QUESTION 488
What is defined as inference of information from other, intermediate, relevant facts?

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

Correct Answer: D
Explanation:
Circumstantial evidence is defined as inference of information from other, intermediate, relevant facts. Secondary evidence is a copy of evidence or oral description of its contents. Conclusive evidence is incontrovertible and overrides all other evidence and hearsay evidence is evidence that is not based on personal, first-hand knowledge of the witness, but was obtained from another source. Computer-generated records normally fall under the category of hearsay evidence.
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 9: Law, Investigation, and Ethics (page 310).

QUESTION 489
Why would a memory dump be admissible as evidence in court?

A. Because it is used to demonstrate the truth of the contents.
B. Because it is used to identify the state of the system.
C. Because the state of the memory cannot be used as evidence.
D. Because of the exclusionary rule.

Correct Answer: B
Explanation:
A memory dump can be admitted as evidence if it acts merely as a statement of fact. A system dump is not considered hearsay because it is used to identify the state of the system, not the truth of the contents. The exclusionary rule mentions that evidence must be gathered legally or it can't be used. This choice is a distracter.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187).

QUESTION 490
Failure of a contingency plan is usually:

A. A technical failure.
B. A management failure.
C. Because of a lack of awareness.
D. Because of a lack of training.

Correct Answer: B
Explanation:
Failure of a contingency plan is usually management failure to exhibit ongoing interest and concern about the BCP/DRP effort, and to provide financial and other resources as needed. Lack of management support will result in a lack awareness and training.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 9: Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) (page 163).

QUESTION 491
Which type of attack would a competitive intelligence attack best classify as?

A. Business attack
B. Intelligence attack
C. Financial attack
D. Grudge attack

Correct Answer: A
Explanation:
Business attacks concern information loss through competitive intelligence gathering and computer-related attacks. These attacks can be very costly due the loss of trade secrets and reputation.

Intelligence attacks are aimed at sensitive military and law enforcement files containing military data and investigation reports.

Financial attacks are concerned with frauds to banks and large corporations.

Grudge attacks are targeted at individuals and companies who have done something that the attacker doesn't like.

The CISSP for Dummies book has nice coverage of the different types of attacks, here is an extract:

Terrorism Attacks
Terrorism exists at many levels on the Internet. In April 2001, during a period of tense relations between China and the U.S. (resulting from the crash landing of a U.S. Navy reconnaissance plane on Hainan Island), Chinese hackers (cyberterrorists) launched a major effort to disrupt critical U.S. infrastructure, which included U.S. government and military systems.

Following the terrorist attacks against the U.S. on September 11, 2001, the general public became painfully aware of the extent of terrorism on the Internet. Terrorist organizations and cells are using online capabilities to coordinate attacks, transfer funds, harm international commerce, disrupt critical systems, disseminate propaganda, and gain useful information about developing techniques and instruments of terror, including nuclear , biological, and chemical weapons.
Military and intelligence attacks

Military and intelligence attacks are perpetrated by criminals, traitors, or foreign intelligence agents seeking classified law enforcement or military information. Such attacks may also be carried out by governments during times of war and conflict.
Financial attacks

Banks, large corporations, and e-commerce sites are the targets of financial attacks, all of which are motivated by greed. Financial attacks may seek to steal or embezzle funds, gain access to online financial information, extort individuals or businesses, or obtain the personal credit card numbers of customers.
Business attacks

Businesses are becoming the targets of more and more computer and Internet attacks. These attacks include competitive intelligence gathering, denial of service, and other computer- related attacks. Businesses are often targeted for several reasons including

Lack of expertise: Despite heightened security awareness, a shortage of qualified security

professionals still exists, particularly in private enterprise. Lack of resources: Businesses often lack the resources to prevent, or even detect, attacks against their systems.
Lack of reporting or prosecution : Because of public relations concerns and the inability to prosecute computer criminals due to either a lack of evidence or a lack of properly handled evidence, the majority of business attacks still go unreported.

The cost to businesses can be significant, including loss of trade secrets or proprietary information, loss of revenue, and loss of reputation.

Grudge attacks
Grudge attacks are targeted at individuals or businesses and are motivated by a desire to take revenge against a person or organization. A disgruntled employee, for example, may steal trade secrets, delete valuable data, or plant a logic bomb in a critical system or application.

Fortunately, these attacks (at least in the case of a disgruntled employee) can be easier to prevent or prosecute than many other types of attacks because:

The attacker is often known to the victim.
The attack has a visible impact that produces a viable evidence trail. Most businesses (already sensitive to the possibility of wrongful termination suits) have well-established termination procedures

"Fun" attacks
"Fun" attacks are perpetrated by thrill seekers and script kiddies who are motivated by curiosity or excitement. Although these attackers may not intend to do any harm or use any of the information that they access, they're still dangerous and their activities are still illegal.

These attacks can also be relatively easy to detect and prosecute. Because the perpetrators are often script kiddies or otherwise inexperienced hackers, they may not know how to cover their tracks effectively.

Also, because no real harm is normally done nor intended against the system, it may be tempting (although ill advised) for a business to prosecute the individual and put a positive public relations spin on the incident. You've seen the film at 11: "We quickly detected the attack, prevented any harm to our network, and prosecuted the responsible individual; our security is unbreakable !" Such action, however, will likely motivate others to launch a more serious and concerted grudge attack against the business.

Many computer criminals in this category only seek notoriety. Although it's one thing to brag to a small circle of friends about defacing a public Web site, the wily hacker who appears on CNN reaches the next level of hacker celebrity-dom. These twisted individuals want to be caught to revel in their 15 minutes of fame.

References:
ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 10: Law, Investigation, and Ethics (page 187)
CISSP Professional Study Guide by James Michael Stewart, Ed Tittel, Mike Chapple, page 607-609
CISSP for Dummies, Miller L.H.and Gregory P.H.ISBN: 0470537914, page 309-311

QUESTION 492
Which of the following statements pertaining to disaster recovery is incorrect?

A. A recovery team's primary task is to get the pre-defined critical business functions at the alternate

backup processing site.
B. A salvage team's task is to ensure that the primary site returns to normal processing conditions.
C. The disaster recovery plan should include how the company will return from the alternate site to the primary site.
D. When returning to the primary site, the most critical applications should be brought back first.

Correct Answer: D
Explanation:
It's interesting to note that the steps to resume normal processing operations will be different than the steps in the recovery plan; that is, the least critical work should be brought back first to the primary site.

My explanation:
at the point where the primary site is ready to receive operations again, less critical systems should be brought back first because one has to make sure that everything will be running smoothly at the primary site before returning critical systems, which are already operating normally at the recovery site.

This will limit the possible interruption of processing to a minimum for most critical systems, thus making it the best option.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 8: Business Continuity Planning and Disaster Recovery Planning (page 291).

QUESTION 493
A momentary low voltage, from 1 cycle to a few seconds, is a:

A. spike
B. blackout
C. sag
D. fault

Correct Answer: C
Explanation:
A momentary low voltage is a sag. A synonym would be a dip.

Risks to electrical power supply:

POWER FAILURE

Blackout: complete loss of electrical power
Fault: momentary power outage

POWER DEGRADATION

Brownout: an intentional reduction of voltage by the power company.
Sag/dip: a short period of low voltage

POWER EXCESS

Surge: Prolonged rise in voltage
Spike: Momentary High Voltage
In-rush current: the initial surge of current required by a load before it reaches normal operation.

Transient: line noise or disturbance is superimposed on the supply circuit and can cause fluctuations in electrical power

Refence(s) used for this question:
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 462). McGraw- Hill. Kindle Edition.

QUESTION 494
Which of the following is NOT a common category/classification of threat to an IT system?

A. Human
B. Natural
C. Technological
D. Hackers

Correct Answer: D
Explanation:
Hackers are classified as a human threat and not a classification by itself.

All the other answers are incorrect. Threats result from a variety of factors, although they are classified in three types: Natural (e.g., hurricane, tornado, flood and fire), human (e.g. operator error, sabotage, malicious code) or technological (e.g. equipment failure, software error, telecommunications network outage, electric power failure).

Reference:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11- 2010.pdf, June 2002 (page 6).

QUESTION 495
Which of the following best describes what would be expected at a "hot site"?

A. Computers, climate control, cables and peripherals
B. Computers and peripherals
C. Computers and dedicated climate control systems.
D. Dedicated climate control systems

Correct Answer: A
Explanation:
A Hot Site contains everything needed to become operational in the shortest amount of time.

The following answers are incorrect:

Computers and peripherals. Is incorrect because no mention is made of cables. You would not be fully operational without those.

Computers and dedicated climate control systems. Is incorrect because no mention is made of peripherals. You would not be fully operational without those.

Dedicated climate control systems. Is incorrect because no mentionis made of computers, cables and peripherals. You would not be fully operational without those.

According to the OIG, a hot site is defined as a fully configured site with complete customer