RISK ASSESSMENT 3

Omar Salih
Stu#: 12285240

Security Issues that may pose a threat:

1. First and foremost is a open door into the companies data.
    a. No way of monitoring the BOYB's without upgrading the system and adding new controls
        i. Upgrading the system will mean, Buying and Spending for new protocols to be installs
        ii. Need to pay for new licenses for the phones, tablets, computers, etc
    b. Biggest issue is legal.
        i. When there is data spillage onto private BYOB device, who pays to destroy the phone
            1. Do you get to keep your phone number if it has to get destroyed
    c. What rights do you have to give up when you agree to a governmental BYOD policy?
        i. Such issues must be spelled out in a policy
            1. If no policy
                a. Employees might be reluctant to store data on their private devices
2. HOW TO FIX IT
    a. Containerization Solutions
        i. Can segment the government data from the rest of the phone
            1. Samsung Knox
            2. Good Secure EMM Suites
    b. Hypori
        i. Uses virtualized app technology to access sensitive information without actually storing it on the device.
    c. Some agencies are
        i. Issue new guidelines that set boundaries
        ii. Tell employees what they are allowed to do with sensitive information
        iii. Tell employees how to access work email on their personal devices.

1. NASA applied new security requirements to the Employees Microsoft ‘s Exchange ActiveSync in order for the Employees to access the agency’s email using their BYOD devices.

2. NASA states that their, “NASA’s mobility vision program is to provide secure seamless access and share authorized information and services while protecting sensitive data, anyplace, anytime, using any device.”

3. The BYOD is voluntary.

4. NASA will not compensate employees for the costs associated with using their personal devices for work.

5. Participating employees must

    a. Use lockout code protection

    b. Keep their devices up-to-date with the security patches

3. WHAT ARE THE COMPANY gains/losses FOR USING BYOD

    a. Agencies save the cost of buying devices

        i. The endeavor is hardly cost-free

    b. "It saves money if you replace a company phone, but it's not a cost of zero," Suder said.

    c. “You still have the licensing fees from mobile device management, the company doing the containerization and any costs that come from additional security measures."

4. BYOD or NO BYOD

    a. IT leaders ponder whether or not to embrace BYOD

        i. if so

            1. how to craft a policy

                a. BYOD doesn't make sense for every agency

                b. BYOD is not for every agency in the government. Due to the fact that employees are creating their own shadow networks, means that all agencies need to

have some form of BYOD policy that explicitly states the expectations of the agency towards what they expect from their employees.

5. Hancher, who helps federal agencies craft BYOD policies, has a three-part test that should serve as the foundation for any BYOD initiative:

    a. A "yes" answer to any one of those questions can complicate the task of crafting a workable approach, Hancher said.
        i. Does your agency deal with classified data?

        ii. Do you have sensitive personally identifiable information? This is usually less secure than classified information but can include important details such as Social Security numbers.

        iii. Does your agency, as part of its mission, handle information critical to the infrastructure of the country? This could include data about the energy grid, water sources or other information that terrorist organizations would deem valuable.

Brief summary after reading several sources (PARAGRAPH LONG = Links to sources)

Determine what the impacts of the issues will have on security

What does the story mean to us right now? Point out assets, applications, business process, etc that are implicated Describe the risk, the business impact. Be realistic and measured not ever vulnerability possess an existential threat to the organization (paragraph long)

Outline the steps we should take in the short term. (Paragraph) What controls can we realistically put in place to reduce our risk today? {Paragraph)

Outline the long-term fix for the issue. What we need to plan for in the future to make sure we have an effective, sustainable, scalable control in place for this? In some cases, you may not need to, or be able to, implement a BIG FIX. The short term mitigation might be your permanent fix. That's OK, as long as you can support that assessment.