Joshua Main-Smith
UFID: 7160-7655
September 6, 2020

Module 1 Assignment

1. **(20 points) Choose one of the design principles listed in section 1.4 of the textbook. Write a paragraph describing an example of this design principle being followed or not followed. This can be an example from your experience or an example you read about or researched. It does not have to be a computer system.**

   Fail-safe default: The real-world example I immediately thought for this is our court system assuming innocence until proven guilty. That is, the default situation is whoever is on trial is assumed innocent unless a threshold of evidence has been provided to grant a guilty verdict. If the reverse were implemented, i.e. guilt is assumed until proven innocent, then it would result in a terrifying number of false positives. Represented as pseudocode:

```
isGuilty()
{
    if (enoughEvidence == TRUE)
        return TRUE;
    else
        return FALSE;
}
```

2. **(20 points) For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.**

   a. An organization managing public information on its Web server.

   C: Low. As long as the loss of confidentiality lies only in the realm of public information, the consequence of a breach remains low. With the information being publicly available, it would be safe to assume that the information isn't sensitive and would therefore result in minimal harm to the end user/enterprise.

   I: Medium to High. Depending on what the information is used for, the consequence could be anywhere from having an adverse effect on operations to being sever. One example of this being severe would be a weather app. A loss in integrity (a loss in an accurate portrayal of the weather) would undermine the app's primary purpose and might drive users away (a financial hit). A medium score could be a news organization writing an opinion piece while having some publicly available political statistics at the bottom. A loss in integrity here might undermine the news organizations legitimacy, but the primary purpose for the piece probably isn't to showcase the statistics.

   A: Medium to High. For the same reasons above, it depends on what the information is used for. A news organization's publicly available statistics being unavailable isn't too severe in the context of an opinion piece. Alternatively, the CDC's coronavirus public data being unavailable would be catastrophic due to the number of other organizations relying on accurate statistics from the CDC (and due to the CDC being critical infrastructure).

b. A law enforcement organization managing extremely sensitive investigative information.
C: High. A breach in confidentiality could have anywhere from severe to catastrophic consequences. The primary purpose this organization is to get to the truth of whatever it is that they're investigating. A breach could negatively impact their investigation and of the victim/victims involved in the breach, undermining law enforcement's primary purpose.
I: High. For similar reasons given above, this organizations purpose is to investigate the truth, or what likely appears to be the truth, of whatever it is that they're investigating. When the evidence has been tampered with, it undermines one of their primary functions.
A: High. When an item for investigation (a missing laptop from the evidence locker) is unavailable it could mean the difference between a guilty and not guilty verdict. In order to perform the investigation properly, authorized law enforcement needs access to the information.

c. A financial organization managing routine administrative information (not privacy-related information).
C: Medium. The daily functions of an organization may be sensitive for the organization, especially if the service from this organization is novel and innovative. A concern this organization may have is corporate espionage (especially if the above condition is true). But, a breach in confidentiality wouldn't result in a loss of the primary functions for the enterprise. Therefore, the risk is moderate.
I: High. If routine information has been compromised, then the primary purpose of this organization could also be compromised. The routine information is probably essential for the enterprise (otherwise, it wouldn't be routine) and thereby have a negative effect to one of its primary functions. An example would be instead of buying 120 stocks in Tesla 1200 stocks were bought. Multiply these "mistakes" by a couple hundred users, the organization will have a lot of very angry customers looking elsewhere for their money to be handled.
A: High. If the information is routine, it's probably essential for the business. Therefore, having access to this routine information would be vital for the organization to function properly.

d. An information system used for large acquisitions in a contracting organization contains both sensitive, pre-solicitation phase contract information and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
Contract Information
C: High. With the information being sensitive it's important to keep it confidential. A breach in confidentiality could have potentially severe consequences to the individual(s) involved, depending on the sensitive information that has been released.
I: High. With it being a contract, it's important that the integrity of the document be kept with it being a legal agreement between contractor and organization. A breach in integrity could lead to the organization/contractor misinterpreting or being misinformed of what was agreed to in the contract, possibly leading to court trials if unresolved.
A: High. With this being contract information, if there is any dispute about what the responsibilities of the contractor's are it would be customary to refer to the contract agreement. If the contract information is unavailable, then the primary functions of the enterprise could be

hindered until the dispute is resolved. Without the contract information available, this would be difficult to accomplish.

Administrative Information
C: Medium. For the same reasons outlined in c, a confidentiality breach could have an adverse effect on the organization, but it wouldn't hinder their primary functions.
I: High. With the information being routine, it's safe to assume that the information gathered is essential. If the information is altered, then it could potentially hinder some aspect of the primary function of the business.
A: High. For a similar reason given above, the routine information generated is probably needed for the daily functions of the business. With it becoming unavailable, its daily functions would be hindered.

System
CIA: High. With the organization containing sensitive and non-sensitive information it would be important to know what information an attacker had access to. If such information is unavailable or unknown, then it should be assumed a high risk for a breach in confidentiality.

e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.
Sensor Data
C: High. If an attacker has access to the system that controls the distribution of electrical power to their respective departments in a military operation, the attacker could then use this as a pivoting point in determining where and how electrical power is distributed. Sensitive information like this could provide an informed attacker, or even a foreign asset, critical information in finding a way to deny this critical infrastructure an essential utility.
I: High. The essential utility being denied distribution would hinder a military installations daily functions.
A: High. Ability to manage this essential utility is paramount to functioning daily. Without access to SCADA management the installation would be subject to the whims of the attacker.

Administrative Information
C: High. A breach in confidentiality may be more of a concern in critical infrastructure, even for routine administrative information. Such confidentiality breaches could be the subject of a foreign attacker, which has national security ramifications in the context of military infrastructure.
I: High. It's important for the routine administrative information to be accurate, so that the primary functions of this organization can function properly.
A: High. Not only does the routine information generated need to be accurate, but it also needs to be available to function properly.

System
CIA: High. With the organization having sensitive data (energy distribution) and with its functional role in society and with foreign actors potentially having a vested interest in the (un)success of the US, a high risk was assigned to all CIA categories.