Business needs - CORRECT ANSWER-Business continuity plans (BCPs) associated with organizational information systems should be developed primarily on the basis of:

Consists of two or more security zones - CORRECT ANSWER-A segmented network

Nonrepudiation - CORRECT ANSWER-Which cybersecurity principle is most important when attempting to trace the source of malicious activity?

Wireless Protected Access 2 (WPA2) - CORRECT ANSWER-Which of the following offers the strongest protection for wireless network traffic?

Core business functions - CORRECT ANSWER-Outsourcing poses the greatest risk to an organization when it involves:

On a regular basis - CORRECT ANSWER-Risk assessments should be performed

Chain of custody - CORRECT ANSWER-Maintaining a high degree of confidence regarding the integrity of evidence requires a(n):

Stateful - CORRECT ANSWER-A firewall that tracks open connection-oriented protocol sessions is said to be:

Planning - CORRECT ANSWER-During which phase of the system development lifecycle (SDLC) should security first be considered?

System-centric - CORRECT ANSWER-A cybersecurity architecture designed around the concept of a perimeter is said to be:

Physical - CORRECT ANSWER-A passive network hub operates at which layer of the OSI model?

Homogeneous - CORRECT ANSWER-Updates in cloud-computing environments can be rolled out quickly because the environment is:

Eradication - CORRECT ANSWER-During which phase of the six-phase incident response model is the root cause determined?

Payload - CORRECT ANSWER-The attack mechanism directed against a system is commonly called a(n):

Containment - CORRECT ANSWER-Which element of an incident response plan involves obtaining and preserving evidence?

- Who had access to the evidence, in chronological order.
- Proof that the analysis is based on copies identical to the original evidence.
- The procedures followed in working with the evidence. - CORRECT ANSWER-The chain of custody contains information regarding:

Incident - CORRECT ANSWER-NIST defines a(n) _____ as a "violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."

- the estimated probability of the identified threats actually occurring.
- the efficiency and effectiveness of existing risk mitigation controls.
- a list of potential vulnerabilities, dangers and/or threats. - CORRECT ANSWER-A business . impact analysis (BIA) should identify:

Cloud computing - CORRECT ANSWER-_____ is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management or service provider interaction."

- APTs typically originate from sources such as organized crime groups, activists or governments.
- APTs use obfuscation techniques that help them remain undiscovered for months or even years.
- APTs are often long-term, multi-phase projects with a focus on reconnaissance. - CORRECT ANSWER-Which of the following statements about advanced persistent threats (APTs) are true?

- Costs shift to the user
- Worker satisfaction increases - CORRECT ANSWER-Which of the following are benefits to BYOD?

- Organizational risk
- Technical risk
- Physical risk - CORRECT ANSWER-Choose three. Which types of risk are typically associated with mobile devices?

Cloud computing, social media, and mobile computing - CORRECT ANSWER-Which three elements of the current threat landscape have provided increased