Ryan Scott

**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 | **Definitions, description, and examples**  Vulnerability - An exploitable flaw or weakness in a computer system, its security procedures, internal controls, or design. Example: SQL injection.  Threat - A threat is an action or event that may negatively affect a computer system or application because of a vulnerability. Example: virus.  Attack - An offensive technique designed to attack computer systems, networks, infrastructure, and personal computers. Example: Spyware |
| --- | --- |
| **Types of Attacks**  Interception  Interruption  Modification  Fabrication | **Definitions, description, and examples**  Interception - Serves you Wi-Fi and steals your data. Relates to networks/Wi-Fi. Man in the Middle attack.  Interruption - Brings a system down. If a website was unavailable, it could be from an attack, such as DoS. A BotNet will overwhelm the server.  Modification - Changes your files and data. Example: WANNACRY? malware. Encrypts all the contents on your hard drive.  Fabrication - Slip a new account into a computer system. Security risk. |
| **Security**  Confidentiality  Integrity  Availability | **Definitions, description, and examples**  Confidentiality - A set of rules that limit access to information. Examples include 2FA and encryption.  Integrity - Data accuracy and consistency are ensured throughout the data's lifecycle. Unauthorized people cannot edit the data.  Availability - Ensure reliable access to correct information. Prevent bottlenecks! |
| **Countermeasures**  1. Prevention  2. Detection  3. Deterrence  4. Mitigation  5. Deflection  6. Recovery | **Definitions, description, and examples** Prevention - The most effective method; keeps the problem out. Don’t download sketchy attachments.  Detection - tools that monitor suspicious activity. For example, Snorby checks for anomalies.  Deterrence - Increasing the difficulty or cost of an attack. Strips from credit cards are being dumped for chips, as an example.  Mitigation - Reducing loss costs, like insurance. Make sure all important data is segmented so that a leak in one area does not compromise everything.  Deflection - Make yourself less appealing to attackers. Use third-party logins, so you don't have passwords to steal. Consider that Google or Facebook are more prepared than you are.  Recovery - Keep operating (if possible). Backups should be made every day just in case. |
| **Hacker Needs**  Motive  Opportunity  Method | **Definitions, description, and examples**  Motive - Hackers target you because they want your money, privacy, plans, passwords, and anything else that's valuable to them.  Opportunity - This is every opportunity for the hacker to follow through on their intentions, such as weak passwords, poorly written software, old versions of applications, or anything else that is most within your control.  Method - An element necessary for committing a crime, such as insider information, a compromised employee, or known vulnerabilities. |

**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.** 
   1. A threat is an event that negatively affects an organization, such as *an exploit of a vulnerability*. Vulnerabilities expose you to threats and therefore *increase your risk of negative outcomes*.
2. **Describe the difference between integrity and confidentiality. Provide an example that shows the distinction.** 
   1. Generally, confidentiality refers to preventing unauthorized access to something, while integrity refers to protecting data from unreliable changes. If my files are confidential, their integrity cannot be disrupted.
3. **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.**
   1. It is without a doubt that prevention is the best countermeasure. An organization's chances of reducing attacks in the first place can be increased if its employees are tech-savvy and know what to look for in a cybersecurity attack, such as vulnerabilities and phishing attempts. Human error is often responsible for attacks. Other helpful tools such as firewalls and filters can also be employed to reduce risk.
4. **Of the three items in M.O.M., which should a business be most concerned about changing? Provide an example to justify your answer.**
   1. In order to protect your business, the most important thing to do is change the motive behind the attack. If you don't have anything worth stealing, hackers won't even consider your company as a target. For example, using third-party logins like Google or Facebook so that passwords don't reside in your company’s database. There's no reason to steal login information if there are no passwords!