Answers:

1)

a) This is incorrect. The business manager is likely to be focused on getting the business done as opposed to the risk posed to the organization.

b) This is incorrect. The typical information security manager is focused on risk, and on average, he/she will overestimate risk by about 100 percent—usually considering worst case scenarios rather than the most probable events.

c) Correct! Executive management will be in the best position to consider the big picture and the trade-offs between security and functionality in the entire organization.

d) This is incorrect. There is no indication that the assessments are inadequate or defective in some way; therefore, repeating the exercise is not warranted

2)

a) This is incorrect. The security officer supports and implements information security to achieve senior management objectives.

b) Correct! Routine administration of all aspects of security is delegated, but top management must retain overall accountability.

c) This is incorrect. The end user does not perform categorization.

d) This is incorrect. The custodian supports and implements information security measures as directed.

3)

a) Correct! The most important feature of target attacks as seen in advanced persistent threats is that malware secretly sends information back to a command and control server. Therefore, monitoring of outbound server communications that do not follow predefined routes will be the best control to detect such security events.

b) This is incorrect. Server communications are usually not monitored to evaluate the resiliency of server operations.

c) This is incorrect. The effectiveness of an intrusion detection system may not be verified by monitoring outbound server communications.

d) This is incorrect. Nonrepudiation may be supported by technology, such as a digital signature. Server communication itself does not support the effectiveness of an e-commerce framework.

4)

a) This is incorrect. Capturing the authentication handshake and replaying it through the network will not work. Using hashes by itself will not prevent a replay.

b) Correct! A challenge/response mechanism prevents replay attacks by sending a different random challenge in each authentication event. The response is linked to that challenge.

c) This is incorrect. A wired equivalent privacy key will not prevent sniffing, but it will take the attacker longer to break the WEP key if he/she does not already have it). Therefore, it will not be able to prevent recording and replaying an authentication handshake.

d) This is incorrect. Hypertext Transfer Protocol basic authentication is cleartext and has no mechanisms to prevent replay.

5)

a) This is incorrect. IT risk is part of the broader risk landscape and must be integrated into overall risk management activities.

b) This is incorrect. To ensure an objective, holistic approach, IT risk management must be addressed on an enterprisewide basis, making it separate from the IT department.

c) Correct! IT is an enabler of business activities, and to be effective, it must be integrated into business processes.

d) This is incorrect. Communication alone does not necessarily correlate with successful execution of the process.

6)

a) This is incorrect. Penetration testing will not detect an intruder.

b) This is incorrect. Security baselines set minimum security levels but are not related to detecting intruders

c) This is incorrect. Implementing vendor default settings do not detect intruders and is not the best idea.

d) Correct! Honeypots attract hackers away from sensitive systems and files. Because honeypots are closely monitored, the intrusion is more likely to be detected before significant damage is inflicted.

7)

a) This is incorrect. Although the lack of logging for user ad hoc reporting is not necessarily good, it does not represent as serious a security weakness as the failure to install security patches.

b) This is incorrect. Routing network traffic through a single switch is not unusual.

c) Correct! The fact that operating system security patches have not been applied is a serious weakness.

d) This is incorrect. Database security defaulting to the enterprise resource planning system's settings is not as significant.

8)

a) This is incorrect. Implementing on-screen masking of passwords is desirable but will not be effective in reducing the likelihood of a successful social engineering attack.

b) Correct! Social engineering can best be mitigated through periodic security awareness training for users who may be the target of such an attempt.

c) This is incorrect. Increasing the frequency of password changes is desirable but will not be effective in reducing the likelihood of a successful social engineering attack.

d) This is incorrect. Requiring that passwords be kept secret in security policies is a good control but is not as effective as periodic security awareness programs that will alert users of the dangers posed by social engineering.

9)

a) This is incorrect. Monitoring may cause incident durations to become longer as each event is investigated and possibly escalated for further remediation.

b) This is incorrect. Risk tolerance is a determination made by senior management based on the results of a risk analysis and the amount of risk senior management believes the organization can manage effectively. Risk tolerance will not change from implementation of a monitoring process

c) Correct! When a key process is not monitored, that lack of monitoring may lead to a security vulnerability or threat going undiscovered resulting in a security incident. Once consistent monitoring is implemented, identification of vulnerabilities and threats will improve.

d) This is incorrect. Monitoring itself is simply an identification and reporting tool; it has little bearing on how information is escalated to other staff members for investigation and resolution.

10)

a) This is incorrect. The database server would not assist in the correlation and review of the logs.

b) This is incorrect. The domain name server would not assist in the correlation and review of the logs.

c) Correct! To accurately reconstruct the course of events, a time reference is needed, and that is provided by the time server.

d) This is incorrect. The proxy server would not assist in the correlation and review of the logs.