**Information Security Chapter 2 Questions**

Riley McCallay

1. Management has the ability to organize, make decisions and give structure to the security of what needs protecting. Unlike technology, human management can be held personally accountable for every aspect of security, including the technological measures that have been implemented. Human beings who are responsible and held accountable for the safekeeping of information are more motivated to stay competitive in a competitive world. Shortcomings among management could mean being replaced by someone more competent. At the end of the day, management makes the decisions that determine what human and physical and software technological components will define the protection of assets.
2. Data is important because it is the backbone of what makes up the organization. Some companies rely on the projects they are working on, or information they keep for their clients and customers, to function in the first place. Anything from phone numbers, credit card numbers and accounts, order histories, or other personal info about people needs to be kept safe. The organization’s data like projects, software, or things like their physical money and research, are all forms of assets that require protection.

5. Extortion is similar to blackmail. Someone who has gained access to sensitive information can use that information as collateral in order to threaten an organization into doing something. Someone can simply hack into something meant to secure and find out something that shouldn’t have been known. There can be loss of data or finances involved, and an organization might pay up I order to not have their info or data released into the world against their will. The threat might be against the customers and clients of the organization rather than against the organization itself. If valuable information that belongs to others is at stake and an organization was trusted to keep it safe, it could badly hurt that organization’s reputation to have that info released.

6. Employees can make mistakes, such as failing to log out of a computer, leaving a room unlocked, not turning of a workstation, or leaving login info somewhere visible to others. They can also unintentionally give away sensitive info, like talking too loud about something and someone overhearing, or falling victim to a social engineer. They can also intentionally internally sabotage a company just from knowing the right amount of privileged information. Individual employees are probably one of the hardest security risks to control as a whole.

14. Obsolete technology is a massive vulnerability because it is usually replaced very quickly in the technological world. Many people become proficient with it, and know how to take advantage of it and exploit any weaknesses it may have compared to the current level technology of the day. Keeping hardware and software current and up to date is a must to stay competitive, or at least take measures to keep any older or outdated technology protected. The older the technology is, the more vulnerable it becomes over time.