1. **WLAN Vulnerabilities**

A major concern for Alliah is the back patio area. The network may be protected by a firewall, but there was no mention of how employees are authenticated for network connection requests. It would be easy for a red hat to infiltrate the network this way. The WLAN is also vulnerable to wardriving, wireless sniffing, or evil twin attacks. It would be easy for an attacker to drive around and find that the network is not secure. It is not stated which encryption techniques are used for this network either. WPA or WPA2 should be used to secure the network as they have stronger encryption than other methods; WPA2 would be the most secure. The patio would be an insecure area where a red hat could set up an evil twin access point with the same name as the network router, especially because there appears to be no authentication method for requests.

Another major concern with the company network is that website servers are located 100 miles away from headquarters. There is no protection being used to connect to the servers which creates a major vulnerability to the network. The company should use a VPN to access the servers through an encrypted tunnel. A man in the middle attack would be easy to accomplish unless the company upgrades the security of the connection. This could cause catastrophic losses of data, proprietary information, or even customer information.

1. **Mobile Vulnerabilities**

There are 5 employees that constantly travel out of the office. These employees introduce two major vulnerabilities. The first vulnerability would be lost or stolen devices. It was not stated how employees log into the devices. If security practices are not being used this could lead to data loss for the company. It is also not stated if the devices are encrypted. Which could lead to data loss as well. If these devices were stolen, lost, or misplaced the company would be in jeopardy.

Also, since the workers are on the road 80% of the time, they are more than likely using hotspot connections which creates a second vulnerability. A red hat would be able to infiltrate devices and possibly the company network eventually through these devices. The lack of VPN would leave openings for MINTM or packet sniffing attacks.

1. **Mitigation**

The back patio, lack of encryption, and the lack of a VPN all need to be addressed. There are steps that can be taken to mitigate these issues. The back patio could be better protected by changing the default password; This would thwart any wardriving attempts and make the router harder to access. WPA2 encryption should be used to encrypt the network and offer the most up to date protection. In addition to this, configuration of the access point should restrict network access to unknown MAC addresses.

A VPN will reduce the likelihood of a MINTM attack or packet sniffing when remotely connecting to the webservers. The data of the company would be much safer when accessing this way as the VPN would deter red hats from exploiting company data.

BitLocker could be installed on to company devices to protect lost or stolen devices. BitLocker encrypts the entire hard drive of the device. It makes the device difficult to access without the passwords. A remote wipe feature also needs to be implemented within the company just in case devices are stolen or lost to protect the data and connections the devices may have.

The five employees that are always traveling also need to use a VPN when connecting to the network to protect against MINTHM attacks or packet sniffing while traveling and possibly using public or easily accessible Wi-Fi options.

1. **Preventative Measures**

Current regulations can be used to improve the company’s current security posture. The most important for this company would be Payment Card Industry Data Security Standard (PCI DSS). There are 6 objectives within this standard. The most important is to build and maintain a secure network. Since Alliah hosts a social media site, the company could secure all users across their platforms. This would show that Alliah is a reliable company that can protect its customers and users. The company would need a vulnerability management program also. By staying on top of and handling issues that may arise they can identify issues with their network and keep it safe. *(*(n.d.). Requirements and Security Assessment Procedures. Middlebury.)

It is also recommended that Alliah follow the Health Insurance Portability and Accountability Act (HIPAA). HIPPA relates to the protection of the CIA triad. HIPPA focuses on how identifiable health information is stored and transferred. This could create a larger customer base for Alliah as it shows that they are dedicated to protecting their users. ((n.d.). Requirements and Security Assessment Procedures. Middlebury.)

1. **Recommended BYOD Approach**

To improve to BYOD policy, Alliah should incorporate NIST SP 800-114r1. Hardening devices can lower the chances of an employee’s devices being used in a harmful manner. An example would be only installing known and trusted software in addition to antivirus protection. Exploitations can also be thwarted by having patch management in place. The company can also protect itself by requiring complex passwords, disabling unneeded features/services, and not allowing jailbroken devices on to the network. (Mobile Device Security: Bring Your Own Device (BYOD). NIST.)

**D. Sources**

(n.d.). Requirements and Security Assessment Procedures. Middlebury. Retrieved January 28, 2024, from https://www.middlebury.edu/sites/www.middlebury.edu/files/2021-07/PCI\_DSS\_v3-2-1.pdf?fv=Mfsuc4v9

(n.d.). Mobile Device Security: Bring Your Own Device (BYOD). NIST. Retrieved January 28, 2024, from https://csrc.nist.gov/pubs/sp/1800/22/final