
Western Governor's University

**Legal Issues in Information Security**

**C841**

**Kern Grant**

**IHP4 Task 2: Ethics and Cybersecurity**

# C844 Task 2: WLAN & MOBILE SECURITY PLAN

## A. WLAN Vulnerabilities

Two WLAN vulnerabilities that present risks for Alliah are wardriving Evil and its database distance. According to Alliah's scenario details, their work building position is an access point (AP) to provide a Wi-Fi signal to a back patio for employees' use. Alliah's wireless signal broadcasts outside their facility and is a gateway for bad actors to implement such vulnerabilities. The scenario does not give details of WLAN security protection. Their Wi-Fi may have basic security features like login and password, etc. However, I will treat their Wi-Fi network as insecure due to the lack of more information.

Alliah WLAN is vulnerable to a wardriving method attack. A bad actor can park their car within wireless signal range and hack into the Alliah network. Using the appropriate software, a hacker can identify Alliah's SSID and decrypt or crack the password of their wireless network. With access to the network, the actor can share their login detail, monitor, alter, or steal data from the Alliah network.

The second vulnerability is the distance of Alliah data storage. According to the scenario details, Alliah's headquarters and the data server are 100 miles apart. There are no details on how data is protected while being accessed from the data center. While I can assume security protocol like HTTPS is being used to access the data center, the best means to protect data in his scenario will be a Virtual Private Network (VPN), which neither is mentioned in the scenario. Using a VPN is the most secure way of tunneling all data/communicating of Allah.

## B. Mobile Vulnerabilities

The two mobile vulnerability risks to Alliah are stolen/lost devices and public Wi-Fi. According to the scenario, five employees usually work on the road. They also have company-issued smartphones, which will potentially be used to access company data. In addition, no details suggest Alliah using security measures to prevent or mitigate either vulnerability.

An employee's lost or stolen mobile device can be a bad actor gateway to accessing Alliah's sensitive data. Mobile devices provide business communication convenience for employees working on the road. Some work-related communications will include sending emails or accessing data from the Alliah network. Employees may use Public Wi-Fi sources from airports, restaurants, or

hotels for Internet connections. In such locations, bad actors are likely to perform man-in-the-middle (MitM) attacks to intercept network traffic or steal sensitive data because of the insecurity of such networks.

## C. WLAN & Mobile Vulnerability Mitigation

### WLAN

Allah should implement a two-layer approach to mitigate wardriving. First, turn off the Service Set Identifier (SSID) broadcast and deploy MAC filtering on the router configuration. Disabling Alliah SSID broadcast improves the privacy of their Wi-Fi name from the public or bad actors without a wireless network scanner. In addition to that security feature, I will implement MAC filtering. It allows the router to specify what devices can access the network. Their MAC address identifies each device to block or permit network access. Therefore, Alliah can have better security and control of who is using their network.

A Virtual Private Network (VPN) will mitigate security concerns to Alliah's data on the move between their data center and headquarters. VPN services like NordVPN or Google Cloud VPN are great options for Alliah's scenario and security needs. All devices that access the Alliah network must have the VPN platform installed and deployed. Therefore, any communication or connections

from employees to the data center will be tunneled, encrypted, and secured, which mitigates attacks like Man in the Middle.

## Mobile

Alliah mobile users' actions are critical for mitigating the impact of a stolen or lost device. Users misspacing mobile devices is inevitable. Therefore, Alliah should provide a documented company protocol for handling lost or stolen devices. These protocols should be consistently revised or updated as necessary. Additionally, mandatory training on responsive actions for lost or stolen mobile devices should be required. Protocols and training equip users with the best practices to mitigate lost or stolen mobile devices.

Secondly, Alliah should use a Virtual Privacy Network (VPN) to help mitigate Alliah's data from being monitored or stolen when using public Wi-Fi. A VPN is software that secures the communication between a server and a client. Installing VPN apps on all company-enabled devices will address public Wi-Fi vulnerability.

## D. WLAN & Mobile Preventative Measures

Alliah's best preventative measures for WLAN and mobile environments are necessary for current and future security posture. The Sarbanes-Oxley Act (SOX) and Payment Card Industry and Data Security Standard (PCI-DSS) will justify each measure. The Sox Act is a regulation framework for public companies. The practice of safeguarding Information Security is mandatory for compliance. The Sox Act applies to Alliah because it plans to take the company public. PCI-DSS is regulatory compliance for protecting cardholder data. The PCI-DSS applies to Alliah because of the crowd-funded campaign that funded Alliah, and the nature of their business suggests using credit cards for payment. The following WLAN and mobile environment measures will justify Alliah's information security posture according to industry regulations.

Deploying an Enterprise Wi-Fi auditing tool is a preventive measure Allah can take to maintain the security posture of WLAN. One specific tool recommended by (Doherty, 2021, PP. 314-315) is the AirMagnet Wi-Fi analyzer by NetAlly. It monitors and manages all 802.11 wireless network standards and reports network performance, vulnerability, and known security issues. AirMagnet

also generates reports for company audits. Deploying this tool and having regular audits provide excellent information security measures that justify SOX regulatory compliance.

Alliah may have little control over stopping a user's device from being stolen or lost. However, they can reduce the likelihood of it and prevent the mobile device from being the gateway to a data breach. Maintaining an excellent security posture requires user education and software to protect mobile devices. Alliah's user education and training should be a mandatory policy. It should cover some topics: the impact of cybersecurity and data breaches, how devices can be the gateway to data breaches, device location features, safeguarding their devices, etc.
The knowledge employees gain will increase their awareness of mobile device safety. In addition, Alliah should implement Mobile Device Management (MDM). The software allows the IT team to manage/monitor all mobile devices connected to the Alliah network. Features include device authentication access, software updates, tracking, and data wiping. Device authentication is necessary for protecting devices with data like company credit cards that employees may use for business purchases. Device updates provide new system patches for bugs and crashes. Tracking a device may allow a user who temporarily misplaces their

device to locate it before it gets into the hands of a bad actor. The data wipe, and device authentication feature prevents a mobile device in the hands of a bad actor from gaining access to the device or using it as the gateway data and network. The six PCI-DSS objectives, according to (Doherty, 2021, PP. 147-148), are "Build and maintain a secure network, Protect cardholders, Maintain a vulnerability management program, implement strong access control measures, Regularly monitor and test networks, and Maintain an information security policy." Alliah preventative measures align with these objectives for maintaining a security posture for our mobile environments.

## E. BYOD Approach

According to (IBM, 2023), compliance is the act of adhering to the financial reporting, information security, and auditing requirements of the Sarbanes-Oxley Act (SOX Act), a U.S. law that aims to prevent corporate fraud." Alliah aspires to take the company public, so the SOX Act applies. Therefore, they should consider SOX compliance when deciding on a device policy that affects information security. The two options are, Bring Your Own Device (BYOD) or a company-owned device. Restricting the network to company-owned devices is the best security approach to safeguarding Alliha data. The privacy, data safety, and data management security aspects are better than the BYOD policy. Comparing

both options with the deployment of tools like (Mobile Device Management) MDM, and user education, BYOD presents the most information security risk. BYOD mobiles with Alliah deploying MDM tracking and monitoring features can cause privacy issues with personal use. In addition, the policy regulations may be able to restrict who accesses their business data but cannot limit the device's users. Therefore, any user of that device can potentially cause a data breach, willingly or unwillingly. BYOD management of devices will require segregating personnel and business data to prevent mixing or removing the wrong files during a remote wipe. Regarding better security and less complication, it is best to separate business from personal use. As Allah works on safeguarding information security, restricting the network to company-owned devices will provide Allah the best posture for making them SOX compliant.

# References

Doherty, J. (2021). *Wireless and Mobile Device Security*. Proquest Ebook Central. https://ebookcentral.proquest.com/lib/westerngovernors-ebooks/reader.action?docID=6461875&ppg=1

IBM , I. (2023). *What is Sox (sarbanes-oxley act) compliance ?* https://www.ibm.com/topics/sox-compliance