Cybersecurity

Module 2 Challenge Submission File

Assessing Security Culture

Make a copy of this document to work in, and then answer each question below the prompt. Save and submit this completed file as your Challenge deliverable.

Step 1: Measure and Set Goals

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.

[1.Lost or Stolen Devices - if the employee uses their personal device for work, the company's data is at risk when they lose their device.
2.Malware - there is an increasing volume of malicious malware designed to target android smartphones which means that the company's data could be compromised alongside with other data in the smartphone.
3. Links to the cloud - a lot of apps for mobile devices allow users to store their data or documents to a cloud which is most likely not double checked by the employer. The clouds offered by the mobile apps could easily be hacked and would put the company's data at risk.

Source: Leaders' Choice Staff. May 8th, 2019. The Risks of Staff Using Personal Devices for Work.
https://www.leaderschoiceinsurance.com/blog/the-risks-of-staff-using-personal-devices-for-work/]

2. Based on the previous 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.)

```
[The preferred scenario would be that employees should not be allowed to access work related information through their personal devices and it's something that the IT professionals are not able to control and it is hard if not almost impossible to monitor. If using personal devices for work is a must then certain rules and access codes should be implemented and employees must be held accountable for any data leaks.]
```

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.)

```
[Register all the devices that employees bring to work such as smartphones and tablets then monitor which of them were trying to access the work website and through which wifi they're connected to. Monitor how many times all of the employees have logged into the work website using a work device and check if that matches the amount of time that they've been on the website. Give employees a specific amount of time during working hours to work on their online training or for finishing their tasks for them to not have the need to access the company website outside of work.]
```

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.)

```
[To have less than 3 employees to need access to the company website outside of work. The fewer people needing to access the company website outside of work means that the cyber security personnel would have more control over the data because it is easily monitored. Allocate enough time for every work that is needed to be done on a computer so everyone won't have a reason to take their job home with them.]
```

Step 2: Involve the Right People

5. List at least five employees or departments that should be involved. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.

[Management - the management should be in charge of allocating the time for each employee and this includes that everyone is able to finish all of their computer related work within the hours given to them. Management should also make sure that there is someone always monitoring the company website traffic and that the computers at work are up to date and capable of running under heavy load.

Cyber Security Specialist - this person is the one in charge of making sure that all of the devices and computers at work are protected from any type of cyber attacks and has only limited access in the web so that employees won't be able to accidentally click a fake ad that could lead to a data breach. This person should also be able to monitor everything that is being typed and looked at in every computer to make sure no one in the company does any suspicious activity.

Supervisor/Manager - this person is assigned to make sure that everything that has been approved by the management is implemented properly and being put to practice everyday by all of the employees. This person is also in charge of getting feedback from everyone that has any concern about computer related work and making sure that the issue is brought to the management immediately to be addressed. This person is basically the eyes of the management and is responsible for the overall activity during working hours and should remind everyone if there are any new policies or rules that should be done.

Employees - employees are responsible for managing their time properly so that they're able to finish all the tasks with their given time and won't have to access or continue the work at home. Employees should also be responsible for whatever they're doing when in front of a computer while at work and making sure that they only open and look up websites that are work-related and nothing else. Employees should be educated with the different types of cyber attacks that could happen at work while they're in front of the computer because awareness is the first step to preventing these types of attacks.

Security - this person is in charge of making sure that no one stays in the building past working hours and no one gets in after everybody leaves. This person is also in charge of making sure that no one takes anything from the building with them when leaving the premises.]

Step 3: Training Plan

6. How frequently will you run training? What format will it take (e.g., in-person, online, a combination of both)?

[Training will be done every month. It will be an in-person only training wherein the employees are assigned to watch a video during their work hours about cybersecurity and would have to answer some questions afterwards. This is followed up by a rounding with their manager every week to make sure that everything is running smoothly and any issues they have could be addressed. All of the training has a specific deadline. The manager in charge should make sure that everyone finishes it in a timely manner.]

7. What topics will you cover in your training, and why? (This should be the bulk of the deliverable.)

[Phishing attacks - employees are required to watch a video making them aware of the different types of phishing attacks so that they'd be more cautious when working in front of a computer. This will raise everyone's awareness of how easily the company's data could be breached just by a simple click on the internet. This will make them act defensive and assume that any unknown links or ads could be a potential threat to the company and to their personal information. This will also make them think about the whole internet as a whole seriously and it is something powerful they have control over and that comes with great responsibility.

Passwords - this will educate them on why the passwords should be updated more frequently than what they were expecting. The purpose of this is to make sure that they know how important passwords are when it comes to protecting their data and the company's assets. This should make them think harder the next time they change their password and make sure that it is strong enough to not get easily cracked.

Removable media - this will educate them on how a simple usb or charging cable could breach the computer and have it compromised. This will make them think twice whenever they think about charging their phones in a random usb port. This will also make them aware of all of the devices connected to their work computer and make sure they check it everyday that there is nothing attached to the ports that are supposed to be empty.

Physical security - this should open their eyes that anything that contains any information about the company should stay within the building. They

should make sure that any papers or documents in either physical or online form should be kept within the workplace only. Proper disposal of any data will be taught and should make them aware of how these little things could lead to a leak or breach if not handled properly. This will make them more cautious of their actions even if something is supposedly “trash” or “unusable”.

Mobile device security - this will make them even more aware and give them insight on why the use of mobile devices within the workplace is prohibited. This will explain to them how a simple picture taken during work hours could be used against them or the company. This will make them think about the cloud storage that they’re currently using and the documents and data that they’re saving in those. This will make them cautious with how they use public wifi and how their device could be a target in such situations.

Source: Jordan Daly. 2023. 12 Essential Security Awareness Training Topics for 2023. https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020]

8. After you’ve run your training, how will you measure its effectiveness?

[There will be a weekly rounding of the employees with the manager which includes how much work they’ve done in front of their computer and how much work has to be carried over the next day. This conversation will also include about the non work-related websites that they have opened and their use of personal mobile devices while being on the clock. These issues will be addressed and the first-time offenders get a warning, the second offense will require double the amount of training in a month but the same amount of rounding with the manager, and lastly third offense offenders will get a written agreement with the manager and the head of management themselves that if the employee continues with this kind of behavior suspension will be enforced. The effectiveness will be measured by the productivity of the employees during work hours and through the continuous monitoring of their activity while in front of the computer.]

Bonus: Other Solutions

9. List at least two other potential solutions. For each one, indicate the following:
    a. What type of control is it? Administrative, technical, or physical?

b. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
c. What is one advantage of each solution?
d. What is one disadvantage of each solution?

```
[Limited internet and computer access
   a. This is an administrative control that will be implemented by the
      cyber security specialist.
   b. This control is preventive. This will limit the access on the internet
      and computer so that the employees are only able to do work-related
      activities in front of the computer and will therefore prevent
      accidental clicks on the unwanted ads and websites.
   c. One advantage of this solution is that employees are less susceptible
      to cyber attacks because of the personalized and heavily monitored
      computer configuration.
   d. A disadvantage to this solution is that employees might have the
      tendency to reach for their mobile devices to search up things that
      they're not able to on their work computer.]
```

```
[Full time cctv monitoring
   a. This is a physical control that will be monitored by a cyber security
      personnel 24/7/
   b. This control is preventive, deterrent, and detective. This will
      prevent any illegal activity if caught in time as everybody's movement
      is seen real time. This is also a deterrent as the employees would act
      more accordingly once they see that they are surrounded by cameras.
      This could also be used to detect and review any situation wherein
      there has been a data or document or employee that has been
      compromised. This will tell about what went wrong in a situation and
      could give answers as to who should be held responsible.
   c. One advantage of this is that everything is being recorded and could
      easily be replayed when there is a breach or an illegal activity. This
      could help identify people involved and solve a problem when everyone
      is a suspect until proven innocent.
   d. One disadvantage of this is that there is one more person to add to
      the list that the company has to pay to continuously watch the
      activities through the screen. This could also mean more money
      allotted for the cameras to be installed.]
```