**CIS-481: Introduction to Information Security**

**In-Class Exercise #1**

Names of team members: Trevor Rawleigh, Samantha Conway, Noah Smith, Elise Timmons

Logistics

A. Get together with other students on your assigned team

B. Discuss and complete the assignment together. 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 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 creating an information security *rectangle*, instead presenting FOUR characteristics of information, which would you choose and why? *(8 points)*

First and foremost, **Confidentiality** from the original triad would remain. If the information is accessible to anyone and everyone, then that defeats the whole purpose of the security and safeguarding of data, to include sensitive information such as social security numbers, personally identifiable information (PII), and health information.

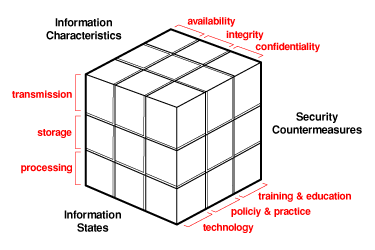
Secondly, **Availability** would stay from the original three as well. If the information is so well guarded that no one can get access, then the information is useless. Information and data need to be accessible in order to benefit the organization/person that controls that data.

Third segment would be **Accuracy**. If the information is not correct when entered, then it is not only useless, but will cause issues when pulled into reports that could influence a multitude of other departments.

The last leg of the info-sec rectangle, I would consider **Personal Responsiblilty**. Time and time again we are told that humans are the weakest link when it comes to information security. Not only do we fall prey to scams and fraudulent attempts to gain access to databases, but simply a lack of knowledge can lead to leaks of information. Such as taking home work on a personal drive could unintentionally compromise the data that was extracted.

**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 points)*



Breaking down the 3 ‘sides’, we can look at the information states first. This is how data is currently being used, either being sent to other departments (transmission), “at rest” as stated by Whitman and Mattord (2018, p. 52) in a database which will fall under storage, and data that is being processed, either through reports or being manipulated through SQL statements.

The next side we will look at is security countermeasures. These seem to focus more so on the human element of securing data. From training on how to properly use and secure data, to broad policies that affect companies as a whole.

The final side is the CIA triad as discussed earlier. These are the 3 fundamentals that should be implemented to every aspect of an information security program, across all industries, as a basic requirement to conduct business.

As shown in the video from the slides, the cube can be ‘rotated’ to incorporate 1 of each of the 3 ‘sides’ and the cube should represent a single aspect that should be focused on. For example, lets take Availability, Storage, and Training & Education. One could ask, does the person that is responsible for the storage of data have the proper training to make sure the information is available to others that need access?

**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)*

Info Sec can be described simply as an art due to the fact that each CIO/CISO or even a developer might have a certain way of going about implementing security. Each take on security can be seen throughout the internet. From sites simply requiring a username and password, to sites requiring a code be input from a separate source (2 factor authentication). There are different variations that are adopted but no one way is correct.

But on that note, Info Sec as a science has been described by Whitman and Mattord (2018), that “Best practices… and other tried-and-true methods can minimize the level of guesswork necessary” (p. 42) when it comes to securing any sort of data. There are many techniques that are recommended and should be adopted if you are to stand a chance in today’s modern technological age.

Lastly, Info Sec as a social science can be easily seen through the end user’s behavior. How an end user actually manipulates a web page will dictate further development. If a user is not happy with the amount, or lack thereof, of features, or if the site is too advanced for a common user to navigate, then the site can be considered useless. It all comes down to the end user’s happiness. Did you succeed in supplying the user with what was requested, or did you fall short in some areas? Only time will tell, on a site to site basis.