Brooks Vasconcellos Unit 2 Homework

**Step 1: Measure and Set Goals**

1. Identify at least 3 potential attacks that can be carried out:
   1. Malware – personal devices particularly mobile devices are more susceptible to malware attacks from something as simple as a malicious app that can infect the company’s intranet with ransomware.
   2. Hacking – personal devices often lack strong, or even updated, data encryption leaving the company’s intranet vulnerable to inherent security risks. One example being an employee connecting to a free or public Wi-Fi Hot Spot that leaves them vulnerable to a man in the middle or snooping attack, potentially granting access to the company’s system.
   3. Physical Attack – the loss or theft of an employee’s personal device with sensitive business information can potentially fall into the wrong hands allowing someone to gain access to valuable company data or even access to the company’s systems.
2. Based on the above scenario, what is the preferred employee behavior?

The preferred employee behavior is that employees take additional care with the personal device that they choose to use for work purposes. Care in what programs they install, how they connect to the internet, and the physical wellbeing of the device.

1. What methods would you use to measure how often employees are currently not behaving according to the preferred behavior?

One method is to send out a survey to all employee’s allowed to access the company’s systems via their personal devices and ask them a series of basic security questions to ascertain how often people use their device in an unsecure manner.

1. What is the goal that you would like the organization to reach regarding this behavior?

The goal to reach is 100% compliance on any personal device set up for company access must have at minimum an MDM program installed.

**Step 2: Involve the Right People**

* Chief Executive Officer – The CEO will be responsible for the final decision on the companies BYOD policy after assessing the risks, determining what his ultimate goals and expectations are for the program, the message that he wishes to be delivered to the employees, and what consequences would result if the policy were not followed.
* Chief Operating Officer – The COO will work with the day-to-day process of rolling out the program to enact the CEO’s vision. Setting expectations with Department heads and HR.
* Chief Financial Officer – The CFO will monitor the budget for the BYOD program and monitor to see the financial impact of the program to see if the benefit outweighs the cost.
* Chief Information Officer – The CIO will be responsible for developing the IT systems required for BYOD program such as the MRM program, dual authentication, provisioning a VPN service, registering employee’s devices, monitoring for loss devices or employee terminations.
* Chief Information Security Officer – The CISO will be responsible for developing and disseminating the training for the BYOD program. They will work with the CIO to coordinate and implement security policies.

**Step 3: Training Plan**

1. How frequently will you run training? What format will it take?

The training will be run online via a training program developed to go over the BYOD program. The training will be required for anybody who chooses to partake in the BYOD program, with requirements to take the class any and every time they change the device that they choose to use. Training from that point on will be required on an annual basis.

1. What topics will you cover in your training and why?
   1. Appropriate Use – specify when and how employees can use their devices in relation to work. List which programs they can use to access and work on company documents and the system. Detail what programs or uses that are not permitted.
   2. Acceptable Devices – State which devices are permitted for use in the BYOD program. Outline which operating systems and device models are compatible with the programs and apps that are required for business use. Also, what programs may need to be installed or uninstalled for security reasons such as an MDM program.
   3. Registration – what devices the employee chooses to use for the BYOD program must be registered with the support of a MDM. (Login, Password, Authentication Code, VPN setup, etc)
   4. Tracking – Monitoring the usage will provide security input similar to IDS.
   5. Revocation – the use of BYOD is at the discretion of the company to revoke due to termination or violation.
2. After you have run your training how will you measure its effectiveness?

Monitor the usage of BYOD by way of the installed MRM and monitor outside access to the company’s intranet. Monitor the productivity of the employees participating in the program and determine the ongoing financial viability of program.

**Bonus: Other Solutions**

Two other possible solutions for the BYOD program would be the required use of dual authentication and MRM programs.

Dual authentication would be a technical control and the MRM would be both an administrative and technical control.

The dual authentication is a preventive and deterrent goal. The MRM would be preventative and if necessary, corrective goal.

Dual authentication provides a more secure log in access and the MRM would be a fail safe in case of loss, theft, or employee termination.

One disadvantage for Dual Authentication would be the time required to log in every time, where as MRM could affect employee satisfaction due to the control it places on their personal device.