as Someone who is using resources in a way that is not authorized. A recent case in Ohio involved an internal employee who was spending most of his day on dating website looking for the love of his life. The employee was taken to court for hacking the company resources.

The following answers are incorrect:

hackers. Is incorrect because while hackers represent a very large problem and both the frequency of attacks and overall losses have grown hackers are considered to be a small segment of combined computer fraudsters.

industrial saboteurs. Is incorrect because industrial saboteurs tend to go after trade secrets. While the loss to the organization can be great, they still fall short when compared to the losses created by employees. Often it is an employee that was involved in industrial sabotage.

foreign intelligence officers. Is incorrect because the losses tend to be national secrets. You really can't put t cost on this and the number of frequency and occurances of this is less than that of employee related losses.

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 Locations 22327-22331). Auerbach Publications. Kindle Edition.

QUESTION 525
Which of the following is NOT a transaction redundancy implementation?

A. on-site mirroring
B. Electronic Vaulting
C. Remote Journaling
D. Database Shadowing

Correct Answer: A
Explanation:
Three concepts are used to create a level of fault tolerance and redundancy in transaction processing.

They are Electronic vaulting, remote journaling and database shadowing provide redundancy at the transaction level.

Electronic vaulting is accomplished by backing up system data over a network. The backup location is usually at a separate geographical location known as the vault site. Vaulting can be used as a mirror or a backup mechanism using the standard incremental or differential backup cycle. Changes to the host system are sent to the vault server in real-time when the backup method is implemented as a mirror. If vaulting updates are recorded in real-time, then it will be necessary to perform regular backups at the off-site location to provide recovery services due to inadvertent or malicious alterations to user or system data.

Journaling or Remote Journaling is another technique used by database management systems to provide redundancy for their transactions. When a transaction is completed, the database management system duplicates the journal entry at a remote location. The journal provides sufficient detail for the transaction to be replayed on the remote system. This provides for database recovery in the event that the database becomes corrupted or unavailable.

There are also additional redundancy options available within application and database software platforms. For example, database shadowing may be used where a database management

system updates records in multiple locations. This technique updates an entire copy of the database at a remote location.

Reference used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20403-20407). Auerbach Publications. Kindle Edition.
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 20375-20377). Auerbach Publications. Kindle Edition.

QUESTION 526
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. What is the name of this type of evidence?

A. Circumstantial evidence
B. Corroborative evidence
C. Opinion evidence
D. Secondary evidence

Correct Answer: B
Explanation:
This type of supporting evidence is used to help prove an idea or a point, however It cannot stand on its own, it is used as a supplementary tool to help prove a primary piece of evidence. Corrobative evidence takes many forms.

In a rape case for example, this could consist of torn clothing, soiled bed sheets, 911 emergency calls tapes, and
prompt complaint witnesses.

There are many types of evidence that exist. Below you have explanations of some of the most common types:
Physical Evidence

Physical evidence is any evidence introduced in a trial in the form of a physical object, intended to prove a fact in issue based on its demonstrable physical characteristics. Physical evidence can conceivably include all or part of any object.

In a murder trial for example (or a civil trial for assault), the physical evidence might include DNA left by the attacker on the victim's body, the body itself, the weapon used, pieces of carpet spattered with blood, or casts of footprints or tire prints found at the scene of the crime.
Real Evidence
Real evidence is a type of physical evidence and consists of objects that were involved in a case or actually played a part in the incident or transaction in question.

Examples include the written contract, the defective part or defective product, the murder weapon, the gloves used by an alleged murderer. Trace evidence, such as fingerprints and firearm residue, is a species of real evidence. Real evidence is usually reported upon by an expert witness with appropriate qualifications to give an opinion. This normally means a forensic scientist or one qualified in forensic engineering.

Admission of real evidence requires authentication, a showing of relevance, and a showing that the object is in "the same or substantially the same condition" now as it was on the relevant date. An object of real evidence is authenticated through the senses of witnesses or by circumstantial

evidence called chain of custody.

Documentary
Documentary evidence is any evidence introduced at a trial in the form of documents. Although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence.

Documentary versus physical evidence
A piece of evidence is not documentary evidence if it is presented for some purpose other than the examination of the contents of the document. For example, if a blood-spattered letter is introduced solely to show that the defendant stabbed the author of the letter from behind as it was being written, then the evidence is physical evidence, not documentary evidence. However, a film of the murder taking place would be documentary evidence (just as a written description of the event from an eyewitness). If the content of that same letter is then introduced to show the motive for the murder, then the evidence would be both physical and documentary.

Documentary Evidence Authentication
Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author. Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.

The role of the expert witness
Where physical evidence is of a complexity that makes it difficult for the average person to understand its significance, an expert witness may be called to explain to the jury the proper interpretation of the evidence at hand.

Digital Evidence or Electronic Evidence
Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial.

The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

While many courts in the United States have applied the Federal Rules of Evidence to digital evidence in the same way as more traditional documents, courts have noted very important differences. As compared to the more traditional evidence, courts have noted that digital evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive, and more readily available. As such, some courts have sometimes treated digital evidence differently for purposes of authentication, hearsay, the best evidence rule, and privilege. In December 2006, strict new rules were enacted within the Federal Rules of Civil Procedure requiring the preservation and disclosure of electronically stored evidence.

Demonstrative Evidence
Demonstrative evidence is evidence in the form of a representation of an object. This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial.

Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and

models. It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case. To be admissible, a demonstrative exhibit must "fairly and accurately" represent the real object at the relevant time.

Chain of custody
Chain of custody refers to the chronological documentation, and/or paper trail, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic. Because evidence can be used in court to convict persons of crimes, it must be handled in a scrupulously careful manner to avoid later allegations of tampering or misconduct which can compromise the case of the prosecution toward acquittal or to overturning a guilty verdict upon appeal.

The idea behind recoding the chain of custody is to establish that the alleged evidence is fact related to the alleged crime - rather than, for example, having been planted fraudulently to make someone appear guilty.

Establishing the chain of custody is especially important when the evidence consists of fungible goods. In practice, this most often applies to illegal drugs which have been seized by law enforcement personnel. In such cases, the defendant at times disclaims any knowledge of possession of the controlled substance in question.

Accordingly, the chain of custody documentation and testimony is presented by the prosecution to establish that the substance in evidence was in fact in the possession of the defendant.

An identifiable person must always have the physical custody of a piece of evidence. In practice, this means that a police officer or detective will take charge of a piece of evidence, document its collection, and hand it over to an evidence clerk for storage in a secure place. These transactions, and every succeeding transaction between the collection of the evidence and its appearance in court, should be completely documented chronologically in order to withstand legal challenges to the authenticity of the evidence. Documentation should include the conditions under which the evidence is gathered, the identity of all evidence handlers, duration of evidence custody, security conditions while handling or storing the evidence, and the manner in which evidence is transferred to subsequent custodians each time such a transfer occurs (along with the signatures of persons involved at each step).

Example:
An example of "Chain of Custody" would be the recovery of a bloody knife at a murder scene: Officer Andrew collects the knife and places it into a container, then gives it to forensics technician Bill. Forensics technician Bill takes the knife to the lab and collects fingerprints and other evidence from the knife. Bill then gives the knife and all evidence gathered from the knife to evidence clerk Charlene. Charlene then stores the evidence until it is needed, documenting everyone who has accessed the original evidence (the knife, and original copies of the lifted fingerprints).

The Chain of Custody requires that from the moment the evidence is collected, every transfer of evidence from person to person be documented and that it be provable that nobody else could have accessed that evidence. It is best to keep the number of transfers as low as possible.

In the courtroom, if the defendant questions the Chain of Custody of the evidence it can be proven that the knife in the evidence room is the same knife found at the crime scene. However, if there are discrepancies and it cannot be proven who had the knife at a particular point in time, then the Chain of Custody is broken and the defendant can ask to have the resulting evidence declared inadmissible.

"Chain of custody" is also used in most chemical sampling situations to maintain the integrity of

the sample by providing documentation of the control, transfer, and analysis of samples. Chain of custody is especially important in environmental work where sampling can identify the existence of contamination and can be used to identify the responsible party.

References:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 23173-23185). Auerbach Publications. Kindle Edition.
http://en.wikipedia.org/wiki/Documentary_evidence
http://en.wikipedia.org/wiki/Physical_evidence
http://en.wikipedia.org/wiki/Digital_evidence
http://en.wikipedia.org/wiki/Demonstrative_evidence
http://en.wikipedia.org/wiki/Real_evidence
http://en.wikipedia.org/wiki/Chain_of_custody

QUESTION 527
Which of the following item would best help an organization to gain a common understanding of functions that are critical to its survival?

A. A risk assessment
B. A business assessment
C. A disaster recovery plan
D. A business impact analysis

Correct Answer: D
Explanation:
A Business Impact Analysis (BIA) is an assessment of an organization's business functions to develop an understanding of their criticality, recovery time objectives, and resources needed.
By going through a Business Impact Analysis, the organization will gain a common understanding of functions that are critical to its survival.
A risk assessment is an evaluation of the exposures present in an organization's external and internal environments.
A Business Assessment generally include Business Analysis as a discipline and it has heavy overlap with requirements analysis sometimes also called requirements engineering, but focuses on identifying the changes to an organization that are required for it to achieve strategic goals. These changes include changes to strategies, structures, policies, processes, and information systems.
A disaster recovery plan is the comprehensive statement of consistent actions to be taken before, during and after a disruptive event that causes a significant loss of information systems resources.
Source: BARNES, James C.& ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley & Sons, 2001 (page 57).

QUESTION 528
When preparing a business continuity plan, who of the following is responsible for identifying and prioritizing time-critical systems?

A. Executive management staff
B. Senior business unit management
C. BCP committee
D. Functional business units

Correct Answer: B
Explanation: