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.

Phishing emails, stolen equipment, malicious software, data breach/exposure, Network connectivity, uncontrollable devices.

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.)

Phishing emails- employees need to make sure the emails are coming from a known source before opening or clicking on links.

Stolen equipment- If employee has personal equipment that is used for work stolen it needs to be reported to the company immediately. Employees need to also make sure that passwords arent saved, and software used for work is logged out after every use.

Malicious software/apps- Employees should research appropriate apps to have and use on personal devices before downloading.

Data exposure- Employees shouldnt be talking about classified or secret company information through the personal devices or personal 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.)

Phishing emails- Do a test multiple times a a year to see if employees are clicking on links within emails.

Stolen Equipment- Do accountability twice a week to see if all employees have hands on all their equipment.

Malicious software- Do a monthly or quarterly malware check on all equipment being used for business and personal use.

Data exposure- Conduct survey on how much data is leaking and notate. After that making sure no data is being saved on personal devices.

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 for all behavior is to make sure less than 2% of these risks are happening per year.

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.

Department head- For the department head their main responsibility would to be conducting the audits on all employees personal devices used for work. This audit would consist of making sure they have proper protection on the computers as well as checking for saved data and malicious software or apps downloaded.

IT- IT would be in place to help make sure we have the right hardware and software in place to allow us to run whatever we need. They will also help us to fix any issues that arise from while we conduct this new project.

Human Resources- HR will be in charge of making sure that all personel are aware of coming changes with the project. They will also have an accountability of how many employees will be in place before, during and after the project.

Finance- We will definitely need finance to control the budget for how much we will be allotted to conduct this project. They will need to make sure that all funds are allocated to our project as well as fix any financial issues that might come up during the project.

CEO- We will need approval from the CEO for all project ideas in order to even be able to move forward. Without the CEO we wouldnt even be able to move forward.

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)?

Quarterly 25% of employees will conduct in person training as well as 100% of employees will conduct yearly online training that will be required.

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

The misuse of personal devices used for business use, and how to properly have your computer set up to help mitigate risks that might aride. The bulk will be cyber awareness.

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

In training we will have scenarios. Once training is complete monthly a penetration test will be ran to see how many employees are falling for phishing emails. With the weekly audits of personal equipment we will hope to notate how many people have stolen or lost equipment.

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?

The employee computers have antivirus
-Technical
-Preventative
-Advantage would be that the employees computers could have a layer of security to detect malicious software that might have been downloaded. Depending on how many layers of security the computer already has including firewalls or encryption it would just help add safety.
-Disadvantage could be the cost depending on how many employees there are it could cost up to $100 per employee.

Backup and recovery Systems
-Technical
-Corrective
-Advantage would be that the company would be able to backup data after a security incident for example stolen device or broken device.
-Disadvantage would be the cost. Backup and recovery systems can run anywhere from $1,300-$2,500 per employee so the price will run high the bigger the company gets.