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. Stolen device-- if a personal device containing sensitive work information is lost or stolen that information can fall into the wrong hands causing security risk to a company
    2. Malicious software/ Malware- People tend to be unaware of their devices possibly having malicious content attached to it; when sensitive data is exposed to a device with malware on it, there is an imminent threat to precious information.
    3. Unsecure Wi-fi- many of us have wi-fi access to not just ours (which in and of itself can be a security breach) but we are often connected to the ones of our friends, relatives, or maybe even a coffee shop we frequently visit we often don’t question if these networks are secure or not and that can cause a lot of problems.

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.)

Preferred employee behavior would look like this: Using devices that are encrypted; ensuring that small security measures are used like VPNs, and the company providing the employees with encrypted devices that would prevent security risks from happening.

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.)

To make sure that employees are up to date with security protocols and are able to efficiently understand and navigate them. This will also provide feedback for

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 make sure that employees are up to date with security protocols and are able to efficiently understand and navigate them. This will also provide feedback for everyone to see what needs to be changed/

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.

CISO: Chief Information Security Officer- A senior-level cybersecurity professional with exceptional leadership skills to serve security practices internally and externally, developing security training models. CISOs are responsible for forming well-rounded teams by educating and supplying groups with proper and up-to-date materials to aid in overall success. This role is key for measuring risk to a company's data

Reporting/Communications: Responsible for documenting the scenarios that are bound to happen and gathering information to draft reports. This role is crucial because reporting what happened, why, and what was done after security incidents can help build a better team because it is easier to identify strengths and weaknesses.

Incident response: This team of people is responsible for developing appropriate response plans, testing, and managing vulnerabilities. You will find roles such as SOC analyst here.

Human resources/HR: Works in connection to ensure the accessibility of training and organizing good departments with proper leadership positions to aid in all of the many sectors in a company. They are also in charge of any disciplinary measures that may be needed as some cybercrimes can have legal/criminal consequences

Finance/CFO/Accounting: Manages the budgets and calculates financial duties. This role is important for gathering data and monitoring the company's budget and financial trends.

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 would be quarterly and depending on what is happening in the cyber world there could be ‘squeeze-ins’ or more frequent meetings if the initial quarterly schedule is not effective; from what I have learned and observed: Cybersecurity is an ever-changing field and cyber threats happen daily and you must stay updated and continually educate yourself on new cyber trends. I think a combination of in-person and online training could be beneficial.

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

Training would involve defining and identifying phishing from common scenarios like websites and email. Explaining the negative impact of neglecting proper cybersecurity practices and suspicious content and carelessly ignoring the unauthorized resources, links, etc… This will cover the main and dead giveaways of a basic phishing attacks that employees should constantly keep an eye out for and pushing the importance of only using trusted sources provided by the IT department.

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

Creating phishing/cybersecurity scenarios/ to measure how well employees are able to recognize, implement, and navigate security protocols. Employees will be subject to training protocols, almost like a driving test where their skills will be tested; if a crucial/critical skill is failed employees will have to complete mandatory training with satisfactory results.

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?

Phishing in technical and preventative. The benefits would include be lessening the number of clicks on suspicious links. A disadvantage could be human error where a small mistake can lead to consequences (like misreading something or clicking on something by accident)

Insider threat would be physical because this requires some sort of control barrier, specifically technical and administrative control. The advantage would include protecting sensitive information and preventing losses in the company. Disadvantages would be sensitive information not being secure anymore and also manipulated which could also impact the company with greater financial loss.

****I used these two sites https://purplesec.us/security-controls/ and https://www.verizon.com/business/resources/articles/s/the-risk-of-insider-threat-actors/website to help me with some of these answers.