Correct Answer: C

QUESTION 36

Which of the following is most relevant to determining the maximum effective cost of access control?

A. the value of information that is protected
B. management's perceptions regarding data importance
C. budget planning related to base versus incremental spending
D. the cost to replace lost data

Correct Answer: A

QUESTION 37

Which one of the following is the MAIN goal of a security awareness program when addressing senior management?

A. Provide a vehicle for communicating security procedures.
B. Provide a clear understanding of potential risk and exposure.
C. Provide a forum for disclosing exposure and risk analysis.
D. Provide a forum to communicate user responsibilities.

Correct Answer: B

QUESTION 38

In developing a security awareness program, it is MOST important to

A. Understand the corporate culture and how it will affect security.
B. Understand employees preferences for information security.
C. Know what security awareness products are available.
D. Identify weakness in line management support.

Correct Answer: A

QUESTION 39

Which of the following would be best suited to provide information during a review of the controls over the process of defining IT service levels?

A. Systems programmer
B. Legal stuff

C.   Business unit manager

D.   Programmer

Correct Answer: C

QUESTION 40

Which of the following best explains why computerized information systems frequently fail to meet the needs of users?

A.   Inadequate quality assurance (QA) tools

B.   Constantly changing user needs

C.   Inadequate user participation in defining the system's requirements

D.   Inadequate project management.

Correct Answer: C

QUESTION 41

Which of the following is not a compensating measure for access violations?

A.   Backups

B.   Business continuity planning

C.   Insurance

D.   Security awareness

Correct Answer: D

QUESTION 42

Risk analysis is MOST useful when applied during which phase of the system development process?

A.   Project identification

B.   Requirements definition

C.   System construction

D.   Implementation planning

Correct Answer: A

QUESTION 43

Which one of the following is not one of the outcomes of a vulnerability analysis?

A. Quantitative loss assessment
B. Qualitative loss assessment
C. Formal approval of BCP scope and initiation document
D. Defining critical support areas

Correct Answer: C

QUESTION 44

Which of the following is not a part of risk analysis?

A. Identify risks
B. Quantify the impact of potential threats
C. Provide an economic balance between the impact of the risk and the cost of the associated countermeasures
D. Choose the best countermeasure

Correct Answer: D

QUESTION 45

A new worm has been released on the Internet. After investigation, you have not been able to determine if you are at risk of exposure. Management is concerned as they have heard that a number of their counterparts are being affected by the worm. How could you determine if you are at risk?

A. Evaluate evolving environment.
B. Contact your anti-virus vendor.
C. Discuss threat with a peer in another organization.
D. Wait for notification from an anti-virus vendor.

Correct Answer: B

QUESTION 46

When conducting a risk assessment, which one of the following is NOT an acceptable social engineering practice?

A. Shoulder surfing
B. Misrepresentation
C. Subversion
D. Dumpster diving

Correct Answer: A

QUESTION 47

Which one of the following risk analysis terms characterizes the absence or weakness of a risk reducing safegaurd?

A. Threat
B. Probability
C. Vulnerability
D. Loss expectancy

Correct Answer: C

QUESTION 48

Risk is commonly expressed as a function of the

A. Systems vulnerabilities and the cost to mitigate.
B. Types of countermeasures needed and the system's vulnerabilities.
C. Likelihood that the harm will occur and its potential impact.
D. Computer system-related assets and their costs.

Correct Answer: C

QUESTION 49

How should a risk be handled when the cost of the countermeasures outweighs the cost of the risk?

A. Reject the risk
B. Perform another risk analysis
C. Accept the risk
D. Reduce the risk

Correct Answer: C

QUESTION 50

Which of the following is an advantage of a qualitative over quantitative risk analysis?

A. It prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities.
B. It provides specific quantifiable measurements of the magnitude of the impacts.
C. It makes cost-benefit analysis of recommended controls easier.
D. None of the above.

Correct Answer: A

QUESTION 51

The absence or weakness in a system that may possibly be exploited is called a(n)?

A. Threat
B. Exposure
C. Vulnerability
D. Risk

Correct Answer: C

QUESTION 52

What tool do you use to determine whether a host is vulnerable to known attacks?

A. Padded Cells
B. Vulnerability analysis
C. Honey Pots
D. IDS

Correct Answer: B

QUESTION 53

Which of the following statements pertaining to ethical hacking is incorrect?

A. An organization should use ethical hackers who do not sell auditing, consulting, hardware, software, firewall, hosting, and/or networking services.
B. Testing should be done remotely.
C. Ethical hacking should not involve writing to or modifying the target systems.
D. Ethical hackers should never use tools that have potential of exploiting vulnerabilities in the organizations IT system.

Correct Answer: D

QUESTION 54

Why would an information security policy require that communications test equipment be controlled?

A. The equipment is susceptible to damage.
B. The equipment can be used to browse information passing on a network.