CIS-481: Introduction to Information Security

Module 1 - Introduction to Information Security

Exercise #1

Team: 3

Participants: Ashley Aguilera Rico, Raveen Bryant, Ryan Foster, Yen Hsieh Hsu, Abby Nguyen

Logistics

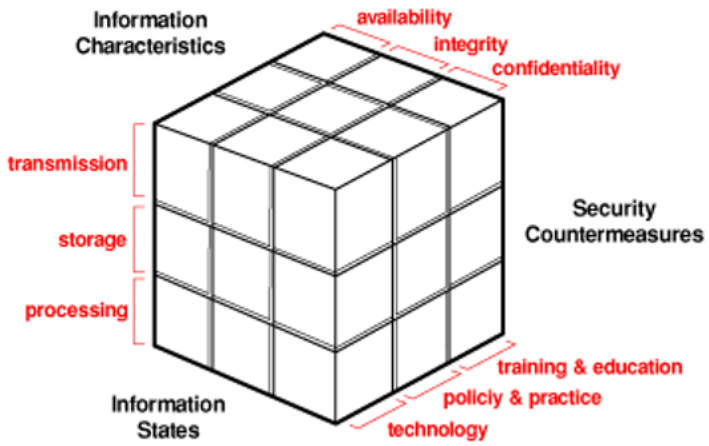
A. Get together with other students on your assigned **Team** in person and/or virtually.
B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, 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?

All of the characteristics are important, but we would personally choose Authenticity over the others if our choice was restricted to one of the remaining characteristics. Authenticity, by definition, is the assurance that a transaction, message, or some other kind of exchange of information is actually from the source that it claims to be from. This is basically proof of identity and is essential, not just in information security, but in everyday life. No one would accept information or products from someone they did not know and that is exceptionally true in information security. The ability to verify the source of information is so important because data from unconfirmed sources can have malicious software that could compromise a system or the information itself could simply be misleading or completely wrong. The other remaining characteristics are important but verifying sources seems to, logically, be the next important aspect of information security.

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.



The first dimension of the McCumber cube is information characteristics and that refers to the foundational principles created within the theory of information security to protect and uphold cyber security protocols. The second dimension is information states and this relates to the large amount of valuable data that is collected, processed, and in need of protection. The 3rd dimension is security countermeasures and refers to the extensive knowledge, measures, and tools that equipt professionals with an expansive toolbelt to calculate and resolve risks.

An interaction of three subcomponents are confidentiality, policy and practice, and storage. Confidentiality is upheld within the policies and practices of a company/organization in which it states the specific rules in regard to keeping information confidential, which coincide with storage, because depending on how the policies state information is stored, will determine how confidential the information is.

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 art since the practice is comparable to a painter applying oils to a canvas, which can be compared to security

teams not overly restricting user access. It can also be described as art because there is no “correct” way or a universal solution to implementing information security, and it all depends on the security team’s creation and ideas. A program we create could be completely different from a program another individual makes but accomplish the same end goal. The program or attempt at intrusion into a system or computer can be sloppy and poorly written or considered by peers to be exceptional and even elegant in its design. There are also no clear rules that explain how to install or create information security programs as they are constantly evolving. Many individuals within the cyber security community will have respect for certain individuals or firms that create good products or are capable of finding openings in secure systems. There are even yearly competitions for penetration testing into systems.

It can be described as science because there are many different tools that have been developed to combat exposure to hacking attempts and safeguarding the integrity of information. Some examples of these tools are encryption tools that safeguard information for storage or transmission, network intrusion detection programs that have been developed, firewall tools, web vulnerability scanning tools for web security, and other network security monitoring tools. All of these tools that have been created require an in-depth knowledge of the fundamentals of how networks and computers work as well as knowledge into computer programming and even math to assist with encryption.

In terms of social science, it comes from the interaction between the users and the system. The systems should be simple enough for users to want to use the system, and be secure enough to block out threats, such as end users needing to access information that security personnel want to protect, increasing the risk in information security. To develop a system to support both points and reduce risks, it is necessary to understand some behavioral aspects of organizational science.