CIS-481: Introduction to Information Security

Module 1 - Introduction to Information Security

Exercise #1

Team: Team X
Participants: Charles Degboe , Sam Martin , Abril, Ricardo, Nicholas

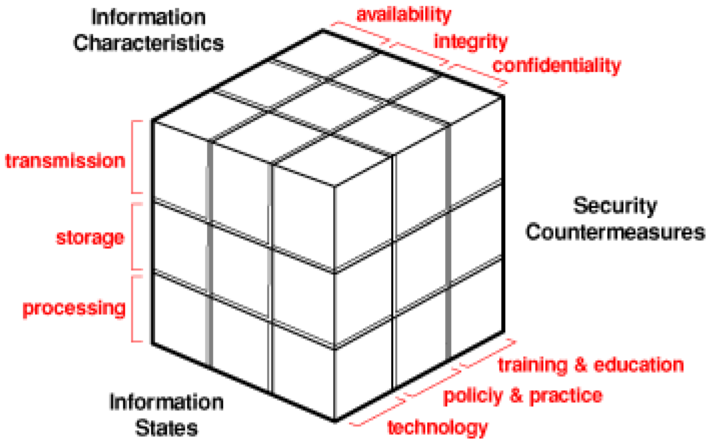
Logistics

A. Get together with other students on your assigned **Team** in person and/or 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 and may impact your performance on assessments, especially with respect to the essay questions.
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 *(8 points)*
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?

We would add authenticity to our information security rectangle making it , confidentiality, integrity, availability and authenticity. Without authenticity an unauthorized user can access our data which can be very crucial. An unauthorized user can put our data at risk , which either be tampered with or data can get stolen. This also helps keep the originality authentication of our data , so that way it can't be mess with and be replaced with something else.

Problem 2 *(9 points)*
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.



McCumber model represents the CIA characteristics which are: Confidentiality, integrity, and availability. The model describes where these components will be placed and how they will be placed. The model is a universal application that serves as a control.

Problem 3 *(8 points)*
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?

Information security can be described as an art and a science in many ways. The way information security can be interpreted as a science is straight forward. The technological principles that are applied to information security can only be defined as a science. There are also many ways as well. One of them is the way that we make decisions based in this field. When addressing different issues and how to fix them, most of our reasoning will be pulled from a study. This is how everything in the science field operates, studies and hypotheses. Anything that is very data reliant will always be some sort of science. Information security can also be seen as an artform too since there is room for creativity and different problems can be solved in different ways. When some protocol is in a test phase, the goal is to find the holes to make the product better. Each developer can have a custom take on things. Something that really reminds me of this is coding in general. Yes, everyone must follow the same syntax or else the code won't interpret, but with that said, there are very many different coding styles that can accomplish the same task. When I think of information security as a social science, what comes to mind is how legislation can impact certain procedures. Yes, there is still a science to it, but society impacts it as well