TEST BANK

THE MANAGEMENT OF NETWORK SECURITY

TECHNOLOGY, DESIGN, AND MANAGEMENT CONTROL

HOUSTON H. CARR
CHARLES A. SNYDER
BLISS N. BAILEY

Management of Network Security **(Carr/Snyder/Bailey)**
Chapter 2 Properties of a Good Network Environment

2.1 Multiple Choice Questions

1) A primary vulnerability of Information Technology (IT) is
A) Malware
B) Flood
C) Fire
D) Deterioration
Answer: A
Diff: 1 Page Ref: 35

2) The physically wired components of a network must be kept safe by
A) Placing them in enclosures
B) Attaching physical alarms
C) Placing them in highly visible locations
D) Disallowing remote access
Answer: A
Diff: 1 Page Ref: 35

3) Network equipment includes which of the following components
A) Servers
B) Hubs
C) Routers
D) All of the above
Answer: D
Diff: 1 Page Ref: 35

4) Network equipment requires
A) Electric power
B) Temperature-controlled environment
C) Safety from physical access and abuse
D) All of the above
Answer: D
Diff: 1 Page Ref: 35

5) Reliability encompasses the traits of
A) Constancy, dependability, stability, and durability
B) Flexibility, monitorability, and performance
C) Resistance, tolerability, rigidity, and strength
D) None of the above
Answer: A
Diff: 1 Page Ref: 35

6) Which of these network devices require electric power and a temperature-controlled environment?
A) Servers
B) Hubs
C) Wireless Access Points
D) All of the above
Answer: D
Diff: 1 Page Ref: 35

7) The paradox for Network Administrators is
A) That a job well-done, i.e. keeping the network reliable and available while remaining invisible and non-intrusive, makes the network administrators appear unneeded
B) Allowing just enough reliability issues to occur to be needed but not enough to appear incompetent
C) Requiring building maintenance to accept responsibility for delivering consistent power while maintaining responsibility for network dependability themselves
D) All of the above
Answer: A
Diff: 2 Page Ref: 36

8) If a network detects a significant number of errors, the response to those errors reduces _____
A) Performance
B) Security
C) Resiliency
D) Redundancy
Answer: A
Diff: 2 Page Ref: 36

9) Resiliency is the ability to
A) Recover from some shock or disturbance
B) Be non-intrusive and invisible
C) Be safe from intrusion
D) Measure the performance against a standard
Answer: A
Diff: 1 Page Ref: 36

10) Reliability is the ability to
A) Ensure that something is error-free or that all errors within reason have been detected; trust in a security device in that it provides the protection expected
B) Recover from some shock or disturbance
C) Determine how something acts as judged against a standard
D) Provide a resource when and where it is required
Answer: A
Diff: 1 Page Ref: 35

11) Performance is
A) Ensuring that something is error-free or that all errors within reason have been detected; trust in a security device in that it provides the protection expected
B) How something acts as judged against a standard
C) Providing a resource when and where it is required
D) The process of protecting data and resources from unauthorized access, use, disclosure, destruction, modification, or disruption
Answer: B
Diff: 1 Page Ref: 36

12) Availability is
A) Ensuring that something is error-free or that all errors within reason have been detected; trust in a security device in that it provides the protection expected
B) How something acts as judged against a standard
C) Providing a resource when and where it is required
D) The process of protecting data and resources from unauthorized access, use, disclosure, destruction, modification, or disruption.
Answer: C
Diff: 1 Page Ref: 36

13) Security is
A) Ensuring that something is error-free or that all errors within reason have been detected; trust in a security device in that it provides the protection expected
B) How something acts as judged against a standard
C) Providing a resource when and where it is required
D) The process of protecting data and resources from unauthorized access, use, disclosure, destruction, modification, or disruption
Answer: D
Diff: 1 Page Ref: 36

14) A network is measured by which of the following characteristics
A) Reliability, availability, performance, and security
B) Resiliency, error rate, response time
C) Reliability, error rate, response time, and security
D) None of the above
Answer: A
Diff: 3 Page Ref: 37

15) Continuity is
A) The ability of a system or business to carry on in face of a disruption or disaster
B) The process of protecting data and resources from unauthorized access, use, disclosure, destruction, modification, or disruption
C) Ensuring that something is error-free or that all errors within reason have been detected; trust in a security device in that it provides the protection expected
D) How something acts as judged against a standard
Answer: A
Diff: 2 Page Ref: 37

16) Electrical power should be _____ so that the voltage levels are maintained
A) Regulated
B) A brownout
C) Spiked
D) Tripped
Answer: A
Diff: 1 Page Ref: 37

17) _____ are examples of overvoltage
A) Power spikes
B) Brownouts
C) Waveforms
D) None of the above
Answer: A
Diff: 1 Page Ref: 37

18) Electrical power has a waveform that should
A) Match the sine wave format
B) Match the longitudinal wave format
C) Vary a great deal without affecting the power quality
D) Should vary between a brownout and a spike
Answer: A
Diff: 2 Page Ref: 37

19) Voltage fluctuations in electrical power are
A) Referred to as noise on the power lines
B) Common occurrences in many areas
C) Not tolerated well by many pieces of network equipment
D) All of the above
Answer: D
Diff: 2 Page Ref: 38

20) A UPS is a(n)
A) Uninterruptible Power Supply
B) Unreliable Power Source
C) Undefinable Power Sine
D) Unsatisfactory Power Supply
Answer: A
Diff: 1 Page Ref: 38

21) An MG set is
A) A Motor-Generator with an electric motor coupled directly to an electric generator; the objective is to create cleaner power or a different voltage or phase
B) Monitoring Grayware that tracks the quality of the electrical power
C) A Motoring-Gramm which is a unit of measure for generator produced power
D) None of the above
Answer: A
Diff: 1 Page Ref: 38

22) A surge protector is a(n)
A) Device that short circuits high-voltage spikes, thus protecting electrical equipment
B) Motor-Generator containing an electric motor coupled directly to an electric generator; the objective is to create cleaner power or a different voltage or phase
C) Uninterruptible power supply for workstations
D) The ability of a system or business to carry on in face of a disruption or disaster
Answer: A
Diff: 1 Page Ref: 39

23) A solid state device that takes in distorted electronic waveforms and creates better waveforms and voltage values is called a
A) Line conditioner
B) Surge protector
C) Motor generator
D) Uninterruptible power supply
Answer: A
Diff: 1 Page Ref: 39

24) UPS devices are different than surge protectors and line conditioners in that they can
A) Store power
B) Recover from high-voltage spikes
C) Create better waveforms and voltage values
D) Carry on in the face of all forms of disaster
Answer: A
Diff: 2 Page Ref: 39

25) Public power is also called
A) Dirty power
B) Clean power
C) Stable power
D) Commercial power
Answer: A
Diff: 2 Page Ref: 40

26) A backup generator is a
A) Fuel based motor that drives an electrical generator and is used during extended power failures
B) Device that stores electric power in batteries for later conversion to AC to run devices during a short-term power outage
C) Solid state device that takes in distorted electronic waveforms and creates better waveforms and voltage values
D) Device that short circuits high-voltage spikes, thus protecting electrical equipment
Answer: A
Diff: 1 Page Ref: 40

27) The term PoE stands for the ability to
A) Deliver power-over-Ethernet
B) Provide-optimum-energy for the information technology (IT) infrastructure
C) Deliver power-on-encounter for technology devices encountered by the network
D) None of the above
Answer: A
Diff: 1 Page Ref: 41

28) The benefits of PoE include the
A) Ability to shutdown a device
B) Ability to reboot a device
C) Ability to restart a device
D) All of the above
Answer: D
Diff: 2 Page Ref: 42

29) Using a battery to power mobile devices _____ the problem of power conditioning, voltage spikes, and brownouts but _____ the requirement for backup batteries and recharging capabilities
A) Solves, introduces
B) Introduces, solves
C) Worsens, also adds
D) Introduces, worsens
Answer: A
Diff: 2 Page Ref: 42

30) Wired networks that are confined to a single building, have all of their wiring within that single building (generally within the walls or ceilings) are considered
A) Internal circuits
B) External circuits
C) Building circuits
D) Wi-Fi circuits
Answer: A
Diff: 1 Page Ref: 43

31) Circuits that go between buildings or from one site to another are
A) External circuits
B) At greater risk than circuits that are contained within a single building
C) Generally buried in conduits and are frequently damaged during new construction
D) All of the above
Answer: D
Diff: 1 Page Ref: 43

32) In situations where the installation or safety of wired circuits is not feasible
A) Terrestrial microwave can be used
B) Optical point-to-point can be used
C) Satellite communications can be used
D) All of the above
Answer: D
Diff: 2 Page Ref: 45

33) Damage to underground wired circuits can usually be avoided by
A) Up-to-date drawings and alert personnel
B) Marking the circuit location by placing a yellow flag above ground
C) Burying the circuit within plastic conduit
D) Burying the circuit beneath plastic cones
Answer: A
Diff: 2 Page Ref: 46

34) The Critical Physical Infrastructure for the network includes all of the following elements <u>except</u>
A) Cabling
B) Fire and security
C) Cooling
D) Burying depth
Answer: D
Diff: 2 Page Ref: 46

35) Connecting an electronic device or network to Earth is called
A) Grounding
B) Gramming
C) Gaming
D) Burying
Answer: A
Diff: 1 Page Ref: 47

36) Which of the following should be used to provide safety for electronics within structures from events such as a lightning strike?
A) Down conductor
B) Lightning rods
C) Air terminals
D) All of the above
Answer: A
Diff: 2 Page Ref: 49

37) Solar flares are
A) Electromagnetic pulses (radiation) from the sun that may interfere with network equipment
B) Another name for lightning strikes
C) Devices placed in a location to alert others of an electrical problem on the ground
D) Conductors that direct excess voltage into the earth
Answer: A
Diff: 2 Page Ref: 51

38) Protecting a network involves control of which of the following?
A) Water and fire damage
B) Physical access
C) Electrical power
D) All of the above
Answer: D
Diff: 2 Page Ref: 52

39) Accidental damage can occur when
A) Computer cables are run across a floor rather than under the floor
B) Moisture collects or floods electrical or network cables
C) Growing companies resort to extension cords or plugs to gain extra electrical outlets
D) All of the above
Answer: D
Diff: 2 Page Ref: 53

40) Which type of security should be the easiest to provide?
A) Physical
B) Data
C) Virtual
D) None of the above
Answer: A
Diff: 3 Page Ref: 56

41) Management policies must control all personnel,whether with _____ or with _____
A) Good clearance, escort services
B) Insurance, fire protection systems
C) Constant monitoring, access control
D) None of the above
Answer: A
Diff: 3 Page Ref: 56

42) _____ are any actions an individual takes that has an undesirable effect on the organization, environment, system, or equipment
A) Acts of humans
B) Acts of God
C) Acts of personnel
D) Acts of employees
Answer: A
Diff: 2 Page Ref: 57

43) Mission-critical capabilities are
A) Required 24 hours a day, 7 days a week
B) Protected, at a minimum, by 400 Watt power supplies
C) Always protected by UPS (Uninterruptible Power Supply)
D) All of the above
Answer: D
Diff: 2 Page Ref: 36

44) The lines up to the premises of the organization generally are the responsibility of the _____; the lines within the premises are the responsibility of the _____
A) Electric utility, organization
B) Management policies, personnel
C) Organization, electric utility
D) Personnel, management policies
Answer: A
Diff: 2 Page Ref: 45

45) All of the following are vulnerabilities of the OSI physical layer except
A) Physical theft of data and hardware

B) Unauthorized changes to the functional environment

C) PIN and password secured locks

D) Keystroke and other input logging

Answer: C
Diff: 3 Page Ref: 56

46) All of the following are controls for the physical layer except
A) Locked & guarded perimeters
B) Electromagnetic shielding
C) Video & audio surveillance
D) Undetectable interception of data
Answer: D
Diff: 3 Page Ref: 56

47) A benefit of PoE-powered voice over IP phone systems that utilize backup power for the switch gear and power injectors in the wiring closet is
A) Increased reliability
B) Increased generator power
C) Decreased risk related to dirty power
D) Decreased continuity
Answer: A
Diff: 3 Page Ref: 41

48) The set of rules that provide requirements for safe installation of electric conductors, equipment, optical fiber, and raceways is called the
A) National Fire Codes
B) National Electrical Installation Code
C) International Construction Code
D) National Construction Code
Answer: A
Diff: 3 Page Ref: 48

49) Although an installation may be safe from a building code viewpoint, all portions may not be at ground potential, making them _____ noise and data corruption
A) Susceptible to
B) Impenetrable to
C) Impervious to
D) Not influenced by
Answer: A
Diff: 2 Page Ref: 48

50) After an unusual event occurs, problems with grounding are frequently tracked down using volt meters. This process is called
A) Detection & correction
B) Prevention & resistance
C) Preparedness
D) Perimeter prevention
Answer: A
Diff: 3 Page Ref: 49

2.2 True/False Questions

1) Events such as circuit switching and lightning strikes can create power surges but grounding can provide a level of protection.
Answer: TRUE
Diff: 1 Page Ref: 47

2) Building codes often specify fire and water protection and this is sufficient for networks and their data.
Answer: FALSE
Diff: 1 Page Ref: 58

3) Flooding is one of the primary vulnerabilities of network equipment.
Answer: TRUE
Diff: 1 Page Ref: 35

4) The physical components of a network must be kept safe by placing them in very visible locations so that network administrators are able to physically monitor them.
Answer: FALSE
Diff: 1 Page Ref: 35

5) Servers, routers, hubs, and switches are all considered network equipment.
Answer: TRUE
Diff: 1 Page Ref: 35

6) Reliability encompasses the traits of flexibility and monitorability.
Answer: FALSE
Diff: 1 Page Ref: 35

7) The only network equipment that must be in a temperature controlled environment are the Servers.
Answer: FALSE
Diff: 1 Page Ref: 35

8) A paradox for network administrators is to balance network reliability with network problems in order to ensure the organization needs their services but not enough to affect the business significantly.
Answer: FALSE
Diff: 1 Page Ref: 36

9) If a network experiences a significant number of detected errors, responses to those errors will result in reduced bandwidth and, therefore, reduced performance.
Answer: TRUE
Diff: 1 Page Ref: 36

10) Resiliency is the ability to recover from some shock or disturbance.
Answer: TRUE
Diff: 1 Page Ref: 36

11) Reliability is the ability to provide a resource when and where it is required.
Answer: FALSE
Diff: 1 Page Ref: 35

12) Performance is how something acts as judged against a standard.
Answer: TRUE
Diff: 1 Page Ref: 36

13) Availability is the process of protecting data and resources from unauthorized access and use.
Answer: FALSE
Diff: 1 Page Ref: 36

14) Security is ensuring that something is error free or that all errors within reason have been detected.
Answer: FALSE
Diff: 1 Page Ref: 36

15) A network is measured by reliability, availability, performance, and security.
Answer: TRUE
Diff: 1 Page Ref: 37

16) Continuity is the ability of a system or business to carry on in face of a disruption or disaster.
Answer: TRUE
Diff: 1 Page Ref: 37

17) Electrical power should be tripped so that the voltage levels are maintained.
Answer: FALSE
Diff: 1 Page Ref: 37

18) Waveforms are examples of overvoltage.
Answer: FALSE
Diff: 1 Page Ref: 37

19) Power quality is unaffected by variations in its waveform.
Answer: FALSE
Diff: 1 Page Ref: 37

20) Voltage fluctuations in electrical power are not tolerated well by many pieces of network equipment.
Answer: TRUE
Diff: 1 Page Ref: 38

21) The acronym UPS stands for Universal Power Standard.
Answer: FALSE
Diff: 1 Page Ref: 38

22) A surge protector is a device that short circuits high voltage spikes, thus protecting electrical equipment.
Answer: TRUE
Diff: 1 Page Ref: 39

23) A Motor Generator is a solid state device that takes in distorted electronic waveforms and creates better waveforms and better voltage values.
Answer: FALSE
Diff: 1 Page Ref: 39

24) UPS devices are different from line conditioners and surge protectors in that they can store power.
Answer: TRUE
Diff: 1 Page Ref: 39

25) Public power is sometimes referred to as clean power.
Answer: FALSE
Diff: 1 Page Ref: 40

26) A backup generator contains a fuel-based motor that drives an electrical generator and can be used during extended power failures.
Answer: TRUE
Diff: 1 Page Ref: 40

27) The term PoE stands for the ability to provide optimum energy for a network infrastructure.
Answer: FALSE
Diff: 1 Page Ref: 41

28) PoE allows network administrators to turn remote network devices on and off.
Answer: TRUE
Diff: 1 Page Ref: 42

29) Battery powered mobile devices allow users to avoid the problems with voltage spikes and brownouts but introduces the problems of backup batteries and recharging.
Answer: TRUE
Diff: 1 Page Ref: 42

30) Internal circuits are contained within a single device while external circuits connect multiple devices.
Answer: FALSE
Diff: 1 Page Ref: 43

31) In situations where wired circuits are not feasible, manual processes must take over for the lack of electronic communication.
Answer: FALSE
Diff: 1 Page Ref: 45

32) Up-to-date drawings and alert personnel can frequently avoid damage to underground wired circuits.
Answer: TRUE
Diff: 1 Page Ref: 46

33) Connecting an electronic device or network to the Earth is called bounding.
Answer: FALSE
Diff: 1 Page Ref: 47

34) Solar flares are electromagnetic pulses (radiation) from the sun that may interfere with network equipment.
Answer: TRUE
Diff: 1 Page Ref: 51

35) Data security is the easiest security to provide.
Answer: FALSE
Diff: 1 Page Ref: 56

36) Management policies must control all personnel, whether through good clearance or with escort services.
Answer: TRUE
Diff: 1 Page Ref: 56

37) Mission-critical capabilities are required 24 hours a day, 5 days a week.
Answer: FALSE
Diff: 1 Page Ref: 36

38) Vulnerabilities of the OSI physical layer include physical theft of data and password secured locks.
Answer: FALSE
Diff: 1 Page Ref: 56

39) Controls for the physical layer include locked & guarded perimeters as well as electromagnetic shielding.
Answer: TRUE
Diff: 1 Page Ref: 56

40) The National Fire Code is a set of rules that provide requirements for safe installation of electric conductors, equipment, optical fiber, and raceways.
Answer: TRUE
Diff: 1 Page Ref: 48

2.3 Essay Questions

1) Describe the various methods of keeping physical components of a network safe.
Answer: Network components should be placed in enclosures with temperature-controlled environments powered by 'clean' or conditioned, reliable power. Additionally, the components and the room where they are placed should have backup power supplies. The location should also provide fire suppression systems and should protect the equipment from floods, condensation, or any type of excess moisture. Finally, care should be taken that accidental damage does not occur by placed power cords and network cables out of the site.
Diff: 3 Page Ref: 35, 52, 53

2) Name nine vulnerabilities of the OSI Physical Layer.
Answer: Loss of Power, Loss of environmental control, Physical theft of data and hardware, Physical damage or destruction of data and hardware, Undetectable interception of data, Unauthorized changes to the functional environment, Removable media (adding/removing resources), Disconnection of physical data links, Keystroke and other input logging
Diff: 3 Page Ref: 55

3) According to the book, reliability encompasses several different traits. Name and describe these traits.
Answer: Constancy - unchanging in properties such as performance, availability
Dependability - trustworthy, providing accurate processing and information
Stability - providing stable resources and processing
Durability - resistant to deterioration
Diff: 3 Page Ref: 35

4) Name seven controls for the physical layer
Answer: Locked and guarded perimeters and enclosures, Electromagnetic shielding, Electronic lock mechanisms for logging and detailed authorization, Video & audio surveillance, PIN and password secured locks, Biometric authentication systems, Data storage cryptography
Diff: 3 Page Ref: 56

5) Describe grounding, it's purpose, and what problems it prevents.
Answer: Grounding means creating a common return path or connection to the ground (or Earth) in electric circuits. The purpose of grounding is to minimize the effect of variations in voltage by creating a low resistance to ground for electric surges and transient voltages. Grounding helps avoid damage to electrical devices. or corrupt data communications signals. These variations in voltage can be caused by lightning strikes or motors activating or dropping of circuit.
Diff: 3 Page Ref: 47

6) Describe the elements of the Network-Critical Physical Infrastructure.
Answer: Cabling refers to the physical cables connecting a wired network, Fire and Security refers to the ability to contain electrical fires and to control access to the physical network devices, Power refers to the ability to provide clean, consistent power even in the event of a power failure, Cooling refers to the ability to maintain a cool environment in order to prevent electrical equipment from overheating, Racks and Physical Structure refers to the physical devices that support the infrastructure.
Diff: 3 Page Ref: 46

7) Provide an example of risk identification and avoidance with respect to external electric circuits.
Answer: External electric circuits go between buildings. These circuits are at greater risk during natural disasters such as fires, tornadoes, earthquakes, and hurricanes. However, the most common risk for these circuits are backhoes during new construction. The best way to avoid damage due to backhoe is to keep up-to-date drawings and employee alert personnel.
Diff: 3 Page Ref: 43 & 45

8) Discuss the paradox of network administrators.
Answer: Network administrators must be both invisible and non-intrusive while keeping the network reliable and available, all with no perceivable down time. One of the paradoxes of network administration, as well as security administration, is that if the job is done successfully, the people doing it are not visible to the users and, therefore, seemingly not required. Obviously, this is not correct.
Diff: 3 Page Ref: 36

9) A network needs to be reliable, accessible, perform well, and be secure. Define these attributes and explain their importance to any organization.
Answer: Reliability encompasses the traits of constancy, dependability, stability, and durability. If a network is not reliable it could interrupt mission-critical processing or communications.
Accessible - a network needs to be easy to reach for its users. If the network is difficult to access, it could reduce productivity.
Performance is how something acts as judged against a standard. A network should perform as intended by its design.
Secure - Security is about protecting data and resources from unauthorized access and use. The network must be safe from intrusion and attacks so that users can be assured data will not be disclosed, destroyed, modified, or processing and communication disrupted.
Diff: 3 Page Ref: 36

10) A user with DSL Internet access at home, sets up his home computer, printer, and DSL modem to receive power through a combination UPS (Uninterruptible Power Supply) with surge protection. A lightning storm travels through his town and his equipment is damaged. Describe why and how the damage probably occurred.
Answer: The user likely failed to connect the DSL phone line through any type of phone filter. As a result, the electrical surge was blocked on the electrical outlets, but still surged via the phone line. A phone surge can obliterate a sensitive DSL modem, router, and a NIC on a PC.
Diff: 3 Page Ref: 51