Assessing Security Culture

Step 1: Measure and Set Goals

1. A) Data Theft commonly occurs due to lost or stolen devices. Passwords may not be secure enough on their personal device giving hackers access to the company's information.

B) Malware can be unknowingly downloaded via a game on their phone or personal email PDF attachment. The company's security could then be compromised next time they log into the network.

C) Hacking is a possibility of using personal devices for work. Personal devices tend to not have the encryption that the company may have and users typically do not update software on their devices regularly.

1. If employees at SilverCorp are using personal devices for anything work-related, they must adhere by the BYOD protocol. All employees must have a Mobile Device Management (MDM) or Mobile Access Management (MAM) tool installed on their device to be able to remotely access and wipe phones, track devices if lost or stolen, and separate personal and company data.
2. SilverCorp could measure this by scanning the access logs to cross reference what devices are accessing the system and have the Management software installed on the devices.
3. The goal of SilverCorp is to have ALL employees have the software installed on the devices in order to access information.

Step 2: Involve the Right People

1) Product Owner would be needed to ensure execution of the Puppet installation or MDM software across all devices. They would also coordinate with everyone the install and writing of the program.

2) Dev ops team would be needed to write the program. They would also hand off or insert the package into the puppet program.

3) Security analysts would be required to monitor traffic on the network. They would ensure follow up of BYOD devices on the network having the Management software installed.

4) Firewall team would be needed to grant access to the Mobile management software.

5) Security developers would need to deploy the puppet program and ensure proper execution of the software and accessibility.

Step 3: Training Plan

The format of the training will be composed of online learning. More specific topics will be targeted with remote online learning courses. Every new employee who joins the company will have to complete the courses as a mandatory requirement with their initial onboarding. Some training courses will be broad based creating general awareness, others will be targeted by specific areas of vulnerability as outlined below. The general courses will be repeated every year. Specific topic courses will be available every 6 months with updated data.

The employees will take courses to create awareness on specific categories of cybersecurity attacks including but not limited to:

A) Phishing scams to teach not to click on unsecured links and not to give out password.

B) Online training with the installation of anti-malware software on the employee's personal devices

C) The training will go over 2 factor authentication and a tutorial on set up and usage.

D) usb drive encryption and not installing unknown devices into company computers or network. If a USB drive is found where to turn it in to ensure the drive is not inserted into a computer for potential intrusion into the network and system.

E) The training will also include information regarding the alternatives to using personal devices at work such as remote desktop connection, working on the server that is protected against a firewall rather than personal computer for any data related activity. Using encrypted USBs issued by the company rather than the external USBs.

F) Adopting common sense measures including logging out before leaving a computer, limiting access to confidential information on a need-to-know basis. Not disclosing protected information on social media. Reporting incidents of potential data breaches, lost or stolen laptop

The training will be effectively measured by random email test, network monitoring, USB drops and employee engagement surveys.