarded. For example, you aren't going to guard a secret recipe for a chocolate chip cookie the same way you would guard a fortune of 50 million dollars because the assets being protected in both instances are worth a value of great difference.

2) The first law of OPSEC is know the threats. Knowing the threats is important to knowing what to protect. To defend critical data successfully, you need to be aware of both the actual as well as potential threats facing the critical data. Knowing the nature of the threats and the ways in which they can threaten your asset is important to stopping these threats from being successful in their endeavors.

5) The difference in assessing threats and assessing vulnerabilities is in assessing threats, you are examining the things which are attempting to do something to the asset you are protecting. These threats might be trying to obtain, destroy, gain control, or cause any sort of harm to your asset. In assessing threats, you are looking at what the offensive force is trying to do and knowing the avenues in which the threat might use to affect your asset will aid in defending your asset. In assessing vulnerabilities, you are examining the things the threat is trying to exploit or could potentially exploit in order to do what it wants with your asset. In assessing vulnerabilities, you should look for spots in your defense which are weak and or could be easily exploited by the threat. Knowing the vulnerabilities to your asset can help you better defend it.

7) When you have cycled through the entire operations security process you are not finished with it. If an attacker is stopped from gaining your data, but isn't caught, what is stopping them from trying again? If you have an asset valuable enough, attackers will keep attacking which means defenders need to keep defending. Your enemy which seeks your data will be relentless which means you must be relentless too. You will need to repeat the cycle to evaluate the effectiveness of countermeasures put in place. Each time the process is repeated, take into account knowledge and experience you gained from the previous mitigation efforts as it will allow you to improve your security and better defend your asset.