| 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.

| 1. Data Theft - Employees using their personal devices won’t be as stringent in regards to using their personal devices as SilverCorp is regarding company devices. 2. Malware - If employees use their personal devices to download attachments such as PDFs and sensitive information it can compromise their device and/or company network if for example a employee downloads an app that could be infected with Malware. 3. Lack of employee training - SilverCorp could lack proper training for employees who otherwise do not know they are not allowed to use personal devices to check work related information such as email or company documents. Lack of training leads to human mistakes. |
| --- |

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 employee behavior is checking with SilverCorp and understanding the dangers of using personal devices to do company work. Employees should check with IT department to ensure their phones are encrypted correctly to ensure company and sensitive information doesn’t have the risks when using their personal devices. |
| --- |

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.)

| I would send a company wide anonymous email survey to see what is not using the preferred behavior. I would also see if I can track the IP address an email is being opened such as targeting emails with emails coming from HR to see who is opening documents and from where such as is it coming from Company IP address or their own personal IP address. |
| --- |

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.)

| The goal for the organization long term is to get it at 5% or below. In the short term given how many people do this behavior would be to get it to about 20% down each quarter until getting down to the desired goal. |
| --- |

### 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.

| 1. The executive management - They need to be involved not only as they probably use their personal devices but also to understand what the training is about and it’s goal and to let their employees know how important this is from the top down. 2. IT Department - They are the ones putting the training and goal of the organization together. So everyone should be aware of what is being done and what is being expected to help employees ensure the safety of company data. 3. Heads of departments - The head of the department such as head of HR should be involved as they are the ones that need to make sure their staff is doing the training and are reaching the company goal. 4. Legal - They need to be involved to make sure the training is done with legal representation and in dealing with personal devices being used by employees. 5. Communications department - They need to be involved to help craft the information being sent out to employees and to help with the training materials if needed. |
| --- |

### 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)?

| Training will be run in groups by department. The head manager of the department will need to ensure that everyone in their department is and will make time available for the training. The format will be online such as online training of slides and videos followed by a meeting with the department to answer any questions they have about the training. |
| --- |

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

| The topics that will be covered with be  Phishing - The dangers of opening up phishing emails on personal devices and not paying attention to how the email looks from a phone compared to a laptop/desktop.  Malware - Having unknown apps downloaded on a phone such as a game and the dangers of possible malware being on the phone and how it can affect company networks for example when they log onto their work computer.  Legal Problems - Customers expecting their information to be protected and if there is a breach the possibility it coming from a personal device can ruin the company’s reputation and lawsuits from lack of protecting the information.  Lost devices - If the device is lost or stolen, and if it has company information on there without any encryption, the thieves of the device can only have personal information of the employee but also the company’s information.  Employee training and awareness - Having yearly employee training on security risks using their own device as well as having training as part of the onboarding process of new employees. |
| --- |

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

| To measure the effectiveness I would want to see metrics from each department as to who completed the training and how well they are following the preferred behavior.Then I would compile the data to see how the employees are doing company wide. |
| --- |

### 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?

| Having a BYOD policy   1. Administrative 2. Goal is to bring awareness to employees on the BYOD policy. It is Preventive. 3. Having employees know the risks of using their personal devices and what to do if they are wanting to use their personal devices such as contacting the IT department. 4. Disadvantage would be employees not reading the policy and/or forgetting what steps are needed to ensure using their personal device. |
| --- |

| Installing software on personal devices that the company can track   1. Technical control. 2. Goal is to ensure the company can track the personal device and its risk. It is a preventive control. 3. The company can track the personal device and have the company information go and from the software and mitigating the risk. 4. Disadvantages would be employees would feel their privacy and/or information would be known to the company and therefore would resist such a solution. |
| --- |
|  |

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