CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #1

Team: 6
Participants: Regis Wilson, Kelsey Beeler, Mahendra Khanal, Anthony Combs

Logistics

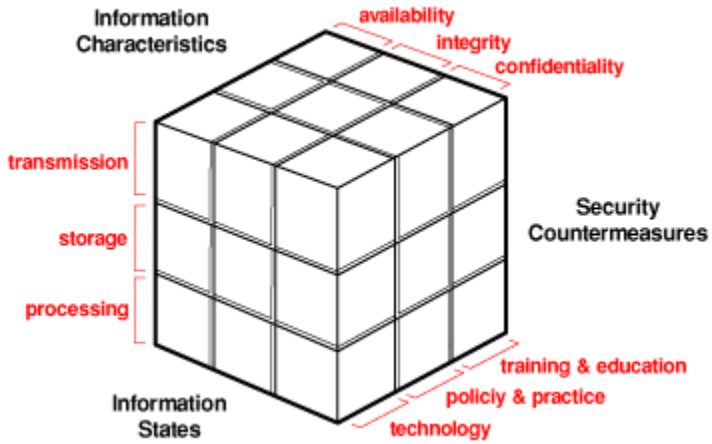
A. Get together with other students on your assigned team in person and virtually.
B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.
C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

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 expanding it into an information security *rectangle* instead by adding a single additional characteristic of information, which would you choose and why? *(8 points)*

Authenticity *- We chose authenticity because it would be important to have the best information and for it to be genuine rather than it being duplicated or reproduced and running the risk of data being compromised or corrupted.*

Problem 2

In 1991, John McCumber proposed a model for Information Security that uses a 3-D cube, as below. Describe each of the three dimensions of the McCumber Cube and comment on the interaction of the three specific sub-components in one of the 27 cells within the Cube. *(9 points)*



1. Information Characteristics: properties that our data should maintain
    a. Confidentiality – making sure that only authorized individuals have access to the data or information.
    b. Integrity – keeping the information reliable so that it is completely uncorrupted
    c. Availability – making sure that individuals have access to the data with the correct format without any type of obstruction or interference
2. Information States: how the information can be held and protected during various tasks
    a. Transmission – transfer of data between information systems
    b. Storage – storing data at rest in an information system
    c. Processing - execution of an operation on an information system
3. Security Measures: procedure or attribute of securing information
    a. Training and Education – ensuring that users of information systems are aware of their roles and responsibilities of protecting information systems
    b. Policy & Practice – managing operations and practices that are in place to help set standards to keep information safe and secure
    c. Technology – Hardware and software that is used to ensure information is protected

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 points)*

The way that the practice of information security can be described as art is because there are no written rules on how to develop a system for information security. This takes creativity and deep thought, along with expertise. The administrator who installs the security system has to decide for themselves which installation best suits them and their needs to ensure that the availability and security of the system are balanced. Much like an painter where he or she must look and assess their canvas, and plenty of other things to make sure that the initial stroke is going to benefit them throughout the duration of the time being used to set up the entire painting. This coincides with an administrator trying to solve a problem and weighing possible solutions to make sure that the outcome will be beneficial.

One way that the practice of information security can be described as a science is that almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware in software. Another reason would be that specific conditions cause virtually all actions in computer systems. Both of these reasons represent information security as a science because they show that all actions within the system have to be cause by some force or how the system would interact with itself.

Security as a social science influences its practice because social sciences deal with understanding how an individual or the behavior of an individual would interact with a system, and the security of a system begins and ends with the people that interact with the given system, whether the initial interaction is intentional or not. Knowing how to pair this with the user experience is sometimes just as difficult as the technical aspects. End users need to use the information you are trying to protect. This is the intersection of all three ideas.