Unit 2 Homework

**Step 1: Measure and Set Goals**

1. Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.

* **BYOD devices are highly susceptible to data theft opportunities specifically when assessing business data through unsecure Wi-Fi such as in a Starbucks or airport.**
* **Device loss or theft could result in a isolated incident or breach resulting in company data being leaked or infiltrated**
* **Malware infection from other apps or documents the user has downloaded on their personal device could be uploaded into company documents or systems.**

1. Based on the above scenario, what is the preferred employee behavior?

**Depending on the company or organization the preferred employee behavior could be as extreme as never being able to access company files without being on company provided equipment. Or the company could only have a certain amount of information be reached outside of work on personal devices. Such as for my old employer we could only access personal information like paychecks or time-off information through personal devices as a base employee. It all depends on the risk of assets to the organization and how they route their server activity.**

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

**I would offer several routes to measure this. The first would be a simple survey to measure the level of education employees have on security. There could also be a tracking system on types of devices and areas in which employees log in. I would also do periodic tests such as sending phishing emails with attachments to see how many employees took the bait.**

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

**For the survey, my goal would be to have only 0%-1% of failures to account for margarine of error. For the tracking system depending on the organization the margin for error could be 0%-20% of log in’s on devices not company provided depending on the information and the level of risk for the asset. Lastly for the phishing emails the preferred goal would be to have 0% to ensure company CIA.**

**Step 2: Involve the Right People**

Now that you have a goal in mind, who needs to be involved?

* **CEO, CFO**, etc. (Top roles in the company): These individuals are at the head of the company overseeing everything. Security needs to be of top-down importance to everyone in the company. These individuals often have access to everything within the organization especially key assets of data. They need to be diligent that nothing they do endangers the company.
* **HR:** These individuals have access to all employee information. It’s integral that all of this information stays sealed for corporate security and to avoid legal action. If any of this information gets out it will tarnish the integrity of the company.
* **CISO, SOC,** etc: This department oversees cybersecurity for the company. They need to ensure all assets are safe while also preventing any cyber-attacks to ensure business can run as usual.
* **Management** (district managers, General managers, etc.): This group manages the front-line workers of the company. They often have access to information from all departments but at a lower level. They not only have to run the company but also have to perform a lot of back-end duties.
* **Base level employee:** This group generally has the lowest level of access but has the highest chance of endangering the company whether through miseducation or improper training. Although they don’t have admin access, they pose the danger of letting in malicious content. The key to these employees is education first.

**Step 3: Training Plan**

Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:

**Training should be run monthly if results aren’t being met but generally should be run quarterly unless additional information has come forward. Surveys should be given out monthly and/or quarterly depending on results discovered. Online should be sufficient but in cases it’s not an in person formal training should be done. An example would be: if an employee fails two surveys, they should attend an in-person training for additional help. When new policies are being implemented and in person training should be held to ensure all questions are addressed.**

**In training both physical and cyber security should be addressed. There should also be given examples of what happens if protocol is not being followed to show the employee what “could” happen and how it would affect the organization. After training has been conducted there should still be annual (monthly to quarterly as needed) surveys given out and random phishing and malicious software given out and reported. For higher asset scenarios monthly training should be advised.**

**Bonus: Other Solutions**

Training alone often isn't the entire solution to a security concern.

* Indicate at least two other potential solutions. For each one, indicate the following:
  + What type of control is it? Administrative, technical, or physical?

**The control based on the above situations are all of the above. Physical security, administrative security and IT security. Physical security including building access, server protection and equipment protection. Administration should be diligent in showing a good example to the other employees by following protocol and teaching other departments. IT needs to bring concerns to the table and ensure safety to business can run as usual.**

* + What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

**Control should have preventative measures put in place such as layering to deter further attacking once one layer is breached. There should also be a set plan for if anything is breached (to any degree) on how to handle the situation so everyone is properly prepared.**

* + What is one advantage of each solution?

**The advantages to these solutions ensure that security is a top-down priority for the entire organization. This not only teaches preventable measures but also ensures if a breach occurs everyone is prepared on what to do to stop the attack from progressing further.**

* + What is one disadvantage of each solution?

**All of this training takes time and resources (money and man hours). As discussed in class each organization has a set amount their willing to spend on any IT issues that may arise. Tackling the most important breach able area first is important so that safety of the most valuable assets are ensured**