| 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.

| Since employees will be using personal devices to access work information. This will allow these devices to be more likely to become infected with malware.  It will also be harder to manage data theft since these devices will be owned by the individual not the company. Data theft can be done through multiple methods including hacking, loss or theft. These devices will have access to client Personal Identifiable Information. Since they are usually not as secure as a company owned device, hackers consider them an easy target.  Another problem with allowing access to work information on personal devices is insecure networks. These insecure networking open up attack vectors for hackers to steal company data. |
| --- |

1. 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 preferred behavior for preventing malware is to avoid downloading suspicious files or clicking on untrusted links. If  The preferred behavior would be for the employee to be responsible with their personal devices and not lose or stolen. Unfortunately, this is something unpreventable. In this case they should notify IT immediately so the device can be wiped so no company data is lost or stolen.  The preferred behavior for unsecure networks is to not connect to unsecured networks. If they do have to use a unsecure network connection using the company VPN so that the traffic is encrypted. Also not connecting to unknown networks too. All internet traffic will have to be routed through the VPN when not on the corporate networks. |
| --- |

1. 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.)

| We will first conduct a penetration test and see how many users are downloading the malicious files. Those who do not pass this penetration test will be required to take a training course about the dangers of downloading malware. Another method to measure how often employees are downloading malware could be run using reports from the antivirus software that was required to be installed on the device. Since users are usually not aware they are even downloading malware this would be a good method to get an accurate count.  We will also make anonymous surveys about losing your devices asking users if they have ever lost their devices before. Since they will be anonymous people will be less likely to be dishonest with them.  We will monitor the VPN connection logs and check to make sure that there is no malicious network traffic. |
| --- |

1. 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.)

| Less than 2% of employees are downloading malware.  Less than 1% of data lost or stolen. We will achieve this by using the remote wiping software and monitoring suspicious activity on the devices.  Less than 1% of users connecting without a VPN connection |
| --- |

### Step 2: Involve the Right People

1. 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 IT department will be involved in this. They will educate the users on why these practices are important and help with any questions they may have. They will also implement that all corporate traffic outside of the company will be required to be accessed through the VPN.  Since data loss is involved the Chief Information Officer will be involved too. They will work with the IT department to monitor devices so that lost or stolen devices are being wiped. So that none of the company's data stays secure.  The CEO will be involved in checking in and making sure these proper procedures are followed.  The Human Resources department will work with IT when onboarding and offboarding employees so they will have appropriate access to computer systems.  Security Architect could also be involved depending on the size of the organization. They help design secure systems. |
| --- |

### Step 3: Training Plan

1. How frequently will you run training? What format will it take (e.g., in-person, online, a combination of both)?

| We will first start with online training and for those who do not pass the malware test will be required to have more online training. If they are a repeat offender of not following these policies then in person training will be required. |
| --- |

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

| We will cover user awareness around not opening suspicious links that could lead to malware. We will also talk about the importance of strong passwords and not sharing your login information. We will talk about the importance of using a VPN when not on the corporate network to keep company data safe. We will talk about the importance of keeping company data safe. We will also explain the risks associated with downloading malware. |
| --- |

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

| Sending out tests periodically at the very least biannually testing on things that were covered in the training. |
| --- |

### Bonus: Other Solutions

1. List at least two other potential solutions. For each one, indicate the following:
   1. What type of control is it? Administrative, technical, or physical?
   2. What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?
   3. What is one advantage of each solution?
   4. What is one disadvantage of each solution?

|  |
| --- |

| [Enter Solution 2 here] |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.