# 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.

Risks: An employee could download an app or other item that is infected w/ a virus or malware which could then use data on the device to steal login credentials or steal data stored locally; an employee could enable access permissions that allow company data to be used/viewed by an unauthorized third party; the employee could be using an outdated operating system that is easily exploitable and potentially no longer serviced, leaving their system vulnerable to attack; No guarantee there is current anti-virus protection, potentially leaving the system open to attack; a disgruntled employee can just save/take data at will; if a device is lost or stolen, there is unlikely to be a means to wipe sensitive data from the device; An employee could click on a malicious email from their personal mail, which could infect their system and leave work information vulnerable.

The three main attacks that can ultimately be carried out are:

1. An attacker steals the data stored on the device. 2. An attacker steals login credentials and accesses additional data on the work network (may not be caught b/c it would appear to be a legitimate login and a new “personal device” would not stand out). 3. An attacker

deletes/destroys data (this is particularly an issue if there is no/not a current backup).

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 not download apps without confirming they are legitimate, Download only from app stores and never from a website or email. Employees should be using a current operating system and downloading all current updates. They should keep antivirus installed and updated. Require use of a VPN when accessing the company network that includes a scan to verify operating system and virus definitions are up to date. Cloud backups should be in place, updating on a regular basis in case of lost/destroyed device or data. Two factor authentication put in place to ensure legitimacy of the party signing in. Do not click on emails/attachments from unknown parties in either personal or work email environments.

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.)

Chosen behavior to mitigate risk: Keep current on OS updates and anti-virus definitions.
As part of a required VPN when accessing the company network, sign on can include a system scan that verifies current antivirus/operating system requirements are met & block connection until any outstanding concerns are addressed.

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.)

100% of employees signing in to the network have up to date virus definitions and operating systems.

## 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 CEO would be involved to look at data provided by all involved parties and make a determination of whether the business will take the recommended action. They will need to determine if the cost is worth the benefit or if they would rather take the risk to continue without spending additional money. The CFO would be involved to look at the company budget and verify the cost of the recommended changes. They would be the one to advise the CEO about potential financial risk as well as what the additional costs of remediation would mean for the company as a whole. The CIO would be able to determine what will be required of the IT department to implement the recommended changes. They could identify any potential hurdles caused by staffing/equipment availability. The IT department would be responsible for implementing and servicing any issues with the required VPN software. They would likely be responsible for maintaining up to date requirements for acceptable system/antivirus definitions updates in order to ensure the VPN scanner is effective in only letting through those users with an acceptable level of protection in place. The training department would be responsible for creating any training material to be disseminated and creating any classroom training programs. They would also be useful in helping to identify common questions or knowledge gaps that arise through training and communicate these back to the other departments/people involved in case there are other concerns that were not previously addressed.
CCO would be involved to ensure proper communication internally and, if necessary, externally. Should there have been a incident that led up to the implementation of this control, they would be the one to ensure communication properly addresses the necessary info without speaking to anything confidential.

## 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)?

There would be an initial in person training with an online quiz to be completed after the classroom portion. The quiz will certify who has been trained/when and by requiring a score of 80% to pass, will confirm employees

have an acceptable level of understanding of the expectations. This initial training will take place starting immediately with a goal of having all employees trained within the month. All new hires would undergo the original training during onboarding. Because the new VPN setup would automatically block anyone who did not meet the requirements, there would be no ongoing/refresher training necessary for the company as a whole. The IT department may require refreshers on their processes regarding system/anti-virus definition updates. This would be most beneficially run internally by that department as the general training department would not likely have the specialized knowledge necessary to complete a comprehensive training on the matter.

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

Training would cover the purpose of an operating system update, reasons for keeping anti-virus current, and how the VPN login process will work. This will be structured in such a way not to just communicate what the new requirement is and how to use it, but the why behind the change in process. Including this perspective, should help ensure less pushback from employees and help foster a greater understanding of cybersecurity risk in general which can carry over into other aspects of the business.

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

Tracking would be put into place to see how often someone attempts to access the VPN but is stopped at the system scan. Frequency of helpdesk tickets regarding this login issue would be monitored. Monthly audits of IT would be conducted to confirm the VPN is properly configured with the correct system/antivirus requirements.

## 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?

For the risk of a lost/stolen device, the company could require installation of software which would allow for a remote wipe. (a)This is a technical control, which (b)would be in place to correct the issue of a lost/stolen phone potentially falling into the wrong hands. (c)Because it is remote, this can be implemented as soon as the device is reported lost/stolen. (d)If there is any delay in reporting, it is still possible for a malicious actor to obtain confidential data.

For the risk of an employee downloading a less than legitimate app which could compromise the system, the company could hold regular training/refreshers on common risks for personal electronic devices. (a)This is a administrative control, which (b)would be designed to act in a preventive manner by educating the employee on risky/proper behavior. (c)The benefit to educating the workforce means they should be more mindful of their download behaviors in general and understand the risks out there; (d) however, there is little that can be done to ensure compliance.



Sources used:
https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate#:~:text=Regardless%20of%20whether%20your%20employees,device%20has%20malware%20on%20it.
https://perception-point.io/byod-security-threats-security-measures-and-best-practices/
https://www.n-able.com/blog/the-top-7-risks-of-bring-your-own-device-msps-should-remember

After consultation with AskBCS, questions #3-8 were answered based on one of the scenarios assessed in the first two questions.