A.

The presence of an Access Point outside, covering a large back patio area, poses a risk for potential "evil twin" attacks. This is because the AP's proximity to other hosts outside of Alliah headquarters provides an opportunity for malicious actors to create a deceptive AP that mimics the genuine one, replicating its characteristics. In the event that employees connect to this fraudulent AP, it grants malicious actors the ability to eavesdrop on wireless communications.

Alliah maintains a Bring Your Own Device policy, permitting users to bring in their personal devices and utilize them on the company's Wireless Local Area Network. However, it's crucial to acknowledge that employee-owned devices can serve as vectors for malware and cyber attacks. This is primarily due to the fact that these devices do not come with a guarantee of proper security configurations.

In essence, the combination of an outdoor AP and a BYOD policy, while convenient, introduces significant security considerations. The potential for "evil twin" attacks underscores the need for robust security measures to safeguard wireless communications within the Alliah network. Additionally, the vulnerabilities of employee owned devices emphasize the importance of

implementing comprehensive security protocols and regular monitoring to mitigate potential risks.

B.

As a mobile vulnerability, BYOD devices represent a potential vector for malware and malicious actors if not properly secured and monitored. In the absence of stringent security configurations and policies, employee-owned devices can pose significant risks to the organization. Given that sensitive business data is stored on these devices, they become prime targets for cyber threats. Malicious actors could exploit these vulnerabilities, leading to the compromise of confidential company information. Consequently, the BYOD policy may inadvertently introduce a single point of failure in the company's security infrastructure, necessitating a robust and comprehensive security strategy to safeguard against potential breaches

Another mobile vulnerability is that if a representative were to lose one of their three devices while not in the office, It can lead to a data breach due to a malicious actor getting access to that lost device. Confidential information including, company data, customer data, financial information and intellectual property are stored on these devices. Therefore it’s important to ensure that in the

event a device is lost, sensitive information on that device is still confidential and untampered with.

C.

Here are steps to alleviate the evil twin vulnerability of having an access point in the backyard area:

1. Enable WPA3 encryption:

Uses the latest encryption standards for enhanced security.

2. Change default authentication information:

Replace default usernames and passwords to prevent unauthorized access.

3. Disable WPS:

Turn off Wi-Fi Protected Setup to prevent exploits.

4. Use strong passwords:

Create complex, hard-to-guess Wi-Fi passwords.

5. Firmware update:

Keep your router's firmware updated for security patches. 6. Broadcast SSID:

Turn off broadcasting to hide your network name.

7. MAC address filtering:

Add an extra layer of security by allowing only specified devices.

8. Deploying IDS:

Monitor suspicious activity on your network.

9. Monitor activities regularly:

Monitor unusual behavior in router logs and network activity.

10. Physical security measures:

Place your access point in a secure location to prevent physical access. 11 User education:

Inform network users about the risks of unsecured networks.

12. Use a network security scanner:

Identify vulnerabilities and threats in your network.

14. Deploy 2FA:

Enable two-factor authentication for router/AP access.

To minimize damage caused by BYOD devices on a WLAN, you will need to:

1. Create a BYOD policy:

Develop a clear and comprehensive BYOD policy that outlines acceptable usage, security requirements, and consequences for non-compliance.

2. Network segmentation:

Implement network segmentation to isolate BYOD devices from critical resources. Use VLANs (Virtual LANs) to separate traffic and control access. 3. Strong authentication and access control:

Require a strong password or passphrase for device authentication. Implement multi-factor authentication (MFA) for added security.

4. Isolate the guest network:

Set up a separate guest network for BYOD devices. This network must have limited access to internal resources and be isolated from sensitive data.

5. Update software regularly:

Educate users on the importance of keeping their devices and apps up to date with the latest patches and security updates.

6. Encoding:

Apply encryption protocols (WPA3 for Wi-Fi) to protect data in transit. Also encourage or mandate the use of device encryption.

To prevent BYOD devices from being used as leveraged vectors to infiltrate company network:

1. Implement Strong Authentication and Access Controls:

   Enforce strong, unique passwords and consider implementing multi-factor authentication (MFA) for accessing sensitive resources.

2. Endpoint Security Software:

   Require the installation of endpoint security software (e.g., anti-virus, anti-malware) on all BYOD devices.

3. Mobile Device Management (MDM):

   Deploy an MDM solution to enforce security policies, remotely wipe devices, and track their location in case of loss or theft.

4. Containerization or Virtualization:

   Encourage the use of containerization or virtualization technologies to isolate corporate applications and data from personal ones.

5. Network Segmentation:

   Segment the network to isolate BYOD devices from critical infrastructure and sensitive data.

For the issue of losing possession of a company device:

1. Use remote management software to manage encryption keys and settings on BYOD devices.
2. Ensure employees enable device encryption through the management interface.
3. Regularly review compliance with encryption policies.
4. Password and biometric authentication:
5. Require a strong password or biometric authentication (e.g. fingerprint, facial recognition) to unlock the device.
6. Train employees on how to create and maintain secure passwords.

   Encrypt backups:

7. Require employees to encrypt backups of their device data.
8. Provides instructions on how to enable backup encryption through device settings.
9. Enable remote wipe feature:
10. Configure remote wipe functionality for BYOD devices using remote management tools.
11. Make sure this capability is clearly communicated to employees.
12. Implement an automatic trigger for remote deletion:
13. Configure automatic triggers for remote wipes based on events such as failed sign-in attempts, long device inactivity, or SIM card deletion. Define thresholds and conditions to trigger remote deletion.
14. Regular training and awareness raising for employees:
15. Conduct training sessions to educate employees on the importance of encryption, strong passwords, and backup encryption.
16. Provide clear instructions on how to enable and use the remote erase feature

D

Preventative measures

WLAN Security Measures:

Use Strong Encryption:

- Implement WPA3 encryption for WLAN to improve security.(FIPS 140-2,2001)

Regular Security Testing and Vulnerability Assessments:

- Perform periodic security testing and vulnerability assessments to identify and remediate potential weaknesses.(www.cisa.gov,2023)

Configure Firewall and IDS/IPS:

- Deploy firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and control traffic.(www.law.cornell.edu/uscode/text/44/3554,2013)

Strong Access Control and Authentication:

- Implement multi-factor authentication (MFA) to access critical systems.

Regular Fixes and Updates:

- Keep all devices and software up to date with the latest security patches.(www.law.cornell.edu/uscode/text/44/3554,2013)

Mobile Environment Security Measures:

Mobile Device Management (MDM):

- Use an MDM solution to enforce security policies on mobile devices.(www.ftc.gov/business-guidance/privacy-security/data-security,2023)

- Require strong passwords or biometric authentication to access mobile devices.(www.law.cornell.edu/cfr/text/45/164.312,2013)

Encrypt Data on Mobile Devices:

- Enable encryption on mobile devices to protect data at rest.(www.law.cornell.edu/cfr/text/45/164.312,2013)

Regular Training and Awareness Raising for Employees:

- Conduct regular training sessions on security best practices, especially for mobile device use.(www.law.cornell.edu/cfr/text/45/164.308,2013)

Remote Deletion and Monitoring:

- Implement remote wipe capabilities and device tracking in case of loss or theft.(www.law.cornell.edu,2013)

E.

Important controls:

COPE devices provide IT departments with a significant level of control and authority, which can significantly reduce the burden of day-to-day device management. This means our IT team can focus on more strategic initiatives instead of getting bogged down with routine equipment maintenance.

Safety and compliance:

For businesses with strict compliance and security requirements, COPE is a great choice. Inherent device usage restrictions help enforce compliance policies, allowing IT to effectively isolate, monitor, and manage an organization's data. This ensures that our sensitive information remains protected. Minimum customization:

COPE devices achieve a balance between work and personal use. Although they allow access to some personal resources, they maintain necessary restrictions that may not be present in more limited company-owned, business-only devices. This provides a level of flexibility that can be appreciated by end users.

Benefits for employees:

One of the problems with BYOD is that employees can feel a financial burden if they use their own devices for work. However, with COPE devices, there is minimal or no cost to employees. This can be a significant benefit, alleviating potential concerns for our team members.

Cost saving potential:

Buying equipment in bulk will result in a significant discount for the company, resulting in significant savings. This aspect will be of particular interest if we are considering a more restrictive device strategy than the traditional BYOD approach.

In summary, implementing the COPE BYOD system provides a balanced solution that meets the needs of both our IT department and our end users. It provides an essential level of control and security for our organization, while saving costs for our employees.

(jumpcloud.com/blog/defining-byod-cope-cobo-cyod,2022)

References

45 CFR § 164.306 - Security standards: General rules. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/cfr/text/45/164.306

45 CFR § 164.308 - Administrative safeguards. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/cfr/text/45/164.308

45 CFR § 164.312 - Technical safeguards. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/cfr/text/45/164.312

44 U.S. Code § 3554 - Federal agency responsibilities. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/44/3554

https://www.cisa.gov/sites/default/files/2023-07/FY22-RVA-Analysis%20-%20Final_508c.pdf

Security requirements for cryptographic modules. (2001). https://doi.org/10.6028/nist.fips.140-2

Lee, B. (2022). Device Management: BYOD, COPE, COBO, and CYOD. *JumpCloud*. https://jumpcloud.com/blog/defining-byod-cope-cobo-cyod#:~:text=The%20phone%20will%20be%20set,a%20too%20lenient%20BYOD%20policy.