Sasha Shahidi

Week 2 Homework: Assessing Security Culture

Step 1: Measure and Set Goals

1. There are several security risks associated with allowing employees to access work information on their personal devices. One attack that can be carried out is a cyberattacker infiltrating the employees' personal device with malware. Personal devices are often not equipped with the strong malware protection that work devices are, and if the employee downloads a virus on that device, it can potentially navigate to the workplaces network (RIPPL, 2019). A second attack that can be carried out is a hacker accessing the contents on the employees' personal device through an unsecure WiFi network. If the employee were to be somewhere with unsecure WiFi and the hacker were to gain access, work content can be compromised (RIPPL, 2019). A third attack that can be carried out is data being stolen directly from an employees' personal device that is acquired by a criminal. If an employees' personal device is lost or stolen, the work contents on that device can be compromised from an attacker if and when the device is opened up (RIPPL, 2021).
2. There are several preferred employee behaviors that SilverCorp can prefer to workers to ensure greater cybersecurity for work content. For one, since over half of the employees at SilverCorp use their personal device for checking work emails and work Slack communications, a preferred employee behavior is to only open email and Slack attachments from sources they trust, so that malicious malwares don't make their way onto the device and compromise information. Another preferred employee behavior is to sign out of the work email, work Slack account, and other work-related applications in between each use, so that if the device is compromised, work information won't be able to be accessed. Another preferred employee behavior would be to check work email, work Slack, and work-related applications on a personal desktop computer if necessary, rather than a personal mobile device. Malicious malware for mobile devices is on the rise (Leaders' Choice Staff, 2019), and a computer can potentially support stronger malware protection and therefore protect company data. Another preferred employee behavior is to backup your personal device, so that if the work content is compromised, the information isn't permanently lost by the company.
3. In order to check how often employees at SilverCorp are not adhering to preferred behavior, I would institute a couple methods. First, I would institute a survey method with an incentive. I would conduct a survey at the end of every week asking employees how many times they downloaded an attachment from an untrustworthy sender on work accounts on their personal devices, and how many times they forgot to logout of their work accounts when they were done. I would also ask if they got any malware on their device from a suspicious download. I would also ask if they backed up their device. The incentive I would provide is that for every employee that successfully follows the preferred employee behaviors for that week, they would receive an extra one hour break that they can use at any time the following week. I would also have an employee be tasked with going around the office randomly and checking employees' accounts to

ensure that no suspicious attachments were downloaded and that they are signed out of their work accounts when it's not in use.

4. The goal that I want SilverCorp to reach regarding the preferred employee behavior is for the survey results to indicate that more than 90% of employees followed the preferred employee behaviors. This would lead to a more secure environment for the organization's important content, and with the incentives provided to the employees, provide a better company culture, as the employees can look forward to a longer break.

Step 2: Involve the Right People

In order to successfully reach the goal of having at least 90% of the employees at SilverCorp follow the preferred employee behaviors, there are several employees and departments that need to be involved.

First, we are going to need to involve a security engineer. The security engineer will be tasked with ensuring that the current plan is effective in order to reach the goal. They will review the preferred employee behaviors that have been created and ensure that they are effective at providing greater security for the organization's information. They will also make sure the methods to ensure employees are adhering to the preferred employee behaviors are effective and that the goal is realistic.

Next, we are going to need to involve the CEO. The CEO is going to be responsible for approving the methods that we're using to ensure employees are following the preferred employee behaviors, since they are responsible for the big decisions that are made in the company. The CEO will also confirm that we can use the incentive of giving employees an hour extra break per week to increase our chances of reaching our goal.

Next, we are going to need to involve the communications department. The communications department will construct the emails that will go out to each employee that will inform the preferred employee behaviors regarding how to use their personal devices for the safety of the company's data. They will also inform the incentives for doing so, as well as the company's goal, effectively bringing everyone in the organization on the same page about the security strategy on their personal devices.

Next, we are going to need to involve the human resources department. The human resources department will conduct the surveys at the end of each week asking the employees if they downloaded suspicious attachments in their work accounts on their personal devices, whether they forgot to sign-out of their work accounts on their personal devices when they weren't using it, and whether they backed up their device that week or not. They will crunch the numbers to determine if the organization met its goal of 90% adherence, and encourage employees who didn't follow the preferences to do so if possible.

Next, we are going to need to involve an IT desk member. The IT desk member will go around to check the work accounts of the employees' personal devices in order to see if they are logged out of their work accounts while it's not in use, and to see if malicious malware has been downloaded from an untrusted source from their work accounts onto their personal device. This will only happen while the employee is in the office. The IT desk member will work with the human resources department to determine if the organization's security goal is met.

Step 3: Training Plan

In order to ensure that the information of the organization is secure and employees are following the preferred employee behaviors, there will need to be a clear and thorough training plan. I will run training once per month, on the last Friday of each month. The training will be online, mostly in the form of videos of employees and management discussing and modeling the best practices that employees will watch. There will also be some reading that goes with the videos. Employees will have a few quiz questions at the end and mark the training complete.

A very important topic that I will cover in my training is that employees should take phishing attempts seriously in their work email and have caution in opening attachments across all work-related accounts. This is because opening problematic emails and clicking on malicious links and opening dangerous attachments can be very detrimental to the safety of the information in the system (Loshin, 2019). Teaching the employees about this in the training plan can teach them about what to look out for when looking through their emails and what malicious attachments might not get caught, guiding them on the best practices (Loshin, 2019). They can also learn about what malicious attachments might look like, guiding where their caution should be (Loshin, 2019). The employees should learn that attackers are always looking for ways to bypass protections, so it is vitally important to be on the lookout (Loshin, 2019).

Another very important topic that I will cover in my training is making sure employees are informed on downloading and updating a strong anti-malware. The use of anti-malware will allow protection from phishing attacks, block ads and spam, and overall protect the business from the malicious malware (Quantech, 2019). These malicious malware can arise from an employee accidentally opening an attachment or clicking on a link that brings malware onto their device (Quantech, 2019). Even though employees will be trained to not open attachments and click on links that can potentially give malware, the chance of it accidentally happening still exists, so further training on maintaining an anti-malware is very beneficial for even further protection of the company's information.

Another very important topic that I will cover in my training is making sure employees are aware and trained on remembering to sign-out of work accounts on personal devices and not staying logged-in in between uses. It is important to sign-out of work accounts on personal devices so that if they ever lose their device, their device gets stolen, or their device is left open and unattended, the organizations' information isn't readily available to be stolen and compromised. They will also be informed to not auto-fill their login credentials onto their accounts and sign-in manually each time.

Another very important topic that I will cover in my training is making sure employees are backing up their personal devices every week if they are using it to access work accounts. This will ensure that if the content they are storing on their personal devices for work is stolen, there will be a backup of the information, so that the organization doesn't fall behind and lose important data. The employees will be asked to backup their devices at least once per week.

After I run the training, I will measure its effectiveness by how much security breach incidents decrease. Each training session will have updated information of these best practices and serve as an opportunity to check-in on if the employees are following the training topics. The effectiveness will largely be discovered through surveys, personal reporting, and management finding out themselves. If employees are reporting that they are following the

preferred employee behaviors, following the training topics that are taught, are not going to management with concerns over a compromised system, and management doesn't discover a breach in organization data, then the training can be seen as effective. However, if security breach incidents persist or even increase, I will know that the training was ineffective, and it will be reassessed and updated thereafter.

Step 4: Bonus: Other Solutions

Since training alone often isn't the entire solution to a security concern, other potential solutions must be considered. When it comes to SilverCorp, there are a couple other potential solutions that stand out, such as not allowing personal devices to be used for work accounts by employees, and providing personal mobile devices to be used for work accounts by employees.

One potential solution is not allowing personal devices to be used for work accounts by employees. This would be considered an administrative control. This control has the goal of preventing employees from getting anywhere near the safety concerns that are associated with using personal mobile devices for work accounts, and is therefore a preventative control. An advantage of this solution is that it would require all employees to use work computers to access their work accounts and complete their tasks, thus eliminating the threat that comes along with using personal devices for work. A disadvantage of this solution is that it can be an inconvenience to the employees to be limited to only using their work devices, and they wouldn't be able to access their work accounts at home.

A second potential solution is providing all employees with a work mobile device to use outside their work computer. This would be considered a physical control. This control has the goal of eliminating the need for employees to use personal mobile devices for work accounts, therefore eliminating the risks associated with them, and is therefore a compensating control. An advantage of this solution is that employees will no longer use their own personal devices to access their work accounts, which would increase the security of the organization. A disadvantage of this solution is that it will cost the organization a lot of money to provide all employees with additional devices when all they had to pay for before was a work computer, and employees used their own personal devices outside of that.

Works Cited

Leaders' Choice Staff. (2019). *The risks of staff using personal devices for work*. Retrieved at https://www.leaderschoiceinsurance.com/blog/the-risks-of-staff-using-personal-devices-for-work/

Loshin, P. (2019). *2019's top email security best practices for employees*. Retrieved at https://searchsecurity.techtarget.com/tip/2019s-top-email-security-best-practices-for-employees

RIPPL. (2021). *The risks and benefits of BYOD at work.* Retrieved at https://rippl.work/articles/the-risks-and-benefits-of-byod-work/

Quantech. (2019). *The importance of using antimalware software*. Retrieved at https://www.quantech.tl/2019/10/18/the-importance-of-using-antimalware-software/