Homework Assignment #1

Mike Pendleton

Boralb Mimani

West Texas A@M University

**CIDM-6341 Topics in Cybersecurity SP2022**

**Homework Assignment #1**

**Total Points: 100**

*The purpose of this assignment is to evaluate the ability of identifying the threats posed to information security, the attacks associated with those threats, and assess the used countermeasures. You can work as group/team of MAX FIVE.*

Q1. [ 20 points] [ Hints : Book Ch1]

1. [10 points] Define: Confidentiality, Integrity, Availability, Vulnerability, Cyber Attack, Attack Vector, Payload, Identification, Authentication, and Authorization.
   1. Confidentiality – means to keep access to information only to whom needs access in order to prevent informational access from those who should not see the data.
   2. Integrity – data that is not corrupted, complete and whole.
   3. Availability – how data is accessible, to those that have access to the data.
   4. Vulnerability – potential weakness in an asses, such as software or hardware which can include the defensive control systems.
   5. Cyber Attack – an act that can damage or compromise information and systems supporting the information
   6. Attack Vector – how intruders enter an environment and are able to leverage exploits on vulnerabilities
   7. Payload – The malicious code that damages the system dependent on the intent of the attack.
   8. Identification – Access control where an unverified entity who seeks access to resources provided by labels where they are known by the system.
   9. Authentication – Access control mechanism that requires verification and validation of unauthenticated entities identity
   10. Authorization – Access control mechanism which represents the authenticated entity with the corresponding assets and access levels.
2. [10 points] What are the various types of malwares? How do worms differ from viruses? Do Trojan horses carry viruses or worms? What is ransomware? How does an organization protect against ransomwares?
   1. Various types of malware
      1. Viruses, worms, Trojan horses, polymorphic threats and hoaxes.
   2. How do worms differ from viruses?
      1. Worms can self-replicate, where virus’s require assistance from the host or other network means
   3. Do Trojan horses carry viruses or worms?
      1. Viruses
   4. What is ransomware?
      1. Ransomware encrypts the systems drives after the payload has ran. This attack then leaves a droplet in a .txt file instructing on how to get the system decrypted and how much they are requesting.
   5. How does an organization protect against ransomware?
      1. Keep the Anti-virus software up to date, leverage hardware security appliances, and regular backups maintained. If ransomware does encrypt a system(s), the only true way to recover 100% is through reliable backups.

Q2. [20 points] Assume that a security model is needed to protect information used in COVID-19 patient treatment in a Clinic (example – say … “Best Care Clinic”). Use the CNSS model to identify each of the 27 cells needed for complete information protection. Write a brief statement that explains how you would address the components represented in each of the 27 cells. [Hints; see an example attached in the last page]

Integrity—Technology—Storage: Medical documents maintain a secure documentation for all patient records. Utilizing integrity technology in order to securely store patient information that could only be modified if needed and authorized with the patients knowledge on why it is getting modified.

Q3. [20 points – 5 points each] [ Hints: Book Ch2]

1. What is the difference between criminal law and civil law? Which law amended the Computer Fraud and Abuse Act of 1986, and what did it change?
2. What is intellectual property? Is it offered the same protection in every country? What laws currently protect intellectual property in the United States and Europe?
3. What is a policy? How does it differ from a law?
4. What is digital forensics, and when is it used in a business setting?

Q4. [20 points – 5 points each] [Hints : Book Ch3]

1. What is planning? How does an organization determine if planning is necessary? What are the three common levels of planning?
2. What is InfoSec governance? What should a board of directors recommend as an organization’s InfoSec objectives? What are the five basic outcomes that should be achieved through InfoSec governance?
3. What is a systems development life cycle methodology? How does the SecSDLC differ from the more general SDLC? What is the primary objective of the SecSDLC? What are its major steps, and what are the major objectives of each step?
4. What do you mean by managerial, operational, and technical security controls? Why is maintenance needed for information security management systems?

Q5. [20 points] [Hints: see content folder/web-links]

1. [ 10 points] Write brief notes on “Critical Software: Enhancing the Security of the Software Supply Chain”.
2. [ 10 points] Name some Cyberattacks. As a systems administrator how can you plan to protect against them? Can you use packet sniffing software like “Wireshark”?. Please see attached lab-1.
   * 1. Wannacry, Sodinokibi and NetWalker are recent examples of ransomeware attacks.
     2. All important assets that cannot be simply re imaged and start over without a loss of data should be backed up. Ransomeware is extremely dangerous if infected as the private key is not known, unless the ransom is paid. Staying up to date with AV dat content and leveraging technologies such as EDR/XDR and IPS with proxies with help protect and monitor the environment against new/zero day and known threats.
     3. Ransomeware typically requires a downloader in order to get the payload from the wan to the local system. Wireshark is extremely important in investigating the IOC, in order to determine where the threat is coming from and what protocols are being used.

*Note: Submit your answer as a PDF file via WTClass Homework1 link in the Resources/*[*Assignments*](https://wtclass.wtamu.edu/webapps/blackboard/content/listContentEditable.jsp?content_id=_1175319_1&course_id=_29230_1) *folder*

**Example1:**

Question: Assume that a security model is needed to protect information used in the class you are taking—say, the information in your course’s learning management system. Use the CNSS model to identify each of the 27 cells needed for complete information protection. Write a brief statement that explains how you would address the components represented in each of the 27 cells.

Answer: In general, C.I.A. is confidentiality, integrity, and availability.

Confidentiality: Only allow students access to class if they have registered and paid for the ISA 3100 course at KSU for the fall semester of 2018. Controls to prevent unauthorized access to class would include taking roll call, learning each student’s name and face, and verifying them against the computerized printout of each registered student.

Integrity: Require students to carry their photo ID cards and present them on demand. Provide each student with a syllabus that contains the course description, course objectives, and instructor’s contact information, including office hours and phone number. The syllabus must also include information about the withdrawal policy, grading, and an integrity statement that must be read and signed before the student can receive a final grade for the semester.

Availability: Ensure that the classroom is accessible and provides a secure environment to promote well-organized learning. The controls include requiring the professor to be present at the beginning of class and have operational equipment so students can use their laptops for note taking.

Confidentiality—Policy—Storage: An example of protecting the confidentiality of class information in storage by means of policy would be issuing rules to keep access restricted to unauthorized viewers. One such rule could be to lock file cabinets that contain the information.

Confidentiality—Policy—Processing: An example of protecting the confidentiality of class information in processing by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being processed. For instance, only registered students in the class should be allowed to attend and listen to lectures.

Confidentiality—Policy—Transmission: An example of protecting the confidentiality of class information in transmission by means of policy would be issuing rules to keep access restricted to authorized viewers while information is being transmitted. For instance, a policy may require that all transmission of confidential data over public networks must be encrypted.

Confidentiality—Education—Storage: An example of protecting the confidentiality of class information in storage by means of education would be to train students and faculty about which people have authorized access to the information in storage.

Confidentiality—Education—Processing: An example of protecting the confidentiality of class information being processed by means of education would be to train students and faculty to verify whether people are authorized to get the information before class starts by using a student ID or schedule.

Confidentiality—Education—Transmission: An example of protecting the confidentiality of class information being transmitted by means of education would be to train students and faculty to close classroom doors during a lecture so that others outside could not hear it.

Confidentiality—Technology—Storage: An example of protecting the confidentiality of class information being stored by means of technology would be using locks on file cabinets that contain the information while not in use.

Confidentiality—Technology—Processing: An example of protecting the confidentiality of class information being processed by means of technology would be forcing the use of electronic IDs during classes.

Confidentiality—Technology—Transmission: An example of protecting the confidentiality of class information being transmitted by means of technology would be having a password on a class Web site.

Integrity—Policy—Storage: An example of protecting the integrity of class information being stored by means of policy would be a simple rule that only certified people may alter the information.

Integrity—Policy—Processing: An example of protecting the integrity of class information being processed by means of policy would be a rule that forces students to study in quiet areas without the help of people who are not in the class.

Integrity—Policy—Transmission: An example of protecting the integrity of class information being transmitted by means of policy would be a rule that the teacher is not allowed to drink alcohol before class.

Integrity—Education—Storage: An example of protecting the integrity of class information being stored by means of education would be teaching people who store the information the names and roles of others who are authorized to change it.

Integrity—Education—Processing: An example of protecting the integrity of class information being processed by means of education would be informing students not to risk receiving incorrect information by studying with people who are not in the class.

Integrity—Education—Transmission: An example of protecting the integrity of class information being transmitted by means of education would be providing instructors with effective ways to teach.

Integrity—Technology—Storage: An example of protecting the integrity of class information being stored by means of technology would be electronically storing all data on a device that requires authorization to modify.

Integrity—Technology—Processing: An example of protecting the integrity of class information being processed by means of technology would be creating PowerPoint presentations to verify what the teacher says.

Integrity—Technology—Transmission: An example of protecting the integrity of class information being transmitted by means of technology would be printing the PowerPoint presentations and giving a copy to each student.

Availability—Policy—Storage: An example of protecting the availability of class information being stored by means of policy would be a policy that only authorized students are allowed access to certain stored information.

Availability—Policy—Processing: An example of protecting the availability of class information being processed by means of policy would be a rule that only authorized people are allowed to enter the classroom.

Availability—Policy—Transmission: An example of protecting the availability of class information being transmitted by means of policy would be a rule that only students are allowed into the classroom.

Availability—Education—Storage: An example of protecting the availability of class information being stored by means of education would be teaching correct storage processes so information doesn’t get lost.

Availability—Education—Processing: An example of protecting the availability of class information being processed by means of education would be instructing those who teach the information to speak up so everyone in the classroom can hear.

Availability—Education—Transmission: An example of protecting the availability of class information being transmitted by means of education would be teaching students to remain quiet in the classroom so everyone can hear.

Availability—Technology—Storage: An example of protecting the availability of class information being stored by means of technology would be making the information available on the Internet via a password-protected Web site.

Availability—Technology—Processing: An example of protecting the availability of class information being processed by means of technology would be a teacher making PowerPoint files available to students via the Internet.

Availability—Technology—Transmission: An example of protecting the availability of class information being transmitted by means of technology would be a teacher using a microphone so lectures are loud enough for all students to hear.