A. Describe two WLAN vulnerabilities that present risks for Alliah, based on the details in the scenario.

A: WLAN Vulnerabilities

1. **Insecure encryption protocols**

If Alliah's WLANs are using outdated or weak encryption protocols such as WEP or an improperly configured WPA2, they can present vulnerabilities that can be exploited. For example, WEP is vulnerable due to its small 24-bit initialization vector and 40-bit key size, which weakens the RC4 cipher encryption. Most modern attacks can exploit weak encryption practices, allowing attackers to eavesdrop and manipulate network traffic. This can allow unauthorized access, and an attacker can impersonate an employee's device or inject malicious packets to compromise the network.

2. **Back Patio WAP Vulnerability**

The wireless access point (WAP) at the back patio is vulnerable to various attacks, such as disassociation, interference, or unauthorized access. A wireless access point and client use management frames such as disassociation or de-authentication frames to manage connections. An attacker can exploit this vulnerability by creating an evil twin access point using tools like Aircrack-ng to broadcast de-authentication frames. With enough transmit power, the attacker can disassociate the employees from Alliah's wireless AP. The evil twin can disrupt service and allow an attacker to gain unauthorized access to Alliah's network.

B. Describe two mobile vulnerabilities that present risks for Alliah, based on the details in the scenario.

B: Mobile vulnerabilities

1. **Unmanaged BYOD policy**

The first vulnerability would be the implementation of Alliah's BYOD policy without proper security measures and policies. Without comprehensive policy management, employee mobile devices can be used as attack vectors for security threats like malware and data breaches. For example, employee devices can be exposed to man-in-the-mobile attacks or drive-by downloads, which install malicious software without the employee's knowledge. The lack of security controls leads to risks of malware spreading within Alliah's network, including unauthorized data exfiltration or data tampering with sensitive information.

2. **Lack of Data Segmentation**

The second vulnerability is inadequate segmentation between the company's and personal data on mobile devices. When employees use personal mobile devices for work, separating company and personal data is challenging. The lack of data segmentation poses significant security risks if employee mobile devices are compromised, lost, or stolen. This can result in sensitive company data being leaked to unauthorized parties, mainly if confidential data is accessed and stored on insecure networks. The lack of data segmentation increases the risk of data leakage and unauthorized access to Alliah's confidential information.

C. Summarize the steps for mitigating *each* identified WLAN and mobile vulnerability, including the specific tools or documentation that will be needed for mitigation.

C: Mitigation Steps

1. **Implement WPA3 for enhanced security.**

"WPA3 is currently the strongest encryption (CISA, 2021)". Since Alliah's company employee size is increasing each month, upgrading to WPA3 in enterprise mode using IEEE 802.1X for secure authentication with GCMP-256 encryption would provide protection for sensitive data being transmitted on the network. This feature will enable Alliah to incorporate the AAA framework, providing accountability and no-repudiation for user activity on the network. WPA3 provides enhanced encryption and protection against brute force attacks. These mitigations would prevent eavesdropping and tracking user sessions on the network. For tools and documentation reference, use the Cisco WPA3 Deployment Guide (Cisco, 2024) and CISA Security guidance on securing wireless networks (CISA, 2021) for best practices. This will improve Alliah's security with enhanced protection for data transmissions, including mechanisms for providing accountability and preventing unauthorized access.

2. **Cisco's Adaptive Wireless IPS (wIPS) and WPA3**

Implementing Cisco's Adaptive Wireless IPS (wIPS) and WPA3 in Enterprise mode ensures that protected management frames are used on all network connections to protect against deauthentication attacks. (wIPS) is designed to detect and mitigate rogue access points such as evil twins and potential denial-of-service attacks on wireless access points. (wIPS) also provides separate pre-configured profiles for WLAN environments to ensure compliance for different enterprise or business sectors. For

tools and documentation, reference the Cisco wIPS Configuration guide (Cisco, n.d) for setup and configuration details. This mitigation will improve the security of Alliah's wireless network and performance, with increased protection against unauthorized devices and network attacks

3. **Implement MDM and BYOD policies.**

Implement an MDM platform, a BYOD policy, proper end-user guidelines, and acceptable use policies to mitigate insecure mobile devices. An MDM platform can provide device compliance checks, enforce security policies such as password requirements and encryption for iOS/Android devices. Alliah's security policies can be used to identify approved devices and company requirements that will not compromise Alliah's infrastructure. Additionally, Alliah can incorporate NAC to enforce device compliance checks on mobile devices to ensure devices entering the network are up-to-date and virus-free. For tools and documentation, reference the NIST SP 1800-22 (NIST, 2023) for best practices in MDM implementation in Alliah's BYOD policy detailing the AUP and compliance rules. This mitigation will help Alliah establish control over personal mobile devices, reducing the risk of malware infections and data breaches by ensuring devices comply with security standards

4. **MDM with containerization**

Implement MDM and containerization to maintain a clear separation between Company and Personal Data. Containerization helps in separating corporate data from personal data on mobile devices. MDMs support encryption mechanisms to securely store data, including anti-virus software and data loss prevention mechanisms to prevent sensitive data from leaving the company. MDM can securely remote wipe

company data without affecting the user's personal data through containerization if an employee's device is lost or stolen. For tools and documentation, reference the "data access restricted between the personal and work container profile applications (NIST, 2023)" for configuration of containerization features. By Alliah securely managing corporate data on personal devices, it will reduce the risk of data leaks even when a device is lost or stolen.

D. Recommend preventive measures to maintain the security posture of WLAN and mobile environments in a small business, such as Allah. Reference federal, state, or industry regulations that justify these measures.

D: Preventative Measures

1. **WLAN Security**

"Continous Monitoring Recommendations (NIST, 2012)" Allah should continuously monitor their WLANs to detect rogue APs or misconfigured WLANs using insecure protocols to prevent network interference, such as DoS attacks. The NIST guidelines support ongoing monitoring and GDPR compliance to ensure a company knows its data protection responsibilities. If Alliah is collecting PII from EU citizens, it is recommended to follow GDPR's "GDPR checklist for data controllers (GDPR, n.d)." This checklist guides protecting PII and the responsibilities of the Data Controller, Data Processor, and the Company. If necessary, a Data Protection Officer (DPO) is recommended to help with data protection and GDPR compliance to meet industry regulations and prevent non-compliance fines.

2. **Mobile environment**

If Alliah is collecting PHI, it is recommended to follow the "Security Rule (HHS, n.d)" and HIPPA's security standards to maintain their security posture. Developing and

enforcing mobile security policies on how protected health information (PHI) is processed, transferred, and stored is critical for Alliah to maintain security and regulatory compliance. Implementing data encryption and secure access controls ensures that sensitive data remains protected. These practices align with HIPPA's security rules, which require strict safeguards in encrypting data and ensuring secure access controls. This ensures compliance with HIPPA regulations, reduces the risk of data breaches, and improves the overall security posture of mobile devices at Alliah.

E. Recommend a solution for the company's BYOD approach, including research to justify your recommendation.

Alliah should follow the best practice guide NIST SP 1800-22, which was collalaborated with The National Cybersecurity Center of Excellence (NCCoE) to help provide cybersecurity best practices in a BYOD environment. "Mobile Device Management that provisions configuration profiles to mobile devices, enforces security policies, and monitors policy compliance (NIST, 2023)." Alliah should implement a EMM or MDM solution with mobile security policies and standards that enforce data encryption, authentication, regular updates, remote wipe, and containerization features. Different access controls and mechanisms can be implemented to segment sensitive data and a remote wipe capability for lost, compromised, or stolen devices. The (NIST) Cybersecurity Practice Guide guides how companies can use commercially available MDM products to meet their security and privacy standards in a BYOD environment.

References

CISA. (2021, February 9). *Securing Wireless Networks*. Retrieved from https://www.cisa.gov/news-events/news/securing-wireless-networks

Cisco. (2024, April 9). *WPA3 Deployment Guide*. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/wpa3-dg.html

Cisco. (n.d). *Cisco Adaptive Wireless Intrusion Prevention System*. Retrieved from https://www.cisco.com/c/en/us/td/docs/wireless/mse/3350/70/wIPS/configuration/guide/wips_70/msecg_appA_wIPS.html

NIST. (2012 February). *Guidelines for Securing Wireless Local Area Networks (WLAN)*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf

GDPR.EU. (n.d). *GDPR checklist for data controllers*. Retrieved from https://gdpr.eu/checklist/

HHS. (n.d). *HIPPA Security Rule*. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf?language=es

NIST. (2023). *Mobile Device Security: Bring Your Own Device (BYOD).* Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-22.pdf