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

Being able to connect to the network from the patio is a nice addition but it can also pose a risk to the network as someone from outside the company but within the vicinity coverage area of the patio network would be able to gain access and able to packet sniff or monitor network traffic for potential vulnerabilities. With the data center being within 100 miles from Alliah headquarters there needs to be some sort of implementation in place to securely connect to the data servers, whether it is through the use of encrypted tunneling such as that of a VPN or IPsec, there needs to be something in place that authenticates, authorizes, and accounts individuals taking part in this connection.

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

The five account representatives pose a vulnerability risk for the Alliah company, with them being on the road at least 80% of the time their data and valuable information could be at risk for theft and having their devices stolen which would put valuable company data at great risk. Another mobile risk factor to come into play is for employees to use public WiFi and unsecured networks wherever they happen to go. This is a huge consideration to take note of as the correct steps to safely connect and secure to the corporate network must be put in place so no one is able to eavesdrop or potentially intercept valuable information pertaining to the company whilst using an unsecured public network.

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

As stated before, the patio area is a nice addition to the company as it is able to give access to employees of the company to the network whilst being outside. The risk to this is having someone else from outside the company being able to intercept and interpret traffic on the network and potentially gaining further access within the network. To prevent such things from occurring, we can use WPA2 on the network which enables the strongest encryption for enterprise networks and uses an SAE (Simultaneous Authentication of Equals). I see this as a great security option because it offers the highest level of security and if the company was ever needing to expand then WPA2 Enterprise would be able to handle the necessary security measures for this type of environment.

With the Distance of the Alliah headquarters and their web site servers being 100 miles away from each other we need to implement a secure solution to connect to the servers and for this we should be using a VPN to connect as it provides data integrity, confidentiality, and authentication. With taking into account the use of VPN solutions, we refer to the National Security Agency and Cybersecurity and Infrastructure Security Agency information sheet on the “Hardening and Remote Access VPN Solutions”. As stated, “Virtual Private Networks (VPNs) allow users to remotely connect to a corporate network via a secure tunnel. Through this tunnel, users can take advantage of the internal services and protections normally offered to on-site users, such as email/collaboration tools, sensitive document repositories, and perimeter firewalls and gateways.” Essential to the security of the network and to protect the network from attacks that may intercept transmission between the headquarters and the web servers, the implementation of a secure VPN to tunnel transmission & information would be deemed vital for the security of the network and web server in its entirety.

The five account representatives that travel at least 80% of the time want to take the right measures to protect and secure any corporate data within the device and corporate data in transit to and from the corporate networks. This means that to protect data in transit we should be implementing safety measures such as the use of a VPN and using secure protocols such as SSH and HTTPS to access systems within the corporate network or whilst browsing the web on an unsecured public network. Any corporate employees using devices that may hold sensitive data should be using Mobile Device Management suites provided by the company in order to be able to erase and wipe the system in case the device is stolen or taken. This would prevent sensitive data from falling into the wrong hands if it is unable to be retrieved using GPS.

D.  Recommend preventive measures to maintain the security posture of WLAN and mobile environments in a small business, such as Alliah.

To maintain security posture of both WLAN and mobile within a small business such as with the Alliah company, my recommendation would be enabling a defense in depth strategy as seen on Chp 4, pg 137 of *“Wireless and Mobile Device Security” by Jim Doherty*. As stated, “with a defense in depth, security controls are applied to networks and systems in layers, the rationale being that should an attacker breach the perimeter, there will be layers of security devices to protect assets located deeper inside the network.” This would ensure we are covering all bases to secure a WLAN to the fullest extent. This would include but not be limited to physical, logical/technical controls as well administrative controls whilst being applicable to both WLAN and mobile environments. MFA's, Password complexity requirements, the use of secure encrypted tunnels such as VPN's with the use of mobile devices, the use of secure protocols to access the website servers such as SSH and IPsec, and MDM’s to manage corporate data on BYOD devices if need be. The use of authorization and authentication using WPA2-PSK for a small business environment would be ideal as it would provide adequate security measures and ensure confidentiality through encryption while on the wireless network. As well as implementing security controls and preventive measures to maintain a security posture, the use of careful policy making should be established to ensure these security measures are being implemented across the board in a standardized and orderly manner that maintain consistency across the business. The California Customer Privacy Act (pp.149), ensures that personal data is protected and that the Integrity and confidentiality of the data is protected and not misused in any manner. This is important as it pertains directly to the Alliah business which is a social media provider and holds access to vast amounts of user account information. These regulatory standards must be held up to by law and the Alliah business would need to be held accountable for protecting this information through the use of adequate security measures placed throughout the business.

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

In a company like Alliah the means to implement a BYOD policy would greatly reduce costs and administration overhead and incorporate a more cooperative and collaborative environment. But in issuing such a policy we must take into consideration the risks of incorporating it. BYOD's must be highly secure with the intention of avoiding data loss and data integrity. The company should ensure basic security requirements are met like passwords and biometrics to gain access to such devices. The company must ensure they are using the latest up to date systems to patch any security vulnerabilities or threats. The use of company policies and training for employees on how to use their devices and prevent sensitive data from falling into the wrong hands is of the upmost importance as well as training on how to read and prevent common attacks like shoulder surfing and phishing attacks against company employees. The use of Enterprise Mobility Management as an overhead to implement updates and security settings for such devices should also be put into place so the company is able to issue such settings and security patches to ensure the safety of corporate data across the board. According to the NIST Special Publication 1800-22B of Mobile Device Security,“EMM’s can help BYOD deployments improve the security posture of the organization by providing a 655 baseline of controls to limit attack vectors and help protect enterprise information that is on a 656 personally owned device. EMMs can also provide an additional layer of separation between enterprise 657 data and personal data on a mobile device.” Implementing such an approach can improve the overall safety and security of users and corporate data alike.

F.  Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized

G.  Demonstrate professional communication in the content and presentation of your submission.

References:

*Selecting and Hardening Remote Access VPN Solutions*, media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI\_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF. Accessed 29 June 2023.

Doherty, Jim. “Chapter 4/ Security Threats Overview: Wired, Wireless, and Mobile .” *Wireless and Mobile Device Security*, Jones & Bartlett Learning, Burlington, MA, 2022, pp. 137–137.

Doherty, Jim. “Chapter 4/ Security Threats Overview: Wired, Wireless, and Mobile .” *Wireless and Mobile Device Security*, Jones & Bartlett Learning, Burlington, MA, 2022, pp. 149

*Mobile Device Security - NIST*, www.nccoe.nist.gov/sites/default/files/2022-11/mdse-nist-sp1800-22a-draft-2.pdf. Accessed 30 June 2023.