As wireless and mobile technologies continue to grow in presence and popularity, the world is becoming more and more connected. Unfortunately, this also means that devices and networks are becoming more and more vulnerable to outside threats. Businesses must identify and mitigate these vulnerabilities and threats in order to protect employees’ personal information and ensure the organization is secure from passive leaking of proprietary information.

In this task you will assume the role of an IT professional who is responsible for identifying wireless and mobile vulnerabilities, as outlined in the scenario below. You will then present your findings and recommend solutions to mitigate these risks and prevent future threats.

SCENARIO

You are a network professional on the IT team at Alliah Company, a new but fast-growing social media provider. One year ago, Alliah launched a social media website aimed at young professionals. The company also released a mobile app for accessing the site from cellular devices. Alliah was able to launch its website with money generated by a crowd-funded campaign, but most of the funds were spent on the site and app development, with relatively little money (and time) devoted to the internal office network infrastructure.

Alliah has 35 full-time employees, all of whom have offices or shared work spaces in a three-story building that serves as the company headquarters. The building is an old warehouse that was converted for office use and is approximately 10,000 square feet. Currently, the employees occupy only two floors; the third floor is vacant and available for expansion.

The Alliah WLAN has a gigabit managed switch, a multiservice wireless LAN controller, and seven wireless access points strategically located to provide coverage to office staff. One access point services a large back patio area for employee use. The network is protected by a firewall. The Alliah website servers are located in a data center 100 miles from Alliah headquarters.

Five employees are account representatives who are on the road at least 80 percent of the time, and each rep has a company-issued laptop, tablet, and smartphone. They use a large, shared office in the headquarters building when they are not traveling.

Employees use company-owned computers that connect to the WLAN, and, in an effort to control costs during the launch, Alliah has a bring your own device (BYOD) policy.

The IT staff consists of five employees; three are devoted to website maintenance, one manages the headquarters’ computers and network, and another employee assists with the website and the office network. IT staff uses wired Ethernet connections to remotely access the website servers.

The Alliah website is successful, attracting more and more visitors each month. Jennifer, the CEO, anticipates hiring more employees and is considering a strategy that would take the company public within a few years. In preparation, she wants to ensure that Alliah’s wireless networking infrastructure is highly secure, especially because it may need to grow quickly in a short period of time, and she wants to understand the security risks the company faces. She also wants to decide if Alliah should continue allowing BYOD or restrict network access to company-owned devices only, or if a compromise solution is available.