Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/26/2022 10:38:49 am • Time spent: 02:17

Score: 50% Passing Score: 80%

Question 1: ✔ Correct

Which of the following is a policy that defines appropriate and inappropriate usage of company resources, assets, and communications?

- Business continuity plan (BCP)
- Disaster recovery plan (DRP)
- ➡ Acceptable use policy (AUP)
- Business impact analysis (BIA)

EXPLANATION

An acceptable use policy (AUP) is a policy that defines appropriate and inappropriate usage of company resources, assets, and communications.

A business impact analysis (BIA) identifies critical processes and assets and the effect of their loss on the company.

A disaster recovery plan (DRP) addresses how a corporation should respond to a disaster.

A business continuity plan (BCP) addresses how a corporation responds to the disruption of critical systems.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_aup_01_secp7.question.fex

Question 2: ✔ Correct

Which of the following defines an acceptable use agreement?

- A legal contract between the organization and the employee that specifies that the employee is not to disclose the organization's confidential information.
- ➡ An agreement that identifies employees' rights to use company property, such as internet access and computer equipment, for personal use.
- An agreement that prohibits an employee from working for a competing organization for a specified period of time after he or she leaves the organization.
- An agreement that outlines the organization's monitoring activities.

EXPLANATION

An acceptable use agreement identifies employees' rights to use company property, such as internet access and computer equipment, for personal use.

A non-compete agreement prohibits an employee from working for a competing organization for a specified period of time after he or she leaves the organization. An employee monitoring agreement outlines the organization's monitoring activities. A non-disclosure agreement is a legal contract between an organization and an employee that specifies that the employee is not to disclose the organization's confidential information.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_aup_02_secp7.question.fex

Question 3: ✕ Incorrect

Your organization allows employees to bring their own devices into work, but management is concerned that a malicious internal user could use a mobile device to conduct an insider attack.

Which of the following should be implemented to help mitigate this threat?

- Implement a Network Access Control (NAC) solution.
- Implement an AUP that specifies which apps are allowed for use with organizational data.
- ➡ Implement an AUP that specifies where and when mobile devices can be possessed within the organization.
- ~~Implement a guest wireless network that is isolated from your organization's production network.~~

EXPLANATION

To mitigate the threat of an insider attack, you should consider implementing an AUP that:

- Specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high-security areas.
- Notifies users that personally owned devices are subject to random searches if brought on site.

A Network Access Control (NAC) solution would not help mitigate an insider attack with mobile devices.

Implementing an Acceptable Use Policy (AUP) that specifies which apps are allowed for use with organizational data would not help mitigate an insider attack with mobile devices.

Implementing a guest wireless network that is isolated from your organization's production network would not help mitigate an insider attack with mobile devices.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_aup_03_secp7.question.fex

Question 4: ✔ Correct

Which of the following could be an example of a malicious insider attack?

- A user has lost a company-owned device.
- A user has not implemented appropriate security settings.
- A user's device has become infected with malware.
- A user uses the built-in microphone to record conversations.

EXPLANATION

If a user is so inclined, he or she could use their mobile device to conduct a malicious insider attack. For example, they could:

- Use the built-in camera, which nearly all modern mobile devices have, to take pictures of sensitive internal information.
- Use the built-in microphone to record conversations.
- Use the built-in video function to record proprietary processes and procedures.
- Use the device's mobile broadband connection to transfer stolen data to parties outside the organization, bypassing the organization's network security mechanisms.

If a user copies sensitive data to their device, the organization could potentially lose control of that information. Even the question of who owns the data after it has been copied to a personal device becomes problematic. Consider the following scenarios:

- A user may not have implemented appropriate security settings on their device, allowing anyone who gains access to the device to view sensitive data.
- A user may lose the device, allowing anyone who finds it to access sensitive data.
- A device may become infected with malware, potentially exposing sensitive data.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_byod_secp7.question.fex

Question 5: ✕ Incorrect

Which device deployment model gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data?

- CYOD
- COPE
- VDI
- ~~BYOD~~

EXPLANATION

The Corporate-Owned, Personally Enabled (COPE) model gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data. Because the company owns the device, it can be secured more easily and wiped clean if lost or stolen. One disadvantage of this model is that employees who are not free to choose their own devices may end up bringing their own anyway.

The Bring Your Own Device (BYOD) model has users bringing in their personal devices and using them for business use.

The Choose Your Own Device (CYOD) model provides slightly more flexibility in giving users a limited selection of devices to choose from.

A virtual desktop interface (VDI) can be used with any device deployment model. A VDI allows mobile devices to establish a remote connection to a virtualized desktop.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_cope_secp7.question.fex

Question 6: ✔ Correct

Users in the sales department perform many of their daily tasks, such as emailing and creating sales presentations, on company-owned tablets. These tablets contain sensitive information. If one of these tablets is lost or stolen, this information could end up in the wrong hands.

The chief information officer wants you to implement a solution that can be used to keep sensitive information from getting into the wrong hands if a device is lost or stolen.

Which of the following should you implement?

- An Acceptable Use Policy (AUP)
- A guest wireless network that is isolated from your organization's production network
- A mobile device management (MDM) infrastructure
- A Network Access Control (NAC) solution

EXPLANATION

A mobile device management (MDM) infrastructure, such as Microsoft Intune, can be used to wipe data clean from a device that has been lost or stolen.

A Network Access Control (NAC) solution can remediate devices before allowing them to connect to your network. An Acceptable Use Policy (AUP) can be used to define which kind of data is allowed on personally owned devices and which kind of data is prohibited. A guest wireless network that is isolated from your organization's production network allows user-owned devices to gain internet access, but it quarantines them from the rest of your organization's production network.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_mdm_secp7.question.fex

Question 7: ✔ Correct

If a user's BYOD device (such as a tablet or phone) is infected with malware, that malware can be spread if that user connects to your organization's network. One way to prevent this event is to use a Network Access Control (NAC) system.

How does an NAC protect your network from being infected by a BYOD device?

- The NAC forces BYOD devices to connect to a guest network that is isolated from your production network.
- ➡ The NAC remediates devices before allowing them to connect to your network.
- The NAC specifies which apps can be used while the BYOD device is connected to the organization's network.
- The NAC notifies users that personally owned devices are subject to random searches if brought on site.

EXPLANATION

The NAC remediates devices before allowing them to connect to your network. This means that the NAC performs the following types of device management tasks before allowing a device to connect to the network:

- Operating system updates
- App updates
- Anti-malware installation
- Anti-malware definition updates

An alternative to using an NAC solution is to force BYOD devices to connect to a guest network that is isolated from your production network. An Acceptable Use Policy (AUP) specifies which apps can be used while the BYOD device is connected to the organization's network. An AUP also notifies users that personally owned devices are subject to random searches if brought on site.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_nac_01_secp7.question.fex

Question 8: ✕ Incorrect

The IT manager has tasked you with implementing a solution that ensures that mobile devices are up to date, have anti-malware installed, and have the latest definition updates before being allowed to connect to the network.

Which of the following should you implement?

- VDI
- NAC
- ~~MDM~~
- BYOD

EXPLANATION

A Network Access Control (NAC) solution can remediate devices before allowing them to connect to your network. This includes defining that a device is fully updated, has anti-malware installed, and has the latest definition updates.

The Bring Your Own Device (BYOD) model has users bringing in their personal devices and using them for business use.

A mobile device management (MDM) infrastructure, such as Microsoft Intune, can be used to track, manage, and even remotely wipe a user's mobile device.

A virtual desktop infrastructure (VDI) can be used with any device-deployment model. A VDI allows mobile devices to establish a remote connection to a virtualized desktop.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_nac_02_secp7.question.fex

Question 9: ✕ Incorrect

Which of the following BEST describes a virtual desktop infrastructure (VDI)?

- Provides enhanced security and better data protection because most of the data processing is provided by servers in the data center rather than on the local device.
- Specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high-security areas.
- Defines which kinds of data are allowed or which kinds of data are prohibited on personally owned devices brought into the workplace.
- ~~Gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data.~~

EXPLANATION

A virtual desktop infrastructure (VDI) can be used with any of the above models, including BYOD, to allow mobile devices to establish a remote connection to a virtualized desktop. Using a VDI provides enhanced security and better data protection because most of the data processing is provided by servers in the data center rather than on the local device.

The Corporate-Owned, Personally Enabled (COPE) model gives businesses significant control over device security while allowing employees to use their devices to access both corporate and personal data.

A possible remedy for the loss of sensitive date is to implement an Acceptable Use Policy (AUP) that defines which kinds of data are allowed on personally owned devices and which kinds of data are prohibited.

A possible remedy for malicious insider attacks is to implement an AUP that specifies where and when mobile devices can be possessed within the organization. For example, the possession of mobile devices may be prohibited in high-security areas.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_vdi_secp7.question.fex

Question 10: ✕ Incorrect

Users in the sales department perform many of their daily tasks, such as emailing and creating sales presentations, on their personal tablets.

The chief information officer worries that one of these users might also use their tablet to steal sensitive information from the organization's network. Your job is to implement a solution that prevents insiders from accessing sensitive information stored on the organization's network from their personal devices while still giving them access to the internet.

Which of the following should you implement?

- A guest wireless network that is isolated from your organization's production network
- A mobile device management (MDM) infrastructure
- ~~An Acceptable Use Policy (AUP)~~
- A Network Access Control (NAC) solution

EXPLANATION

A guest wireless network that is isolated from your organization's production network allows user-owned devices to gain internet access, but it quarantines them from sensitive information on your organization's production network.

A mobile device management (MDM) infrastructure, such as Microsoft Intune, can be used to wipe data from a device that has been lost or stolen. A Network Access Control (NAC) solution can remediate devices before allowing them to connect to your network. An Acceptable Use Policy (AUP) can be used to define which kind of data is allowed and prohibited on personally owned devices.

REFERENCES

9.8.2 BYOD Security Facts

q_boyd_sec_wifi_secp7.question.fex