# 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 employers and the employees all around the globe adapted many new strategies and procedures during and after the pandemic such as work from home, bring your own device enabling employees to work from their own devices and much more. This led to a rising issue of cyber attacks taking place on individual's devices especially with employees who are allowed to access work material on their personal equipment.

Some of the potential attacks are

1) **Social engineering attack** - The social engineering phishing attacks usually have a pattern where the attacker will send the employees phishing emails and text messages with links containing virus and malware which will compromise the personal and work data of the employees.

   These attackers often conduct very thorough search on an organization and will gain the email addresses of all the employees they could find online and using those email addresses and other details obtained

using open source, the hacker will send email and text correspondence to the employees impersonating as the employer asking for logins and password and additional personal information, often they are also impersonate as a member from HR department asking to verify the employees their identity by downloading the malware contained attachments.

2) **Man-in-the-middle Wifi attack -** The Man-in-the-middle attack could take place if an employee connects their personal device to a public wifi or an unsecured network, unknowing the risk it entails. As soon as the attacker establishes that bridge between the user and the network, all the personal and work data will be chained through the man-in-the-middle causing data leak or data manipulation.

3) **Malicious applications attack** - Many applications nowadays which looks legit and innocent enough, upon downloading it will require the users to accept the terms and conditions along with permissions which will allow the app to have access to certain files or folder on the device and as majority of the users tend to ignore going through the permissions section, it eventually ends up leaking data of the employee, which can be either personal or work related. Additionally, there are often many applications for games, photo editing, movies, etc. containing virus and malware which once downloaded will expose the device data.

**Citations:**
https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/

https://www.kaspersky.com/resource-center/threats/top-seven-mobile-security-threats-smart-phones-tablets-and-mobile-internet-devices-what-the-future-has-in-store

Classroom slides (2.1 Introduction to Security Within the Organization)

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.)

The most preferred employee behavior all the employers expect is being very cautious about any and all the material they access coming from external

sources, however there are other expectations too to prevent from each type of above attacks.

1) **Social engineering attack-** To avoid the data compromise through this type of attack it is preferred that the employees do not share on social media about their personal work related information such as a badge number or email address, access links and attachment only from a known and a trusted source, confirming with an IT personnel about the legitimacy of any correspondence received asking for personal information to verify their identity and be self aware about the fact that their personal device also contains work

2) **Man-in-the-middle Wifi attack -** While it is difficult to put strict restrictions on employees using public wifi or other unsecured networks for personal use,however, it is preferred for the employees to avoid accessing work communications and applications via open/public Wifi or unknown internet connections. It is preferred for all the employees, especially the ones using personal devices for work, only to use company provided VPN or private home connectivity with strong router logins. Additionally, to be mindful of such high risk unsecured wifi even for personal usage as the device may remain corrupt for future usage as well.

3) **Malicious applications attack -** This type of Malware attack can be difficult to be suspicious about and therefore, it is strongly preferred that the employees install Anti-Virus or Anti-Malware software on their laptops and computers before they download any applications for personal or work use and to regularly update those softwares and scan their devices on a daily basis. Additionally, if they are operating from their mobile devices, they can run a scan and check from their app store (for IOS system) and play store (for androids system) the applications they have on their and it will detect if any applications contain harmful data which may corrupt their devices. Lastly, they can always contact their company's IT department to confirm an application's legitimacy.

**Citations:**

https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/

Classroom slides (2.1 Introduction to Security Within the Organization)

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.)

It is an extremely important step to measure the employees' behaviors to prevent any data leakages, manipulation or compromise.

1) **Social engineering attack -** The IT department will deploy every month pentesting email links which will look like a phishing email to all the employees in order to test and track the results on how many employees actually failed to recognize it as a phishing email and clicked on it. Additionally, sending all the employees once every twice a month Q&A surveys to assess their understanding and mindset on such phishing attacks.

2) **Man-in-the-middle Wifi attack -** The VPN detection tool will be utilized in order to detect the type of network the employees are using. Also, the deep packet inspection (DPI) and deep flow inspection (DFI) will be conducted during network monitoring to ensure the traffic's packet length and also its size for a suspicious payload. The networks will be monitored constantly and any disruption can be traced back to the network from where it began.

3) **Malicious applications attack -** The URLs accessed by the employees will be monitored closely by the IT team and similar to the phishing test, Malware tests will be conducted quarterly where the employees will be requested to download an application using a link provided, the assessment will show the number of employees clicked on the link in order to download the application. The monthly system surveys will be sent to all the employees where they will be asked to run their anti-virus or anti-malware scans and report back the findings in the survey.

**Citations:**

https://www.spiceworks.com/it-security/data-security/articles/man-in-the-middle-attack/

https://www.imperva.com/learn/application-security/social-engineering-attack/

Classroom slides (2.1 Introduction to Security Within the Organization)

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.)

My goal for the organization is to have less than 5% of the employees downloading and accessing links from suspicious email, attempting to access the work material from unsecured and open Wifi, using devices for work without any proper antivirus or anti-malware software installed and accessing suspicious URLs for work sessions.

## 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.

The employees that will be involved in implementing this training program will be

1) **Security Strategy Team -** This team will analyze the successful phishing/malware attacks and network manipulation in the last year occurred due to the employees using their personal devices for work.

   This data then will be utilized to create a training plan to educate employees and additional training plans for the employees who will continue to fail the pentesting email test.

2) **Chief Information Security Officer -** The Security Strategy Team Manager will meet up with the company's CISO explaining the percentage of successful phishing/malware attacks in last year which was 12% as this percent of employees downloaded attachments from external unknown addresses, used unsecured wifi connections to connect to work applications and displayed lack of IT security awareness.

   The Security Strategy Manager will then request for a budget approval to carry out a plan with the IT Security Department and HR department in order to bring down the number to less than 5%.

3) **HR Department -** Once the budget will be approved for the Security Strategy Team, they will advise the HR department about their plan of conducting an IT security awareness training starting with incentives and disincentives to be awarded amongst the employees based on their responses to the penetration tests and security audits. The Security Strategy Team will pair up with the HR coordinator and request to suggest the best time to run the training along with the effective number of employees per session.

4) **Communications Department -** Based on the suggestions provided by the HR department the date and the location of the training along with the relative training material will be distributed amongst the employees.

**5) Pentesting Firm -** The Security Strategy Team will then contact the company's regular Pentesting firm in order to conduct a phishing test against the trained employees and also to monitor and report back the percentage compared to the previous year.

**Citation:**
Classroom slides (2.1 Introduction to Security Within the Organization)

## 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)?

The HR department suggested that based on the number of employees, it will be more reliable to conduct quarterly training to ensure 100% attendance with 25% of employees for each training session.

The training will be delivered in person to ensure employees' active participation.

**Citation:**
Classroom slides (2.1 Introduction to Security Within the Organization)

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

```
The topics that we will cover in our training will be:

   1) Identifying phishing correspondence received via social engineering
      attack. This will assist employees in looking out for small details
      before clicking on any links or responding back to that
      correspondence.

   2) Unsecured/open wifi risks to a device. This will awake awareness
      amongst the employees which will prevent them from using unsecured
      networks for personal or work usage.

   3) Advantages of antivirus and antimalware and how to install, run and
      update them. As many employees may already have these software
      installed, others may not have. This will prompt the individuals in
      being more active and installing regular software updates and running
      thorough scans to ensure device safety.

   4) Identify common malware attacks and its causes, which will include
      reading URLs, using HTTPS websites, removing unknown and unwanted
      browsing extensions from the devices. This is to ensure that employees
      understand the consequences of a malware attack and how to identify a
      potential malicious site or an attachment.

   5) Company's IT security policy for employees using personal devices for
      accessing work related material and also for the employees using
      company provided devices. This will assist them in creating
      self-awareness while accessing work material which is sensitive in
      nature and will contribute highly towards a safe work practice.
```

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

```
After successful pentesting phishing campaigns, it will be considered a
success if the click through rate has gone down 5% or lower and how the
employees responded to the monthly surveys.
```

## 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?

**Technical Control** - It is a preventive control by installing a Firewall and hiding the server behind it which will only allow corporate VPN connections to pass through.

The biggest advantage of having a firewall will be that it will reduce the Man-in-the-middle attack as employees will no longer be able to use any network connections other than their VPNs to access work data from their personal devices and which will work as a shield from potential phishing and malware attacks.

However, a disadvantage of having a firewall is that it is considered to be a costly investment, as from its initial purchase to its updates and maintenance a firewall can consume a large chunk from a company's annual budget.

**Citation:**
https://purplesec.us/security-controls/

**Administrative Control -** It is a detective control by conducting frequent audits on an employee's access rights towards various softwares and applications and to remove any outdated permissions.

These audits will mitigate cyber risk by removing unwanted users from having access to company's data and will assist the organization in staying more compliant. Though, often these audits are conducted by an employee manually and therefore, there is risk of inconsistency and human error.

**Citation:**
https://purplesec.us/security-controls/