DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
(ARTIFICIAL INTELLIGENCE & MACHINE LEARNING)

Subject: MIS **Sem: BE/** VII

Identify the five factors that contribute to the increasing vulnerability of information resources, and provide a specific example of each one?

1. Today's interconnected, interdependent, wirelessly networked business environment.

Example: The Internet

2. Smaller, faster, cheaper computers and storage devices.

Examples: Netbooks, thumb drives, iPads

3. Decreasing skills necessary to be a computer hacker.

Example: Information system hacking programs circulating on the Internet

4. International organized crime taking over cybercrime.

Example: Organized crime has formed transnational cybercrime cartels. Because it is difficult to know exactly where cyberattacks originate, these cartels are extremely hard to bring to justice.

5. Lack of management support.

Example: Suppose that your company spent $10 million on information security countermeasures last year, and they did not experience any successful attacks on their information resources. Short-sighted management might conclude that the company could spend less during the next year and obtain the same results. Bad idea.

Compare and contrast human mistakes and social engineering, and provide a specific example of each one?

Human mistakes are unintentional errors. However, employees can also make unintentional mistakes as a result of actions by an attacker, such as social engineering.

Example: Tailgating

Social engineering is an attack through which the perpetrator uses social skills to trick or manipulate a legitimate employee into providing confidential company information.

Example: An attacker calls an employee on the phone and impersonates a superior in the company.

Discuss 10 types of deliberate attacks.

1. Espionage or trespass - an unauthorized individual attempts to gain illegal access to organizational information.

2. Information extortion - an attacker either threatens to steal, or actually steals, information from a company. The perpetrator demands payment for not stealing the information, for returning stolen information, or for agreeing not to disclose the information.

3. Sabotage and vandalism - deliberate acts that involve defacing an organization's website, possibly causing the organization to lose its image and experience a loss of confidence by its customers.

4. Theft of equipment and information - stealing computing devices and storage devices.

5. Identity theft - deliberate assumption of another person's identity, usually to gain access to his or her financial information or to frame him or her for a crime.

6. Compromises to intellectual property

7. Software attacks - malicious software penetrates an organization's computer system. Today, these attacks are typically profit-driven and web-based.

8. Alien software - clandestine software that is installed on your computer through duplicitous methods. It is typically not as malicious as viruses, worms, or Trojan horses, but it does use up valuable system resources.

9. Supervisory control and data acquisition - large-scale distributed measurement and control system. SCADA attacks attempt to compromise a system to cause damage to the real-world processes that the system controls.

10. Cyberterrorism and cyberwarfare - attackers use a target's computer systems, particularly thorough the Internet, to cause physical, real-world harm or severe disruption, usually to carry out a political agenda.