**CIS 481 – Intro to Information Security**

**CLASS EXERCISE # 1**

Grading ID: A7386

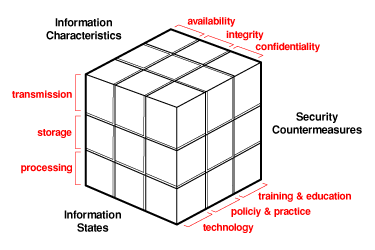
**Problem 1**

The CIA triad presents three essential characteristics of information that must be protected. However, most agree that these three characteristics are not the only ones that need to be protected. Other characteristics include authenticity, accuracy, possession, timeliness and utility. If you were tasked with creating an information security *rectangle*, instead presenting FOUR characteristics of information, which would you choose and why? (8 pts.)

To methodically encompass the characteristics necessary for protection, I largely agree that the CIA triad is a very good starting point. To create an information security rectangle, I would retain the three characteristics from the triad: availability, integrity, and confidentiality, and add the characteristic of possession to create the fourth point. Possession is related in many ways to availability but is still a distinct element. Where availability refers the accessibility of a system resource, such as a measurement of system uptime, possession refers specifically to the ownership of the information. I feel that it is critical for some entity to retain responsibility for the security of information in a system. Without that element, there is no accountability, and thus no incentive to keep the information in the system fully secure. If there is no accountability for the system, the other characteristics become largely irrelevant.

**Problem 2**

In 1991, John McCumber proposed a model for Information Security that uses a 3-D cube, as below. Describe the three dimensions of the McCumber cube. (9 pts.)



Information characteristics: Also refers to the desired goals of the McCumber Model, and is congruent with the three characteristics of the CIA triad. This dimension refers to the overall capability for information in the system to retain its accuracy while still being accessible by those who need it, and only those who need it.

Information States: Refers to the three distinct “phases” that information can be in while a user interacts with it. Stored data is secured, yet easily retrievable. It moves into the transmission state when a user requests access to stored data or returns modified data back to storage. The data moves to a processing state when the user modifies the data that he/she has retrieved.

Security Countermeasures: Refers to the practices that an administrator/system enacts in order to protect the data within. Training and education refers to the administrator’s practice of guiding users on the proper use of the system. Policy and practice refers to the rulesets that the administrator enacts upon the users to ensure that they do not compromise the data and follow the guidelines as given in their training. Lastly, technology refers to the hardware/software components of the system that are used to protect the data, such as a database that stores encrypted user passwords for login authentication.

**Problem 3**

How can the practice of information security be described as both an art and a science? How does security as a social science influence its practice? (8 pts.)

Information security is both an art and a science because there isn’t one correct answer on how to protect and secure the information in a system. A security approach must be dynamically created given the nature of the system as well as the nature of the people who interact with it. That being said, there are well-documented and effective strategies that can be used as a sort of reference for determining the best approach. Security is also seen as a social science because its implementation can be influenced and guided by the users and the environment just as much as the information itself. If people in an organization exhibit certain patterns or behaviors that occur when they regularly interact with a system, these must be taken into account when determining an approach to security.