Instructions

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

Step 1: Measure and Set Goals

Answer the following questions:

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.

-Logic bombs from unhappy employees, lack of a content filter can allow malicious internet content to be downloaded to the personal device and infect the network, information leak that sensitive information could be copied or downloaded to employees personal device

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.

-Employees prefer to do work related activities on their personal devices, the preferred behavior would be to use secure company devices that are properly controlled and restricted by administrators

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.

-Install alert programs and instant messaging applications so employees can be informed by the administrators of proper company policy and procedure of handling company devices to protect assets, information, and integrity

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.

-Goal for the organization would be to have no loss of revenue due to malware, employees only use proper company procedure on company time, ensure that a content blocker does not allow for email downloads to occur without consent from IT admins

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.

-There would be 5 employees that would oversee that the policies are enforced. The lead supervisor of the team would be the CISO(chief information security officer). There would be 2 IT admins and 2 cyber security analysis personnel that would monitor the intranet of the company. The 2 IT admins would make sure that the company's use policy was not bypassed in any way that would compromise company integrity. The need for 2 IT admins would be in case one of the 2 employees would not be at their desk, for example, if one of the employees need to take a break. The 2 cyber security analysis employees would be monitoring any malicious activity that did breach company intranet and alert the rest of the cyber security team in the company of the breach. The need for 2 cyber security analysis employees would be in case one of the 2 employees would not be at their desk, for example, if one of the employees needs to take a break. Any and all unusual activities would be reported up the chain of command to the CISO.

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:

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

Online training should be conducted once every 4 months and in person lunch-in training should be conducted every 6 months

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

The training will go over what malicious activity is trending online and what to look out for and avoid, along with reducing click rates as much as possible.

After you've run your training, how will you measure its effectiveness?

For any employee that violates the company use policy, have one-on-one counselling with the employee and instruct them on how they need to conduct themselves while using company equipment. The effectiveness can be measured by tracking the employees click rates and activity online by use of scan tools and content filters. This will track employees' progress of

what they are applying what they learned in training.

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

Bonus: Other Solutions

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

Indicate at least two other potential solutions. For each one, indicate the following:

What type of control is it? Administrative, technical, or physical?

Administrative and Technical, Administrative because there is employee oversight. Technical because there is programs and procedures that will guide employees and systems in a safe manner

What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

Mostly Preventative in order to avoid any catastrophe from happening, but also detective to monitor anything that might happen

What is one advantage of each solution?

If carried out properly a preventative control would not have any damage to the network or company. There would also not be any loss of revenue due to an employee bringing down the network. The deterrent solution's advantage would be discouraging other employees from making the same mistakes. The detective advantage would be finding the exact source of where the threat or attack originated. The corrective advantage would be training and the best communication option to have the employee fully understand the implications of their actions to the company. The compensating advantage would be employees might remember what they are supposed to do because they feel they might be rewarded for their good actions.

What is one disadvantage of each solution?

The disadvantage of a preventative solution is that it basically means the company has no trust or faith in its employee to do the right thing on a device. The deterrent disadvantage would be that discouraging someone of doing something is just going by "word-of-mouth" and there is no actual guarantee that the malicious threats or attacks would be prevented in the first place. The Detective disadvantage would be people might feel that they are being watched over too much with a content filter and not have as much freedom to get work done the way they want. The corrective disadvantage would be that people do not like being lectured for their mistakes and to correct a mistake takes away company productivity time. The compensating

disadvantage is that it would cost the company money and employees might expect a hand out from work that they should be doing in the first place to keep their company secure.

Submission Guidelines

Submit this homework assignment in a Google Doc.

You can submit all four steps in the same document. Make sure that anyone can view and comment on your document.

Title your document with the following format: [Your Name] Unit 2 Homework

Submit the URL of the Google Doc in Bootcamp Spot.