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.

- There is a possibility that their devices may be stolen and this may allow the attacker to access sensitive information on the device.
- Employees may click on the fake links from their emails and it may cause an phishing attack.
- An attacker may pretend to be an owner and can reach others credentials.
- An attacker can find users login and password information on other websites.

1-) SOCIAL ENGINEERING
2-) PHISHING ATTACK
3-) CREDENTIALS REUSE
4-) MALWARE
5-) STOLEN HARDWARE
6-) BRUTE FORCE ATTACK

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.)

- Employees should adhere to security policies and guidelines.
- They must be trained on the danger of phishing attacks.(they should be careful not to click on any fake emails)
- Their devices must be encrypted to prevent the risk of their devices being stolen. (they should change their password at least one every quarter)

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.)

- I would hire a penetration testers to begin a phishing compaign that will send out phishing emails to users in the company. So, it will show us the percentage of employees fall for the phishing attempt.
- Secondly, I conduct a survey to measure employees knowledge about the security policies and guidelines at the company twice a year. (it would be suddenly and on an unscheduled day)

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.)

- Employees are going to change their passwords once every quarter for security.
- To have over %90 of employees have knowledge about the security policies and guidelines.
- To have less than %3 of employees fall for the phishing attempt in a month.

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.

- **CIOS:** CIOS's responsibility is to ensure that the company's data is safe. And also, they will develop and disseminate information security policies, training to personal.
- **HUMAN RESOURCES (HR):** HR is responsible for internal communications, scheduling trainings and tracking attendance.
- **SECURITY:** Security team is responsible for developing training exercise with HR and gives details of scheduling and delivery.
- **PENTESTING TEAM:** They are responsible to test employees and show the percentage of it.
- **SECURITY OPERATION CENTER MANAGER (SOC):** They are responsible for identifying anad responding to security breaches.

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)?

According to me the best way to learn is in person. I would run training in person and at least twice a year.

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

I would focus on phishing attacks and encryption. Because these are the most risky ones for a company and i would emphasize them. It will be useful in case the device is stolen, and also it wil reduce the risk of phishing attacks if they get trained well.

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

After employees have done their training, I would wait for a while (like a month) and I would get them tested unexpected and unscheduled day so it will show me if the effectiveness of the training.

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?

1. SECURITY CONTROL is the first solution for system, process and technology that protects the CIA of the company. The business can set up a camera system in the building, and they can also address employee behavior and security culture by educating them.

a. It is “Administrative” control. (requiring employees to adhere to guidelines and security policies.
b. It has “Corrective” goal. (it fixes an incident and possibly prevent reoccurrence).
c. The advantage of this solution is knowing whether employees have enough knowledge or how strong the worker team is.
d. Being constantly tested might make employees feel uncomfortable or pressured.

2. DEFENSE IN DEPTH is the second solution. It is a layering security control which is defending the system in multiple ways ensures that remains protected even if one of them fails. If a company faces any attack, it will be very protectable for them. For instance; forcing developers to authenticate using SSH keys and passwords.

a. It’s “Technical” control.
b. It has “Preventive” goal.
c. The advantage of this solution is protecting the system in multiple ways so it can not be easy to access the server.
d. There might be some possible distributions such as Human Errors from one of the employees. As known it is very difficult to access the server if the company uses SSH keys or password but there is a possibility that any employee might act intentionally or unintentionally (I mean any attack from inside of team) in the company.