Information security is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing measures and controls to ensure the confidentiality, integrity, and availability of information.

Confidentiality ensures that information is accessed only by authorized individuals or systems. It involves preventing unauthorized disclosure of information. This can be achieved through encryption, access controls, and secure communication protocols.

Integrity ensures that information remains accurate and complete. It involves preventing unauthorized modification or tampering of data. This can be achieved through the use of checksums, digital signatures, and access controls.

Availability ensures that information is accessible and usable when needed. It involves protecting against disruptions or denial of service attacks. This can be achieved through redundancy, backup systems, and disaster recovery plans.

There are various threats to information security, including malware, hacking, social engineering, and physical theft. Organizations need to implement a combination of technical, administrative, and physical controls to mitigate these threats.

Key steps in information security include risk assessment, vulnerability assessment, and implementing appropriate security controls. Regular monitoring, incident response, and continuous improvement are also important for maintaining information security.

Overall, information security is essential to protect sensitive and valuable information from unauthorized access or misuse. It is a crucial aspect of any organization's operations to ensure trust, privacy, and compliance with legal and regulatory requirements.

1. Which of the following represents a potential security risk in computer systems?

a) Firewall

b) Intrusion Detection System (IDS)

c) Weak password

d) Encryption

Correct answer: c) Weak password

Explanation: Weak passwords are vulnerable to unauthorized access and can be easily cracked, compromising the security of the system.

2. What is the purpose of a firewall in network security?

a) Encrypt data transmission

b) Monitor and block unauthorized access

c) Authenticate users

d) Filter spam emails

Correct answer: b) Monitor and block unauthorized access

Explanation: A firewall acts as a security barrier between a trusted internal network and an untrusted external network, monitoring incoming and outgoing network traffic to block or allow access based on predefined rules and policies.

3. Which of the following encryption algorithms is considered to be the most secure?

a) DES

b) AES

c) RSA

d) SHA

Correct answer: b) AES

Explanation: AES (Advanced Encryption Standard) is widely regarded as the most secure encryption algorithm currently in use. It is used to encrypt sensitive data, such as financial transactions and government communications.

4. What does the term "phishing" refer to in the context of information security?

a) Unauthorized access to a computer system

b) Manipulating hardware components to gain access

c) Sending malicious emails to deceive individuals into revealing sensitive information

d) Overloading a system with excessive network traffic

Correct answer: c) Sending malicious emails to deceive individuals into revealing sensitive information

Explanation: Phishing is a type of cyber attack where attackers impersonate legitimate organizations or individuals and send fraudulent emails to deceive recipients into revealing sensitive information, such as passwords or financial details.

5. What is the purpose of a vulnerability scan in information security?

a) To detect and fix security flaws in software

b) To encrypt sensitive data during transmission

c) To monitor network traffic for suspicious activities

d) To authenticate users and control access

Correct answer: a) To detect and fix security flaws in software

Explanation: A vulnerability scan is a systematic process of identifying security vulnerabilities in software, operating systems, or networks, allowing organizations to take necessary actions to fix those vulnerabilities and minimize the risk of exploitation by attackers.

6. \_\_\_\_\_\_\_ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.  
a) Network Security  
b) Database Security  
c) Information Security  
d) Physical Security  
View Answer

Answer: c  
Explanation: Information Security (abbreviated as InfoSec) is a process or set of processes used for protecting valuable information for alteration, destruction, deletion or disclosure by unauthorised users.

7. From the options below, which of them is not a threat to information security?  
a) Disaster  
b) Eavesdropping  
c) Information leakage  
d) Unchanged default password  
View Answer

Answer: d  
Explanation: Disaster, eavesdropping and information leakage come under information security threats whereas not changing the default password of any system, hardware or any software comes under the category of vulnerabilities that the user may pose to its system.

8. From the options below, which of them is not a vulnerability to information security?  
a) flood  
b) without deleting data, disposal of storage media  
c) unchanged default password  
d) latest patches and updates not done  
View Answer

Answer: a  
Explanation: Flood comes under natural disaster which is a threat to any information and not acts as a vulnerability to any system.

9. \_\_\_\_\_ platforms are used for safety and protection of information in the cloud.  
a) Cloud workload protection platforms  
b) Cloud security protocols  
c) AWS  
d) One Drive  
View Answer

Answer: a  
Explanation: Nowadays data centres support workloads from different geographic locations across the globe through physical systems, virtual machines, servers, and clouds. Their security can be managed using Cloud workload protection platforms which manage policies regarding security of information irrespective of its location.

10. Which of the following information security technology is used for avoiding browser-based hacking?  
a) Anti-malware in browsers  
b) Remote browser access  
c) Adware remover in browsers  
d) Incognito mode in a browser  
View Answer

Answer: b  
Explanation: Cyber-criminals target browsers for breaching information security. If a user establishes a remote browsing by isolating the browsing session of end user, cyber-criminals will not be able to infect the system along with browser with malware, ultimately reducing the attack surface area.

11. The full form of EDR is \_\_\_\_\_\_\_  
a) Endpoint Detection and recovery  
b) Early detection and response  
c) Endpoint Detection and response  
d) Endless Detection and Recovery  
View Answer

Answer: c  
Explanation: It is a collective name for tools that monitor networks & endpoints of systems and record all the activities for further reporting, analysis & detection in a central database. Analyzing the reports generated through such EDR tools, loopholes in a system or any internal, as well as external breaching attempts can be detected.

12. \_\_\_\_\_\_\_ technology is used for analyzing and monitoring traffic in network and information flow.  
a) Cloud access security brokers (CASBs)  
b) Managed detection and response (MDR)  
c) Network Security Firewall  
d) Network traffic analysis (NTA)  
View Answer

Answer: d  
Explanation: Network traffic analysis (NTA) is an approach of information security for supervising the traffic in any network, a flow of data over the network as well as malicious threats that are trying to breach the network. This technological solution also helps in triage the events detected by Network Traffic Analysing tools.

13. Compromising confidential information comes under \_\_\_\_\_\_\_\_\_  
a) Bug  
b) Threat  
c) Vulnerability  
d) Attack  
View Answer

Answer: b  
Explanation: Threats are anything that may cause damage or harm to a computer system, individual or any information. Compromising of confidential information means extracting out sensitive data from a system by illegal manner.

14. Lack of access control policy is a \_\_\_\_\_\_\_\_\_\_\_\_\_  
a) Bug  
b) Threat  
c) Vulnerability  
d) Attack  
View Answer

Answer: c  
Explanation: Access control policies are incorporated to a security system for restricting of unauthorised access to any logical or physical system. Every security compliance program must need this as a fundamental component. Those systems which lack this feature is vulnerable.

15. Possible threat to any information cannot be \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
a) reduced  
b) transferred  
c) protected  
d) ignored  
View Answer

Answer: d  
Explanation: When there lies a threat to any system, safeguards can be implemented, outsourced, distributed or transferred to some other system, protected using security tools and techniques but cannot be ignored.