**A.** The first vulnerability is that there are too many access points on the network. This is bad because it makes the network more at risk of an evil twin attack. An evil twin attack is when an attacker makes a network with the same name as the legitimate network to intercept traffic. The second vulnerability is that there is an access point on the outside of the building, more specifically in the patio. This could cause problems because an attacker could access the network being farther away from the building where physical security measures could be taken like a car for example.

**B.** The first mobile vulnerability would be the BYOD policy. BYOD is tricky because of the wide variety of hardware and software of mobile devices making it hard to optimize for each device. BYOD also makes it harder to push out timely updates to patch security vulnerabilities. The second mobile vulnerability is the high number of devices they give to employees. Each device basically increases the risk of an attack. Devices could be lost or stolen as well.

**C.** The first WLAN vulnerability that may be addressed is the creation of evil twin access points by attackers, which can be detected by a wireless intrusion prevention system (WLAN). IT staff members should routinely check the networks that are reachable within the confines of their establishment to ensure that there are only legitimate access points available. Reducing the access point's broadcast strength or restricting its accessibility to the patio itself are two ways to stop WLAN vulnerabilities associated with the Patio access point. Using mac filtering is another way to prevent hackers from accessing the network, but it can be difficult if two-factor authentication, a captive portal, or a BYOD policy are in place. In order to prevent malicious access and signal overlap from nearby wifi signals outside of your company, your organization should be implementing a basic level of security, as advised by NIST, after analyzing networks for potential threats. This analysis should include scanning wireless networks to create a heat map of the signals to ensure they remain inside the building. They must double check a number of things with the utilized gadgets in order to reduce the risk that comes with BYOD. To start, all BYOD devices need to be password protected in order to restrict easy access to any important data they may contain. The next step is to set permissions for the network resources that each user's device is allowed to access. Additionally, apps that are permitted on devices must be added to a blacklist, otherwise, those programs may have backdoors that provide hackers easy access.I would advise deleting at least one gadget from each of the five traveling employees who each have three. The majority of modern tablets' features, if not all of them, come from laptops, and they can be equipped with Bluetooth keyboards to make using the device easier for writing reports and other documents. I would suggest taking away each of these five employees' laptops or tablets, at the very least. To guarantee they have all security updates implemented, their devices also need to be enabled for auto updates and password protection. An MDM solution, specifically designed for these kinds of devices, should already be in place to handle all of this.

**D.** I would make sure that the principles of Authentication, Authorization, and Accountability (AAA) are adhered to rigorously. This will ensure that only those with the right credentials may access the information they require and help prevent unwanted access. This will help the company obtain SOX compliance if they go public as anticipated in the future. It is imperative to ensure that the network undergoes regular analysis as it evolves and changes in order to pinpoint any necessary modifications. NIST 1800-22 (Draft) states that MDM features can be deployed to BYOD mobile devices on the network by employing EMM to secure them.

**E.** To make the BYOD function in a secure manner we would need many things. Firewall and content blocker for the browser would be a good start because employees would need to browse the web. We would need an acceptable use policy to outline what the employee can do with the device and the data in the device. An example could be that the employee can’t download apps that are not on the app store. We could also implement multi factor authentication to the device and biometrics if the device supports it. We could implement a VPN so that the data is not subject to a man in the middle attack on an unsecure network. We could have the data on said devices be encrypted as well with a key. To add to the policy we could make it mandatory to keep the device up to date every week. Publication NIST SP 800-114 would be a good guideline for the company to follow for guidelines on securing BYOD devices.

**F.**

Souppaya, M. (2016, July). *User’s Guide to telework and bring your own device (BYOD ...* nvlpubs.nist.gov. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf

Yasar, K., & Chouffani, R. (2024, January 23). *What is BYOD (bring your own device)?: Definition from TechTarget*. WhatIs. https://www.techtarget.com/whatis/definition/BYOD-bring-your-own-device