**Chapter 1 – Introduction to Information Security**

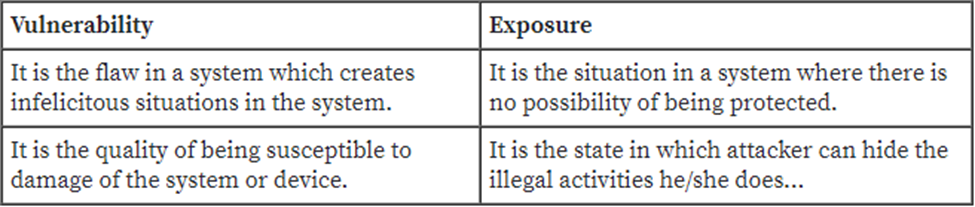
1. Differentiate between a threat agent and threat.

A screenshot of a cell phone

Description automatically generated

1. What is the difference between vulnerability and exposure?

* Vulnerability
* Is a weakness in a system which may lead to its inappropriate function like system failure or any threats like hacker, attacker, intruder and many more
* Exposure
* The state in which there is no chance of any protection from the harmful sources



1. What are the three components of the CIA triangle?

* Confidentiality: the certainly of secured data that only authorized users can use it/ unauthorized users cannot access it
* Integrity: the certainly of being real, complete and corrupted free
* Availability: the certainly of being available all the time and all the required resources

1. The CIA triangle is said to be incomplete. Why is it so commonly used then in security?

* They are used to express the ideology of security clearly and effectively, so that it can be easily understood
* They are used to assure that the data stored is free from corruption, risks and threats
* The required data or resources are available completely with not interruption of intruders

1. Describe the critical characteristics of information

A screenshot of a computer screen

Description automatically generated

1. Identify the six components of information systems.

A screenshot of a cell phone

Description automatically generated

1. Why is the top-down approach to information security superior to the bottom-up approach?

A screenshot of a social media post

Description automatically generated

* Top-down approach has the top-level managers who will assign the goals to be achieved, procedures and processes to achieve them and has the expected outcomes.
* It has clear planning and management to run the system
* It involves formal development strategy for developing the lifetime of the systems

1. Distinguish between vulnerability, threat and control?

* Vulnerability: Vulnerability is a weakness in the security system, for example in procedures, design or implementation that might be exploited to cause loss or harm. For instance, a system may be vulnerable to unauthorized data manipulation because the system does not verify a user’s identity before allowing data access.
* Threat: A threat to a computing system is a set of circumstances that has the potential to cause loss or harm. To see the difference between a threat and vulnerability, consider the illustration. There are many threats to a computer system, including human initiated and computer-initiated ones.
* Control: We use a control as a protective measure. That is a control is an action, device, procedure, or technique that removes or reduces vulnerability, threat is blocked by control of vulnerability

1. Why is methodology important in the implementation of information security?

* Methodology is a technique that has a sequence of all procedures to complete the tasks. It is important in information security because it ensures that the data is stored in orderly and secured manner
* It has the process of identifying the threats and the procedures to remove the threats like hacker
* The two main reason to implement the methodology in information security are:

1. First, it has all the processes and procedures to follow that no unauthorized user can access the data and the work is divided and specified in the authorized users
2. Second, the procedure to follow to achieve the expected goals and outcomes and no intruder can interrupt the process
3. List the phases of the SecSDLC

A screenshot of a cell phone

Description automatically generated

**Chapter 2 – The Need for Security**

1. What is the difference between a skilled hacker and an unskilled hacker, other than skill levels? How does the protection against each differ?

* Hacker: refers to the skilled computer experts who, with the help of their technical knowledge, uses bugs or try to exploit and break into computer systems

A screenshot of a cell phone

Description automatically generated

1. Why is information security a management problem? What can management do that technology cannot?
2. Information security management problem

* The staff required in the information security department and their salaries, is also handled by management team and information technology (IT) team can only advice
* The decisions regarding the polices and regulations are taken by management and IT again gives advice

1. Problems which are handled completely by management

* Information security faces the first problem with the assts required and what should be the value of assets. This issue is not an IT problem and is dealt by top management system
* Information technology department should also invest some money for the security of information, which is again dealt by management team and IT department just provides the data about the risk analysis

1. Why is data the most important asset an organization possesses? What other assets in the organization require protection?

* Data is the record of transactions for any organization
* It is also the ability of any organization to deliver the value to customers
* All the businesses like educational institution / government agency, can create and move the goods and services with the help of data the organization processes
* The value of data attracts the attackers to steal, misuse and corrupt the data

1. Which management groups are responsible for implementing information security to protect the organization’s ability to function?

* In an organization, many actions are performed by management groups while implementing information security
* Even though all the government and business officers deny being responsible for the implementation of information security as they have a belief that this task is technically complex

1. Has the implementation of networking technology created risk for businesses that use information technology? Why?

* Networking: allows two or more groups or individuals that share a common area of interest to exchange ideas or information. Users can access and can also use the accessed resources which are provided by devices on the network
* When it comes to the business world, networking has brought a new revolution, but is also considered as a risk creator for the businesses that use information technology

1. What is information extortion? Describe how such an attack can cause losses, using an example not found in the text.

* When an attacker holds onto to some asset and demands some property or cash in return, is called extortion. When the property that is stolen is some confidential information or data and the culprit uses internet to perform this crime, then it is called as cyber extortion or information extortion

1. Why are employees one of the greatest threats to information security?

* Employees are the one who use access and use the data of data of the organization in their everyday work activities
* Employees may sometimes commit some mistakes, and each mistake may lead to some series threat to the organization confidentiality, integrity and also affect the availability of the data
* Employees may also cause the disclosure of some classified data and may enter some incorrect data
* Employees may also delete or modify some important information unknowingly and save the data in some unprotected or unsafe areas which may lead to failure in protection of data

1. How can you protect against shoulder surfing?

* Shoulder surfing is a technique in which attacker gets the personal information of the victim by looking over the victim’s shoulder
* It is suggested that employees should not access any confidential information in the presence of some other person

1. How has the perception of the hacker changed over recent years? What is the profile of a hacker today?
2. Perception of the hacker

* Hackers are known to be the people who can get the data or information by finding out the way through the complex computer networks
* Hackers generally spent whole of their time to examine and classify the type and structure of the targeted system
* This helps them in using their skills or the fraud ways to gain the control over the information owned by some other person

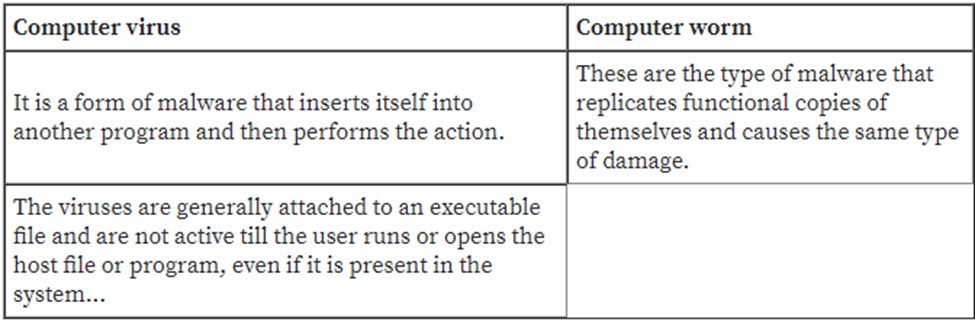
1. Current profile of a hacker

* In early days of hacking, it was observed that the hacker’s profile contained the same information as, a mile of age ranging from 13-18 and they had limited parental supervision

1. What are the various types of malware? How do worms differ from viruses? Do Trojan

horses carry viruses or worms?

* Trojan horse
* Computer viruses
* Worms
* Ransomware
* Logic bombs
* Back doors



1. What is the difference between a denial-of-service attack and a distributed denial of- service attack? Which is more dangerous? Why?

A screenshot of a cell phone

Description automatically generated

**Chapter 3- Legal, Ethical and Professional Issues**

1. What is the difference between laws and ethics?

A screenshot of a cell phone

Description automatically generated

1. Define civil law and explain what it accomplishes.

* Civil Law: is a wide variety of law pertaining relations among and between individuals, entities and organizations and generally governs a state
* Accomplishment of Civil Law
* Civil law accomplishes relationship between individuals and organizations
* It includes contract law, employment law, family law and tort law

1. Which law was specifically created to deal with encryption policy in the U.S.?
   * It provides guidance on the use of encryption
   * It provides protection from government intervention
2. What are the primary examples of public law?

* Civil law: is a wide variety of law pertaining relations among and between individuals, entities and organizations and generally governs a state
* Public law: is a law governs relationships between government and individuals and those relationships are of direct concern to society
* It regulates the structure and administration of government industries

1. If you work for a financial services organization such as a bank or credit union, which 1999 law affects your use of customer data? What other effects does it have?

* The law for use of computer data is the Financial Services Modernization Act in 1999. This Act is also known as a Gramm-Leah-Bliley Act of 1999
* It protects the right of customers when they deal with an organization

1. Define policy.

* A course or principle of action adopted or proposed by an organization or individual

1. What is privacy in an information security context?

* In information security context, privacy is defined as how the information you supply will be protected
* This addresses the question on whether the information will be confidential, whether they will sell it and whether the information will be leaked or not

1. What is another name for Kennedy-Kassebum Act (1996), and why is important to organizations that are not in healthcare industry?

* The Kennedy-Kassebum Act is also known as Health Insurance Portability and Accountability Act of 1996 HIPPA
* It is important to organizations which are not present in Health care industries as it also

1. What is PCI DSS and why is it important for information security?

* PCI DSS stands for Payment Card Industry Data Security Standard
* Information security is a method of protecting from unauthorized access for information and information systems and protecting the intellectual property of an organization
* PSI DSS are generally designed / created for customers account data