CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #1

Team: 1

Participants: Jacob Forcht, Trevor Hagel, Zack Graas

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 *(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.

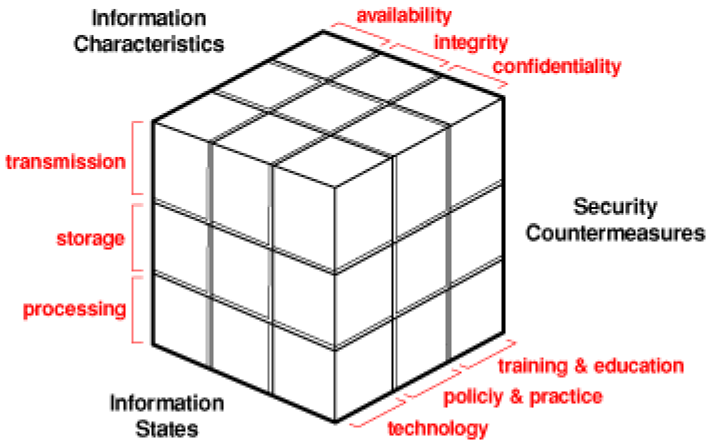
If you were tasked with expanding it into an information security *rectangle* instead by adding a single additional characteristic of information, which would you choose and why?

The CIA triad indicates that the three essential characteristics of information that has to be secured are Confidentiality, Availability, and Integrity. However, if you were to add one more characteristic, then authenticity would be the best fit. You always want to make sure that the information you're getting is coming from the person entering all this information and not a robot. For Example, a lot of logins ask for the users to check to see if they are a robot by doing a test to see if they know certain images. This is testing the authenticity of a person because they don't want robots activating an account that doesn't belong to a real person. Another way to test the authenticity of information is by asking personal questions. Banks use this technique to see if it is the actual person that owns that bank account. They can ask a variety of questions from "Where did you go to elementary school?" to "What was the name of the first pet you own." Finally, authenticity could help lead to accuracy of the information to see if the information is true and real.

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.

I will talk about the technology used to protect storage availability. Availability means that the asset is able to be used when needed. Some things that could interrupt this could be DDoS attacks, power outages, natural disasters, and hardware failure. To protect the availability with a technology control against attacks one could get an anti-DDoS protection package. It appears to be sold by many companies that will provide a network solution that detects and diverts the attack while still letting valid traffic through. A technological control that could protect availability from power outages could be an uninterruptible power supply or USP. This device would provide power during a power outage and allow the asset to still be used. If the power is going to be out for a long period the UPS could even give power to a system so that it could failover to a backup system allowing the system to still be accessed when needed. A technological control that could protect availability from natural disasters could be a failover system to reroute traffic to during a natural disaster. A technological control that could protect availability from a hardware failure would be a software backup system. An example of this would be having a RAID storage configuration that includes data redundancy so if a hard drive fails there is a copy of that lost data somewhere else in the system.



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?

The practice of information security can be described as both an art and a science. As a science, the practices of security can be based around quantifiable data and design. Best practices can be made through statistical analysis of threats and the possible loss of a data breach. As an art, information security is constantly changing and requires thought and action that is not quantifiable.

Security as a social science influences its practice in every organization. The weakest part of every security system is the people. Humans make mistakes and cannot always be predicted, and therefore their actions cannot be quantified. To maintain security in your system, you have to study info-sec as a social science as well as a hard science, otherwise there will be holes in the system. Security practices must be designed with humans in mind, so it can't just always be assumed that practices will be followed every single time. There has to be fail-safes that ensure data security.