QUESTION 1549
Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS) attack on a publicly facing .....

A. Prevention of authorized access
B. Execution of unauthorized command
C. Defacement of website content
D. Unauthorized access to resources

Answer: C

QUESTION 1550
Which of the following is MOST important to present to stakeholders to help obtain support for implementing a new information?

A. A statement of generally accepted good practices
B. An overview of competitors' information security strategies
C. The potential impact of current threats
D. An assessment of current technological exposures

Answer: C

QUESTION 1551
Which of the following is the BEST indicator to demonstrate whether information security investments are optimally supporting organizational objecti.....

A. Percentage of security-related initiatives completed within budget
B. Percentage of current security resource utilization
C. Ratio of security costs to the value of assets
D. Ratio of security incidents from known risk versus unidentified risk

Answer: C

QUESTION 1552
An organization wants to implement an emerging technology to support operations.
What should the information security manager do FIRST when ..... recommendation?

A. Review key risk indicators (KRIs).
B. Review existing security policies.

C. Develop a business case.
D. Assess the potential security impact.

Answer: D

QUESTION 1553
Which of the following will BEST enable the identification of appropriate controls to prevent repeated occurrences of similar types of information.....

A. Review existing preventive controls for security weaknesses.
B. Perform a root cause analysis of the security incidents.
C. Review lessons learned with key stakeholders.
D. Perform a business impact analysis (BIA) of the security incidents.

Answer: B

QUESTION 1554
Which of the following should be done FIRST when considering a new security initiative?

A. Conduct a benchmarking exercise.
B. Conduct a feasibility study.
C. Perform a cost-benefit analysis.
D. Develop a business case.

Answer: C

QUESTION 1555
Which of the following is the BEST way to monitor for advanced persistent threats (APT) in an organization?

A. Search for threat signatures in the environment.
B. Network with peers in the industry to share information
C. Search for anomalies in the environment.
D. Browse the Internet to learn of potential events.

Answer: B

QUESTION 1556
Which of the following is the MOST effective way to incorporate risk management practices into a new business process?

A. Conduct quality assurance reviews.
B. Review threat assessments.
C. Update company policies.
D. Enforce change management.

Answer: D

QUESTION 1557
An incident response team has determined there is a need o isolate a system that is communicating with a known malicious host on the Internet, following stakeholders should be contacted FIRST?

A. The business owner
B. Key customers
C. System administrator

D. Executive management

Answer: A

QUESTION 1558
Which of the following BEST indicates the value a purchased information security solution brings to an organization?

A. Cost savings he solution brings to the information security department
B. Degree to which the solution matures the information security program
C. Costs and benefits of the solution calculated over time
D. Alignment to security threats and risks

Answer: D

QUESTION 1559
Which of the following is a PRIMARY responsibility of a data owner?

A. Conducting data privacy impact assessments
B. Approving access to information
C. Performing user access audits
D. Processing entitlement changes

Answer: B

QUESTION 1560
When creating a bring your own device (BYOD) program, it is MOST important to:

A. ensure the organization's ownership of data and management of the device.
B. establish metrics to evaluate the effectiveness of the program.
C. develop remote wipe capabilities and procedures.
D. balance the costs between private versus business usage and define the method to track usage.

Answer: A

QUESTION 1561
Which of the following is the GREATEST benefit of information asset classification?

A. Supporting segregation of duties
B. Defining resource ownership
C. Helping to determine the recovery point objective (RPO)
D. Providing a basis for implementing a need-to-know policy

Answer: B

QUESTION 1562
Which of the following BEST enables new third-party suppliers to support an organization's information security objectives?

A. Mandating a right-to-audit clause in supplier contracts
B. Requiring approval of new suppliers by the information security manager
C. Conducting security awareness training courses for third parties
D. Addressing security risk in the supplier sourcing process

Answer: D

QUESTION 1563
The PRIMARY advantage of challenge-response authentication over password authentication is that:

A. it is less expensive to implement.
B. there is no requirement for end-to-end encryption.
C. user accounts are less likely to be compromised.
D. credentials sent across the network are encrypted.

Answer: C

QUESTION 1564
When developing an information security strategy, the MOST important requirement is that:

A. a schedule is developed to achieve objectives.
B. critical success factors (CSFs) are developed.
C. standards capture the intent of management.
D. the desired outcome is known.

Answer: D

QUESTION 1565
Which of the following is the MOST important security consideration when planning to use a cloud service provider in a different country?

A. Ability to enforce contractual obligations
B. Ability to meet service level agreements (SLAs)
C. Ability to logically separate client data
D. Ability to meet business resiliency requirements

Answer: C

QUESTION 1566
Which of the following should be define FIRST when creating an organization's information security strategy?

A. Budget
B. Policies and processes
C. Objectives
D. Organizational structures

Answer: C

QUESTION 1567
Senior management learns of several web application security incidents and wants to know the exposure isk to the organization. What is the information security manager's BEST course of action?

A. Perform a vulnerability assessment.
B. Review audit logs from IT systems.
C. Activate the incident response plan
D. Assess IT system configurations

Answer: A

QUESTION 1568

Which of the following sites would be MOST appropriate in the case of a very short recovery time objective (RTO)?

A. Redundant
B. Shared
C. Warm
D. Mobile

Answer: A

QUESTION 1569
Which of the following is the BEST indication that a recently adopted information security framework is a good fit for an organization?

A. The framework includes industry-recognized information security best practices.
B. The number of security incidents has significantly declined
C. The business has obtained framework certification.
D. Objectives in the framework correlate directly to business practices

Answer: D

QUESTION 1570
Which of the following is the BEST indication that a recently adopted information security framework is a good fit for an organization?

A. The framework includes industry-recognized information security best practices.
B. The number of security incidents has significantly declined
C. The business has obtained framework certification.
D. Objectives in the framework correlate directly to business practices

Answer: D