Week 2 Homework: Assessing Security Culture

By: Ben Qualey

1/10/2021

Step 1: Measure and Set Goals

1. Stolen Credentials, Phishing, Malware, Stolen Data and Information Leaks

2. In an ideal situation employees would not be using work-related applications or work accounts on their personal devices. Instead, all of this activity would be done on work devices that can be serviced and monitored by the company.

3.Keep logs to see what devices and profiles are connecting to the business accounts and applications.

4. I would like for the organization to implement a BYOD (Bring Your Own Device) data management policy, to harden its protection against potential attacks in regards to employees using personal devices for work. The policy could include things like: requiring strong passwords, multi-factor authentication, increasing funding for a work device program or even investing in a virtual desktop infrastructure to manage potential risks. To get funding and approval for a policy update I would need to collect solid metrics that show training may not be enough to remedy the situation and present that information to the correct people.

Step 2: Involve the Right People

With the end goal of getting a successful policy in place I will have to navigate various parts of the organization and ultimately cultivate a policy and plan to get the CEO and C-Suite executives to sign off on.

CISO (Chief Information Security Officer) This is the main person I will be dealing with, and the initial training would come from within their department. They would be responsible for overseeing what would be included in the training and possible policy should it be deemed necessary.

CIO (Chief Information Officer): I would need to work with the CIO in order to collect the log and device data required to prove the need for the organization to require staff training and a potential new policy. They would also be pivotal in facilitating any technological solutions should they be required to remedy the situation.

COO (Chief Operating Officer): the training would need to approved by the COO to make sure that the employees are scheduled accordingly and have the proper availability to attend the training.

CFO (Chief Financial Officer): I would have to get approval by the CFO to make sure the training is funded, and that the potential of having occupied employees for a period of time is understood and accounted for.

CEO (Chief Executive Officer): They would have to agree that security was an issue in regards to the current device policy and see the need for training to secure the organizations sensitive data.

Step 3: Training Plan

The training policy that I would recommend would come in two-parts.

1: A rotating Quarterly classroom training sessions for 25% of the staff each quarter, with the goal of the entire staff having received some form of training by the year end.

2.Monthly / Weekly reminders of security issues and “best-practices”, with a goal of fostering a security culture mindset within the organization.

In the training I would try to bring focus on the main issues that are present within the cyber-security landscape and how it relates to the company. Since one of the main issues with the company is the use of personal devices for business purposes, I would go over the most common attacks, and walkthrough situations where using a personal device would make it much easier for the attackers. I would contrast the ease of the attack on personal devices to the security strategies the organization has for their devices.

I think opening discussion on why employees need to use their personal devices for work would be critical for progressing within the organization and making sure that there is mutual understanding of the danger of such activities. Transparency would be a critical factor in finding a solution for this and making sure that the employees are not feeling attacked for their workflow.

I would most likely end with training on best practices for accessing the company data in a safe and secure manner.

After the training, continued monitoring of hardware that accesses business accounts and applications would be the measure of effectiveness. If the rate of personal devices accessing the data goes down after the training, that would be considered a success. If this metric remains unchanged, that information could then be used as a way to secure funding and approval for an updated BYOD data management policy.

Step 4: Other Solutions

-Mandate a work device program and only allow work devices in regards to business

-Technical, Physical controls

-Preventative, and Corrective

-Secures the data on the company devices

-Cost prohibitive, may incur productivity loss.

-register personal devices if used in a working capacity and manage read/write privileges for sensitive data

-Technical Control

-Deterrent, preventative and detective

-Cost effective and relatively transparent

-Not the most secure option