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

**Module 1 - Introduction to Information Security**

**Exercise #1**

**Team: 3**

**Participants: Dustin Thompson, Destinee Matsoumou, Bryce Watson, George Flarsheim, Bradley Lawton**

**Logistics**

1. Get together with other students on your assigned **Team** in person and/or virtually.
2. 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.
3. 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)*

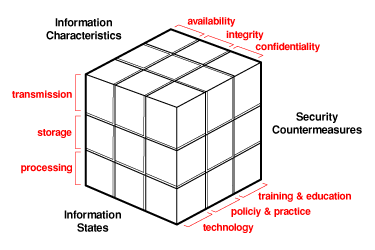
The CIA triad presents three essential characteristics of information that must be protected. However, most agree that these three characteristics are not the only ones that need to be protected. Other characteristics include *authenticity*, *accuracy*, *possession*, *timeliness*, and *utility*.   
If 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?

I argue that timeliness is baked into the idea of data. If data is not authentic or relevant, then it is not useful. Thus, I would not choose authenticity as the 4th side. I will argue for possession as the 4th side.

Possession should make up the fourth side of the CIS rectangle. Confidentiality covers users or the people with the rights, privileges, and needs to access the information. Integrity covers the authentic state of the data; if it is not authentic, it is useless. Availability covers access to the data not only by people, but also by information systems. Possession can be a breach without a breach of confidentiality. This will be an increasing threat to organizations as hackers gain access to an ever-increasing set of information. This includes the rise in social media gathering our information and social engineering in terms of organizations wanting to know our shopping habits and more. Who has a right to this data? Do individual users give up exclusive rights to this data? Can it be used against organizations, such as in ransomware attacks? And you could also include advances in computing such as quantum computing which will allow rival states to gather data while encrypted and much more easily decrypt it later, thus making possession an option for the 4th side of the CIA.

**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.



Using the McCumber Cube as the primary tool in information security, an organization can more confidentially address its information security concerns. The information characteristics side of the cube covers the traits of the information trying to be managed by its subcomponents coming from the CIA triad. Next is the Information States. They can be thought of as the when and where of the problem Whether in storage processing or transmission the data must still be protected, and the method of protection might have to vary depending on the situation. The security countermeasures dimensions of the cube are best thought of as how and in what manner you will use to secure the data. Each subcomponent covers a form of security measure whether through technology policy or training.

Putting this into perspective, say a company has data in storage and has covered all the security countermeasures for confidential information while in storage. All effort in storage becomes wasted if the data is sent unencrypted over Wi-Fi. The value of that information drops in lost confidentiality; if the company had used the McCumber cube as a lens, they would have made sure not to cover its confidentiality in storage but in processing and transmission. In the case of the transmission confidential technology cell, the company could have covered this issue by using encryption technology on data transmission. To truly cover all bases of transmission security, the company will still need to train employees on how to use encryption and set policies to ensure the use of the technology. This shows a solid view of how even looking at one cell will cause you to look at those around it, helping to ensure a security system with less likelihood of failure.

**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?

Yes, the practice of information security can be described as an art and a science. You need both artistic ability and technical skills to manage it. The text compared info security workers to painters applying oils to canvas. This is because you don’t want to overwhelm the users as an information security worker. You want to be careful with the structure of the system you design so it’s easy for the user to use and understand. Also, the complexity of an entire organization’s information system cannot be met by one tool or technique. While there are tools and techniques for securing different pieces of the information system there is not a one size fits all approach. It takes the expertise of systems administrators to employ techniques that allow access to data without restricting it too much. User access needs to be timely, accurate and authentic.   
  
This is also how security as a social science can influence how systems are made and their practices. Information security workers design a system based on the user’s capability to grasp it. Because social science examines the behavior of people as they interact with systems. Information security needs the art side of things to appease the general user and not make it too complex.