Question: 1

Which of the following is an example of a corrective control?

A. Diverting incoming traffic upon responding to the denial of service (DoS) attack
B. Filtering network traffic before entering an internal network from outside
C. Examining inbound network traffic for viruses
D. Logging inbound network traffic

Answer: A

Explanation:
Diverting incoming traffic corrects the situation and. therefore, is a corrective control. Choice B is a preventive control. Choices C and D are detective controls.

Question: 2

To determine how a security breach occurred on the corporate network, a security manager looks at the logs of various devices. Which of the following BEST facilitates the correlation and review of these logs?

A. Database server
B. Domain name server (DNS)
C. Time server
D. Proxy server

Answer: C

Explanation:
To accurately reconstruct the course of events, a time reference is needed and that is provided by the time server. The other choices would not assist in the correlation and review1 of these logs.

Question: 3

An organization has been experiencing a number of network-based security attacks that all appear to originate internally. The BEST course of action is to:

A. require the use of strong passwords.

B. assign static IP addresses.
C. implement centralized logging software.
D. install an intrusion detection system (IDS).

Answer: D

Explanation:
Installing an intrusion detection system (IDS) will allow the information security manager to better pinpoint the source of the attack so that countermeasures may then be taken. An IDS is not limited to detection of attacks originating externally. Proper placement of agents on the internal network can be effectively used to detect an internally based attack. Requiring the use of strong passwords will not be sufficiently effective against a network-based attack. Assigning IP addresses would not be effective since these can be spoofed. Implementing centralized logging software will not necessarily provide information on the source of the attack.

Question: 4

A serious vulnerability is reported in the firewall software used by an organization. Which of the following should be the immediate action of the information security manager?

A. Ensure that all OS patches are up-to-date
B. Block inbound traffic until a suitable solution is found
C. Obtain guidance from the firewall manufacturer
D. Commission a penetration test

Answer: C

Explanation:
The best source of information is the firewall manufacturer since the manufacturer may have a patch to fix the vulnerability or a workaround solution. Ensuring dial all OS patches are up-to-date is a best practice, in general, but will not necessarily address the reported vulnerability. Blocking inbound traffic may not be practical or effective from a business perspective. Commissioning a penetration test will take too much time and will not necessarily provide a solution for corrective actions.

Question: 5

An organization keeps backup tapes of its servers at a warm site. To ensure that the tapes are properly maintained and usable during a system crash, the MOST appropriate measure the organization should perform is to:

A. use the test equipment in the warm site facility to read the tapes.
B. retrieve the tapes from the warm site and test them.
C. have duplicate equipment available at the warm site.

D. inspect the facility and inventory the tapes on a quarterly basis.

Answer: B

Explanation:
A warm site is not fully equipped with the company's main systems; therefore, the tapes should be tested using the company's production systems. Inspecting the facility and checking the tape inventory does not guarantee that the tapes are usable.

Question: 6

Which of the following processes is critical for deciding prioritization of actions in a business continuity plan?

A. Business impact analysis (BIA)
B. Risk assessment
C. Vulnerability assessment
D. Business process mapping

Answer: A

Explanation:
A business impact analysis (BIA) provides results, such as impact from a security incident and required response times. The BIA is the most critical process for deciding which part of the information system/ business process should be given prioritization in case of a security incident. Risk assessment is a very important process for the creation of a business continuity plan. Risk assessment provides information on the likelihood of occurrence of security incidence and assists in the selection of countermeasures. but not in the prioritization. As in choice B, a vulnerability assessment provides information regarding the security weaknesses of the system, supporting the risk analysis process. Business process mapping facilitates the creation of the plan by providing mapping guidance on actions after the decision on critical business processes has been madetranslating business prioritization to IT prioritization. Business process mapping does not help in making a decision, but in implementing a decision.

Question: 7

In addition to backup data, which of the following is the MOST important to store offsite in the event of a disaster?

A. Copies of critical contracts and service level agreements (SLAs)
B. Copies of the business continuity plan
C. Key software escrow agreements for the purchased systems
D. List of emergency numbers of service providers

Answer: B

Explanation:
Without a copy of the business continuity plan, recovery efforts would be severely hampered or may not be effective. All other choices would not be as immediately critical as the business continuity plan itself. The business continuity plan would contain a list of the emergency numbers of service providers.

Question: 8

An organization has learned of a security breach at another company that utilizes similar technology. The FIRST thing the information security manager should do is:

A. assess the likelihood of incidents from the reported cause.
B. discontinue the use of the vulnerable technology.
C. report to senior management that the organization is not affected.
D. remind staff that no similar security breaches have taken place.

Answer: A

Explanation:
The security manager should first assess the likelihood of a similar incident occurring, based on available information. Discontinuing the use of the vulnerable technology would not necessarily be practical since it would likely be needed to support the business. Reporting to senior management that the organization is not affected due to controls already in place would be premature until the information security manager can first assess the impact of the incident. Until this has been researched, it is not certain that no similar security breaches have taken place.

Question: 9

Which of the following is the MOST important consideration for an organization interacting with the media during a disaster?

A. Communicating specially drafted messages by an authorized person
B. Refusing to comment until recovery
C. Referring the media to the authorities
D. Reporting the losses and recovery strategy to the media

Answer: A

Explanation:

Proper messages need to be sent quickly through a specific identified person so that there are no rumors or statements made that may damage reputation. Choices B, C and D are not recommended until the message to be communicated is made clear and the spokesperson has already spoken to the media.

Question: 10

During the security review of organizational servers it was found that a file server containing confidential human resources (HR) data was accessible to all user IDs. As a FIRST step, the security manager should:

A. copy sample files as evidence.
B. remove access privileges to the folder containing the data.
C. report this situation to the data owner.
D. train the HR team on properly controlling file permissions.

Answer: C

Explanation:
The data owner should be notified prior to any action being taken. Copying sample files as evidence is not advisable since it breaches confidentiality requirements on the file. Removing access privileges to the folder containing the data should be done by the data owner or by the security manager in consultation with the data owner, however, this would be done only after formally reporting the incident. Training the human resources (MR) team on properly controlling file permissions is the method to prevent such incidents in the future, but should take place once the incident reporting and investigation activities are completed.

Question: 11

If an organization considers taking legal action on a security incident, the information security manager should focus PRIMARILY on:

A. obtaining evidence as soon as possible.
B. preserving the integrity of the evidence.
C. disconnecting all IT equipment involved.
D. reconstructing the sequence of events.

Answer: B

Explanation:
The integrity of evidence should be kept, following the appropriate forensic techniques to obtain the evidence and a chain of custody procedure to maintain the evidence (in order to be accepted in a court of law). All other options are pan of the investigative procedure, but they are not as important as preserving the integrity of the evidence.

Question: 12

Which of the following has the highest priority when defining an emergency response plan?

A. Critical data
B. Critical infrastructure
C. Safety of personnel
D. Vital records

Answer: C

Explanation:
The safety of an organization's employees should be the most important consideration given human safety laws. Human safety is considered first in any process or management practice. All of the other choices are secondary.

Question: 13

The PRIMARY purpose of involving third-party teams for carrying out post event reviews of information security incidents is to:

A. enable independent and objective review of the root cause of the incidents.
B. obtain support for enhancing the expertise of the third-party teams.
C. identify lessons learned for further improving the information security management process.
D. obtain better buy-in for the information security program.

Answer: A

Explanation:
It is always desirable to avoid the conflict of interest involved in having the information security team carries out the post event review. Obtaining support for enhancing the expertise of the thirdparty teams is one of the advantages, but is not the primary driver. Identifying lessons learned for further improving the information security management process is the general purpose of carrying out the post event review. Obtaining better buy-in for the information security program is not a valid reason for involving third-party teams.

Question: 14

The MOST important objective of a post incident review is to:

A. capture lessons learned to improve the process.
B. develop a process for continuous improvement.
C. develop a business case for the security program budget.
D. identify new incident management tools.

Answer: A

Explanation:
The main purpose of a post incident review is to identify areas of improvement in the process. Developing a process for continuous improvement is not true in every case. Developing a business case for the security program budget and identifying new incident management tools may come from the analysis of the incident, but are not the key objectives.

Question: 15

Which of the following is the BEST mechanism to determine the effectiveness of the incident response process?

A. Incident response metrics
B. Periodic auditing of the incident response process
C. Action recording and review
D. Post incident review

Answer: D

Explanation:
Post event reviews are designed to identify gaps and shortcomings in the actual incident response process so that these gaps may be improved over time. The other choices will not provide the same level of feedback in improving the process.

Question: 16

The FIRST step in an incident response plan is to:

A. notify- the appropriate individuals.
B. contain the effects of the incident to limit damage.
C. develop response strategies for systematic attacks.
D. validate the incident.

Answer: D

Explanation:
Appropriate people need to be notified; however, one must first validate the incident. Containing the effects of the incident would be completed after validating the incident. Developing response strategies for systematic attacks should have already been developed prior to the occurrence of an incident.

Question: 17

An organization has verified that its customer information was recently exposed. Which of the following is the FIRST step a security manager should take in this situation?

A. Inform senior management.
B. Determine the extent of the compromise.
C. Report the incident to the authorities.
D. Communicate with the affected customers.

Answer: B

Explanation:
Before reporting to senior management, affected customers or the authorities, the extent of the exposure needs to be assessed.

Question: 18

A possible breach of an organization's IT system is reported by the project manager. What is the FIRST thing the incident response manager should do?

A. Run a port scan on the system
B. Disable the logon ID
C. Investigate the system logs
D. Validate the incident

Answer: D

Explanation:
When investigating a possible incident, it should first be validated. Running a port scan on the system, disabling the logon IDs and investigating the system logs may be required based on preliminary forensic investigation, but doing so as a first step may destroy the evidence.

Question: 19

The PRIMARY consideration when defining recovery time objectives (RTOs) for information assets is:

A. regulatory' requirements.
B. business requirements.
C. financial value.
D. IT resource availability.

Answer: B

Explanation:
The criticality to business should always drive the decision. Regulatory requirements could be more flexible than business needs. The financial value of an asset could not correspond to its business value. While a consideration, IT resource availability is not a primary factor.

Question: 20

What task should be performed once a security incident has been verified?

A. Identify the incident.
B. Contain the incident.
C. Determine the root cause of the incident.
D. Perform a vulnerability assessment.

Answer: B

Explanation:
Identifying the incident means verifying whether an incident has occurred and finding out more details about the incident. Once an incident has been confirmed (identified), the incident management team should limit further exposure. Determining the root cause takes place after the incident has been contained. Performing a vulnerability assessment takes place after the root cause of an incident has been determined, in order to find new vulnerabilities.