Unit 7 Critical Thinking Questions

1. **WeServeU Bank is requesting your assistance once again, this time with a question about physical security. They are thinking about installing a security camera in their public office, as well as a digital keypad lock for the private offices. What are the benefits of these security measures, and what considerations do they need to take to make such measures actually useful? (Connect with your instructor to find out if you have pre-paid access to simulation software to learn more about security installations.)**

The benefits of the cameras are that if anything wrong were to happen, they would have a higher chance of figuring out who caused a problem by being able to watch the video on the cameras. Whoever installs it would need to make sure it is in a hidden place so that it can't destroy it, but still able to get a full 360° view of the area. For the keypad locks, this would add extra security to the offices, as if someone tried to get into them they would have to pass through this keypad. They would need to make sure that these are good keypads that can't get hacked by people, as they can also be bypassed using special techniques.

2. **Why do well-designed sites give a generic "invalid username or password" response to incorrect password entries? What's another version of this that relates to password resetting?**

This is done so that if someone is trying to intrude into someone's account, they don't know which they got wrong. This makes it harder to get into the account. If they knew which field was wrong, it would be easier for them to get into the account as they would force their efforts on that one field.

3. **Consider DLM (data lifecycle management). Describe one piece of hypothetical "data" (a password, a document, an image, etc.) and discuss how it might move through at least FOUR stages in the DLM model.**

Stage 1: Data Acquisition and Capture - the information is entered into some kind of data infrastructure and accessible to certain roles within a hierarchy on whatever devices offer an access point to the proprietary system.

Stage 2: Data Backup and Recovery - data that has been entered into the system undergoes some kind of archival process that ensures redundancy.

Stage 3: Data Management and Maintenance - at this stage, data usage ensures the record meets certain validations to be accessible for users with access to the infrastructure. When data is published, it's made available to people outside of the system.

Stage 4: Data Retention or Destruction - in the final stage of the life cycle, data is retained or destroyed.

4. **Explain the difference between sensitive and non-sensitive PII and give examples of each.**

Sensitive PII is information that if lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Non-sensitive PII is any information that permits the identity of an individual to be directly or indirectly inferred. Examples of sensitive PII include your full name, Social Security Number, driver's license, financial information, and medical records. Examples of non-sensitive PII include your zip code, race, gender, and date of birth, which are easily accessible from public sources.

5. Consider the three major methods of destroying data. Compare the relative benefits and drawbacks of any TWO of the methods and explain at least one kind of data owner who might consider using that method.

The three major methods of destroying data are overwriting, degaussing, and physical destruction. **Overwriting** is covering up old data with information. **Degaussing** is erasing the magnetic field of the storage media. **Physical destruction** is employing techniques such as disk shredding to get rid of data. The benefit of **overwriting data** is that you can get rid of the data without having to destroy anything. However, it can be time-consuming when compared to the previously mentioned methods. Also, data overwriting may not be able to clean data from inaccessible regions such as host-protected areas. The benefits of **degaussing** are that it is a quick method and that it also protects you, your clients and your employees. However, there are some limitations. It is most effective when used on magnetic media such as hard drives and tapes, but not as effective on flash drives and SSDs. The main benefit of **physical destruction** is that it provides the highest guarantee of complete data destruction. The possibility that someone can recreate or recover the data from a disk or drive that's been physically destroyed is highly unlikely. However, this method is very prone to human error and manipulation. The majority of methods leave large portions of a hard drive's structure intact. For all these methods, they do the same thing in the end and anyone will use any method.