**Defining Cybersecurity Template**

**Part 1 – Key Terms in Cybersecurity**

For each item in the table, write a definition and provide a concrete example of what is being described.

| **Threats**  Vulnerability  Threat  Attack | **Vulnerability- A weakness in a system that can be exploited, such as card numbers in a reciept**  **Threat- A motive or circumstance that can cause harm to a system, such as a threat to steal money if the attacker has access to the account**  **Attack- Exploiting a vulnerability, such as illegally downloading the private information of a system’s users** |
| --- | --- |
| **Types of Attacks**  I  I  M  F | **Interception- reading or “sniffing” communications in transit in order to perform an attack, this is usually passive and is hard to detect**  **Interruption- Disable a computer service in order to perform an attack, such as DOS’ing a service to prevent a service from operating**  **Modification- Change or corrupt data in order to perform an attack, such as changing data that may be used to exploit a system.**  **Fabrication- Create data in order to perform an attack, such as inserting documents in a way that may be exploited** |
| **Security**  C  I  A | Confidentiality- Not allowing information to be disclosed without authorization  Integrity- No authorized modification of information, not allowing anyone to modify information without authorization  Availability- System remains reliable for access and service, only allowing the authorized personnel to access the system’s files. |
| **Countermeasures**  1.  2.  3.  4.  5.  6. | **Prevention- Block an attack or close the vulnerability**  **Deterrence- Make an attack more difficult to perform**  **Deflection- Make an attack less attractive**  **Mitigation- Make the effects of an attack less severe**  **Detection- Monitor systems for the existence of an attack**  **Recovery- Resume business operations after an attack** |
| **Hacker Needs**  M  O  M | **Definitions, description, and examples**  **Method- The methods of which the hacker plans to attack**  **Opportunity- The exploitation of a vulnerability to perform an attack**  **Motive- The reason for the hacker performing the attack, such as financial or pure spite.** |

**Part 2 – Analysis Questions**

Answer the following questions.

1. Describe the difference between a vulnerability and a threat. Provide an example that shows the distinction.

A vulnerability is only a way in which the system can be compromised. In contrast, a threat may be a ransom or an actual threat to exploit the found vulnerability.

1. Describe the difference between integrity and confidentiality. Provide an example that shows the distinction.

Integrity is not allowing unauthorized personnel to modify a system’s information, whereas confidentiality means not allowing unauthorized personnel to access a system’s information. For example, illegal fabrication or modification is an example of a break in integrity, whereas the illegal obtaining of files is an example of a break in confidentiality.

1. Of the six countermeasures, in which of them do you believe a business should invest the most resources? Provide an example to justify your answer.

Deterrence is the most important countermeasure a business should be investing in. For example, businesses may rely on other companies to store their users’ information. Signing in using google or microsoft is an excellent way of safely protecting the information of their users.

1. Of the three items in M.O.M., which should a business should be most concerned about changing? Provide an example to justify your answer.

The method of the attack should be the biggest concern to a business. By tightening up security, a business could mitigate any vulnerabilities that may be present in their system.