**Week 2 Homework: Assessing Security Culture**

This week we learned about security culture and how to promote it within organizations.

It’s important that all employees are aware of common security risks and treat security seriously. The majority of cyberattacks aim to exploit human weaknesses with methods like phishing.

For this reason, people are most often the weakest link in an organization’s security defenses.

**Scenario**

* Employees at SilverCorp are increasingly using their own personal devices for company work.
* Specifically, over half of all employees check their work email and communications via Slack on their personal mobile phones.
* Another 25% of employees are doing other work-related activities using work accounts and work-related applications on their personal phone.
* Allowing sensitive work information to be shared on employees’ personal devices has a number of security implications.
* You must research these security risks and use the security culture framework to develop a plan to mitigate the concerns.

**Instructions**

Compose the answers to the following four steps in a Google Doc.

**Step 1: Measure and Set Goals**

Answer the following questions:

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.
   * Worms - malware that copies itself to spread from computer to computer without any human interaction and it doesn’t have to attach itself to a software program to cause damage.
   * Phishing - Emails that are sent out to target an individual/company, based on the more access they have are more likely to be attacked, that try to get victims to reveal passwords and other personal information like credit cards to hurt the company.
   * Malware - attacks using software variants including; viruses, ransomware, and spyware made by attackers to harm and damage data and systems or to gain access to a network.
2. Based on the above scenario, what is the preferred employee behavior?
   * For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.
     1. Based on the above scenarios, for worms, would be to focus on using anti-malware and also by teaching your employees not to download anything that will download itself onto the hard drive and make changes to the device(s).
     2. For phishing, there are a lot of scenarios that can affect the company. But the main thing is to add a “Phishing” button on the top of emails if employees don’t know who the email came from or if there are spelling errors they can click that button and the IT department can look at it and no further action is required from them. The other behavior they can have is to just not open the email if they don’t recognize the name. For instance I get a lot of “[iCloud] Update Needed” titled emails in the subject line. I just delete them right away.
     3. For malware, similar to the worm scenario, I would get precautions put into place like getting an anti-malware program set up on the devices, and also remind them about not downloading anything that will affect the hard drive or make changes to the device(s) and to always look into suspicious emails.
3. What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?
   * For example, conduct a survey to see how often people download email attachments from unknown senders.
     1. I would send out a survey to their company email and get the results back and based upon their answers I would look into what areas we need to improve. Whether it be downloading content, losing their personal device, or not having the proper safety measures in place on their device(s).
4. What is the goal that you would like the organization to reach regarding this behavior?
   * For example, to have less than 5% of employees downloading suspicious email attachments.
   * The goal would be to have ZERO employees downloading suspicious email attachments each month. To better quantify that would be to have write ups given to employees, and if there is 2% or less employees getting write ups each month that will be a success. If we have a month where it is over 2% then at the end of that quarter we will have a training session for all employees in each department if there was a breach.

**Step 2: Involve the Right People**

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

* Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.
* CEO - This individual will be in charge of being at each training session to say a few words at the beginning to let his employees know that the training they are going through is important to him and the upkeep of the company so they can stay successful. Employees will pay attention to things if the CEO of their company comes by and says that a session they are going through is important.
* HR - If there is a breach and we need to terminate an employee, we need to have HR present during each confrontation with the victim(s)/individual(s) to make sure we go through the termination process correctly and we don’t do anything unlawful.
* IT - This department is required to train, inform, and answer any questions on how to stop breaches. They will also be in charge of mitigating any risks that happen on a daily basis whether it is from hackers, phishing schemes, or malware downloads.
* Security Department - This department is required to be the brute force for the company. They will be there to escort the employee out the door so they can’t get any unwanted access to other areas in the building while leaving after being terminated.
* COO - This individual is required to get each department set up for a training time whenever there is a need for it, and to also be in charge of making sure that the operations don’t fall during the training period.

**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:

<https://www.travelers.com/resources/cyber-security/cyber-security-training-for-employees>

Governance and Compliance pdf from class is another source.

* How frequently will you run training? What format will it take? (i.e. in-person, online, a combination of both)
* What topics will you cover in your training and why? (This should be the bulk of the deliverable.)
* After you’ve run your training, how will you measure its effectiveness?

This portion will require additional outside research on the topic so that you can lay out a clear and thorough training agenda.

Date: 1/4/2021

Author: Taylor Kadrlik

At SilverCorp we have goals set in place to be better at our security. With the current state of the world and the fact that some of our employees work from home and use their personal devices; our training and ability to understand the threats that can affect us are prevalent to keeping us safe. Within reading this document you will understand the multiple factors that we are going to focus on during the workday to keep our information, network, and employees safe and then how to take corrective action to facilitate a dependable work environment.

We will be having training every quarter of the year to make sure that all our employees are knowledgeable about the different threats that pertain to everyone on the campus. The training will be a combination of in person and online sessions. Everyone learns at a different pace and in different ways, to ensure everyone learns all that we are asking of them, we will have multiple choice questions, short answers, and true and false questions after a video when we do online seminars. You will be able to re-watch the video if you have any hesitation on answering a question. The video will go from start to finish and you must watch it all over again, be sure to pay attention the first time. Our goal for this test and training is to get everyone to score a 85%-100% on the questions. The topics throughout these training seminars will cover; different phishing techniques, external files that could hurt the network or computers from being clicked on by social media or email links, proper way to access our VPN (Virtual Private Network) and RDP (Remote Desktop Protocol) to access your files and documents, and lastly proper password generating techniques.

Our goal is to have zero external files downloaded each year and 98% or higher phishing emails reported by employees. Seeing how a lot of us are going to be at home working, we must understand these threats and to learn how to recognize and mitigate them.

The VPN and RDP logins will be monitored to ensure protection from threats. The password and username combination must meet the requirements like listed above or the log-in process will not work. Each month there will be phishing emails sent out to your work email and if you don’t report the phishing email we are going to require you to go to a training seminar to enhance your understanding of phishing emails and the threat they pose to the company’s safety and your own safety. As for your passwords if you are trying to generate one, they will have to have certain characteristics associated with them, and if they fail the test that we have required for them, you will have to produce another one until it fits the standards needed.

**Bonus: Other Solutions**

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

Sources: <https://www.atlantic.net/hipaa-compliant-hosting/how-to-best-mitigate-cybersecurity-risks-and-protect-your-data/>

<https://bap.org.ph/cybersecurity/the-pros-cons-of-updating-your-software/>

* Indicate at least two other potential solutions. For each one, indicate the following:
  + What type of control is it? Administrative, technical, or physical?
  + What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
  + What is one advantage of each solution?
  + What is one disadvantage of each solution?
    - Keep software up to date - Technical control that has the goal of preventative and corrective measures put in place. One advantage of this is that after the update there might have been some patches that affected the operational mainframe or the security mainframe to better equip you in the future. The disadvantage of this is, you might have a personal preference of how the system looks after the update. I remember back in 2013-2014 when Apple had its update on all the iPhones. Changing the look when the update was done was a huge change and not many of the people living on my college floor liked it. But we all had to deal with it and move on. We couldn’t change it because they were in charge of the display on everyone’s phone.
    - Implement Multi-factor Identification - Administrative control that has the goal to deter and prevent unrestricted access. One advantage of this is that you will be better protected from unwanted access from bots or hackers. A disadvantage is that there are multiple steps to gain access. When you are trying to get that app on your phone and you enter in your password but it logs you out to keep your device safe for some reason you have to enter your password, and then get a text message/email code to enter in and make sure you are who you say you are. It’s very time consuming.