CISMP Practice Questions Three

1. Which of the following would BEST reduce the risk of excessive personal use of email affecting a company's network?
    a. email replication from central to local mail servers
    b. company policy on acceptable use of email
    c. use of a firewall
    d. use of digital signatures

2. What is the name of the attack whereby multiple computers threaten a single host to prevent service?
    a. Distributed denial of service
    b. Denial of service
    c. Masquerading
    d. Brute Force

3. Local Area Network (LAN) is:
    a. a communications network across an organisation's multiple locations
    b. a community of security people in a local geographic area
    c. the network of telephone lines in a town
    d. the private communications network of an organization, usually on one site

4. Who is responsible for deciding how often a system SHOULD be backed up?
    a. The IT manager
    b. The hardware owner
    c. The data owner
    d. The managing director

5. Information systems are key business assets. An information security policy and the supporting operating procedures are needed to ensure that:
    a. a security baseline is defined
    b. security controls are implemented
    c. a security framework is provided
    d. security protection meets the business needs

6. The factor MOST LIKELY to gain senior management support for a security proposal is:
    a. the quality of the security controls to be implemented
    b. how cheaply the proposal can be implemented
    c. the business benefits that will follow implementation
    d. the improvement in security that will follow implementation

7. Heads of department SHOULD take an active part in a risk assessment because:
   a. senior management will only accept the report if heads of department are involved
   b. they can escalate their departments' priorities
   c. it is only the manager that can speak for the department
   d. they can take an organisational view of the risks

8. For a business continuity plan to cover adequately the business needs of the organization, the MOST important requirement is that:
   a. it should be fully documented
   b. the business impacts should be understood
   c. there should be a contingency manager
   d. all data should be held off site

9. Employees SHOULD be required to sign a security undertaking when:
   a. they handle peoples personal records
   b. they join an organization
   c. they work in a sensitive area
   d. they get promoted to a management or supervisory role

10. Senior management has asked you to help set up an ecommerce website. Your message with respect to security is:
    a. security is an additional cost that will have to be charged to sales
    b. security will give customers the confidence to do business
    c. customers may be deterred by the need to conform to security requirements
    d. security can reduce risks to zero

11. Why SHOULD active content in Internet messages be treated with caution even when apparently legitimately signed?
    a. active content can malfunction
    b. even signed code can be malicious
    c. it requires a frames compliant browser
    d. it must be run in a restricted environment

12. Which of the following security controls COULD be described as detective controls?
    a. Information classification
    b. Audit trails
    c. Access controls
    d. Change controls

13. In deciding whether to buy or build a security product:
    a. the information systems manager should decide which is to be preferred
    b. it's always cheaper, better and more reliable to buy
    c. creating your own is always more secure, and therefore preferable
    d. the choice should depend upon the requirements, availability of products and cost of each option

14. How can data classification help ensure that information is held safely in the cloud?
    a. it can reduce the organisation’s responsibility to protect the data as any confidential information is now the responsibility of the service provider
    b. it can reduce the service costs by removing all the security controls to less confidential information
    c. it can improve the protection of service level agreements negotiated with the supplier
    d. it can identify confidential information where additional protection controls such as encryption should be implemented

15. A macro virus is one that infects:
    a. Memory
    b. All executable files
    c. Boot sectors
    d. A data file

16. which of the following personnel aspects of business continuity is the MOST important?
    a. ensuring that people are trained in the use of the plans
    b. ensuring that individuals are key to the process
    c. arranging the business process so that key people are always on site
    d. transport to the disaster store

17. Every third party connection SHOULD have:
    a. a legal advisor
    b. an information security manager
    c. an IT specialist
    d. a connection owner

18. Access by third parties must be controlled so that they CANNOT:
    1. introduce viruses or other malicious code
    2. put too much traffic on the network
    3. access critical business systems
    4. deny doing damage to the network
        a. 2 and 4 only
        b. 1 and 3 only
        c. 1, 2 and 3 only
        d. 3 and 4 only

19. Which of the following would cause a business contingency plan to be updated?
    a. change of CEO
    b. changes to business processes
    c. change of car parking allocations
    d. new users being added to an access list

20. Why is it important to have a minimum password length?
    a. to help the users remember them
    b. to reduce the risk of a successful brute force attack
    c. to ensure that the system has enough permutations to avoid duplication
    d. any default design has a standard length