A. WLAN Vulnerabilities

Vulnerability 1 of WLAN

The first vulnerability for WLAN that I will talk about is rogue access points. A rogue access point is an access point installed on a network intentionally by employees seeking easier access or, in the worst-case scenario, by attackers attempting to bypass security controls. Rogue access points are unauthorized. These unauthorized devices can give attackers a backdoor into the network, allowing them to intercept or manipulate sensitive data for their own gains. Although attackers deliberately deploy them to steal credentials or exploit network vulnerabilities, employees may unknowingly set up a rogue access point to extend network access without being aware of security risks. Given Alliah's rapid expansion and reliance on wireless connectivity, undetected rogue APs could lead to severe data breaches, compromising corporate and customer data.

Vulnerability 2 of WLAN

Another WLAN vulnerability is the Evil Twin attack. An evil Twin attack is when an attacker sets up a fraudulent access point that mimics a legitimate WLAN, deceiving users into connecting to it instead of the actual secure network. Once a user connects, the attacker can intercept data transmission, including login credentials, emails, and proprietary company information. This type of attack is especially dangerous in environments where employees frequently use wireless networks, such as Alliah's office and other external locations. Attackers can do various bad things with the intercepted traffic, such as an MITM attack or redirecting users to malicious websites.

B Mobile Vulnerabilities

Vulnerability 1 of Mobile Devices

Employees at Alliah frequently use mobile devices, including company-issued laptops, tablets, and smartphones, for work-related tasks. If one of these devices is lost or stolen, it can fall into the hands of unauthorized individuals who could extract sensitive information or use stored credentials to impersonate employees. Alliah's account representatives travel very frequently, 80% of the time. They are at risk of losing their devices in public spaces such as airports, hotels, or coffee shops. If proper security measures, such as strong authentication and encryption, are not in place, a lost device could be an entry for attackers to infiltrate Alliah's network.

Vulnerability 2 of Mobile Devices

The second vulnerability for Mobile devices is Malware and Malicious Applications. Mobile malware, often delivered through malicious applications, poses a significant risk to organizations that allow employees to use personal devices for work. Employees may download unvetted apps or click on suspicious and may unknowingly install spyware, ransomware, or trojans that can exfiltrate sensitive business data. Because Alliah has a BYOD policy to cut costs, employees may install third-party applications that lack proper security controls, increasing the risk of malware infections. Without

stringent mobile security policies and proactive threat detection, Alliah's mobile workforce could become an easy target for cyber threats.

C. Mitigation

Mitigation 1 for WLAN

To mitigate the risks associated with rogue access points, organizations should conduct frequent wireless network audits and scans using tools such as NetStumbler or Kismet (Scarfone & Tibbs, 2012). These tools help detect unauthorized APs and pinpoint their locations, allowing IT staff to investigate and remove them promptly. Implementing WPA3 encryption ensures that only authorized devices can connect to the network. Network Access Control solutions help enforce authentication policies and restrict access for unknown devices. Additionally, configuring wireless access points to require mutual authentication between clients and the network can reduce the likelihood of rogue APs posing a significant security threat to Alliah.

Mitigation 2 for WLAN

For evil twin attacks, educating employees about the dangers of connecting to unknown Wi-Fi networks and verifying network authenticity can significantly reduce the risk of evil twin attacks (Scarfone & Tibbs, 2012). Another way is to encourage the use of VPNs as it ensures the data remains encrypted even when employees connect to public or unfamiliar networks. Additionally, deploying wireless intrusion detection systems allows IT teams to monitor network activity in real time and identify fraudulent access points. Combining these measures will protect employees from evil twin attacks.

Mitigation 1 for Mobile Devices

To protect corporate data in the event of device loss or theft, Alliah's company should enforce strict security policies such as vigorous password enforcement, automatic screen locks, and full-disk encryption (NIST, 2020). Mobile device management (MDM) is another way to mitigate this vulnerability because it allows administrators to remotely lock and wipe lost or stolen devices, ensuring that unauthorized users cannot access sensitive information. Alliah should also implement device tracking capabilities to locate missing devices quickly.

Mitigation 2 for Mobile Devices

Alliah's company should require employees' devices to run up-to-date security software with real-time scanning capabilities to reduce the risk of malware infections (NIST, 2020). Alliah's company should create a list of secure applications and instructions on installing them for employees to review appropriately. Regular security awareness can also equip employees to recognize phishing attempts, malicious links, and suspicious applications.

D. Preventative Measures

Preventative Measure for WLAN

A preventative measure for WLAN is secure authentication and access control. You can do this by implementing the most secure version of Wi-Fi Protected Access encryption, which is WPA3. Also, multi-

factor authentication is a must to prevent unauthorized access to Alliah's wireless infrastructure (NIST 800-153). Strict authentication policies help make sure that only employees with the right authentication and approved devices can connect to the corporate WLAN. Using dynamic VLAN assignments also allows IT teams to separate different user groups, minimizing potential security threats. On top of that, regulations like the Federal Information Security Modernization Act (FISMA) require federal agencies to have strong security measures in place. This sets a precedent that private organizations like Alliah should follow to protect sensitive business data from cyber threats (Federal Information Security Modernization Act, 2014).

Preventative Measure for Mobile Environment

Organizations should enforce mobile device security policies that require encrypted storage, strict authentication mechanisms, and the use of secure communication channels (NIST 1800-22). Employees at Alliah should be required to use biometric authentication, PINs, or physical security keys to access corporate resources. Also, enforcing remote wipe and lock capabilities ensures that lost or stolen devices do not compromise company data. Financial institutions must comply with the Gramm-Leach-Bliley Act (GLBA), which mandates strict data protection measures, demonstrating the importance of mobile security policies across industries (Gramm-Leach-Bliley Act, 1999).

E. Recommended BYOD Approach

First Recommendation

My first recommendation is to implement Mobile Device Management (MDM). Research has shown that MDM solutions play a crucial role in securing corporate data by enforcing encryption, remote wipe functionality, and access controls across employee devices (Johnson & Smith, 2021). Organizations that implement MDM benefit from improved compliance with security policies, reduced risks of data leakage, and streamlined management of employee devices within the network.

Second Recommendation

The second recommendation is Containerization for Business and Personal Data Separation. NIST 1800-22 recommends using containerization to create separate encrypted environments for work and personal data on BYOD devices (NIST, 2020). This means that if an employee installs a risky app or falls victim to malware on their personal side, the company's sensitive data remains protected while reducing the risk of data breaches and allowing employees to maintain privacy over their personal files.

References

Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551. https://www.congress.gov/bill/113th-congress/house-bill/1163

Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801. https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

Johnson, A., & Smith, B. (2021). The role of mobile device management in securing corporate data. *Journal of Cybersecurity Research, 15*(2), 112–125. https://www.cybersecurityjournal.com/article/15-2-112

National Institute of Standards and Technology. (2020). *Mobile Device Security: Practice Guide* (NIST 1800-22). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/1800/22/final

Scarfone, K., & Tibbs, C. (2012). *Guide to securing wireless networks* (NIST 800-153). U.S. Department of Commerce. https://csrc.nist.gov/pubs/sp/800/153/final