Andrew Plum

Mr. Alves-Foss

Cyb 110

8/26/21

Ch. 1 Homework

1) The difference between a vulnerability and a threat is a threat is something which has the potential to cause harm whereas a vulnerability is something a threat can exploit to cause harm. When the threat is very potent and the vulnerability is very great, there is a high level of risk of an adverse effect occurring to an entity. An example of a threat might be a computer virus, and an example of a vulnerability might be a computer operating system with poor defense against this virus. This would mean that the data stored in this computer system is at high risk.

2) Six items that might be considered logical controls would be passwords, firewalls, encryption, intrusion detection systems (host-based or network-based), intrusion prevention systems, and access controls (like dual authentication systems). Logical controls, like physical and administrative controls, enable you to prevent unauthorized activities. Logical controls are not physical. Logical controls are sometimes referred to as technical controls.

5) You can consider your environment to be secure when there are no threats and no vulnerabilities meaning there would be no risk. However, this is an unrealistic reality. Threats and vulnerabilities to systems have always existed, and even though you may not be able to make your system 100% secure, you will be able to at least get it to be adequately secure. However, you want to be reasonable when putting in place security measures; you always want to make sure the cost of the security does not outweigh the value of the asset being guarded.

6) The layers I might use to secure myself against someone removing confidential data from my environment on a USB flash drive is number one a password which isn't written down to access my user on my computer which would be a part of the host layer of defense. If I have a desktop, I could unplug and hide the power cord every time I am done using it. This would be an example of a physical defense which would at least slow down the attacker as they would have to find the hidden power cord or find a new one which is compatible with the desktop computer. I could also put in place certain access controls like admin permission that are required to access the file. This would be a part of the data layer of defense. Another thing I could do at the data layer of defense is if I really cared about the data, I could also encrypt the data which would make it meaningless until decrypted if the attacker gained possession of it. These are only some of the measures I could put in place to better defend my data (the instructions did not say how many examples we need of defense).

7) If you lose a shipment of encrypted backup tapes that contain personal and payment information for your customers, the principles of the Parkerian Hexad affected are the possession or control principle. Because the data is encrypted, confidentiality is not affected. The integrity of the data is not affected because the data on the main system remains unchanged. The availability of the data is not affected because the data is still available on the main system. Possession or control of the data is affected because the data on the backup tapes has been lost and someone else could potentially gain possession

or control of this data. The authenticity of the data is not affected because the data is still from you and your customers and that cannot be changed or taken advantage of because the data is encrypted. The utility of the data is also not affected because the encrypted data is not very useful to the person who gains possession or control of it until it is decrypted; the utility of the data in the main system is still useful because it remains unaltered. So overall, the only principle from the Parkerian hexad affected because of this event is the possession or control principle.

10) The CIA triad and Parkerian hexad have several advantages and disadvantages. One of the advantages of the CIA triad is its simplicity, and it can be easy to use to discuss security issues. One of the disadvantages of the CIA triad is that it is sometimes not complex enough to describe more complex security issues. One of the advantages of the Parkerian hexad is because it is more complex, it can be used to describe security issues more accurately than the CIA triad. One of the disadvantages of the Parkerian hexad is it is less widely known than the CIA triad.