**CIS 481 – Intro to Information Security**

**IN-CLASS EXERCISE # 1**

Names of team members: Team 9: Corey Cooley, Taylor Payne, Will Brown, & John Hopson

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don’t just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

**Problem 1**

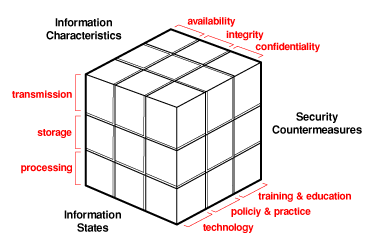
The CIA triad presents three essential characteristics of information that must be protected. However, most agree that these three characteristics are not the only ones that need to be protected. Other characteristics include authenticity, accuracy, possession, timeliness and utility. If you were tasked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

*Our security rectangle includes confidentiality, integrity, availability, and accuracy. We decided the triad is still a solid base to build security on and that accuracy stands above the remaining characteristics. In the triad we deal with privacy, wholeness, and accessibility, all of which are the prime characteristics of information security.*

*In relegating the remaining characteristics to lower priorities, we feel like possession and authenticity can be addressed through encryption and verification. An asset’s utility is also a characteristic that is morphable depending on the organization and even on divisions, teams, and individuals in an organization. Accuracy, however, is important not just for banks and hospitals, but for any organization. Data that is not accurate is worse than useless, it can be harmful. Communications and networks that can’t provide accurate transmissions can bring down every other part of an information system.*

**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.)



*The basic concept of the three-dimensional design is to address the need for secure information, as well as to achieve security goals that information security must address. Each view of the cube represents a different interdependent perspective. The three dimensions are Information Characteristics, Security Countermeasures, and Information States. As it relates to the McCumber Cube, confidentiality in the information characteristics dimensions is to prevent the disclosure of sensitive information from unauthorized people/users, resources, and processes. Integrity is the protection of system information or processes from intentional or accidental modification and availability is the assurance that systems and data are accessible by authorized users when needed.*

*When we are looking at the information states, we see that processing is performing operations on data to achieve a desired objective. Storage represents when data is at rest, and that information is stored in memory or on a disk. Finally, transmission is the data in transit, transferring data between information systems. The third and final side is Security Countermeasures, and is focused on the ability to enhance security through management. Policies are implemented in the form of administrative controls that provide a foundation for how information assurance is to be implemented within an organization. Technology is the software and hardware-based solutions designed to protect information system such as firewall or antivirus. Training and education is ensuring that users of the information are aware of their roles and responsibilities relating to the protection of the information system and following standards that are set forth by the company.*

*These three perspectives relate all together. The security countermeasures are put in place and basically required to achieve the full confidentiality and integrity of data in the information system through training employees and using the appropriate technology to keep information safe. Proper training and policies allow employees to follow a formal process in using the data, and creates an environment that emphasizes the importance of data security. The information states, which include transmission, storage, and processing, are heavily related to each of the other dimensions. Storage requires technology in order to encrypt sensitive data, and this data is given availability or not depending on who needs to access the data, and allows sensitive data to remain safe. During the processing stage, the data has to be unencrypted in order to be processed in the system, and so policies are put into place in order to protect the information as it is being processed. Finally, in transmission, the packets can be encrypted or unencrypted depending on policies or procedures and these allow you to securely and confidentially transfer information ensuring it is received with integrity while remaining available to only those in your network that have permission.*

**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 can be an art in the sense that there are no set-in stone rules for how it is to be done. An art piece can be created with paints, pencils, markers, etc. by filling in an outline or free handing a design. Security can be designed in any way the project champions or other security professionals see fit for their circumstances. This allows for different implementation strategies and techniques depending upon the security “artist” behind the project.*

*Information security can be viewed as a science as well, just like chemistry or other scientific subjects. Certain objects and conditions in the current environment can cause various actions that computers output. Computers have many vulnerabilities that all relate to a different piece of hardware or software design flaw that can only are exposed when specific circumstances/conditions occur. Rather than attempting a security technique that could be exposed like a volatile chemical, there are certain techniques that are tested and trusted to mitigate security risk. Utilizing engineering concepts and techniques helped to pull information security out of the early time of being nearly entirely a by-the-seat-of-their-pants art to a more scientific practice. While there is no perfect security manual, just like there is no perfect science to developing software the trusted methods when used can help to develop a more secure system.*

*Social science as it relates to information security revolves around the individuals who are utilizing the system. The user will always be the weakest link in the information security chain if they are not properly trained and informed on procedures, but also if the security plans in place are too strict causing an excess burden on users (i.e. password requirements) that may cause them to circumvent security measures. Users need to be able to understand and use the system effectively, but newly introduced security measures and protocols may hinder their ability to access or utilize resources in the same fashion as they always have causing backlash. The security team needs to work in tandem with the users to ensure they are informed of changes and use the system properly.*