QUESTION 281
When speaking to an organization's human resources department about information security, an information security manager should focus on the need for:

A. an adequate budget for the security program.
B. recruitment of technical IT employees.
C. periodic risk assessments.
D. security awareness training for employees.

Correct Answer: D
Explanation:
An information security manager has to impress upon the human resources department the need for security awareness training for all employees. Budget considerations are more of an accounting function. The human resources department would become involved once they are convinced for the need of security awareness training. Recruiting IT-savvy staff may bring in new employees with better awareness of information security, but that is not a replacement for the training requirements of the other employees. Periodic risk assessments may or may not involve the human resources department function.

QUESTION 282
An organization without any formal information security program that has decided to implement information security best practices should FIRST:

A. invite an external consultant to create the security strategy.
B. allocate budget based on best practices.
C. benchmark similar organizations.
D. define high-level business security requirements.

Correct Answer: D
Explanation:
All four options are valid steps in the process of implementing information security best practices; however, defining high-level business security requirements should precede the others because the implementation should be based on those security requirements.

QUESTION 283
An extranet server should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

Correct Answer: C
Explanation:
An extranet server should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be true of placing it on the external router, although this would not be possible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the extranet on the same physical device.

QUESTION 284
The MAIN reason for deploying a public key infrastructure (PKI) when implementing an information security program is to:

A. ensure the confidentiality of sensitive material.
B. provide a high assurance of identity.
C. allow deployment of the active directory.
D. implement secure sockets layer (SSL) encryption.

Correct Answer: B
Explanation:
The primary purpose of a public key infrastructure (PKI) is to provide strong authentication. Confidentiality is a function of the session keys distributed by the PKI. An active directory can use PKI for authentication as well as using other means. Even though secure sockets layer (SSL) encryption requires keys to authenticate, it is not the main reason for deploying PKI.

QUESTION 285
Which of the following is the MOST important item to include when developing web hosting agreements with third-party providers?

A. Termination conditions
B. Liability limits
C. Service levels
D. Privacy restrictions

Correct Answer: C
Explanation:
Service levels are key to holding third parties accountable for adequate delivery of services. This is more important than termination conditions, privacy restrictions or liability limitations.

QUESTION 286
Which of the following BEST ensures that modifications made to in-house developed business applications do not introduce new security exposures?

A. Stress testing
B. Patch management
C. Change management
D. Security baselines

Correct Answer: C
Explanation:
Change management controls the process of introducing changes to systems to ensure that unintended changes are not introduced. Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Security baselines provide minimum recommended settings. Stress testing ensures that there are no scalability problems.

QUESTION 287
The MOST effective way to ensure network users are aware of their responsibilities to comply with an organization's security requirements is:

A. messages displayed at every logon.

B. periodic security-related e-mail messages.
C. an Intranet web site for information security.
D. circulating the information security policy.

Correct Answer: A
Explanation:
Logon banners would appear every time the user logs on, and the user would be required to read and agree to the same before using the resources. Also, as the message is conveyed in writing and appears consistently, it can be easily enforceable in any organization. Security-related e-mail messages are frequently considered as "Spam" by network users and do not, by themselves, ensure that the user agrees to comply with security requirements. The existence of an Intranet web site does not force users to access it and read the information. Circulating the information security policy atone does not confirm that an individual user has read, understood and agreed to comply with its requirements unless it is associated with formal acknowledgment, such as a user's signature of acceptance.

QUESTION 288
An internal review of a web-based application system finds the ability to gain access to all employees' accounts by changing the employee's ID on the URL used for accessing the account. The vulnerability identified is:

A. broken authentication.
B. unvalidated input.
C. cross-site scripting.
D. structured query language (SQL) injection.

Correct Answer: A
Explanation:
The authentication process is broken because, although the session is valid, the application should reauthenticate when the input parameters are changed. The review provided valid employee IDs, and valid input was processed. The problem here is the lack of reauthentication when the input parameters are changed. Cross-site scripting is not the problem in this case since the attack is not transferred to any other user's browser to obtain the output. Structured query language (SQL) injection is not a problem since input is provided as a valid employee ID and no SQL queries are injected to provide the output.

QUESTION 289
The BEST reason for an organization to have two discrete firewalls connected directly to the Internet and to the same DMZ would be to:

A. provide in-depth defense.
B. separate test and production.
C. permit traffic load balancing.
D. prevent a denial-of-service attack.

Correct Answer: C
Explanation:
Having two entry points, each guarded by a separate firewall, is desirable to permit traffic load balancing. As they both connect to the Internet and to the same demilitarized zone (DMZ), such an arrangement is not practical for separating test from production or preventing a denial-of-service attack.

QUESTION 290
The BEST metric for evaluating the effectiveness of a firewall is the:

A. number of attacks blocked.
B. number of packets dropped.
C. average throughput rate.
D. number of firewall rules.

Correct Answer: A
Explanation:
The number of attacks blocked indicates whether a firewall is performing as intended. The number of packets dropped does not necessarily indicate the level of effectiveness. The number of firewall rules and the average throughput rate are not effective measurements.

QUESTION 291
Primary direction on the impact of compliance with new regulatory requirements that may lead to major application system changes should be obtained from the:

A. corporate internal auditor.
B. System developers/analysts.
C. key business process owners.
D. corporate legal counsel.

Correct Answer: C
Explanation:
Business process owners are in the best position to understand how new regulatory requirements may affect their systems. Legal counsel and infrastructure management, as well as internal auditors, would not be in as good a position to fully understand all ramifications.

QUESTION 292
An intrusion detection system should be placed:

A. outside the firewall.
B. on the firewall server.
C. on a screened subnet.
D. on the external router.

Correct Answer: C
Explanation:
An intrusion detection system (IDS) should be placed on a screened subnet, which is a demilitarized zone (DMZ). Placing it on the Internet side of the firewall would leave it defenseless. The same would be tmc of placing it on the external router, if such a thing were feasible. Since firewalls should be installed on hardened servers with minimal services enabled, it would be inappropriate to store the IDS on the same physical dcvice.

QUESTION 293
Which of the following is the MOST important risk associated with middleware in a client- server environment?

A. Server patching may be prevented
B. System backups may be incomplete
C. System integrity may be affected

D. End-user sessions may be hijacked

Correct Answer: C
Explanation:
The major risk associated with middleware in a client-server environment is that system integrity may be adversely affected because of the very purpose of middleware, which is intended to support multiple operating environments interacting concurrently. Lack of proper software to control portability of data or programs across multiple platforms could result in a loss of data or program integrity. All other choices are less likely to occur.

QUESTION 294
The main mail server of a financial institution has been compromised at the superuser level; the only way to ensure the system is secure would be to:

A. change the root password of the system.
B. implement multifactor authentication.
C. rebuild the system from the original installation medium.
D. disconnect the mail server from the network.

Correct Answer: C
Explanation:
Rebuilding the system from the original installation medium is the only way to ensure all security vulnerabilities and potential stealth malicious programs have been destroyed. Changing the root password of the system does not ensure the integrity of the mail server. Implementing multifactor authentication is an aftermeasure and does not clear existing security threats. Disconnecting the mail server from the network is an initial step, but does not guarantee security.

QUESTION 295
Which of the following ensures that newly identified security weaknesses in an operating system are mitigated in a timely fashion?

A. Patch management
B. Change management
C. Security baselines
D. Acquisition management

Correct Answer: A
Explanation:
Patch management involves the correction of software weaknesses and helps ensure that newly identified exploits are mitigated in a timely fashion. Change management controls the process of introducing changes to systems. Security baselines provide minimum recommended settings. Acquisition management controls the purchasing process.

QUESTION 296
The MOST effective way to ensure that outsourced service providers comply with the organization's information security policy would be:

A. service level monitoring.
B. penetration testing.
C. periodically auditing.
D. security awareness training.

Correct Answer: C
Explanation: