Week 2 Homework: Assessing Security Culture

Step 1: Measure and Set Goals

1. Three potential attacks that can be carried out by allowing employees to access work information on their devices are data theft, stolen devices, and finally Malware

* Data Theft - can happen when unchecked usage of personal devices are used with sensitive information on them. If an account they have for personal use is hacked, it could ultimately end up exposing corporate data and confidential information.
* Stolen Devices - If an employee's device is stolen, the best-case scenario is that this is an inconvenience. But in the worst-case scenario, you’re dealing with a complete disaster. For instance, the employee might be storing their passwords; both personal and corporate; in an unsecured notes application, which would make it easy for someone who acquires the device to hack corporate accounts.
* Malware - If employees download various types of information and files using personal devices like PDFs, Apps, and videos this can lead to security risks. For example, an employee might download a game to their mobile device that carries a hidden virus or malware. This malware could then be passed onto the company network when the employee next logs in from the infected device.

1. The preferred employee behavior when it comes to using personal devices for company work is to get all employees to stop or when using a personal device to be on the company VPN.
2. First, the company should start with a baseline on where they are at with employees using a personal device to see how many do it regularly. Conducting a survey would be the easy way to go about this.
3. SilverCorp should work to get personal device usage down to 5% or lower by one year, halving the total number of employees who use their devices each quarter.

Step 2: Involve the Right People

1. Five employees or departments that need to be involved are.

* Cyber Security team - They are the department that will be dealing with the security of the information at risk. They need to make sure that the plan put in place will prevent company information from being hacked.
* IT Department - IT Department would be the hand and feet so to speak of the Cyber Security team in the situation. They are to help inform and show the best way of going about training. The ones training HR Department.
* HR Department - Human Resources are the ones who would be actual train the vast majority of the company. Show them best practices and keep employees up to date on their training in these criteria
* Finance Department - Finance Department is in control of how fast these training and practices can be rolled out. Since they are the ones in charge of the money.

* CISO (Cheif Information Security Officer) - CISO would be the person overseeing all this to make sure it goes smoothly and the department gets what they need. They are also the ones who would inform the CEO of the progress of the training and how far had or behind they are in their goal.

Step 3: Training Plan

1. The train should run every quarter and be a mix of in-person and online classes. The training should go over the risk of personal devices for work along with how employees should stop or mitigate their activity on their devices for work. After each quarter the IT and Cyber Security Department should look at what department as a whole kept having a security issue along with which individual employees were not securing their devices. This will give a good estimate of who needs to go through further training and who doesn't.

Bonus: Other Solutions

1. Company VPN - would also be a solution for personal devices for work. This is an example of technical control where using technology to help prevent security incidents. This is also a preventive control in that it is used in the hope that it will prevent attacks from occurring. One plus of this solution is that it does not cost a large amount of money to implement. One negative would be you would need employees to monitor the VPN in case of crashes and glitches in the server.
2. Company-provided devices for high-risk employees - would also be a solution for personal devices for work. This is an example of physical control because the company would be providing devices to us instead of relying on the device of the employees. This is also a preventive control in the hope that it stops employees' devices from being used for work. One plus of this is if the device is stolen or lost the company can then immediately whip anything on the phone remotely that would be sensitive for others to see. One negative would be the cost of providing phones, laptops, and internet/cellular service for these employees.