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.

Employees losing or having their personal devices stolen, giving unauthorized users access. Connecting to unsecured WiFi, which makes their device vulnerable to attack. Increased risk of phishing attacks.

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 don’t have access to company intranet on their personal devices. Only company devices can connect to the intranet, and only those who need one have it. No phishing attacks. No communications regarding sensitive information outside of work email, all emails with sensitive information are encrypted.

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.)

Remove the ability to access the company intranet on personal devices. Conduct a survey asking employees who would need access to the company intranet outside of work. Conduct classes educating employees on the dangers of phishing, hire a firm to run a phishing campaign to determine which employees still need more training. Start tracking all employee-involved phishing incidences.

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.)

No access to company intranet on personal devices. Limited usage of company devices outside of the office. Provide proper training leading to less than 3% of employees being involved-implement the same training to all company new-hires. Employees encrypt all emails that contain sensitive information, provide training so all employees are aware of what sensitive information is defined as.

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.

HR-Will set up a process for determining which employees will most likely need devices outside of the office. Also, they will be responsible for keeping track of which employees will need extra training. Will work with IT on scheduling training.

IT-To set up company-owned devices that will be used outside of the office, ensuring they are secure and able to be located if lost/stolen. To continuously ensure that security software on the devices are up-to-date. To keep track of all devices that are issued to employees. Will develop the classes. Work with recruiting on developing a class for new-hires. Will be the instructors for the classes.

Recruiting-Will work with IT to develop a class for new-hires on avoiding phishing attacks and other basic security processes. Will work with HR on scheduling new-hire training.

Finance-Will work with IT to help develop a budget on what devices and security software can be purchased. Will work with IT and Recruiting to develop a budget on what will need to be purchased for training.

Management-Will be responsible for ensuring their personnel are meeting security standards and getting necessary training. Will work with HR on tracking who will need additional training and when.

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)?

Standard cyber training once a year in-person, new-hire training in-person once hired, phishing-avoidance training once a year in-person (more training for those who need it).

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

Annual standard cyber training will cover the basics of computer safety and will focus on the most common user errors and cover what information that should be considered sensitive and how to encrypt emails containing that information.

New-hire training will give an in-depth lesson on how to avoid phishing attacks-the same curriculum will be used for current employees that are deemed to need more training.

The annual phishing-avoidance training will be a refresher on how to avoid phishing and what to do if one falls victim. Employees who fall victim to an attack will be given a more in-depth course.

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

```
Annual cyber training-After the first year, were the most common user errors
covered in the training, or not. If the most common problems were not
covered in the class and if less than 5% of employees sent unencrypted
emails containing sensitive information, the class was successful.

New-hire phishing class-New employees will be tracked, if in the first year
less than 5% are victims of phishing attacks, the training is successful.

Remedial phishing class-If after the first year, less than 2% of employees
who take the class are involved in a phishing attack, the class is
successful.

Annual phishing-avoidance class-If after the first year, phishing attacks
are reduced by at least 50%, the class is successful.
```

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?

```
To avoid phishing, the company email connected to the intranet will be
internal and will only be able to receive emails from other company email
addresses. A separate network will be set up for basic internet usage, and
will not have access to the intranet. Desktops will be used for the
intranet. Laptops will be used for the separate network.
   A. Technical
   B. Preventative
   C. It almost entirely eliminates phishing attacks.
   D. May be difficult and expensive to implement.
```

```
If an employee is involved in 3 or more phishing incidences in a year, they
are terminated.
   A. Administrative
   B. Corrective
   C. It will motivate employees to be wary of potential phishing attacks.
   D. May be difficult to enforce.
```