# Cybersecurity

## Module 2 Challenge Submission File

Employees at SilverCorp are increasingly using their own personal devices for company work.

- Specifically, over half of all employees check their work email and communications via Slack on their personal mobile phones.
- Another 25% of employees are doing other work-related activities, using work accounts and work-related applications, on their personal phone.

## 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.

By allowing employees to access work information on their personal devices, they leave themselves open to unauthorized access, whether intentionally or not. Personal devices often lack the security measures and oversight often found in devices provided by  and managed by the company. They risk multiple types of attacks, including man in the middle (MITM), malware and phishing scams.

Types of attacks

1. Man in the Middle (MITM)

a. If employees were to use their personal devices on public, unsecure wifi, this could make them more susceptible to MITM attacks. Someone could intercept the sensitive data by providing a free Wi-Fi hotspot to capture user credentials.

2. Malware
    a. Most people don’t always go through everything and analyze if it's safe before they download things to their devices, especially their personal devices. This could be an issue if an employee downloads a file, app or others that could contain malware. An attacker can deploy malware such as keyloggers or other spyware to capture the daily activity or gain user credentials. Bad parties could then even gain control of the device, or obtain sensitive information connected to the company. This could then spread when an employee connects to the companies’ network - potentially affecting many others.

3. Phishing Attacks
    a. Most people don’t consistently check their systems and security controls are regularly updated, especially when its their personal device that’s not being monitored for this. As stated before, most people also don’t always thoroughly check everything they download or click on is secure, let alone up to company standards. This is also true for browsing apps such as personal email and social media, or via SMS - they could click on bad things posing as legitimate, and can trick employees into providing sensitive information. For example, attackers can set up an attack where users are shown a fake login page, tricking them into providing their user credentials. A company is even more susceptible when their employees aren’t properly trained to parcel out phishing attempts versus authentic queries. In general, having the employees use their own devices gives hackers more opportunities to target employees. Without stringent security controls or monitoring that systems are updated, employees increase the exposure to more threats when devices are used for both personal and work purposes.

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.)

Good behavior for employees who use personal devices would be those in which would minimize risks for both the employee and the company, alike.

1. Employees that are using weak passwords, or re-using the same password for multiple channels should begin to use strong and unique passwords, and not reuse them for multiple logins.
2. Employees are not using MFA,or security software including anti-virus, anti-malware, and are not ensuring their systems are up to date. Employees should utilize the company-provided MFA, security software and do regular scans to ensure their systems are secure and up to date.
3. Employees are not using VPNs when connecting to public networks, such networks are unsecure. Employees should always use VPN when connecting to outside networks.
4. Employees don't always report when they lose a device. Employees should report lost or stolen devices to the company IT department so they can remotely wipe the device or their data.

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 initially monitor the network to track and analyze employee behavior. I would be looking at how often the network was being accessed from unsecure networks or see how many devices require security updates. I would also determine the amount of devices who have enabled the MFA capability, and how many devices are in compliance with password policies.

Then I would utilize the social engineering or fake phishing attack to the employees and assess how many employees are clicking on or downloading links from these fake phishing emails. It would be useful to create a log of security incidents - such as viruses, unauthorized access, attempted data breaches, etc. Log and monitor all database access overall.

These tactics would help gain a comprehensive understanding of employee behavior in regards to following security protocols. It will help to pinpoint which actions to take in order to improve and maintain compliance.

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.)

Ideally, 100% compliance would be best, but unrealistic in all categories. I think there are some areas such as using MFA, password requirements or VPN which you could make 100% compliance with. You can make these requirements so that if an employee wants to use company data, they would have to abide by these in order to get into the system. These can be monitored to ensure everyone is compliant.

However, areas such as clicking on bad links, downloading random attachments, or ensuring their devices are completely updated would be best to be around 5-7% realistically. Since it is their own device, they are free to download apps and attachments from their personal email however they want. The best you can do would be to educate via training and try to spread awareness, as well as use the best security software.

## 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.

After you get the results from the information garnered in the above question, you would then take these to the CEO/CIO, CISO and director of HR, also whoever does the training for the company.

1. CISO (Chief Information Security Officer) - manages risk to an organization’s data throughout the lifecycle. Responsible for protecting the company’s data, often supervises multiple teams, such as:
    a. Network security - Director of networking/Director of network security are in charge of networks and they have system administrators, network administrators and physical network technicians on staff. They may also manage the help desk.
    b. Incident response - IR Manager/SOC manager manages an Incident Response unit.SOC manager employs SOC analysts, also known as security analysts or incident handlers.
    c. Application Security - Security Architect is in charge of application security. A security architect typically manages security engineers and software engineers.

2. CIO (Chief Information Officer) - Develops IT systems that support the business. Typically reports to the CEO

They would create an action plan to develop training for new policies and protocols, and during this training, each session would bring their devices and would update their devices accordingly to be up to company standards.
-

In regards to the fake-phishing emails, those results could show that 15% clicked on or downloaded the “malicious” files. The IR manager would relay the results to the CISO / CIO and they would come up with a budget and plan to bring the number down to below 5%.
The SCF team develops training plan with HR to educate employees, as well as supplemental security training that me be required after initial training. HR will provide the best dates and locations, and will break the employees into groups based upon size of the company. They will need to get 100% of employees trained within 6 months. Making this schedule will be up to them. The SCF team has to decide on consequences for clicking on the links and those who didn’t.They will also work with HR to give out information about the upcoming training to specific parties.
The SCF team will implement the training and will continue to analyze employee behavior afterwards.

Because there will be multiple changes, the Director of Networking would ensure the help desk is prepared for the overhaul of computer issues that will no doubt occur when making this amount of changes with large groups of people at a time. Making sure they are fully staffed, are trained ahead of time,have all equipment they need and don't get overwhelmed would be up to them.

They will continue to run scans on employees who have completed training, and within that 6 month period, if employees that are already trained but continually show on scans that they are not following protocol, after multiple incidents, will have to join another group in training again. After all training is done, SCF team will run scans on all employees and will continually analyze their behaviors - positive and negative. If the amount of those clicking on bad links is still above 10%, they will target if there are specific employees that are having more issues than others, send out survey to employees after training asking what they thought about training, what they are struggling with, what they think are good and bad changes, and if they had any suggestions. They could also work with help-desk team to see what the most common problems are for employees coming in with issues.

## 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)?

Combination of both -

a. The initial training would be in person, and perhaps once a year in person from then on in general.
b. Online training should be every 3 months - which would mostly be a checklist that each employee would have to complete with screenshot proof for each item. The list would be "computer is up to date, security system test completed, changed password, etc". Then a short email of security info with a quiz at the end. Then at the end, once completed, employees would receive points or better gifts if done within 24/48 hours after email was sent out. Then a smaller gift if done within 96 hours, then no gift after that point. If it takes longer than 5 days, the IT team will be notified, and those individuals will have to schedule time with IT department to do in-person training again.

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

Employees that are using weak passwords, or re-using the same password for multiple channels should begin to use strong and unique passwords, and not reuse them for multiple logins.Employees that had weaker passwords likely didn't have a backup if their credentials were stolen. Employees should use a multi-factor authentication (MFA) for every login associated with the company. That way, should their credentials be compromised, the hackers can still not get into their account without the MFA.

Employees are not using security software, but they should now use the security software provided to them by the company. The security software contains anti-virus, anti-malware, password manager, among other features. Employees should have this installed on all of their devices with company data. Maintaining this could include employees running regular scans through the software to ascertain how secure their device is. These should be scheduled at certain, designated time intervals in order to ensure employees are following through.

Employees should regularly check their devices, apps and security software are updated. The scans through the security software take less than five minutes.

Employees have been clicking on emails and links from unknown sources. They should now check to make sure things they are clicking on or are downloading are indeed authentic. Don't click on anything that looks suspicious or open anything from someone you don't know. The security software will help here as well.

Employees have been connecting to public wi-fi when doing work outside the office. These networks are typically unsecured and can lead to attacks. Employees should now utilize the company-provided VPN - when using public wifi networks.

Employee behaviors should aim towards minimizing the risks overall. Having basic guidelines, training and competent software is critical for

```
security for the company. These changes would most likely go smoother should the company explain how abiding by them is beneficial for both company and employee. The company should provide software such as anti-virus, anti-malware, password manager and MFA/VPN, and potentially be able to use things such as password manager for both personal and work-related logins if they are to use their own devices for the company. Going into how employees could be affected personally should their personal data be hacked would help to ensure they understand it's a win-win by being as secure as possible. It would benefit both parties should the employee abide by security standards.
```

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

```
I would again do the simulated-phishing scam and determine how many opened or downloaded the links again. Hopefully, the percentage would go down.

I would monitor the network to see how often the network was accessed from unsecure networks or see how many devices are behind in security updates. In monitoring the network, I would check to see how many malware or attempted data-breaches did occur, and also check the security software to show what was stopped by utilizing the new software, VPN, MFA, etc.
```

## 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?

```
[Enter Solution 1 here]
   1. Having a badge that plugs into the computer or has to be scanned on
      camera in order to use the company data system.
         a. Physical
```

    b. Preventative Control - ensure only employee can get into the data system
    c. Can determine what employee is doing what with the badge, more secure, not easy to copy badge, only use one place at a time with badge
    d. Badges can be lost and if employee is already using their own device, that may be annoying.

2. Requiring employees to adhere to policies, otherwise consequences can escalate
    a. Administrative
    b. Deterrent, Corrective (for those who are not following protocols)
    c. Could force some reluctant employees to comply if they knew there could be severe repercussions if they didn’t abide by the rules
    d. Could lower overall morale