

Chp 3 NS

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 2/8/2022 7:41:55 pm • Time spent: 02:55

Score: 100%

Passing Score: 80%



Question 1: ✓ Correct

You maintain a network for an industrial manufacturing company. You are concerned about the dust in the area getting into server components and affecting network availability.

Which of the following should you implement?

- ➡ Positive pressure system
 Backup generator
 Negative pressure system
 UPS
 Line conditioner

EXPLANATION

Use positive pressure systems. Positive pressure systems protect the air quality in the facility by causing air to be forced out through doors, windows, and other openings.

Negative pressure systems draw air in, potentially bringing in airborne particles such as dust, smoke from a fire, or contamination from a chemical leak. Positive pressure systems are more energy-effective.

Line conditioners (also known as power conditioners) are used to improve the quality of power by performing one or more of the following:

- Removing noise caused by electromagnetic interference (EMI) and radio frequency interference (RFI)
- Providing small amounts of additional power to protect against power dips or sags
- Protecting against spikes and surges

Most UPS systems include line conditioners.

Question 2: ✓ Correct

Which of the following is the most important thing to do to prevent console access to the router?

- ➡ Keep the router in a locked room.
- Set the console and enable secret passwords.
- Disconnect the console cable when not in use.
- Implement an access list to prevent console connections.

EXPLANATION

To control access to the router console, you must keep the router in a locked room. A console connection can only be established with a direct physical connection to the router. If the router is in a locked room, only those with access are able to make a console connection. In addition, even if you had set console passwords, users with physical access to the router could perform router password recovery and gain access.

Question 3: ✓ Correct

Which of the following fire extinguisher types is best used for the electrical fires that might result when working with computer components?

- Class A
- Class B
- ➡ Class C
- Class D

EXPLANATION

For electrical fires, choose a Class C fire extinguisher. Class C fire extinguishers use a gas (CO₂ or Halon) to remove oxygen from a fire. When purchasing a fire extinguisher, purchase the type of extinguisher that is best suited for the type of fires that are likely to occur in that area.

A Class A fire extinguisher uses water or soda acid and is best for fires using typical combustible materials (wood, paper, cloth, plastics).

A Class B fire extinguisher uses either CO₂ or FM200, but it is best suited for petroleum, oil, solvent, or alcohol fires.

A Class D fire extinguisher uses a dry powder and is best for sodium and potassium fires.

Question 4: ✓ Correct

Which kind of access control technology allows more than just the identity of an individual to be transmitted wirelessly to either allow or deny access?

- Keypad locks
- Smart card
- Proximity card
- Biometric locks

EXPLANATION

Unlike proximity cards that only transmit the owner's identity, smart cards can contain and transmit many more pieces of information.

Biometric locks and keypad locks don't transmit data wirelessly. In contrast, they require physical interaction.

Question 5: ✓ Correct

Which deviation in power is the longest in duration?

- Surge
- Transient
- Blackout
- Sag

EXPLANATION

A blackout is generally a longer outage of power. The rest of the events are relatively short durations of less than a few seconds.

Question 6: ✓ Correct

Which option is a benefit of CCTV?

- Provide a corrective control
- Increase security protection throughout an environment
- Expand the area visible by security guards
- Reduce the need for locks and sensors on doors

EXPLANATION

A primary benefit of CCTV is that it expands the area visible by security guards. This helps few guards oversee and monitor a larger area.

CCTV does not reduce the need for locks and sensors on doors and does not provide a corrective control (it is a preventative, deterrent, or detective control). CCTV does not increase security protection throughout an environment, as the range is limited to areas over which it is aimed.

Question 7: ✓ Correct

You are an IT consultant. You are visiting a new client's site to become familiar with their network. As you walk around their facility, you note the following:

- When you enter the facility, a receptionist greets you and escorts you through a locked door to the work area where the office manager sits.
- The office manager informs you that the organization's servers are kept in a locked closet. An access card is required to enter the server closet.
- She informs you that server backups are configured to run each night. A rotation of tapes are used as the backup media.
- You notice the organization's network switch is kept in the server closet.
- You notice that a router/firewall/content filter all-in-one device has been implemented in the server closet to protect the internal network from external attacks.
- The office manager informs you that her desktop system no longer boots and asks you to repair or replace it, recovering as much data as possible in the process. You take the workstation back to your office to work on it.

Which security-related recommendations should you make to this client?

- Replace the tape drive used for backups with external USB hard disks.
- Implement a hardware checkout policy.**
- Keep the network infrastructure devices (switch and all-in-one device) in a locked room separate from network servers.
- Upgrade the server closet lock to a biometric authentication system.

EXPLANATION

In this scenario, you should recommend the client implement a hardware checkout policy. A checkout policy ensures that hardware containing sensitive data does not leave the organization's premises without approval and without recording the device's serial number, make, and model number.

A biometric server room lock is probably not necessary in this scenario. It is acceptable to keep servers and network devices, such as routers and switches, in the same room, as long as that room is kept secure. There's no security advantage to using external hard drives instead of tape backup media.

Question 8: ✓ Correct

Which special network area is used to provide added protection by isolating publicly accessible servers?

- DMZ
- VLAN
- Intranet
- Internet

EXPLANATION

A demilitarized zone (DMZ) is an area of the network where extra security is placed to protect the internal network from publicly accessible servers like web servers and email servers.

A VLAN may be used to create a DMZ, but it is not inherently a DMZ.

The internet and intranet zones are the areas on the outside and inside of a network that a DMZ is designed to protect.

Question 9: ✓ Correct

Which of the following allows an easy exit of an area in the event of an emergency, but also prevents entry? (Select two.)

- Bollard
- PTZ CCTV
- Turnstile
- Mantrap
- Double-entry door

EXPLANATION

A double-entry door has two doors that are locked from the outside and have crash bars on the inside, allowing for an easy exit. Double-entry doors are typically used only for emergency exits, and alarms sound when the doors are opened. A turnstile is a barrier that permits entry in only one direction. Turnstiles are often used to permit easy exit from a secure area. Entry is controlled through a mantrap or other system that requires authentication for entry.

A mantrap is a specialized entrance with two doors that creates a security buffer zone between two areas. Once a person enters into the space between the doors, both doors are locked. To enter the facility, authentication must be provided. This may include visual identification and identification credentials.

Bollards are short, sturdy posts used to prevent a car from crashing into a secure area.

Question 10: ✓ Correct

To answer this question, complete the lab using the information below.

 **You have already answered this question.**
You are not allowed to view the lab again.

[Launch Lab](#)

You completed the lab correctly.

[View Lab Report](#)

Question 11: ✓ Correct

Power, heating, ventilation, air conditioning systems (HVAC), and utilities are all components of which term?

- Infrastructure
- Hot aisle
- Cold aisle
- Network protection

EXPLANATION

These components are all part of the infrastructure that supports network and server operations.

The cold and hot aisles are part of the HVAC system, but do not make up the infrastructure themselves.

Network protection is not part of the infrastructure.

Question 12:

✓ Correct

Components within your server room are failing at a rapid pace. You discover that the humidity in the server room is at 60% and the temperature is at 80 degrees.

What should you do to help reduce problems?

- Add a humidifier to the server room.
- Add line conditioners in the server room.
- Add a separate A/C unit in the server room.
- Add a de-humidifier to the server room.

EXPLANATION

Keep the temperature between 70 and 74 degrees to prevent components from overheating. In many cases, the server room is the hottest location in your building because of the heat generated by the computer components. In most cases, you need a separate A/C unit installed in the server room so that you can maintain temperature without affecting the rest of the building.

Keep humidity between 40% and 60% to prevent electrostatic discharge (ESD). Line conditioners (also known as power conditioners) are used to improve the quality of power by performing one or more of the following:

- Removing noise caused by EMI and RFI
- Providing small amounts of additional power to protect against power dips or sags
- Protecting against spikes and surges

Question 13: ✓ Correct

You walk by the server room and notice that a fire has started. What should you do first?

- Turn on the overhead sprinklers.
- Grab a fire extinguisher and try to put out the fire.
- Make sure everyone has cleared the area.
- Call the fire department.

EXPLANATION

Your first action should be to ensure the safety of others. Make sure that people are out of the area. Fires and other hazards can quickly spread, so fast action is required to make sure that everyone is safe.

Call the fire department after you have taken steps to warn people who might be in danger. In most cases, you should not try to put out fires on your own, as they can quickly get out of control.

Question 14: ✓ Correct

What is the recommended humidity level for server rooms?

- 10% or lower
- 30%
- 50%
- 70% or higher

EXPLANATION

Keep humidity between 40% and 60% to prevent electrostatic discharge, which causes electrical charges that can damage computer components.

Question 15: ✓ Correct

Which device is used to ensure power to a server or network device during short power outages?

- Backup generator
- Surge protector
- Uninterruptible power supply
- Line conditioner

EXPLANATION

An uninterruptible power supply (UPS) provides continuous power using batteries for a short period of time. Often, it is paired with a backup generator that can provide power over a longer time period when provided with enough fuel.

Although a UPS often contains both surge protection and line conditioning, neither can maintain power during an outage.

Question 16: ✓ Correct

Most equipment is cooled by bringing cold air in the front and ducting the heat out of the back. What is the term for where the heat is sent in this type of scenario?

- Back aisle
- Front aisle
- Cold aisle
- Hot aisle

EXPLANATION

The hot aisle is where all of the heat is sent from the servers and network equipment to be transmitted to the HVAC return vent.

The cold aisle is where the chilled air is sent so that the equipment can duct it through to cool the devices.

Neither front nor back aisle is the correct term used in environmental controls.

Question 17: ✓ Correct

Your company has five salesmen who work out of the office and frequently leave their laptops laying on their desks in their cubicles. You are concerned that someone might walk by and take one of these laptops. Which of the following is the BEST protection implementation to address your concerns?

- ➡ Use cable locks to chain the laptops to the desks.
- Implement screen saver passwords.
- Require strong passwords in the Local Security Policy.
- Encrypt all company data on hard drives.

EXPLANATION

In this case, your main concern is that someone might steal the laptops. The best protection against physical theft is to secure the laptops in place using a cable lock.

Requiring strong passwords or using encryption might prevent unauthorized users from accessing data on the laptops, but these measures do not prevent physical theft.

Question 18: ✓ Correct

You want to use CCTV to increase your physical security, and you want the ability to remotely control the camera position. Which camera type should you choose?

- C-mount
- Bullet
- Dome
-  PTZ

EXPLANATION

A Pan Tilt Zoom (PTZ) camera lets you dynamically move the camera and zoom in on specific areas (cameras without PTZ capabilities are set looking a specific direction). Automatic PTZ mode automatically moves the camera between several preset locations. Manual PTZ lets an operator remotely control the position of the camera.

A bullet camera has a built-in lens and is long and round in shape. Most bullet cameras can be used indoors or outdoors. A c-mount camera has interchangeable lenses, is typically rectangular in shape, and carries the lens on its end. Most c-mount cameras require special housing to be used outdoors. A dome camera is a camera protected with a plastic or glass dome. These cameras are more vandal-resistant than other cameras.

Bullet, c-mount, or dome cameras can also be PTZ cameras.

Question 19: ✓ Correct

Burning, pulping, and shredding are three ways to securely dispose of data in which form?

- Disk
- Cloud
- Tape
-  Paper

EXPLANATION

Although tape and disk could be destroyed by industrial shredders, pulping can only be done to paper by using water and chemicals to dissolve the paper.

Data in the cloud must be disposed of with tools from the cloud provider.

Question 20: ✓ Correct

It is important to follow correct procedures when running electrical cables next to data cables in order to protect against which environmental concern?

- Temperature
- Airflow
- Electromagnetic interference
- Humidity

EXPLANATION

Electromagnetic interference is when electrical devices or cabling puts out electromagnetic pulses that can cause issues with data cabling and other unshielded devices.

Temperature, humidity, and airflow are all important parts of environmental control, but they do not interfere with data cabling.

Question 21: ✓ Correct

Which of the following can be used to stop piggybacking at a front entrance where employees should swipe smart cards to gain entry?

- Install security cameras
- Deploy a mantrap
- Use weight scales
- Use key locks rather than electronic locks

EXPLANATION

Piggybacking is when an authorized or unauthorized individual gains entry into a secured area by exploiting the credentials of a prior person. Often, the first person authenticates, unlocks the door, and then holds it open for the next person to enter without forcing them to authenticate separately. Piggybacking can be stopped by a mantrap. A mantrap is a single-person room with two doors. It often includes a scale to prevent piggybacking. Mantraps require proper authentication before the inner door unlocks to allow authorized personnel into a secured area. Those who fail to properly authenticate are held captive until authorities respond.

A security camera may deter piggybacking, but it does not directly stop it.

Using weight scales inside a mantrap stops piggybacking, but they are not useful or effective without the mantrap.

The use of conventional keys as opposed to electronic locks has little effect on preventing piggybacking and may actually make piggybacking more prevalent.

Question 22: ✓ Correct

Which device is used to allow a USB device to charge but blocks the data transfer capabilities of the device?

- USB data blocker
- Faraday cage
- Air gap
- Bollard

EXPLANATION

A USB data blocker prevents data from being transmitted while allowing the device to draw power. This is useful for charging devices on unknown USB ports, such as those at public charging stations.

An air gap is a network or device not connected to the rest of the network.

A bollard is physical protection to keep a vehicle from crashing into a secured area.

A Faraday cage prevents wireless emissions from being leaked.

Question 23: ✓ Correct

Which device is often employed by power companies to protect cabling infrastructure from having cables added or removed and to prevent emissions from being retrieved from the air?

- Faraday cage
- USB data blocker
- Air gap
- PDS

EXPLANATION

A protective distribution system (PDS) keeps cabling secure while also preventing electronic emissions.

A USB data blocker prevents data from being transmitted while allowing the device to draw power.

An air gap is a network or device not connected to the rest of the network.

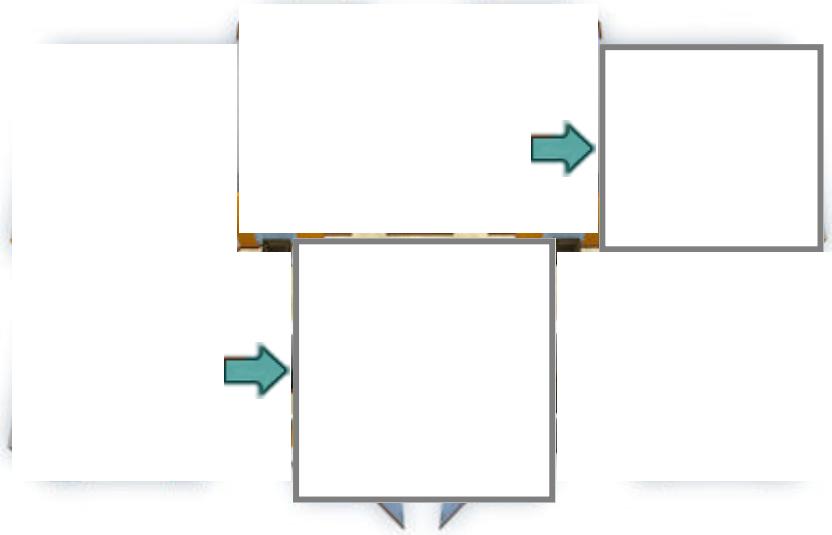
A Faraday cage prevents wireless emissions from being leaked, but it does not protect cabling.

Question 24: ✓ Correct

You are the security administrator for a small business. The floor plan for your organization is shown in the figure below.

You've hired a third-party security consultant to review your organization's security measures. She has discovered multiple instances where unauthorized individuals have gained access to your facility, even to very sensitive areas. She recommends that you provide employees with access badges and implement access badge readers to prevent this from happening in the future.

Click on the office locations where access badge readers would be most appropriate.

**EXPLANATION**

Access badge readers are typically implemented at building entrances to control access to a facility. Only individuals who have an authorized access badge are allowed to enter the facility. Individuals who do not have an access badge must be cleared and admitted by security personnel. Additional access badge readers can be implemented within the facility to further restrict access to sensitive areas, such as the server room.

Question 25: ✓ Correct

If a fingerprint or retina scan is required to open a secured door, which kind of physical security has been implemented?

→ Biometric locks

Mantrap

Access list

Double-entry door

EXPLANATION

Biometric locks use unique physical characteristics of a person to authenticate his or her access to a secured item. Often, these locks take the form of fingerprint scanners or retina scanners.

An access list is incorrect because it is a list of names that a guard checks.

Mantraps and double-entry doors are also incorrect because they are styles of entryways and don't check physical characteristics.