Two plausible WLAN vulnerabilities from Alliah's WLAN network can be a misconfigured access point and the potential for rogue access points. A misconfigured access point can include things like using default credentials, incorrect settings, and failure to update the access points firmware. This can have the effect of allowing attackers to take control of the access point, intercept data, or create more entry points into the network. A rogue access point is something an employee may setup without malicious intent, however this can lead to Man-In-The-Middle (MITM) attacks as well as data theft from anyone using the rogue access point. Attackers can use this rogue access point to setup an evil twin access point.

Two plausible Mobile vulnerabilities can be losing mobile devices or having them stolen, and unapproved or malicious applications that employees may download unknowingly. Lost or stolen devices are a big vulnerability because there are five account representatives who are on the road about eighty percent of the time. Each of these representatives has 3 company owned devices each, a laptop, tablet, and smartphone. If just one of these devices is lost or stolen and the devices are not encrypted or are not capable of remote wipes, then sensitive data is at risk. Unapproved or malicious apps are also a risk because users may download apps from unofficial sources and can allow high level permissions without being fully aware of the damage it can cause. These malicious apps can install spyware or even grant unauthorized access to internal systems.

To mitigate the misconfigured access point vulnerability, we can start with performing regular firmware updates on the access points. Replace any default usernames and passwords with complex ones. Create a baseline configuration template for the APs and run regular scans to ensure the APs continue to match the baseline.

To mitigate the rogue access point vulnerability, the first step would be to train and educate employees to not create any personal hotspots. A Wireless Intrusion Detection/Prevention System (WIDS/WIPS) can be used to scan for unauthorized SSIDs as well as block any rogue devices when detected. Conducting regular site surveys with wireless survey tools such as Ekahau or AirMagnet can help to detect any rogue APs as well.

To mitigate the vulnerability of lost or stolen devices, device encryption should be used. BitLocker on Windows is a good example of this. On top of encryption, a remote wipe feature should be implemented with Mobile Device Management (MDM) to instantly wipe a device of any sensitive data if it reported lost or stolen.

To mitigate the vulnerability or any unapproved or malicious applications, we should start with whitelisting and blacklisting applications. This would be done within the MDM. This will prevent known malicious apps from being downloaded and only allowing trusted applications on the device. Educating employees on the risk of how using administrator or root privileges on a device while installing certain applications can lead to elevated privileges being granted to those applications.

Alliah Company should adopt the NIST Cybersecurity Framework to help them develop policies that cover their WLAN and mobile device vulnerabilities. According to NISTs Guidelines for Securing WLANs (2012), “A standardized configuration provides a base level of security, reducing vulnerabilities and lessening the impact of successful attacks.” Enforcing strong AP encryption like WPA2/WPA3 and routine scanning for rogue APS and misconfigurations are procedures that should be in their WLAN policy. NISTs Guidelines for Securing WLANs (2012) states “Organizations should do largely the same vulnerability monitoring for WLAN components that they do for any other software: identifying patches and applying them and verifying security configuration settings and adjusting them as needed.” Requiring devices to be enrolled in an MDM, having a whitelist and blacklist of applications, full disk encryption, and remote wipes should all be standard procedures included in their mobile device policy (NIST, 2023a). Any BYOD devices should be on a separate segmented network from corporate devices. Lastly, using a Security Information and Event Management (SIEM) tool to help monitor logs from any APs, network devices, and MDM systems can help to quickly detect any anomalous activity and prevent damage (NIST, 2023a). Since Alliah Company is a social media provider, customer data will be collected and will need to be protected while aligning with the California Consumer Privacy Act (CCPA) for consumers in California, and the General Data Protection Regulation (GDPR) for European consumers. For California consumers, “businesses must implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.” (CCPA, 2018). The GDPR requires the use of security monitoring software, multi-factor authentication, strong password policies, hash functions for data integrity, and encryption of information to protect personally identifiable information (GDPR, 2016)

Alliah Company has decided to opt with a BYOD policy to control costs during their launch. They can keep the BYOD policy, but some changes need to be made to make it secure. A formal BYOD policy must be implemented with the use of an MDM or Enterprise Mobile Management (EMM). Using an MDM/EMM, all personal devices must be registered, encryption must be enforced, installation of apps must be controlled and monitored, devices must be continually patched, and multifactor authentication must be implemented (NIST, 2023b). The justification for this policy is that it is very cost effective while still maintaining an acceptable security posture. Business owned devices can be too costly to implement (NIST, 2023b). User convenience is also another justification because employees are much more familiar with their own devices, which can have the result of increased productivity. According to RocketIT (2023), two positive aspects of BYOD are lowered technology costs, which Alliah Company may need to prioritize, and a productivity boost since employees are more comfortable with their own devices.

References:

National Institute of Standards and Technology (NIST). (2012). *Guidelines for Securing Wireless Local Area Networks (WLANs)*.

https://csrc.nist.gov/pubs/sp/800/153/final

National Institute of Standards and Technology (NIST). (2023a). *Mobile Device Security: Bring Your Own Device (BYOD)*

https://csrc.nist.gov/pubs/sp/1800/22/final

National Institute of Standards and Technology (NIST). (2023b). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*

https://www.nist.gov/publications/guidelines-managing-security-mobile-devices-enterprise-0

California Legislative Information (CCPA). (2018). *California Consumer Privacy Act of 2018*

https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.100.

Intersoft Consulting (GDPR). (2016). *General Data Protection Regulation*

https://gdpr-info.eu/

RocketIT (RocketIT). (2023). *The Pros and Cons of BYOD (Bring Your Own Device) Policies*

https://rocketit.com/the-pros-and-cons-of-byod-bring-your-own-device-policies/?utm_source=chatgpt.com