

Correct Answer: B

Explanation:

This will expose any weaknesses in the plan and ensure the primary site has been properly repaired before moving back. Moving critical assets first may induce a second disaster if the primary site has not been repaired properly.

The first group to go back would test items such as connectivity, HVAC, power, water, improper procedures, and/or steps that has been overlooked or not done properly. By moving these first, and fixing any problems identified, the critical operations of the company are not negatively affected.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 9: Disaster Recovery and Business continuity (page 621).

QUESTION 562

Which of the following is NOT a task normally performed by a Computer Incident Response Team (CIRT)?

- A. Develop an information security policy.
- B. Coordinate the distribution of information pertaining to the incident to the appropriate parties.
- C. Mitigate risk to the enterprise.
- D. Assemble teams to investigate the potential vulnerabilities.

Correct Answer: A

Explanation:

Writing a corporate security policy is normally a task of upper management in an organization. Other tasks would usually be performed by a Computer Incident Response Team.

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 64).

QUESTION 563

Which of the following proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

- A. Direct evidence.
- B. Circumstantial evidence.
- C. Conclusive evidence.
- D. Corroborative evidence.

Correct Answer: A

Explanation:

Direct evidence can prove a fact all by itself and does not need backup information to refer to. When using direct evidence, presumptions are not required. One example of direct evidence is the testimony of a witness who saw a crime take place. Although this oral evidence would be secondary in nature, meaning a case could not rest on just it alone, it is also direct evidence, meaning the lawyer does not necessarily need to provide other evidence to back it up. Direct evidence often is based on information gathered from a witness's five senses.

The following answers are incorrect:

Circumstantial evidence. Is incorrect because Circumstantial evidence can prove an intermediate fact that can then be used to deduce or assume the existence of another fact. Conclusive

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

evidence. Is incorrect because Conclusive evidence is irrefutable and cannot be contradicted. Conclusive evidence is very strong all by itself and does not require corroboration.

Corroborative evidence. Is incorrect because Corroborative evidence is supporting evidence used to help prove an idea or point. It cannot stand on its own, but is used as a supplementary tool to help prove a primary piece of evidence.

QUESTION 564

Valuable paper insurance coverage does not cover damage to which of the following?

- A. Inscribed, printed and Written documents
- B. Manuscripts
- C. Records
- D. Money and Securities

Correct Answer: D

Explanation:

All businesses are driven by records. Even in today's electronic society businesses generate mountains of critical documents everyday. Invoices, client lists, calendars, contracts, files, medical records, and innumerable other records are generated every day.

Stop and ask yourself what happens if your business lost those documents today.

Valuable papers business insurance coverage provides coverage to your business in case of a loss of vital records. Over the years policy language has evolved to include a number of different types of records. Generally, the policy will cover "written, printed, or otherwise inscribed documents and records, including books, maps, films, drawings, abstracts, deeds, mortgages, and manuscripts." But, read the policy coverage carefully. The policy language typically "does not mean "money" or "securities," converted data, programs or instructions used in your data processing operations, including the materials on which the data is recorded."

The coverage is often included as a part of property insurance or as part of a small business owner policy. For example, a small business owner policy includes in many cases valuable papers coverage up to \$25,000.

It is important to realize what the coverage actually entails and, even more critical, to analyze your business to determine what it would cost to replace records.

The coverage pays for the loss of vital papers and the cost to replace the records up to the limit of the insurance and after application of any deductible. For example, the insurer will pay to have waterlogged papers dried and reproduced (remember, fires are put out by water and the fire department does not stop to remove your book keeping records). The insurer may cover temporary storage or the cost of moving records to avoid a loss.

For some businesses, losing customer lists, some business records, and contracts, can mean the expense and trouble of having to recreate those documents, but is relatively easy and a low level risk and loss. Larger businesses and especially professionals (lawyers, accountants, doctors) are in an entirely separate category and the cost of replacement of documents is much higher.

Consider, in analyzing your business and potential risk, what it would actually cost to reproduce your critical business records. Would you need to hire temporary personnel? How many hours of productivity would go into replacing the records? Would you need to obtain originals? Would original work need to be recreated (for example, home inspectors, surveyors, cartographers)?

Often when a business owner considers the actual cost related to the reproduction of records, the

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

owner quickly realizes that their business insurance policy limits for valuable papers coverage is woefully inadequate.

Insurers (and your insurance professional) will often suggest higher coverages for valuable papers. The extra premium is often worth the cost and should be considered.

Finally, most policies will require records to be protected. You need to review your declarations pages and speak with your insurer to determine what is required. Some insurers may offer discounted coverage if there is a document retention and back up plan in place and followed. There are professional organizations that can assist your business in designing a records management policy to lower the risk (and your premiums). For example, ARMA International has been around since 1955 and its members consist of some of the top document retention and storage companies.

Reference(s) used for this question:

<http://businessinsure.about.com/od/propertyinsurance/f/vpcov.htm>

QUESTION 565

What can be defined as a momentary low voltage?

- A. Spike
- B. Sag
- C. Fault
- D. Brownout

Correct Answer: B

Explanation:

A sag is a momentary low voltage. A spike is a momentary high voltage. A fault is a momentary power out and a brownout is a prolonged power supply that is below normal voltage.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 6: Physical security (page 299)

QUESTION 566

Which of the following outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations?

- A. The Computer Security Act of 1987.
- B. The Federal Sentencing Guidelines of 1991.
- C. The Economic Espionage Act of 1996.
- D. The Computer Fraud and Abuse Act of 1986.

Correct Answer: B

Explanation:

In 1991, U.S. Federal Sentencing Guidelines were developed to provide judges with courses of action in dealing with white collar crimes. These guidelines provided ways that companies and law enforcement should prevent, detect and report computer crimes. It also outlined how senior management are responsible for the computer and information security decisions that they make and what actually took place within their organizations.

QUESTION 567

Which of the following backup methods is primarily run when time and tape space permits, and is

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>

used for the system archive or baselined tape sets?

- A. full backup method.
- B. incremental backup method.
- C. differential backup method.
- D. tape backup method.

Correct Answer: A

Explanation:

The Full Backup Method is primarily run when time and tape space permits, and is used for the system archive or baselined tape sets.

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 69.

QUESTION 568

Which of the following would best describe secondary evidence?

- A. Oral testimony by a non-expert witness
- B. Oral testimony by an expert witness
- C. A copy of a piece of evidence
- D. Evidence that proves a specific act

Correct Answer: C

Explanation:

Secondary evidence is defined as a copy of evidence or oral description of its contents. It is considered not as reliable as best evidence. Evidence that proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses is considered direct evidence. The fact that testimony is given by an expert only affects the witness's ability to offer an opinion instead of only testifying of the facts.

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 569

Which of the following is the biggest factor that makes Computer Crimes possible?

- A. The fraudster obtaining advanced training & special knowledge.
- B. Victim carelessness.
- C. Collusion with others in information processing.
- D. System design flaws.

Correct Answer: B

Explanation:

The biggest factor that makes Computer Crimes possible is Victim Carelessness. Awareness and education can reduce the chance of someone becoming a victim.

The types and frequency of Computer Crimes are increasing at a rapid rate. Computer Crime was once mainly the result of insiders or disgruntled employees. Now just about everybody has access to the internet, professional criminals are taking advantage of this.

Specialized skills are no longer needed and a search on the internet can provide a fraudster with a plethora of tools that can be used to perpetuate fraud.

[Download Full Version SSCP Exam Dumps\(Updated in Feb/2023\)](#)

All too often carelessness leads to someone being a victim. People often use simple passwords or write them down in plain sight where they can be found by fraudsters. People throwing away papers loaded with account numbers, social security numbers, or other types of non-public personal information. There are phishing e-mail attempts where the fraudster tries to redirect a potential victim to a bogus site that resembles a legitimate site in an attempt to get the users' login ID and password, or other credentials. There is also social engineering. Awareness and training can help reduce the chance of someone becoming a victim.

The following answers are incorrect:

The fraudster obtaining advanced training and special knowledge. Is incorrect because training and special knowledge is not required. There are many tools widely available to fraudsters.

Collusion with others in information processing. Is incorrect because as more and more people use computers in their daily lives, it is no longer necessary to have someone on the inside be a party to fraud attempts.

System design flaws. Is incorrect because while System design flaws are sometimes a factor in Computer Crimes more often than not it is victim carelessness that leads to Computer Crimes.

References:

OIG CBK Legal, Regulations, Compliance and Investigations (pages 695 - 697)

QUESTION 570

Which backup method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup?

- A. differential backup method
- B. full backup method
- C. incremental backup method
- D. tape backup method.

Correct Answer: A

Explanation:

The Differential Backup Method is additive because the time and tape space required for each night's backup grows during the week as it copies the day's changed files and the previous days' changed files up to the last full backup.

Archive Bits

Unless you've done a lot of backups in your time you've probably never heard of an Archive Bit. An archive bit is, essentially, a tag that is attached to every file. In actuality, it is a binary digit that is set on or off in the file, but that's crummy technical jargon that doesn't really tell us anything. For the sake of our discussion, just think of it as the flag on a mail box. If the flag is up, it means the file has been changed. If it's down, then the file is unchanged.

Archive bits let the backup software know what needs to be backed up. The differential and incremental backup types rely on the archive bit to direct them.

Backup Types

Full or Normal

The "Full" or "normal" backup type is the most standard. This is the backup type that you would use if you wanted to backup every file in a given folder or drive. It backs up everything you direct it to regardless of what the archive bit says. It also resets all archive bits (puts the flags down).

[SSCP Exam Dumps](#) [SSCP PDF Dumps](#) [SSCP VCE Dumps](#) [SSCP Q&As](#)

<https://www.ensurepass.com/SSCP.html>