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.

The potential security risks of allowing employees to access work information on their personal devices are unsecured networks, lost/stolen devices and Insufficient policies. Unsecured networks can create security issues as these networks are open to anyone which can allow attacks such as snooping and honeypots. Lost/stolen devices can cause large scale issues because if the device is not able to be wiped, this can cause a major breach which could result in a company's data being leaked or spyware/malware being installed. Insufficient policies are an issue because if users are able to visit any website, then they are more prone to visiting malicious websites that are able to steal data which may result in a breach. Companies should allow vpn sessions that prevent users from visiting websites that may be malicious but also allow a secure session to do company work.

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.)

Based on the previous scenario, the preferred employee behavior when it comes to these risks are as follows

- Employees should avoid the use of public or unsecured networks. The ideal solution to this would be using the company vpn connection (along with a RSA secure token) and using a secure private network at home as these options will allow you to have a more secure session that will protect you from certain attacks (Man in the middle, tailgating) (Stouffer, 2023).
- Employee self-awareness is key to preventing company property from getting lost/stolen. Employees can ensure that devices are properly protected by securely locking the device in their office before leaving work, as well as making certain the device is not left unattended at all times (*Laptop theft prevention* 2023).
- They should also keep devices secure by having more secure passwords that require changing after a few months to ensure the data stays safe. Two factor authentication can also help keep devices secure and protect unauthorized access and breaches from occurring. The company's policy can be updated as well such that it gives employees the opportunity to have their devices encrypted or provide them with devices that have encryption (*Password expiration* 2022).

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.)

The methods I would use to measure how often employees are currently not behaving to the preferred behavior are by sending them fake phishing emails to assess if they click on the link instead of reporting it. I would also conduct quarterly quizzes after assigned training material to see how much material they are absorbing through the training material. Employees should also be engaged in learning more about the security of their devices and company data which is why interactive training seminars can be held quarterly.

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 ideal goal that I would like the organization to reach is 0% of unwanted
behavior but as we discussed in class this is not always possible. We are
going to aim to have less than 5% of employees download suspicious email
attachments. We get to this goal by conducting assessments and educating the
staff members. Employees will be receiving quarterly courses that will
educate them about the security risk that might occur for example phishing.
After the course is complete, they will be assigned a quiz that they will
need to score 95+ on to complete the activity. However, if they do not meet
that benchmark then they will be redirected to additional resources to help
bridge the gap in their knowledge. Employees will also be sent fake phishing
emails and we can monitor to see how many individuals click on the link
instead of reporting it. We hope to have less than 5% of individuals who
click on this link. If they do, they will be directed to a mandatory
refresher course on the risks of such emails, followed by a short quiz.
```

Step 2: Involve the Right People

5. For each person or department, describe in 2–3 sentences what their role and responsibilities will be.

```
Chief Executive Officer (CEO)
   -  The CEO is responsible for all parties listed (COO,CFO,CISO and CIO).
      They will be in charge of the company and the direction the company is
      heading in. Furthermore, they will approve any resources that will be
      needed in the training of employees as well as any devices or software
      that will be needed for the protection of company data (Murray, 2023).

Chief Operating Officer (COO)
   -  The COO is responsible for communicating any policy changes to the
      employees
   -  They ensure that the business is able to operate daily as well as
      provide training to employees to raise awareness of risks (Murray,
      2023).

Chief Financial Officer (CFO)
   -  The CFO is responsible for the company's finances.
```

```
   - They will approve any training plans as well as any software or
     hardware purchases needed (Murray, 2023).

Chief Information Security Officer (CISO)
   - The CISO manages risks that will occur to an organization's data.
   - They will communicate the potential risks and build a plan to train
     employees accordingly (Murray, 2023).

Chief Information Officer (CIO)
   - The CIO will develop the IT systems needed to support the business.
   - CIO will also collect data from surveys, quizzes and simulated
     phishing scenarios and see what needs to be done to improve scores and
     awareness of security policies (Murray, 2023).
```

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 will take place quarterly but can take place earlier if an employee
has committed an offense such as clicking on a simulated phishing email. The
format of the training will be a combination of both in-person and online
training. Quizzes will be conducted upon completion of training and a score
of 95% will be needed in order to complete any training modules.
```

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

```
In the training courses the topic of cybersecurity and company policies will
be addressed and employees will be educated on how to stay alert for
threats. Employees will also be educated about current threats that they can
be vulnerable to and what steps are required to prevent any data breaches.
More specifically, they will be educated about threats such as phishing,
ransomware, code injection, brute force attacks, and malware. They will also
be given examples of breaches that have occurred in the media recently as
providing this information will allow them to understand the relevance of
```

this training. Allowing the employees to understand their shared responsibility will assist in colleagues being vigilant of not only themselves but other colleagues as well. A widespread knowledge of this information will help not only educate our employees but also keep company data safe. The use of a VPN remote connection as well as two factor authentication will be demonstrated so employees can use that to have a secure work session as well as prevent unauthorized logins. Training will also cover how to install anti-malware software on personal devices as a preventative measure.

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

The effectiveness of training will be tested by looking at quiz scores of each training module that they have completed as well as looking at the percentage of individuals who have clicked on the simulated phishing emails that have been sent. It is also important to get feedback from employees on these training sessions to see what is working and what can be done to improve the quality of the courses so that they are more effective. These training sessions, quizzes, and feedback will be conducted on a quarterly basis to ensure the material is always up to date and fresh in the minds of each employee.

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?

One solution the company can implement is by providing employees with encrypted devices.

a. This change would be administrative.
b. The goal of this control is preventative as providing employees with encrypted devices will prevent data breaches from occurring and in the case of a lost or stolen device the drives can be wiped.
c. The advantage of this solution is that it provides security to company data as the devices are encrypted so if an employee were to work from

outside the workplace, data breaches are less likely to occur. Providing devices also prevents employees from using these devices for personal use like replying to messages, playing games or visiting unwanted websites (Murray, 2023). This eliminates the risk of any smishing or malware being downloaded by malicious websites.

d. The one big disadvantage of this would be the cost of providing devices to all employees and properly recording and encrypting all information as well.

The second solution the company can implement to improve the security of the devices is using VPN sessions for work being done on personal devices.

a. This would be an administrative change that would be made.
b. The goal of this control is to be preventative as users would be more secure on a VPN connection as opposed to using an unsecured or open network which could result in a breach.
c. The advantage of this solution is that it would establish a more secure connection than a public network and can prevent attacks like man-in-the-middle (Murray, 2023).
d. A disadvantage to using VPN sessions would be that the cost of setting it up may be high and internet speed may be reduced.

References:

1. Murray, A. (2023, March). *Security Within The Organization* . Lecture.
2. Murray, A. (2023, March). *Risk Management and Threat Modeling*. Lecture.
3. Murray, A. (2023, March). *Governance and Compliance*. Lecture.
4. *Laptop theft prevention*. Public Safety | Brown University. (n.d.). Retrieved March 23, 2023, from https://dps.brown.edu/crime-prevention/safety-tips/laptop-theft-prevention#:~:text=Never%20prop%20open%20your%20door,that%20you%20have%20a%20laptop.
5. *Password expiration policy and best practices - password expiration date*. KirkpatrickPrice Home. (2022, December 16). Retrieved March 24, 2023, from https://kirkpatrickprice.com/blog/password-expiration-policy-and-best-practices/

6. Stouffer, C. (n.d.). *Public wi-fi: An ultimate guide on the risks + how to stay safe*. Norton. Retrieved March 24, 2023, from https://us.norton.com/blog/privacy/public-wifi#