CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #1

Team: 5
Participants: James Hoagland, Ethan Grimes, Gregory Ellis, Holli Grubbs

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)*

If we were tasked with adding a fourth characteristic onto the CIA triad, I believe it would be beneficial to add timeliness. Without the delivery of information in a timely matter it can lose too much or all its value if it is delivered too late. Timeliness is also especially important in information security today because technology is evolving every day at a rapid pace. New threats and vulnerabilities need to be addressed in a timely manner because if unchecked they can wreak havoc on systems, sometimes to a degree that is unrepairable.

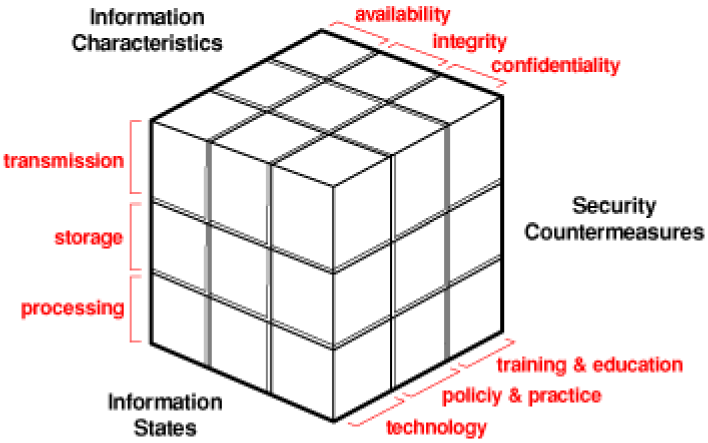
Another reason we would add timeliness to the information security *rectangle* is because many business decisions that are made today and impact our future is based on real-time data collection. If businesses today were not able to collect and decipher that large amounts of data, they receive in a timely manner then they would be unable to compete in todays market.

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)*

The John McCumber cube features three dimensions, each having three attributes. To start off, the Information characteristics dimension has availability, integrity, and confidentiality. These three attributes also make up the CIA triad, the industry standard for computer security since the creation of the mainframe.

Availability allows authorized users—whether it's a person or a computer—to be able to obtain information without any obstacles. Integrity is when information is whole, complete, and uncorrupted. And finally, confidentiality is when information is protected from being exposed or leaked out to unauthorized personnel.

The next dimension is Security Countermeasures. This dimension is made of three characteristics: Training and education, policy and practice, and technology. Training and education instruct users how to implement and maintain the security of a system. Policy and practice provide system users with the rules and regulations that must be followed when using said system in order to minimize risks. Technology is the final characteristic within this dimension. Technology can either create more or less risks depending on how advanced it is. Outdated technology can have outdated system security and be susceptible to outside users and slow performance. The more advanced the technology is, the better the security and performance levels.



The final dimension is Information States. The three characteristics are as follows: transmission, storage, and processing. Transmission is how information and data are transferred throughout the system. Storage is how data and information are stored. Finally, processing is how data is extracted or manipulated from stored files.

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)*

Just like art, the practice of information security is not tied down by rules and there is no universal solution. Companies can have similar practices, but they will never be the same. The practice of Information security is a science as well. It utilizes cutting-edge technology that enhance performance levels and manage all future actions in computer systems. It also monitors the vulnerability and risks involved in a system. Security influences the way individuals interact with the system. If there is low security, then it will be easier for individuals to tamper with the system or worse. High security maintains low risks and create more acceptable/supportable security profiles.

As the book describes in chapter one, a system can have unintended functions or operations. Attackers can learn of these unintended functions or operations and exploit them. The idea of security as a social science is a way of looking how people interact with information systems. By looking at it this way, and using one example of the attacker exploiting certain functions or operations, we can see how it would influence the way security personnel protect the information within the system.