Question 1 of 41

The primary objective of a threat agent using a replay attack technique is to

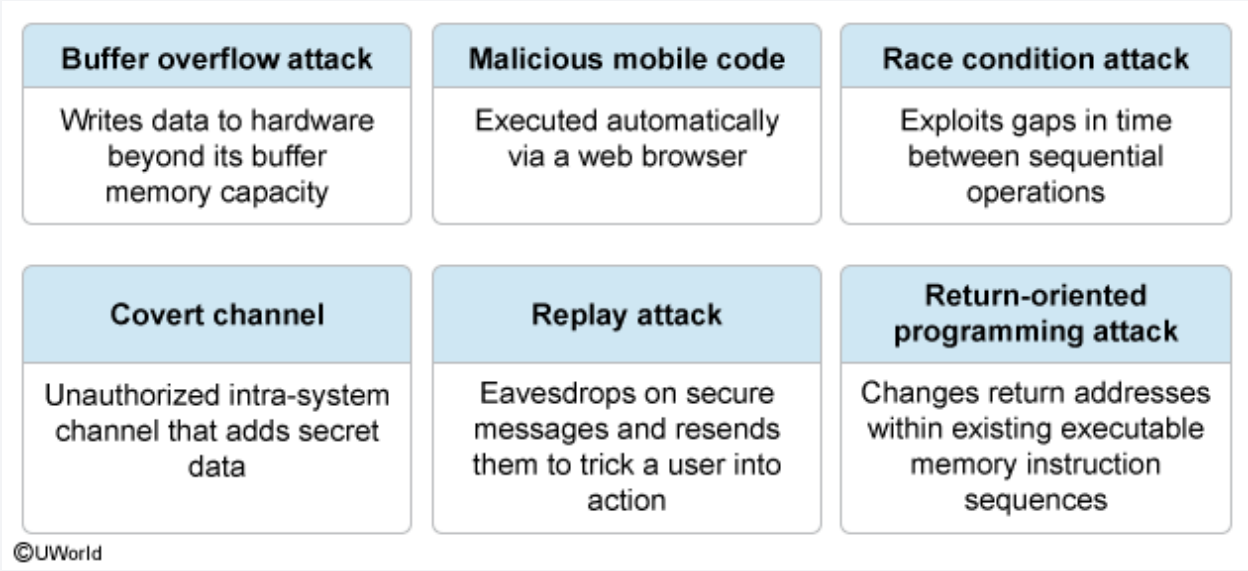
A. Change stored return addresses in coding.

B. Inject malicious code into mobile applications.

C. Perform actions during process sequence gaps.

D. Utilize information captured during transmission. ✓

Explanation:



Cyberattacks involve the illegal use of computers or other technologies to gain or deny access to data or services. **Threat agents** can use diverse types of attacks and techniques to exploit an organization's threat vectors. A **threat vector** is a medium that might be the target of a cyberattack, such as web applications, networks, email systems, and wireless devices.

In a **replay attack**, the threat agent **intercepts information** while it is being transmitted and **resubmits** it to trick another system or person into providing more information or performing an action. For example, if an encrypted banking password is intercepted, the attacker may later resubmit it to transfer funds. The **attacker appears as the original sender** because the encrypted password matches. A preventive control against this type of attack would be adding time/session stamps to all original encrypted messages.

(Choice A) Rather than inject harmful instructions, return-oriented programming attacks change return addresses to exploit existing code. This technique circumvents data execution prevention (DEP) controls.

(Choice B) In a malicious mobile code attack, software executes automatically via a web browser without the recipient's consent or knowledge.

(Choice C) A race condition (ie, time-of-check-to-time-of-use condition) attack is a technique that exploits a brief gap in time during a processing sequence, such as the

moment between when a password is entered and when it is verified in a database.

Things to remember:
In a replay attack, the threat agent intercepts information (eg, encrypted password) while it is being transmitted and resubmits it to trick another system or person into providing more information or performing an action.

Question 2 of 41

What type of attack is most likely to target unpatched vulnerabilities in mobile operating systems?

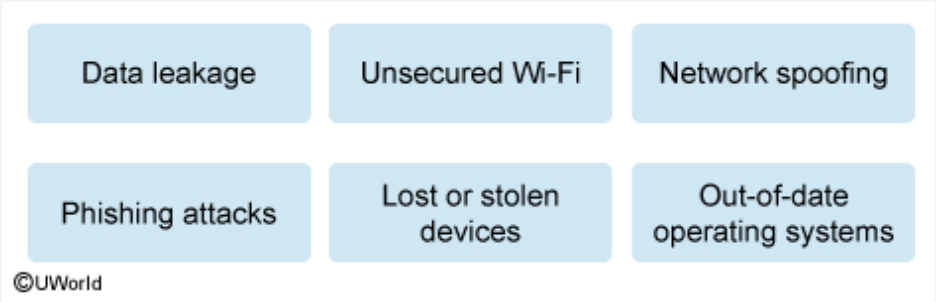
A. Adware virus.

B. Smishing attack.

C. Wi-Fi spoofing.

D. Zero-day exploit. ✓

Explanation:



Organizations must assess the **security risks** associated with **mobile devices** (eg, cell phones, laptops). The growing use of mobile devices, whether **employer- or employee-owned** (under bring-your-own-device [BYOD] policies), increases the attack surface. Threat actors employ a variety of techniques to attack mobile devices.

A **zero-day exploit** is most likely **to target unpatched vulnerabilities** in mobile operating systems. Because new attack techniques arise daily, software vendors may not be aware of a flaw in their product. The "zero" in *zero-day* means that the **software vendor has zero days to prepare a patch** because an attacker exploits the vulnerability before the vendor knows it exists.

(Choice A) An adware virus adds software to a mobile device as part of a monetization scam. A device is infected with the virus when its user clicks on a malicious ad link or downloads a malicious file or application.

(Choice B) A smishing attack is a social engineering attack that occurs when a mobile device user is tricked into clicking on a malicious link sent through a text message that appears to be from someone the user knows but is, in fact, from a bad actor.

(Choice C) Wi-Fi spoofing involves creating a fake, unsecured Wi-Fi network where the data and credentials of users who log in can be accessed.

Things to remember:
A zero-day exploit is most likely to target unpatched vulnerabilities in mobile operating systems. The "zero" in *zero-day* means that the software vendor has zero days to prepare a patch because an attacker exploits the vulnerability before the vendor knows it exists.

Question 3 of 41

An enterprise resource planning (ERP) system has which of the following advantages over multiple independent functional systems?

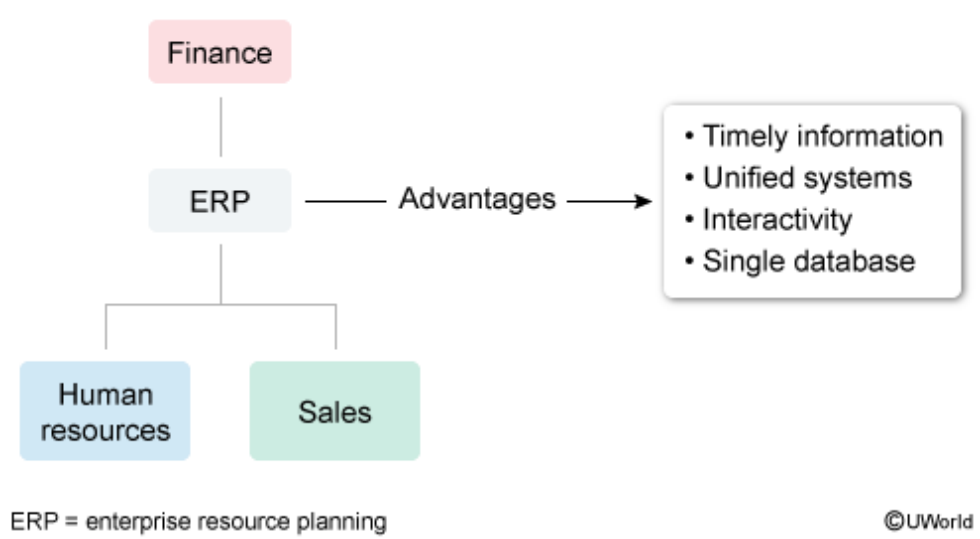
A. Modifications can be made to each module without affecting other modules.

B. **Increased responsiveness and flexibility while aiding in the decision-making process.** ✓

C. Increased amount of data redundancy since more than one module contains the same information.

D. Reduction in costs for implementation and training.

Explanation:



An enterprise resource planning (ERP)system is a packaged (ie, off-the-shelf) business information system. ERP systems **automate** business processes, share common data, and facilitate reporting in a real-time environment.

ERP systems may replace disparate legacy systems, each of which was designed to support a discrete grouping of business functions. The consolidation of these systems in one ERP system allows the organization to **integrate** data from different functional areas (eg, sales and procurement) within a single system in a **single database**. This integration facilitates information exchange and collaboration among functional areas as well as with vendors and customers. Greater collaboration among stakeholders may improve **flexibility**, **responsiveness**, and **decision-making**, which are advantages of using ERP systems instead of multiple independent systems.

ERP systems are composed of modules, programs that automate specific business functions. For example, the finance module may process financial transactions, generate financial reports, and provide invoicing and expense reporting capabilities. These modules are interconnected, so modifications to one module can affect other modules **(Choice A)**. Modules also share a single database, which reduces data redundancy and inconsistency **(Choice C)**.

(Choice D) The volume and diversity of business processes and functions supported by ERP systems increases complexity, which may then lead to higher costs for implementation and training.

Things to remember:
Enterprise resource planning systems integrate data from different functional areas, customers, and vendors. This integration facilitates collaboration, thereby improving responsiveness, flexibility, and decision-making.

Question 4 of 41

The ability of an information system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities is known as

A. Agility.

B. Scalability.

C. Resilience. ✓

D. Interoperability.

Explanation:

Business resilience refers to an organization's **ability to endure, recover from, and capitalize on unexpected challenges**. Business resilience planning complements business continuity planning by addressing not only physical risks but also risks that impact an organization's mission (eg, organizational disruptions, market volatility).

Business resilience planning allows organizations to develop several aspects of resilience:

- **Financial:** enduring unexpected changes in revenues or expenses
- **Operational:** adjusting to changes in supply or demand
- **Organizational:** prioritizing employee retention and promoting high employee performance
- **Reputational:** making adjustments in response to constructive criticism
- **Business model:** adapting to changes in technology, market trends, or regulations
- **Technological:** responding to cybersecurity threats by establishing business continuity and disaster recovery plans

(Choice A) Agility refers to the ability of an organization or system to adapt to changes or new requirements, not to withstand adverse conditions.

(Choice B) Scalability is the capacity of a system to handle increased workload (eg, additional users) without decreasing performance, rather than its ability to deal with stressful situations.

(Choice D) Interoperability is the ability of different systems or organizations to work together and exchange information effectively, rather than maintain operations under stress.

Things to remember:
Business resilience refers to an organization's ability to endure, recover from, and capitalize on unexpected challenges.

Question 5 of 41

A service auditor assessing inherent risk in a SOC 2® engagement should consider each of the following factors relevant to assertion-based examination engagements, **except**

A. The complexity involved in describing the boundaries of the service organization's system.

B. The fairness of the service organization's system description in prior examinations.

C. The length of time the service organization's system has been in existence.

D. The nature of further procedures needed to evaluate the fairness of the system description. ✓

Explanation:

Assertion-based examinations: inherent risk factors
• Complexity of the subject matter or assertion • Length of time the entity has had experience with the subject matter or assertion • Practitioner's prior experience with the entity's assessment of the subject matter or assertion

A SOC 2® engagement requires a service auditor to assess risk by obtaining an understanding of the subject matter (ie, management's system description and controls). Inherent risks (eg, human error) are organic and cannot be eliminated through management's controls, even if those controls are suitably designed and are operating effectively.

According to AT-C 205, when assessing inherent risk in an assertion-based examination (eg, SOC 1®, SOC 2®), the practitioner may consider factors such as

- The complexity of the subject matter or assertion **(Choice A)**
- The length of time during which the entity has had experience with the subject matter or assertion **(Choice C)**
- The practitioner's prior experience with the entity's assessment of the subject matter or assertion **(Choice B)**

Further procedures are performed by the service auditor after the engagement has been planned and a risk assessment completed. Risks are assessed to establish materiality levels and to determine the nature of further procedures needed to obtain sufficient appropriate evidence. Thus, further procedures performed to evaluate the fairness of management's system description in a SOC 2® examination would support the service auditor's opinion.

Things to remember:
When assessing inherent risk in an assertion-based examination, the practitioner may consider the complexity of the subject matter or assertion; how long the entity has had

experience with the subject matter or assertion; and any prior experience the practitioner has with the entity's assessment of that subject matter or assertion.

Question 6 of 41

What is a potential risk associated with having data centers distributed globally instead of concentrated in one geographic location?

A. Data loss.

B. Reduced accessibility.

C. Regulatory noncompliance. ✓

D. Slower performance.

Explanation:

Although cloud computing can increase employee productivity and decrease IT costs, it can also increase cybersecurity risks. One such risk is that cloud service providers (CSPs) may distribute their data centers in different geographical locations around the world.

Distributing data centers in different geographical locations implies that client data may also be stored in different geographical locations. This approach may **result** in **regulatory noncompliance** because **countries** (eg, the General Data Protection Regulation [GDPR] for countries in the European Union) have differing laws and may prohibit data from being stored or processed in other geographic areas.

(Choice A) Distributing data centers across different geographic locations allows the CSP to backup data to different locations, ensuring that multiple copies of the data exist in case of data loss (eg, due to a natural disaster) in one data center.

(Choice B) Geographically distributed data centers can continue to operate even if one location is compromised, thereby ensuring service accessibility.

(Choice D) Distributing data centers geographically allows the CSP to set up data centers closer to end users, resulting in faster performance because it takes less time for the data to travel between the end user and the data center.

Things to remember:
Regulatory noncompliance is a potential risk associated with having data centers distributed globally as opposed to concentrated in one geographic location.

Question 7 of 41

What is the primary role of the fact table in a star schema?

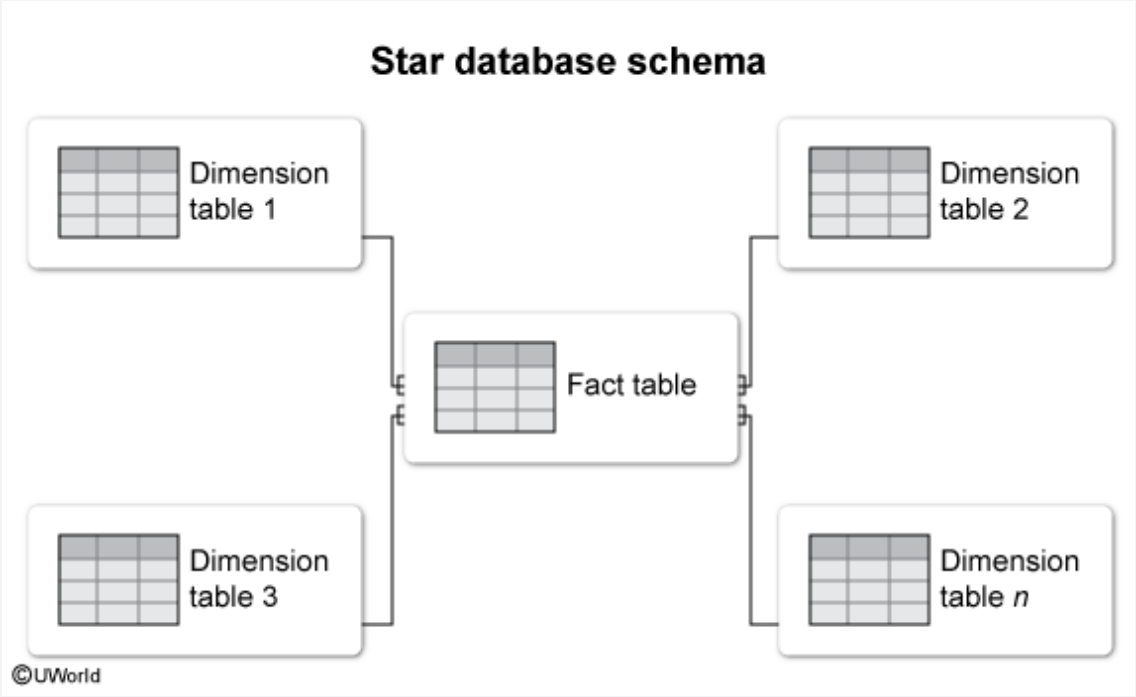
A. To store descriptive data about records.

B. To store foreign keys to dimension tables. ✓

C. To store metadata about a database's structure.

D. To store summarized data about attributes.

Explanation:



A **database schema** is a blueprint of a database's underlying **structure**. Typically presented as a diagram, schemas show the tables, attributes (ie, fields), keys (primary and foreign), and relationships (ie, associations) in a database. The **star** model, the basic schema for data warehouses and data marts, has a **central fact table** that is **associated with multiple dimension tables** (points of the star).

The primary role of the fact table in a star schema is to **store foreign keys** to dimension tables. Foreign keys on the fact table **create a relationship** with the primary keys of dimension tables. This relationship provides a context for the facts in a database. For example, a fact table holds quantitative numerical data (eg, quantity on hand), which is related to the qualitative data (eg, product description) held in a dimension table.

(Choice A) Dimension tables, not fact tables, store descriptive data about records.

(Choice C) Metadata (data about data) is stored separately in tools such as data catalogs or dictionaries, not in fact tables or dimension tables. The purpose of metadata is to provide other information about a data type (eg, an attribute holds a character or integer).

(Choice D) While data in a fact table can be summarized through querying, the "facts" about attributes are stored at the lowest level and are not pre-summarized directly in a