mirroring is the less cost-efficient data redundancy strategy.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 45).

QUESTION 515
Which of the following specifically addresses cyber attacks against an organization's IT systems?

A. Continuity of support plan
B. Business continuity plan
C. Incident response plan
D. Continuity of operations plan

Correct Answer: C
Explanation:
The incident response plan focuses on information security responses to incidents affecting systems and/or networks. It establishes procedures to address cyber attacks against an organization's IT systems. These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial of service, or unauthorized changes to system hardware or software.
The continuity of support plan is the same as an IT contingency plan. It addresses IT system disruptions and establishes procedures for recovering a major application or general support system. It is not business process focused. The business continuity plan addresses business processes and provides procedures for sustaining essential business operations while recovering from a significant disruption. The continuity of operations plan addresses the subset of an organization's missions that are deemed most critical and procedures to sustain these functions at an alternate site for up to 30 days.
Source: SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 8).

QUESTION 516
Notifying the appropriate parties to take action in order to determine the extent of the severity of an incident and to remediate the incident's effects is part of:

A. Incident Evaluation
B. Incident Recognition
C. Incident Protection
D. Incident Response

Correct Answer: D
Explanation:
These are core functions of the incident response process.
"Incident Evaluation" is incorrect. Evaluation of the extent and cause of the incident is a component of the incident response process.
"Incident Recognition" is incorrect. Recognition that an incident has occurred is the precursor to the initiation of the incident response process.
"Incident Protection" is incorrect. This is an almost-right-sounding nonsense answer to distract the unwary.

References:
CBK, pp. 698 - 703

QUESTION 517
Which of the following tasks is NOT usually part of a Business Impact Analysis (BIA)?

A. Calculate the risk for each different business function.
B. Identify the company's critical business functions.
C. Calculate how long these functions can survive without these resources.
D. Develop a mission statement.

Correct Answer: D
Explanation:
The Business Impact Analysis is critical for the development of a business continuity plan (BCP). It identifies risks, critical processes and resources needed in case of recovery and quantifies the impact a disaster will have upon the organization. The development of a mission statement is normally performed before the BIA.

A BIA (business impact analysis) is considered a functional analysis, in which a team collects data through interviews and documentary sources; documents business functions, activities, and transactions ; develops a hierarchy of business functions; and finally applies a classification scheme to indicate each individual function's criticality level.

BIA Steps
The more detailed and granular steps of a BIA are outlined here:

1. Select individuals to interview for data gathering.
2. Create data-gathering techniques (surveys, questionnaires, qualitative and quantitative approaches).
3. Identify the company's critical business functions.
4. Identify the resources these functions depend upon.
5. Calculate how long these functions can survive without these resources.
6. Identify vulnerabilities and threats to these functions.
7. Calculate the risk for each different business function.
8. Document findings and report them to management.

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Location 21076). Auerbach Publications. Kindle Edition.
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 905-910). McGraw-Hill. Kindle Edition.

QUESTION 518
Under United States law, an investigator's notebook may be used in court in which of the following scenarios?

A. When the investigator is unwilling to testify.
B. When other forms of physical evidence are not available.
C. To refresh the investigators memory while testifying.
D. If the defense has no objections.

Correct Answer: C
Explanation:
An investigator's notebook cannot be used as evidence is court. It can only be used by the investigator to refresh his memory during a proceeding, but cannot be submitted as evidence in any form.

The following answers are incorrect:

When the investigator is unwilling to testify. Is incorrect because the notebook cannot be submitted as evidence in any form.
When other forms of physical evidence are not available. Is incorrect because the notebook cannot be submitted as evidence in any form.
If the defense has no objections. Is incorrect because the notebook cannot be submitted as evidence in any form.

QUESTION 519
Which backup method does not reset the archive bit on files that are backed up?

A. Full backup method
B. Incremental backup method
C. Differential backup method
D. Additive backup method

Correct Answer: C
Explanation:
The differential backup method only copies files that have changed since the last full backup was performed. It is additive in the fact that it does not reset the archive bit so all changed or added files are backed up in every differential backup until the next full backup. The "additive backup method" is not a common backup method.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 69).

QUESTION 520
Which of the following rules pertaining to a Business Continuity Plan/Disaster Recovery Plan is incorrect?

A. In order to facilitate recovery, a single plan should cover all locations.
B. There should be requirements to form a committee to decide a course of action. These decisions should be made ahead of time and incorporated into the plan.
C. In its procedures and tasks, the plan should refer to functions, not specific individuals.
D. Critical vendors should be contacted ahead of time to validate equipment can be obtained in a timely manner.

Correct Answer: A
Explanation:
The first documentation rule when it comes to a BCP/DRP is "one plan, one building". Much of the plan revolves around reconstructing a facility and replenishing it with production contents. If more than one facility is involved, then the reader of the plan will find it difficult to identify quantities and specifications of replacement resource items. It is possible to have multiple plans for a single building, but those plans must be linked so that the identification and ordering of resource items is centralized. All other statements are correct.
Source: BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 162).

QUESTION 521
A copy of evidence or oral description of its contents; which is not as reliable as best evidence is what type of evidence?

A. Direct evidence
B. Circumstantial evidence
C. Hearsay evidence
D. Secondary evidence

Correct Answer: D
Explanation:
Secondary evidence is a copy of evidence or oral description of its contents; not as reliable as best evidence

Here are other types of evidence:

Best evidence -- original or primary evidence rather than a copy of duplicate of the evidence
Direct evidence -- proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses
Conclusive evidence -- incontrovertible; overrides all other evidence
Opinions -- two types: Expert -- may offer an opinion based on personal expertise and facts, Non-expert -- may testify only as to facts
Circumstantial evidence -- inference of information from other, immediate, relevant facts
Corroborative evidence -- supporting evidence used to help prove an idea or point; used as a supplementary tool to help prove a primary piece of evidence
Hearsay evidence (3rdparty) -- oral or written evidence that is presented in court that is second hand and has no firsthand proof of accuracy or reliability

(i) Usually not admissible in court
(ii) Computer generated records and other business records are in hearsay category
(iii) Certain exceptions to hearsay rule:

(1) Made during the regular conduct of business and authenticated by witnesses familiar with their use
(2) Relied upon in the regular course of business
(3) Made by a person with knowledge of records
(4) Made by a person with information transmitted by a person with knowledge
(5) Made at or near the time of occurrence of the act being investigated (6) In the custody of the witness on a regular basis

Reference:
KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 310.
And CISSP for Dummies, Peter Gregory, page 270-271

QUESTION 522
The first step in the implementation of the contingency plan is to perform:

A. A firmware backup
B. A data backup
C. An operating systems software backup
D. An application software backup

Correct Answer: B

Explanation:
A data backup is the first step in contingency planning. Without data, there is nothing to process. "No backup, no recovery".
Backup for hardware should be taken care of next.
Formal arrangements must be made for alternate processing capability in case the need should arise.
Operating systems and application software should be taken care of afterwards.
Source: VALLABHANENI, S. Rao, CISSP Examination Textbooks, Volume 2: Practice, SRV Professional Publications, 2002, Chapter 8, Business Continuity Planning & Disaster Recovery Planning (page 506).

QUESTION 523
How often should tests and disaster recovery drills be performed?

A. At least once a quarter
B. At least once every 6 months
C. At least once a year
D. At least once every 2 years

Correct Answer: C
Explanation:
Tests and disaster recovery drills should be performed at least once a year. The company should have no confidence in an untested plan. Since systems and processes can change, frequent testing will aid in ensuring a plan will succeed.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

QUESTION 524
Which of the following groups represents the leading source of computer crime losses?

A. Hackers
B. Industrial saboteurs
C. Foreign intelligence officers
D. Employees

Correct Answer: D
Explanation:
There are some conflicting figures as to which group is a bigger threat hackers or employees. Employees are still considered to the leading source of computer crime losses. Employees often have an easier time gaining access to systems or source code then ousiders or other means of creating computer crimes.

A word of caution is necessary: although the media has tended to portray the threat of cybercrime as existing almost exclusively from the outside, external to a company, reality paints a much different picture. Often the greatest risk of cybercrime comes from the inside, namely, criminal insiders. Information security professionals must be particularly sensitive to the phenomena of the criminal or dangerous insider, as these individuals usually operate under the radar, inside of the primarily outward/external facing security controls, thus significantly increasing the impact of their crimes while leaving few, if any, audit trails to follow and evidence for prosecution.

Some of the large scale crimes committed agains bank lately has shown that Internal Threats are the worst and they are more common that one would think. The definition of what a hacker is can vary greatly from one country to another but in some of the states in the USA a hacker is defined