Andrew Plum

Mr. Alves-Foss

Cyb 110

10/13/21

Ch. 9 Homework

1) The three major concerns of physical security in order of importance from most important to least important is protecting people, data, and equipment. People is the most important thing to protect because unlike data and equipment, people are not easily replaced if killed from a business perspective. You can't keep a business running for example if your experienced employees are killed. People are also very fragile compared to most equipment. Data is the next most important thing to protect because after all, that is the asset which is being protected. Defense in depth should be used to protect the data. The final but least important thing of the three important things to protect is equipment. Equipment is the least important of the three important things to protect because it represents the easiest and cheapest category of assets to replace. To be successful in protecting all three of these things requires foresight and planning.

5) To block access to a vehicle you could install preventative physical access controls. This could be a gate that opens and closes when authorized as well as an accompanying concrete wall around the compound. This gate will vary in effectiveness depending on what kind it is and if a vehicle could just drive through it. Roadblock spikes at the entrance that come up when activated and go down when deactivated could also be implemented. This way if vehicle were to drive over it, its tires would be blown out immobilizing the vehicle. Trees, large boulders, and cement planters could also be placed in front of buildings or next to driveways to prevent vehicle access.

6) Three examples of physical controls that act as deterrents are signs, fake cameras, and light timers. Deterrent controls are designed to discourage attackers and generally indicate the presence of other security measures. Signs that tell attackers what is preventing them gaining access to the asset are designed to discourage attackers from attacking. Fake cameras, although they don't record anything, are effective at discouraging attackers because the attacker will be led into believing someone is at the other end of the camera watching them or that their actions are being recorded. Light timers installed in homes for instance where the lights turn on and off can be effective at deterring a criminal as they indicate human activity and that someone could be home.

8) A lock would be a part of the preventative security control as it stands between the asset and criminal and prevents them from obtaining it. It uses physical means to keep unauthorized entities from breaching your physical security. The lock wouldn't be a deterrent control as it isn't alerting you to any other physical security controls. The lock also wouldn't be a detective control because it isn't reporting anything to a system or a person and alerting them of an attack.

9) Residual data is data which is left after people have ineffectively erased it on the data storing device like a hard drive. Because the data was erased ineffectively, it could be recovered if someone really wanted to do so. Residual data is a concern when protecting the security of your data because if residual data is left on a storage device that is thrown away, it could be recovered by someone if the storage device remains intact. This can be very bad if the data is sensitive and if it falls into the wrong hands. To

deal with the problem of residual data, data storage devices that are thrown away are destroyed thoroughly and rendered effectively useless so the data can’t be recovered.